

**Botschaft
zum Bundesgesetz über den Datenschutz
(DSG)**

vom 23. März 1988

Sehr geehrte Herren Präsidenten,
sehr geehrte Damen und Herren,

wir unterbreiten Ihnen den Entwurf zum Bundesgesetz über den Datenschutz mit dem Antrag auf Zustimmung.

Gleichzeitig beantragen wir Ihnen, die folgenden parlamentarischen Vorstösse abzuschreiben:

1971 P 10 898 Gesetzgebung über Computer (N 11. 12. 72, Bussey)

1977 P 77.381 Öffentliche und private Informationszentren
(N 17. 1. 78, Carobbio)

1982 P 82.336 Stellenangebote und Persönlichkeitsschutz
(N 8. 10. 82, Crevoisier)

1984 P 84.598 Persönlichkeitsschutz des Arbeitnehmers
(N 22. 3. 85, Reimann)

1984 P 84.909 Datenschutz. Übergangsregelung
(N, noch nicht behandelt, Leuenberger)

Des weitern beantragen wir Ihnen, den nachstehenden Initiativen keine Folge zu geben:

1977 77.223 Persönlichkeits- und Datenschutz. Bundesverfassung (noch nicht behandelt, Gerwig)

1977 77.224 Persönlichkeits- und Datenschutz-Gesetz (noch nicht behandelt, Gerwig).

Wir versichern Sie, sehr geehrte Herren Präsidenten, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

23. März 1988

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Stich

Der Bundeskanzler: Buser

Übersicht

Der Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen und die enorme Intensivierung der Datenverarbeitung und -verbreitung in Gesellschaft, Wirtschaft und Staat haben die Risiken von Persönlichkeitsverletzungen stark anwachsen lassen. Das Privat- und das Verwaltungsrecht bieten in der bestehenden Form keinen ausreichenden Schutz gegen Verletzungen der Persönlichkeit, die auf Informationstätigkeiten beruhen. Mit der vorliegenden Gesetzgebung soll diese Lücke geschlossen und ein wirksamer Schutz für die von Datenbearbeitungen betroffenen Personen geschaffen werden.

Der Gesetzesentwurf enthält in einem allgemeinen Teil eine Reihe von materiellen Datenbearbeitungsgrundsätzen, die für Organe des Bundes ebenso wie für private Datenbearbeiter gelten. Er sieht vor, dass jede Person vom Inhaber einer Datensammlung Auskunft über die eigenen Daten verlangen kann. Zu diesem Zweck sollen Datensammlungen registriert werden. Die Registrierpflicht ist für die Bundesorgane eine umfassende, während private Bearbeiter nur solche Sammlungen melden müssen, die unter dem Gesichtspunkt des Persönlichkeitsschutzes mit besonderen Risiken behaftet sind. Schliesslich sind auch Datenübermittlungen ins Ausland, die von ihrem Umfang her oder wegen der Art der Informationen datenschutzrechtlich bedeutsam sind, meldepflichtig.

Soweit der Entwurf die Datenbearbeitung von Privatpersonen regelt, stellt er eine Ergänzung und Konkretisierung des Persönlichkeitsschutzes des Zivilgesetzbuches dar. Er legt beispielhaft fest, unter welchen Voraussetzungen eine Datenbearbeitung zu einer Persönlichkeitsverletzung führt. Er gibt dem Richter aber auch Anhaltspunkte, in welchen Fällen eine Persönlichkeitsverletzung gerechtfertigt sein kann, weil die privaten oder öffentlichen Interessen an der betreffenden Datenbearbeitung überwiegen. Dabei nimmt der Entwurf vor allem Rücksicht auf die Informationsbedürfnisse der Wirtschaft. Kommt es über die Zulässigkeit privater Datenbearbeitungen zu Auseinandersetzungen, so müssen diese vom Zivilrichter entschieden werden.

Eingehend regelt das Gesetz die Datenbearbeitung der Bundesverwaltung und anderer Bundesorgane. Es legt die datenschutzrechtliche Verantwortung fest und bestimmt, welche Rechtsgrundlagen für verschiedene Bearbeitungen nötig sind. Es gibt den Bundesorganen Anweisungen für die Beschaffung und die Bekanntgabe von Personendaten und für weitere Formen der Datenbearbeitung. Den besonderen Geheimhaltungsbedürfnissen von Organen des Staatsschutzes und der militärischen Sicherheit wird dabei Rechnung getragen.

Über die Einhaltung des Gesetzes soll ein Eidgenössischer Datenschutzbeauftragter wachen. Er kann – bei privaten Datenbearbeitern allerdings nur in besondern Fällen – Abklärungen vornehmen und Empfehlungen abgeben. Er ist aber nicht befugt, verbindliche Anordnungen zu treffen. Hingegen hat er das Recht, der Eidgenössischen Datenschutzkommission eine Angelegenheit zum Entscheid zu unterbreiten. Diese Kommission beurteilt zudem Streitigkeiten zwischen Bürger und

Verwaltungsorganen in Datenschutzfragen. Ihre Entscheide können ans Bundesgericht weitergezogen werden.

Der Entwurf regelt aber auch die Datenweitergabe zu Zwecken der medizinischen Forschung. Daten, die einem Berufsgeheimnis, namentlich dem Arztgeheimnis, unterstehen, sollen mit Einwilligung der Betroffenen oder aufgrund einer Bewilligung einer vom Bundesrat eingesetzten Sachverständigenkommission für Forschungsarbeiten freigegeben werden können. Die Kommission darf aber eine Bewilligung nur erteilen, wenn die Forschung nicht mit anonymisierten Daten durchgeführt werden kann und es für die Forscher unmöglich oder unverhältnismässig schwierig wäre, die Einwilligung der Berechtigten einzuholen; zudem müssen die Forschungsinteressen gegenüber den Geheimhaltungsinteressen überwiegen. Mit dieser Regelung, die im wesentlichen als Ergänzung des Strafgesetzbuches konzipiert ist, soll ein Ausgleich zwischen dem Persönlichkeitsschutz der Patienten und dem öffentlichen Interesse an einer leistungsfähigen medizinischen Forschung geschaffen werden.

Mit der Revision des Bundesstrafprozesses und des Rechtshilfegesetzes sollen ferner datenschutzrechtliche Grundsätze, namentlich für das gerichtspolizeiliche Ermittlungsverfahren und für den Informationsaustausch mit INTERPOL, gesetzlich verankert werden.

Mit dieser Gesetzgebung folgt die Schweiz einer weltweiten Entwicklung in fast allen Industriestaaten. Der Entwurf führt zudem völkerrechtliche Grundsätze des Datenschutzes näher aus und leistet damit einen Beitrag zur Schaffung zuverlässiger Rahmenbedingungen für den internationalen Informationsaustausch.

Botschaft

1 Allgemeiner Teil

11 Das Bedürfnis nach Datenschutzrecht

111 Im allgemeinen

Wenn Informationen über Menschen gesammelt und bearbeitet werden, ist deren Persönlichkeit davon betroffen. Die Betroffenheit kann stärker oder schwächer sein und positive oder negative Reaktionen hervorrufen. Informationstätigkeit kann zu einer erwünschten zwischenmenschlichen Kommunikation führen, aber auch dazu, dass eine Person sich in ihren Entfaltungsmöglichkeiten beeinträchtigt oder benachteiligt fühlt.

Der Umgang mit Personendaten kann sich in verschiedener Weise nachteilig und verletzend auf die betroffene Person auswirken. So werden Menschen unsicher, wenn sie nicht mehr überblicken, wer alles Daten über sie bearbeitet, sie also nicht wissen, wie ihre Umwelt über sie informiert ist^{1)*}. Viele Menschen empfinden es als anmassend, wenn durch indiscretes Auskundschaften Informationen über sie beschafft werden²⁾. Betroffene können benachteiligt oder unbillig behandelt werden, wenn für private oder behördliche Entscheide unrichtige, unvollständige oder nicht mehr aktuelle Angaben verwendet worden sind³⁾. Eine Person kann ein Leben lang mit einem Makel behaftet bleiben, wenn Daten mit negativen Angaben über sie auf unbestimmte Zeit aufbewahrt und immer wieder benutzt werden. Persönlichkeitsverletzungen sind denkbar, wenn Daten im Übermass bearbeitet werden, wenn etwa ein Fehlverhalten in der Öffentlichkeit unnötig angeprangert wird⁴⁾, wenn mehr Daten erhoben werden, als für die Abwicklung eines Vertrages notwendig ist, oder wenn Amtsstellen unbeschränkt Daten bereithalten und untereinander austauschen⁵⁾. Vom Betroffenen negativ erlebt wird vielfach auch die zweckwidrige Verwendung von Daten; er schätzt es kaum, wenn beispielsweise Informationen über sein Arbeitsverhältnis oder über Sozialmassnahmen in einem anderen Zusammenhang wieder genutzt werden.

112 Wachsende Informationstätigkeit aufgrund neuer Informationstechniken

Seit dem Zweiten Weltkrieg hat sich die systematische Nutzung von Informationen über Personen ausserordentlich stark entwickelt und neue Formen angenommen. Die Erweiterung der Handelsbeziehungen, der Einsatz neuer Verkaufsstrategien und neuer Methoden der Unternehmensführung, die Zunahme und Diversifizierung der Kreditgeschäfte bringen es mit sich, dass immer grössere Mengen von personenbezogenen Daten in immer komplexerer Weise bearbeitet werden. Im staatlichen Bereich haben die Ausweitung der Staatsaufgaben

*) Die Anmerkungen befinden sich am Schluss der Botschaft.

und zusätzliche Ansprüche an die Qualität staatlicher Leistungen ebenfalls zu einer Steigerung der Informationsbearbeitung geführt.

Diese Entwicklung hin zur Informationsgesellschaft ist durch moderne Informations- und Kommunikationstechnologien überhaupt erst ermöglicht worden. Der Einsatz der automatisierten Datenverarbeitung erlaubt es, die Informationen ungleich systematischer und gründlicher aufzuarbeiten, als das mit herkömmlichen Arbeitsmethoden möglich ist. Die heutige Technik ermöglicht ein beinahe unbeschränktes Erfassen, Zusammenführen, Aufbereiten von und Verfügen über Informationen. Sie gestattet es, Datensammlungen gezielt zu verknüpfen oder zu trennen, auszuwerten und an Dritte zu übertragen. Die Bearbeitungsmöglichkeiten werden durch die Verbindung von automatisierter Datenverarbeitung und neuen Kommunikationstechniken noch gesteigert. Der Trend geht dahin, verteilte Datenbestände sowie verteilte Rechnerleistung und Computerintelligenz in lokalen, regionalen oder internationalen Netzwerken zu verknüpfen.

Mit den neuen Technologien kann zusätzlicher Aufschluss über das Verhalten von Personen gewonnen werden. Zu erwähnen sind nicht nur die Video-Aufzeichnungen, sondern auch die immer alltäglicheren Formen automatischer Zulassungs-, Zeit-, Leistungs- oder Kommunikationskontrollen. Solche Überprüfungen erfolgen etwa bei der Bedienung elektronischer Geräte und Anlagen, beim Passieren von Sicherheitstüren oder beim automatischen Lesen von Ausweis- und Kreditkarten. Neue Informationen werden auch bei den automatisierten Zweiwegkommunikationssystemen erhoben, so etwa bei Videotex. In zunehmendem Mass werden Daten nicht mehr über das Eintippen, sondern über ein EDV-unterstütztes Lesen oder Aufnehmen von Texten, Bildern, Tönen oder weiteren Zeichen erfasst.

Mit der geschilderten Entwicklung ist das Potential für Persönlichkeitsverletzungen angewachsen. Zudem ist der einzelne vielfach nicht mehr in der Lage, auch nur annähernd abzusehen, wer wann wo welche Daten über ihn bearbeitet; er hat die Herrschaft über die Daten, die ihn angehen, weitgehend verloren. Damit wird er der Möglichkeit beraubt, selber zu bestimmen, wem er welche Mitteilungen machen will. Er ist auch oft nicht mehr imstande, Fehler und Missbräuche in der Informationsverarbeitung zu erkennen und die Verantwortlichen ausfindig zu machen.

Die elektronische Datenverarbeitung hat aber unter dem Gesichtspunkt des Datenschutzes auch positive Seiten. So ermöglicht sie namentlich, Personendaten mit vernünftigem Aufwand zu anonymisieren.

113 Allgemeine Ziele eines Datenschutzgesetzes

Ein Datenschutzgesetz hat nicht den Zweck, die Entwicklungsmöglichkeiten im Bereich der Informationstechnologien zu verhindern oder einzuschränken. Die mit diesen Technologien ermöglichten Erfolge in Wissenschaft, Wirtschaft und Verwaltung sollen und können nicht rückgängig gemacht werden und müssen auch in Zukunft möglich sein. Es sind aber gewisse Leitplanken für die Datenbearbeitung zu setzen, die garantieren, dass die Entfaltung der Persönlichkeit

nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt wird. Jedermann soll, soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können⁶⁾.

Das bedeutet vorab, dass das Privat- und Familienleben vor Beeinträchtigungen geschützt werden muss. Die Privatsphäre einer Person soll von Informationsbedürfnissen anderer Personen oder staatlicher Stellen abgeschirmt werden, sofern nicht ein überwiegendes Interesse an einer solchen Informationsbeschaffung besteht⁷⁾. Des weitern sollen Informationen über die Ausübung verfassungsmässiger Rechte, wie der Glaubens- und Gewissensfreiheit, der Meinungsfreiheit oder des Stimm- und Petitionsrechts besonders geschützt werden, garantieren doch diese Rechte in besonderem Mass die Entfaltung der Persönlichkeit. Ein Datenschutzgesetz muss ferner verhindern, dass der einzelne zu einem rechtlosen Objekt von Informationstätigkeiten wird. Er soll vielmehr Bild und Kenntnisse, die die Umwelt von ihm hat, mitbestimmen können. Deshalb hat er grundsätzlich ein Recht zu erfahren, wer was über ihn weiss und zu welchen Zwecken die entsprechenden Daten bearbeitet werden. Nur so kann er in seiner privaten, beruflichen oder gesellschaftlichen Tätigkeit jeweils situationsgerecht entscheiden. Er soll aber auch die Möglichkeit haben, ihn betreffende Informationen berichtigen oder löschen zu lassen oder von den Informationsbearbeitern Verschwiegenheit zu verlangen.

114 Die Rechtslage in der Schweiz

114.1 Im privatrechtlichen Bereich

In den privatrechtlichen Beziehungen richtet sich der Datenschutz heute vorab nach den Grundsätzen des allgemeinen Persönlichkeitsschutzes, wie sie in Artikel 28 ff. des Zivilgesetzbuches (ZGB) verankert sind. Nach der seit dem 1. Juli 1985 geltenden Fassung von Artikel 28 Absatz 1 ZGB kann derjenige, der «in seiner Persönlichkeit widerrechtlich verletzt wird», «zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, den Richter anrufen». Dabei muss der Begriff der Persönlichkeit in einem weiten Sinne verstanden werden; er umfasst alle physischen, psychischen, moralischen und sozialen Werte, die einer Person kraft ihrer Existenz zukommen⁸⁾. Diese sehr allgemeine Umschreibung des Persönlichkeitsschutzes im Gesetz lässt aber weitgehend offen, in welchen Situationen eine widerrechtliche Persönlichkeitsverletzung tatsächlich vorliegt. Sie gibt auch keine Anhaltspunkte, unter welchen Umständen Datenbearbeitungen gerechtfertigt sind.

Die *Rechtsprechung* ihrerseits hat zur Frage, wann eine Datenbearbeitung zu einer Persönlichkeitsverletzung führt, erst einige wenige Anhaltspunkte und Kriterien herausgearbeitet. Eine Persönlichkeitsverletzung kann danach vorliegen, wenn die Informationstätigkeit die Privat- und Geheimsphäre beeinträchtigt⁹⁾. Dabei umfasst die *Geheimsphäre* jene Tatsachen und Lebensvorgänge, von denen nur die betroffenen Personen oder mit ihnen besonders Vertraute Kenntnis haben sollen, während zur *Privatsphäre* die übrigen Bereiche des Privatlebens

gehören, die einer breiten Öffentlichkeit nicht zugänglich sein sollen. Des weiteren gelten aber auch die Schädigung von Ehre und gesellschaftlichem Ansehen sowie die Bearbeitung von unrichtigen Personendaten, die den Betroffenen «in einem falschen Licht erscheinen lassen», als Verletzung der Persönlichkeit¹⁰⁾. Allgemein ausgedrückt ist nach der Gerichtspraxis eine Datenbearbeitung unzulässig, wenn sie einen bestimmten Lebensbereich des Individuums, seine Unbefangtheit oder soziale Geltung zu beeinträchtigen vermag.

Angesichts dieser nur sehr bruchstückhaften Regelung der Datenbearbeitung im geltenden Recht sind vereinzelt von *privaten Organisationen* Initiativen für Datenschutzregelungen ausgegangen. So haben etwa die Schweizerische Institutsleiterkonferenz (ein Verein für Markt-, Meinungs- und Motivforschung) zusammen mit dem Verband Schweizerischer Marktforscher, der Verband von Wirtschaftsauskunfteien in der Schweiz und die Schweizerische Vereinigung für Direktwerbung «Berufsethische Normen» oder Standesregeln für ihre Datenbearbeitungen erlassen. Von besonderer Bedeutung sind sodann die von der Schweizerischen Ärztekammer 1981 beschlossenen «Neuen Grundsätze für Vertrauensärzte» und die «Grundsätze für Betriebsärzte». Erwähnt seien schliesslich die Vereinbarung zwischen dem Arbeitgeberverband Schweizerischer Maschinen- und Metallindustrieller (ASM) und dem Schweizerischen Metall- und Uhrenarbeitnehmerverband (SMUV) von 1983 sowie die Mustervereinbarung der Angestelltenkommission des Schweizerischen Gewerkschaftsbundes über «Neue Techniken und Datenschutz im Betrieb» von 1984; beide Vertragswerke legen wichtige Datenschutzgrundsätze fest.

114.2 Im öffentlichen Recht

Gleichsam als Spiegelbild zum zivilrechtlichen Persönlichkeitsschutz besteht auch ein gewisser verfassungsrechtlicher Schutz gegen unzulässige und übermässige Datenbearbeitung. Gegenüber staatlichen Eingriffen auf dem Wege der Datenbearbeitung können sich die betroffenen Personen zwar nicht auf ein in der Bundesverfassung ausdrücklich verankertes Grundrecht berufen, doch werden sie durch das ungeschriebene Grundrecht der persönlichen Freiheit und durch Artikel 8 der Europäischen Menschenrechtskonvention geschützt. Die persönliche Freiheit gewährleistet «als zentrales Freiheitsrecht nicht nur die Bewegungsfreiheit und die körperliche Integrität, sondern darüber hinaus alle Freiheiten, die elementare Erscheinungen der Persönlichkeitsentfaltung darstellen»¹¹⁾. Nach Artikel 8 ERMK hat jedermann «Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs». Ferner stellen das Stimmgeheimnis und die Petitionsfreiheit gewisse Grenzen für die Informationsbearbeitung dar, vor allem dann, wenn Unterschriften von Initiativen, Referenden oder Petitionen zu politischen oder polizeilichen Zwecken ausgewertet werden sollen¹²⁾. Von Bedeutung ist schliesslich Artikel 4 der Bundesverfassung, weil er dem Betroffenen eine Beteiligung an der Datenbearbeitung garantiert¹³⁾.

Zur Konkretisierung dieser Grundsätze hat der Bundesrat am 16. März 1981, als die Vorarbeiten für eine Datenschutzgesetzgebung bereits im Gang waren, vor-

läufige «Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung» erlassen¹⁴⁾. Die Richtlinien enthalten Rechtsgrundsätze für den Umgang mit Daten und statuieren eine Auskunftspflicht der Bundesverwaltungsstellen gegenüber den betroffenen Personen. Sie bezwecken, die Verwaltung mit den Grundgedanken des Datenschutzes vertraut zu machen und die Einführung des Datenschutzgesetzes des Bundes vorzubereiten. Für grosse Informationssysteme hat der Bundesrat zudem, gleichsam im Vorgriff auf das zu schaffende Datenschutzgesetz, bereichsspezifische Datenschutzregelungen erlassen. Erwähnt seien etwa die Verordnungen vom 20. Oktober 1982 über das Zentrale Ausländerregister (SR 142.215), die Verordnung vom 16. Dezember 1985 über das automatisierte Fahndungssystem (RIPO; SR 172.213.61), die Verordnung vom 29. Oktober 1986 über das militärische Kontrollwesen (SR 511.22), die Verordnung vom 27. September 1982 über den Versuchsbetrieb eines Informationssystems für die Arbeitsvermittlung und Arbeitnehmerstatistik (SR 823.114) so wie eine Anzahl Verordnungen über die eidgenössische Statistik¹⁵⁾.

Verschiedene Kantone kennen bereits Datenschutzgesetze für ihren öffentlichen Bereich. Vorangegangen ist der Kanton Genf, welcher 1976 seine «Loi sur la protection des informations traitées automatiquement par ordinateur» erlassen und diese in einer Totalrevision im Jahre 1981 wesentlich ergänzt hat. In der Folge schufen die Kantone Waadt, Neuenburg, Wallis, Bern, Jura, Tessin und Thurgau Datenschutzgesetze. In andern Kantonen, so in Basel-Stadt, Basel-Landschaft, Solothurn, Zürich, Luzern, St. Gallen und Glarus sind Gesetzesentwürfe in Vorbereitung. In andern Kantonen begnügt man sich vorläufig mit Verordnungen oder blossen Richtlinien.

114.3 Ungenügen des geltenden Rechts

Nach dem Gesagten finden sich bereits im geltenden Recht gewisse Regeln für die Informationsbearbeitung. Insgesamt besteht aber trotz einzelner bedeutsamer Gerichtsentscheide heute noch kein wirksamer Schutz gegen Beeinträchtigungen aus Informationstätigkeit. Privates wie öffentliches Recht vermögen den Schutzbedürfnissen, welche namentlich durch die EDV-unterstützte Datenbearbeitung entstanden sind, nicht genügend Rechnung zu tragen.

Im privatrechtlichen Teil hängt dies vor allem damit zusammen, dass es für die betroffenen Personen vielfach schon unmöglich ist festzustellen, wer Daten über sie bearbeitet. Aber selbst dort, wo dies gelingt, erhalten sie häufig keine Auskunft über die sie betreffenden Datensammlungen und die darin gespeicherten Daten. Auch können sie die Gefährdungen oder Verletzungen durch Datenbearbeitungen meist nur schlecht charakterisieren. Angesichts der offenen Grundnorm von Artikel 28 des Zivilgesetzbuches fehlen ihnen Kriterien, anhand derer sie feststellen können, ob eine Bearbeitung zulässig sei oder nicht. Oft ist es für sie auch schwierig, die Kausalität zwischen einem Informationsvorgang und der Beeinträchtigung ihrer Persönlichkeitsrechte darzutun. Unter diesen Umständen ist jede gerichtliche Beurteilung einer Informationsbearbeitung für den Betroffenen mit erheblichen Prozessrisiken verbunden.

Im öffentlichen Bereich ist bis heute über den gerichtlichen Grundrechtsschutz nur beschränkt und punktuell auf die staatlichen Informationstätigkeiten eingewirkt worden¹⁶⁾. Dazu kommt, dass die Informationsbearbeitungsaufgaben der Verwaltung im allgemeinen nur sehr fragmentarisch geregelt sind. Es bestehen zwar unzählige Vorschriften über die Auskunftspflichten der Bürger sowie mancherlei Regeln über die Datenverwertung oder über Mitteilungspflichten für die Behörden, doch werden damit meistens nur spezifische Zwecke des Gesetzesvollzugs, nicht aber der Schutz des Betroffenen verfolgt. Die beamtenrechtlichen Verschwiegenheitspflichten gewährleisten zwar einen wichtigen Schutz vor Weitergabe von Informationen an Privatpersonen. Sie stellen aber keine geeignete allgemeine Regelung zur Behandlung von Amts- und Rechtshilfeersuchen anderer Verwaltungsstellen dar. In der öffentlichen Verwaltung besteht bislang auch kein Verbot, Daten zweckentfremdet zu verwenden. Zum Teil ungelöst ist ferner die Frage, wie Informationen datenschutzkonform beschafft werden sollen. Im öffentlichen Recht fehlt es zudem an förmlichen Verwaltungs- und Prozessverfahren, die es Personen ermöglichen, sich über die sie betreffenden Daten zu informieren, deren Verwendung und Weitergabe zu kontrollieren und sich gegen Mängel der Bearbeitung zu wehren¹⁷⁾.

115 Diskrepanz zwischen geltendem Recht und Praxis in der medizinischen Forschung

115.1 Persönlichkeitsschutz des Patienten und öffentliches Interesse an der medizinischen Forschung im Spannungsfeld

Informationen über den Gesundheitszustand einer Person gehören zu den heiklen, sensitiven Daten, welche die Intimsphäre im Kern berühren können. Dies trifft insbesondere bei Angaben über schwerere Krankheiten und Gebrechen zu. Viele Menschen empfinden Hemmungen, Dritten nähere Auskünfte über ihren Gesundheitszustand zu erteilen. Sie befürchten, dass damit eine Einbusse an sozialer Geltung oder Nachteile im Beruf verbunden seien. Anders verhält es sich, wenn sich jemand in medizinische Behandlung begibt. Medizinalpersonen gegenüber wird der Patient meistens sehr viele intime Angaben über seine körperliche und geistige Verfassung machen, weil nur so eine erfolversprechende Therapie möglich ist. Er wird allerdings nur vorbehaltlos über seinen Gesundheitszustand Auskunft geben, wenn er Vertrauen in die ihn behandelnde Person, insbesondere den Arzt, hat. Dieses Vertrauen geht namentlich auch dahin, dass über die Wahrnehmungen bei seiner Behandlung Stillschweigen bewahrt wird.

Diese Zusammenhänge sind seit alters her bekannt. Es erstaunt deshalb nicht, dass man im Gesundheitsbereich eine der ältesten Datenschutzregelungen überhaupt kennt: die ärztliche Schweigepflicht. Sie findet ihren Ausdruck bereits im hippokratischen Eid. Heute stellt die Verletzung der ärztlichen Schweigepflicht in den meisten Ländern einen strafrechtlichen Tatbestand dar. So werden in der Schweiz nach Artikel 321 des Strafgesetzbuches u. a. Ärzte, Zahnärzte, Apotheker, Hebammen sowie ihre Hilfspersonen auf Antrag mit Gefängnis oder Busse bestraft, wenn sie ein Berufsgeheimnis offenbaren. Diese Schweigepflicht kann

nur mit Einwilligung des Patienten oder durch eine Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde aufgehoben werden.

Die medizinische Forschung anderseits arbeitet in bedeutendem Ausmass mit personenbezogenen Daten. Häufiger als in andern Forschungsbereichen besteht hier das Bedürfnis nach Angaben, aufgrund derer sich die betroffenen Personen identifizieren lassen (v. a. im Bereich von Erbkrankheiten, Krebsentstehung, krankheitsverursachenden Umwelteinflüssen usw.). Nur Daten mit direktem Personenbezug ermöglichen es beispielsweise, Forschungsergebnisse für die Behandlung einer betroffenen Person direkt nutzbar zu machen, Mehrfacherfassungen als solche zu erkennen, Vergleichsgruppen zu bilden, Langzeituntersuchungen durchzuführen oder ergänzende Rückfragen vorzunehmen. An dieser Forschungstätigkeit besteht unbestrittenermassen ein grosses öffentliches und/oder privates Interesse, vor allem wenn sie der wirksameren Bekämpfung besonders schwerer oder häufiger Leiden dient. In vielen Einzelfällen kann sie die Grundlagen für eine wirksame Therapie oder Prävention schaffen und steht damit im Dienste der Volksgesundheit als solcher.

115.2 Unbefriedigende Regelung im Strafgesetzbuch

Diese strafrechtlichen Bestimmungen über das Berufsgeheimnis (Art. 321 des Strafgesetzbuches) tragen den beschriebenen Entwicklungen in der medizinischen Forschung nicht mehr Rechnung und werden deshalb in der Praxis auch nicht mehr beachtet.

Nach der geltenden Regelung müssen Forscher, wenn sie Einblick in die Krankengeschichten nehmen wollen, die Zustimmung aller Patienten einholen beziehungsweise über den behandelnden Arzt einholen lassen¹⁸⁾. Nun gibt es aber häufig Fälle, wo das Einholen einer solchen Zustimmung recht schwierig ist, etwa weil die Patienten nicht mehr auffindbar sind, weil sie verstreut leben oder gestorben sind. Auch die Weitergabe von Daten an Personen, die selbst einem Berufsgeheimnis unterstehen, stellt grundsätzlich eine Verletzung des Berufsgeheimnisses dar. Dies gilt selbst für die Datenweitergabe unter Ärzten. Das Arztgeheimnis ist an sich auch innerhalb eines Spitals zu wahren, es sei denn, die Datenweitergabe geschehe unter den an der Behandlung eines Patienten direkt Beteiligten. In diesem Fall darf von einer stillschweigenden Einwilligung des Patienten als Rechtfertigungsgrund für die Offenbarung des Arztgeheimnisses ausgegangen werden¹⁹⁾. Denn einem Patienten ist von Anfang an bekannt, dass seine Krankengeschichte im Laufe seiner Spitalbehandlung von mehreren Personen zur Kenntnis genommen wird, ohne dass er allerdings weiss, wer alles an seiner Behandlung beteiligt ist. Darüber hinaus sollte aber mit Rücksicht auf Organisation und Struktur eines Spitalbetriebs generell die Weitergabe von Patientendaten unter dem Spitalpersonal, soweit es unter der gleichen therapeutischen Leitung steht – d. h. in der Regel innerhalb einer bestimmten Spitalabteilung –, zulässig sein.

In den westlichen Industriestaaten wurden seit Ende der sechziger Jahre Anstrengungen für eine gesetzliche Regelung der Datenbearbeitung unternommen. Das erste Datenschutzgesetz war das Hessische Datenschutzgesetz von 1970. In Hessen wurde erstmals eine institutionalisierte, von den datenverarbeitenden Stellen strikt getrennte und nur dem Parlament verantwortliche Kontrollinstanz geschaffen. 1973 erliess Schweden ein Datenschutzgesetz, das für die Errichtung und Führung eines «automatisierten Personenregisters» eine Genehmigung der «Dateninspektion» verlangt. In der Bundesrepublik Deutschland wurde 1977 das Bundesdatenschutzgesetz beschlossen, dem in rascher Folge die Datenschutzgesetze der Bundesländer folgten. In Frankreich wurde anfangs 1978 die «Loi relative à l'informatique, aux fichiers et aux libertés» verabschiedet. 1978 hat Österreich als dritter Nachbarstaat ein Datenschutzgesetz erlassen. Im gleichen Jahr ergingen ein Gesetz in Norwegen und zwei Gesetze in Dänemark (je eines für den privaten und öffentlichen Sektor). 1979 folgte Luxemburg, 1981 Island, Israel sowie – mit einem Dekret – Ungarn. Die letzten grossen Gesetzgebungsschritte erfolgten 1984 in Grossbritannien und 1987 in Finnland und Irland.

Von Interesse ist auch die Rechtsentwicklung in Übersee. In den Vereinigten Staaten von Amerika wurde 1974 ein Datenschutzgesetz geschaffen, das den betroffenen Personen Zugang zu ihren Daten und umfangreiche Rechtsmittel gewährt und den Bundesbehörden klare Bearbeitungsschranken setzt. Die USA ergänzten ihr Bundesgesetz für die Bundesverwaltung durch eine Reihe von Spezialgesetzen, z. B. über den Datenschutz bei der Kreditgewährung, im Bildungs- und Erziehungsbereich, im elektronischen Zahlungsverkehr oder bei Telekommunikationssystemen. Die amerikanischen Bundesstaaten schlossen sich, z. T. aufgrund von Mustergesetzen, mit Datenschutzerlassen für ihre öffentlichen Verwaltungen und mit privatrechtlichen Regelungen an. Ähnlich verlief die Gesetzgebung in Kanada und in Australien. In beiden Ländern hat der Zentralstaat wie in den USA nur beschränkte Kompetenzen zur Privatrechtsgesetzgebung. Kennzeichen aller drei Staaten ist im übrigen, dass sie das Persönlichkeits- und Datenschutzrecht zum Teil schon früher mit den Vorschriften über die Amtsöffentlichkeit und den Zugang zur staatlichen Information koordiniert haben, um Informationsabwehr- und Informationszugriffsbedürfnisse auszugleichen. Das geschah etwa in den USA mit dem «Freedom of Information Act» von 1966.

117 **Internationaler Datenschutz**

Die Entwicklung der Informatik und der Telekommunikation hat zu einer starken Intensivierung der internationalen Wirtschaftstätigkeit und zu einer engeren Kooperation der Staaten und internationalen Organisationen geführt. In vielen privaten und öffentlichen Bereichen macht die Datenbearbeitung nicht mehr an den Landesgrenzen halt. Verschiedene internationale Organisationen haben sich deshalb um völkerrechtliche Regelungen des grenzüberschreitenden Datenverkehrs bemüht²⁰⁾.

Die weitreichendste Regelung für den internationalen Datenschutz hat der *Europarat* mit dem «Übereinkommen Nr. 108 vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten» entwickelt. Das Übereinkommen ist von der Bundesrepublik Deutschland, Frankreich, Spanien, Norwegen, Schweden, Grossbritannien, Luxemburg und Österreich bereits ratifiziert und von weiteren zehn Staaten unterzeichnet worden.

Ziel der Konvention Nr. 108 ist der Schutz der Freiheitsrechte und namentlich des Privatlebens natürlicher Personen gegenüber der automatisierten Verarbeitung von Personendaten. Die Vertragsstaaten verpflichten sich, in ihr Recht gewisse Mindestgrundsätze des Datenschutzrechtes aufzunehmen (Art. 4–11). Die dadurch entstehende Harmonisierung zwischen den Datenschutzregelungen der einzelnen Vertragsstaaten soll ihrerseits ermöglichen, den grenzüberschreitenden Datenverkehr zwischen den Vertragsstaaten zu vereinfachen (Art. 12). Das Übereinkommen regelt des weitern die Zusammenarbeit und gegenseitige Unterstützung der Vertragsstaaten in Datenschutzangelegenheiten (Art. 13–17). Der Europarat hat ferner in den letzten Jahren verschiedene *Empfehlungen* ausgearbeitet, die bereichsspezifische Datenschutzregelungen zum Gegenstand haben. Sie betreffen den Datenschutz bei Medizinaldatenbanken, in der Forschung und Statistik, bei der Direktwerbung, im Sozialversicherungsbereich und bei der Polizei.

Praktisch gleichzeitig mit dem Europarat hat die *Organisation für Wirtschaftliche Zusammenarbeit (OECD)* «Leitlinien für den Schutz des Persönlichkeitsbereiches und den grenzüberschreitenden Verkehr personenbezogener Daten» ausgearbeitet. Der OECD-Rat hat die Leitlinien am 23. September 1980 mit einer Empfehlung den Regierungen der Mitgliedsländer zugestellt, und diese haben den Leitlinien zugestimmt. Die Leitlinien formulieren allgemeine Grundsätze des internationalen Datenverkehrs und Datenschutzes und regeln namentlich die Zusammenarbeit der Mitgliedsstaaten beim internationalen Datenaustausch. Die Bedeutung der OECD-Leitlinien liegt vor allem darin, dass ihnen auch überseeische Staaten (insbesondere die Vereinigten Staaten, Kanada, Japan und Australien) zugestimmt haben und dass sich in diesen Ländern eine grosse Zahl multinationaler Unternehmungen zu ihrer Einhaltung öffentlich verpflichtet haben.

12 Verfassungsrechtliche Rahmenbedingungen

Eine besondere Bestimmung der Bundesverfassung, die den Bund zum Erlass von Datenschutzvorschriften ermächtigt, existiert nicht. Mit dem Datenschutz sollen zwar zu einem wesentlichen Teil die traditionellen Grundrechte konkretisiert und deren Wirkung verstärkt werden, doch vermögen die Grundrechte allein nach herrschender Auffassung keine Sachkompetenz des Bundes zu begründen. Hingegen schliessen verschiedene Bundeskompetenzen auch die Befugnis zum Erlass von Datenschutzregelungen ein.

121 Im privatrechtlichen Bereich

Artikel 64 der Bundesverfassung (BV) ermächtigt den Bund zur Rechtsetzung auf dem Gebiet des Privatrechts. Gestützt darauf kann der Bundesgesetzgeber den bisher nur im Grundsatz geregelten privatrechtlichen Persönlichkeitsschutz durch *spezifische privatrechtliche Datenschutzvorschriften erweitern und stärken*. Dabei darf er auch Bestimmungen erlassen, die – wie etwa eine Registrierpflicht für bestimmte Datensammlungen – an sich öffentlich-rechtlicher Natur sind, sofern sie zur Durchsetzung und einheitlichen Anwendung des Bundeszivilrechts oder zur Vermeidung von Rechtskollisionen notwendig sind²¹⁾.

Im weitem steht dem Bund aufgrund von Artikel 31^{bis} Absatz 2 BV die generelle Befugnis zu, «*Vorschriften ... über die Ausübung von Handel und Gewerbe*» zu erlassen. Gestützt darauf können der privaten Erwerbstätigkeit wirtschaftspolizeiliche Schranken gesetzt werden, wobei das zentrale Schutzgut entsprechender Vorschriften die *Lauterkeit im Geschäftsverkehr* ist. Diese Lauterkeit in der privaten Wirtschaftstätigkeit gilt es auch beim Umgang mit personenbezogenen Informationen zu sichern. Dabei stehen nicht nur solche wirtschaftliche Aktivitäten im Vordergrund, bei denen – wie bei den Rechenzentren – die Datenbearbeitung als solche Hauptzweck ist, sondern jegliche Wirtschaftstätigkeit, bei welcher personenbezogene Daten verwendet werden. Datenbearbeitungen für den privaten persönlichen Gebrauch sowie für wissenschaftliche oder ideelle Zwecke können hingegen nicht gestützt auf Artikel 31^{bis} Absatz 2 BV geregelt werden.

Zu diesen beiden Hauptkompetenzen treten weitere Verfassungskompetenzen hinzu, die den Bund zu bereichsspezifischen Datenschutzregelungen ermächtigen. So können aufgrund von Artikel 34^{ter} Absatz 1 BV zum Schutz der Arbeitnehmer Bestimmungen über private Personalinformationssysteme erlassen werden. Der Bund hat auch die Befugnis, gestützt auf Artikel 31^{quater} BV Kreditinformationssysteme von Banken und Sparkassen zu erfassen oder gemäss Artikel 34 Absatz 2 BV spezielle Regelungen für die Informationstätigkeiten der Privatassekuranz vorzusehen.

122 Im öffentlich-rechtlichen Bereich

Beim Erlass von Datenschutzregelungen für Behörden und Verwaltungsstellen des Bundes kann sich der Bundesgesetzgeber auf die ihm in Artikel 85 Ziffer 1 BV eingeräumte *Organisationsgewalt* abstützen. Diese Verfassungsbestimmung erlaubt, den rechtmässigen Einsatz der Datenverarbeitung als Arbeits- und Organisationsinstrument bei den Bundesstellen zu regeln und Kontrollmechanismen zu schaffen, die einen wirksamen Datenschutz sicherstellen. Sodann kann der Bund gestützt auf die Strafrechtskompetenz von Artikel 64^{bis} BV den Datenschutz mit den Mitteln des Strafrechts verstärken, sei es durch den Erlass neuer Strafnormen oder durch weitere Konkretisierungen der Amts- und Berufsgeheimnisse.

Für den Datenschutz im *kantonalen öffentlichen Bereich* sind die Kantone aufgrund ihrer verfassungsrechtlich garantierten Organisationsautonomie selbst zu-

ständig. Nach kantonalem Verfassungs- und Gesetzesrecht entscheidet sich auch, wie weit die kantonale Datenschutzordnung für die kommunalen Verwaltungen gelten soll. Der Bund hingegen kann für kantonale oder kommunale Verwaltungen nur bereichsspezifische Datenschutzvorschriften erlassen, soweit ihm eine Gesetzgebungskompetenz in der Sache selbst zusteht und der Vollzug den Kantonen übertragen wird (z. B. bei der Bekämpfung übertragbarer Krankheiten, Art. 69 BV). Er hat dabei jedoch auf das kantonale Organisationsrecht Rücksicht zu nehmen.

13 Vorverfahren zur Gesetzgebung

131 Allgemeines Datenschutzrecht

Eine erste Motion zum Erlass eines Datenschutzgesetzes wurde am 17. März 1971 von Nationalrat Bussey eingereicht. Er verlangte eine Gesetzgebung, «welche den Bürger und dessen Privatsphäre gegen missbräuchliche Verwendung der Computer schützt, anderseits jedoch eine normale Entwicklung der Verwendung von Datenverarbeitungsanlagen sicherstellen soll»²²⁾. Der Vorstoss wurde als Postulat überwiesen²³⁾. Am 22. März 1977 reichte Nationalrat Gerwig zwei Parlamentarische Initiativen zum Datenschutz ein. Mit der ersten, formulierten Initiative verlangte er eine Ergänzung der Bundesverfassung durch einen Datenschutzartikel. In der zweiten Initiative, die in der Form einer allgemeinen Anregung gehalten ist, formulierte Nationalrat Gerwig eine Reihe von Anforderungen an ein Datenschutzgesetz.

Ebenfalls im Jahre 1977, noch bevor die nationalrätliche Kommission, welche die Initiativen Gerwig behandelte, über das weitere Vorgehen entschieden hatte, beschloss der Vorsteher des Eidgenössischen Justiz- und Polizeidepartementes (EJPD), Experten mit den Vorarbeiten für ein Datenschutzgesetz zu betrauen. Dabei traf er zwei Grundsatzentscheidungen: Zum einen sollten sich die Vorschläge an die bestehenden Verfassungsgrundlagen halten und daher nur den Privatbereich und den öffentlichen Bereich des Bundes erfassen; auf eine Verfassungsrevision, die eine umfassende, auch den kantonalen öffentlich-rechtlichen Bereich einschliessende Gesetzgebung erlaubt hätte, sollte verzichtet werden. Zum andern sollten die Vorarbeiten in der Anfangsphase für die privat- und die öffentlich-rechtlichen Vorschriften getrennt an die Hand genommen werden.

Entsprechend wurde 1977 unter dem Vorsitz von Professor Mario M. Pedrazzini, St. Gallen, eine erste Expertenkommission mit Vertretern aus Wissenschaft, Privatwirtschaft und Verwaltung eingesetzt, die Datenschutzvorschriften für die Bundesverwaltung ausarbeiten sollte. Nach Erhebungen über den Bestand an Datensammlungen und über die bisher aufgetretenen Datenschutzprobleme lieferte die Arbeitsgruppe Ende 1981 dem Eidgenössischen Justiz- und Polizeidepartement einen Vorentwurf für ein Bundesgesetz über den Datenschutz im Bereich der Bundesverwaltung ab.

In der Zwischenzeit, im September 1979, hatte der Vorsteher des EJPD eine zweite Kommission einberufen, welche Datenschutzregelungen für den Privatbereich zu entwerfen hatte. Auch diese Arbeitsgruppe stand unter der Leitung

von Professor Pedrazzini. Sie führte bei über 100 Unternehmen, Verbänden und Organisationen Erhebungen über Umfang und Verwendung von Datensammlungen und über spezifische Datenschutzprobleme durch. Im Oktober 1982 verabschiedete sie einen Gesetzesentwurf für den privatrechtlichen Bereich.

Im November 1982 gab der Vorsteher des EJPD einem kleinen Ausschuss aus Mitgliedern beider Kommissionen den Auftrag, die beiden Vorentwürfe zu einem einzigen Gesetzesentwurf zusammenzulegen. Damit sollte namentlich zugunsten der Betroffenen eine Rechtszersplitterung vermieden und das Gesetzgebungsverfahren erleichtert werden. Aus diesen Redaktionsarbeiten ging Ende 1983 der *Entwurf für das Vernehmlassungsverfahren* hervor.

Der *Vernehmlassungsentwurf* versuchte in erster Linie, Kriterien dafür anzugeben, wie die Informationsbedürfnisse privater Personen und staatlicher Organe gegenüber den Schutzbedürfnissen der Betroffenen abzuwägen sind. Im privatrechtlichen Bereich geschah dies in der Weise, dass differenzierte Beweislastregeln zugunsten der betroffenen Personen einerseits und für bestimmte Datenbearbeiter andererseits aufgestellt wurden. Im öffentlich-rechtlichen Bereich sah der Entwurf detaillierte Vorschriften über den Umgang von Organen des Bundes mit Personendaten vor. Zudem sollten private Personen wie auch Organe des Bundes, die eine Datensammlung führten, diese unter gewissen Voraussetzungen registrieren lassen. Des weitern regelte der Entwurf die Rechte der betroffenen Personen auf Auskunft über ihre Daten und schuf Rechtsbehelfe, um sich gegen Beeinträchtigungen der Persönlichkeit durch Datenbearbeitungen zu wehren. Als Kontrollinstanz war eine Datenschutzkommission vorgesehen, die im Privatbereich nach dem Vorbild der Kartellkommission konzipiert war, während sich ihre Aufgaben im Bereich der Bundesverwaltung mit denen der Finanzkontrolle vergleichen liessen. Schliesslich sah der Entwurf für Verstösse gegen grundlegende Prinzipien des Datenschutzes verschiedene Strafbestimmungen vor.

132 Datenschutz im Medizinalbereich

Neben den allgemeinen Datenschutzregeln sind in gewissen Sachgebieten zusätzliche Sonderbestimmungen notwendig, so vor allem im Medizinal- und Sozialversicherungsbereich. Auf diesem Gebiet werden oft besonders schützenswerte Daten bearbeitet, wobei die Intimsphäre des Betroffenen berührt sein kann. Andererseits besteht zum Teil ein ausgewiesenes öffentliches Interesse an der Auswertung von Gesundheitsdaten.

Das Bundesamt für Justiz beauftragte deshalb 1980 eine Spezialkommission unter dem Vorsitz von Frau Nationalrätin Yvette Jaggi, Lausanne, mit der Abklärung der datenschutzrechtlichen Fragen im Medizinalbereich. Die Arbeitsgruppe legte in der Folge in einem 1984 erschienenen Bericht eine umfassende Bestandesaufnahme der Informationstätigkeiten im privaten und öffentlichen Medizinal- und Sozialversicherungsbereich vor. Sie stellte deren rechtliche Grundlagen dar und umschrieb die aktuellen Datenschutzfragen. Ihr Bericht mündet in eine Reihe von Empfehlungen, die zum Teil im vorliegenden Entwurf für ein allgemeines Datenschutzgesetz ihren Niederschlag gefunden haben, zum Teil verwaltungsintern weiterbearbeitet werden.

Im Oktober 1983 erteilte der Vorsteher des EJPD einer weiteren Arbeitsgruppe unter der Leitung von Professor Günter Stratenwerth, Basel, den Auftrag, die Datenschutzprobleme in der medizinischen Forschung näher abzuklären. Sie sollte insbesondere einen Ausgleich zwischen den Datenbearbeitungsinteressen der Forscher und den Interessen der Patienten an der ärztlichen Schweigepflicht suchen. In ihrem Bericht vom Dezember 1985 präsentierte die Arbeitsgruppe einen Katalog von Anträgen. Sie gelangte im wesentlichen zum Schluss, dass Forschung mit Personendaten, die dem ärztlichen Berufsgeheimnis unterliegen, grundsätzlich nur mit Zustimmung der Betroffenen durchgeführt werden soll. Sofern ein Betroffener nicht ausdrücklich Einspruch erhebt, soll die Zustimmung aber durch die Bewilligung einer Sachverständigenkommission ersetzt werden können.

Gestützt auf diese Vorarbeiten hat das Eidgenössische Justiz- und Polizeidepartement in Zusammenarbeit mit dem Eidgenössischen Departement des Innern einen Entwurf zu einem Bundesgesetz über die Offenbarung des Berufsgeheimnisses für die medizinische Forschung ausgearbeitet. Im Sommer 1987 führte es dazu ein Vernehmlassungsverfahren durch. Der Gesetzesentwurf übernahm im wesentlichen die von der Arbeitsgruppe Stratenwerth erarbeiteten Grundsätze, beschränkte sich jedoch auf die Regelung der *Datenweitergabe* bzw. Datenbeschaffung. Er bestimmte, unter welchen Voraussetzungen ein Berufsgeheimnis zu Zwecken der medizinischen Forschung aufgehoben werden darf und stellte mithin zu einem wesentlichen Teil Ausführungsrecht zu Artikel 321 des Strafbuches über das Berufsgeheimnis dar. Sein Anwendungsbereich erstreckte sich auf jegliche Forschungstätigkeit, unabhängig davon, ob sie an privaten Forschungsinstituten, bei Forschungsstellen des Bundes oder an kantonalen Universitäten sowie Kantons-, Regional- und Gemeindespitalern stattfindet.

14 Ergebnisse der Vernehmlassungsverfahren

141 Vernehmlassungsverfahren zum allgemeinen Datenschutzgesetz

Am 25. Januar 1984 wurde das Vernehmlassungsverfahren zum Expertenentwurf für das «Bundesgesetz über den Schutz von Personendaten (DSG)» eröffnet. Bis zum Herbst 1984 gingen 156 – z. T. sehr umfangreiche – Stellungnahmen ein. Von den 141 offiziell begrüßten Stellen haben sich 107 zur Vorlage geäußert, darunter sämtliche Kantone. Neben den offiziell begrüßten Stellen haben weitere 49 Personen und Organisationen an der Vernehmlassung teilgenommen.

Die wichtigsten Ergebnisse der Konsultation sind folgende: Eine überwiegende Mehrheit der Vernehmlasser bejahte die Notwendigkeit und die Dringlichkeit einer Datenschutzgesetzgebung. Die Vorlage wurde, soweit sie sich auf die Datenbearbeitung in der Bundesverwaltung bezog, als brauchbar bis gut bezeichnet. Sehr viel umstrittener waren dagegen die Datenschutzvorschriften für den Privatbereich, wo das Urteil insgesamt ungünstig ausfiel. Zwar fanden die Bestimmungen auf diesem Gebiet bei Arbeitnehmerverbänden, öffentlich-rechtlichen Institutionen, Organisationen der Wissenschaft und Bildung und den Kir-

chen fast einhellig Zustimmung. Mehrheitlich eher positiv waren auch die Stellungnahmen der Kantone, politischen Parteien und Berufs- und Frauenorganisationen. Geteilter Meinung waren aber die Informatiker, und vollends abgelehnt wurden die Bestimmungen für den Privatbereich von den Arbeitgeber- und Wirtschaftsorganisationen (mit Ausnahme der Konsumentenverbände) sowie den Vertretern des Sozialwesens. Umstritten war auch das Konzept, für den privaten und öffentlichen Bereich ein einziges Gesetz zu erlassen. Während ein solches «Einheitsgesetz» von gewissen Kantonen, Parteien und Verbänden begrüsst wurde, lehnten andere Kantone und insbesondere die Arbeitgeberorganisationen diese Lösung ab.

Eine ganze Anzahl von grundlegenden Vorschlägen des Entwurfs wurde deutlich *gutgeheissen*. Dies gilt für die Gleichbehandlung von automatisierter und manueller Datenbearbeitung und für die Einführung einer Kategorie von besonders schützenswerten Daten. Zustimmung gefunden haben auch die Registrierungspflicht für bestimmte Arten von Datensammlungen und das Auskunfts- und Berichtigungsrecht der betroffenen Personen. Bejaht wurden ferner, wenigstens dem Grundsatz nach, die Notwendigkeit einer effizienten und unabhängigen Datenschutzkontrolle und die Aufnahme strafrechtlicher Bestimmungen in den Entwurf.

Die *Kritik* am Entwurf ging vor allem dahin, dieser sei mit seinen 69 Artikeln zu umfangreich und zu kompliziert. Er wirke zudem streckenweise zu abstrakt und praxisfremd. Schwierigkeiten hat namentlich der Umstand bereitet, dass im gleichen Artikel vielfach Bestimmungen sowohl für den öffentlich-rechtlichen wie für den privatrechtlichen Bereich enthalten waren. Die im privatrechtlichen Teil vorgesehenen Vermutungen und Fiktionen von Persönlichkeitsverletzungen und Rechtfertigungsgründen waren schwer verständlich. Kritisiert wurde ferner, dass das Gesetz auch beim Vollzug von Bundesrecht durch die Kantone hätte Anwendung finden sollen. Verschiedene Vernehmlassungsteilnehmer verlangten eine differenzierte Behandlung von natürlichen und juristischen Personen. Des weitern wurden gewisse Erleichterungen für bestimmte wirtschaftliche Tätigkeiten, etwa die Beschaffung von Kreditauskünften, gefordert. Ferner wurde gewünscht, dass die bereichsspezifischen Regelungen für die Medien, die Forschung und Statistik, den Staatsschutz und die Steuerbehörden überprüft, ergänzt oder präziser gefasst werden. Dem Modell einer Datenschutzkommission als unabhängiges Kontrollorgan stimmte eine beachtliche Gruppe der Vernehmlasser zu, während eine andere, praktisch gleich grosse Gruppe einen Datenschutzbeauftragten im Sinne eines Datenschutzombudsmanns vorgezogen hätte.

142 Datenschutz in der medizinischen Forschung

Am 27. Mai 1987 wurde das Vernehmlassungsverfahren zum Entwurf für ein «Bundesgesetz über die Offenbarung des Berufsgeheimnisses für die medizinische Forschung» eröffnet. Bis zum Herbst 1987 gingen 54 Stellungnahmen ein. Von den 61 offiziell begrüsstten Stellen haben sich 47 zur Vorlage geäussert, darunter sämtliche Kantone. Neben den offiziell begrüsstten Kreisen haben weitere sieben Organisationen an der Vernehmlassung teilgenommen.

Die Vorlage wurde insgesamt gut aufgenommen. Sie wurde von einer deutlichen Mehrheit der Kantone und nahezu einstimmig von den Hochschulen und den Organisationen der Ärzte und der medizinischen Forschung als taugliche Grundlage für ein künftiges Gesetz anerkannt. Geteilter Meinung waren die politischen Parteien, wobei sich die drei grössten unter ihnen allerdings für die Vorlage aussprachen. Eher ablehnend äusserten sich die Organisationen, die Patienteninteressen vertreten.

Im Sinne einer Kritik wurde mehrheitlich gefordert, den Patientenrechten sei noch besser Rechnung zu tragen und der datenschutzrechtliche Charakter der Vorlage sei deutlicher zum Ausdruck zu bringen. Eine Minderheit zweifelte an der verfassungsrechtlichen Grundlage für eine Regelung des Datenschutzes in der medizinischen Forschung auf Bundesebene. Vereinzelt wurde auch die Schaffung einer zentralen, eidgenössischen Kommission für die Bewilligung von Datenweitergaben zu Zwecken der medizinischen Forschung abgelehnt. Nicht unbestritten war ferner, dass der Datenschutzbeauftragte eine Kontrollfunktion übernehmen sollte.

Viele Vernehmlasser sprachen sich schliesslich dafür aus, den Datenschutz in der medizinischen Forschung nicht in einem Spezialgesetz, sondern im allgemeinen Datenschutzgesetz und – weil es um die Neuregelung des strafrechtlich umschriebenen Berufsgeheimnisses geht – im Strafgesetzbuch zu regeln.

15 Fertigstellung des Entwurfs

Im Frühjahr 1985 nahm der Bundesrat von den Ergebnissen des Vernehmlassungsverfahrens zum allgemeinen Datenschutzgesetz Kenntnis und gab einer kleinen Arbeitsgruppe unter Professor Pedrazzini den Auftrag, den Entwurf im Lichte der Vernehmlassungsergebnisse noch einmal zu überarbeiten. Die Arbeitsgruppe erstellte neue Entwürfe und führte im Mai 1986 mit Vertretern von Arbeitgeber- und Arbeitnehmerorganisationen und wichtigeren Branchen – wie Banken, Versicherungen, Adresshandel – sowie mit Vertretern von Medienunternehmen und Medienschaffenden und mit besonders interessierten Bundesämtern Hearings durch. Sie wollte damit den vom Gesetz besonders verpflichteten Personen und Stellen Gelegenheit geben, ihre konkreten Anliegen gegenüber der neuen Fassung des Gesetzes vorzubringen. In den Hearings wurde die klare Trennung der Vorschriften für den privaten und den öffentlich-rechtlichen Bereich begrüsst, ebenso die Straffung und bessere Lesbarkeit des Entwurfs. In materieller Hinsicht fand der Entwurf teils Zustimmung, teils begegnete er ähnlichen Einwendungen wie der Vernehmlassungsentwurf. Im Februar 1987 lieferte die Arbeitsgruppe der Vorsteherin des EJPD einen neuen Gesetzesentwurf mit Kommentar ab.

Im Auftrag der Departementsvorsteherin wurde die Vorlage von einer verwaltungsinternen Arbeitsgruppe unter der Leitung von Dr. Christoph Steinlin, Vizedirektor im Bundesamt für Justiz, vor allem in systematischer und redaktioneller Hinsicht noch einmal überarbeitet, wesentlich vereinfacht und weiter gestrafft. Gleichzeitig wurden – vor allem durch eine Ergänzung des Strafgesetzbuches – Bestimmungen für ein Bundesgesetz über die Offenbarung des Berufs-

geheimnisses für die medizinische Forschung in die Vorlage eingearbeitet. Zudem wurden der Bundesstraßprozess und das Rechtshilfegesetz mit bereichsspezifischen Datenschutzregelungen für das gerichtspolizeiliche Ermittlungsverfahren und den Informationsaustausch mit INTERPOL ergänzt.

- 2 Besonderer Teil:**
Kommentar zum Entwurf zu einem Bundesgesetz
über den Datenschutz, zur Regelung des Datenschutzes
in der medizinischen Forschung und zur Revision
des Bundesstraßprozesses und des Rechtshilfegesetzes
- 21 Grundzüge des Entwurfs für ein allgemeines Datenschutzgesetz**
- 211 Regelung des öffentlichen und des privatrechtlichen**
Datenschutzes in einem Gesetz

In der Vernehmlassung hatte eine Mehrheit ein Datenschutzgesetz abgelehnt, das sowohl den Privatbereich als auch die Bundesverwaltung erfasst. Dabei wurde zur Hauptsache geltend gemacht, der Datenschutz in der Bundesverwaltung und derjenige im Privatbereich seien von ihrem Konzept her derart unterschiedlich, dass eine Regelung in einem einzigen Erlass kaum möglich sei; eine gemeinsame Normierung führe zu einer Komplizierung des Gesetzes. Nach Auffassung des Bundesrates trifft jedoch der erste Einwand nicht zu und kann dem zweiten Rechnung getragen werden, ohne dass damit die Vorteile, die eine gemeinsame Regelung beider Bereiche mit sich bringt, aufgegeben werden müssen. Für ein Einheitsgesetz spricht vor allem, dass der gesetzgebungspolitische Zweck, der Schutz der Persönlichkeit vor Verletzungen durch das Bearbeiten von Personendaten, im Bereich der Bundesverwaltung und im Privatbereich derselbe ist. Auch müssen die wichtigsten Grundsätze des Datenschutzrechts sowohl im privaten wie im öffentlichen Bereich Geltung haben. Es ist deshalb erwünscht, dass für die Beurteilung datenschutzrechtlicher Fragen auf beiden Gebieten dieselben Behörden – d. h. der gleiche Datenschutzbeauftragte und dieselbe Datenschutzkommission – zuständig sind, wobei allerdings ihre Befugnisse im privaten Bereich sehr viel geringer sein sollen. Auf diese Weise ist eine harmonische, gegenseitig abgestimmte Entwicklung von privatem und öffentlichem Datenschutzrecht am ehesten gewährleistet. Ein einziges Gesetz lässt sich auch rechtfertigen, weil darin privater und öffentlich-rechtlicher Bereich durchaus präzise auseinandergehalten werden können. Zudem wird im Entwurf nun klargestellt, dass die Regelungen für den privatrechtlichen Bereich sich in den Rahmen des allgemeinen Persönlichkeitsschutzes des Zivilgesetzbuches einfügen. Für ein Einheitsgesetz spricht schliesslich der Umstand, dass auf diese Weise Überschneidungen vermieden werden und die Anzahl der Normen auf ein Minimum begrenzt werden können.

212 Geltungsbereich

Der Gesetzgeber, der ein allgemeines Datenschutzgesetz erlassen will, sieht sich vorab mit zwei Hauptschwierigkeiten konfrontiert. Datenschutzrecht ist eine

«Querschnittmaterie», welche gerade im Zeichen der zunehmenden Informatisierung beinahe alle privaten und staatlichen Handlungsbereiche berührt. Weil eine Vielzahl technischer Hilfsmittel zur Verfügung steht, erscheint zudem die Informationsbearbeitung als Gegenstand eines Datenschutzgesetzes in den mannigfaltigsten Formen. Ein allgemeines Datenschutzgesetz kann aber nicht alle denkbaren Ausprägungen der Datenbearbeitung berücksichtigen; es muss vielmehr allgemeine, grundsätzliche Regeln enthalten, die es erlauben, die meisten Probleme wenigstens im Ansatz zu bewältigen, und daneben Raum für die Weiterentwicklung des Datenschutzes lassen. Der Entwurf kann nicht alle nötigen bereichsspezifischen Regelungen schon vorwegnehmen.

Entsprechend verzichtet der Entwurf, wie manches ausländische Gesetz²⁴⁾, auf eine Unterscheidung zwischen manueller und automatisierter Datenbearbeitung. Er will nicht auf konkrete technische Bedingungen abstellen, sondern im Gegenteil gegenüber der Technik und ihrer Entwicklung möglichst neutral bleiben. Dem allgemeinen Charakter des Gesetzes entspricht es auch, dass es grundsätzlich alle Personendaten umfasst. Auf sogenannte «freie Daten», die dem Gesetz nicht unterstehen, wurde verzichtet, weil sich diese Kategorie kaum sachgerecht abgrenzen lässt und überdies selbst mit solchen Informationen in einem bestimmten Kontext eine Persönlichkeitsverletzung bewirkt werden kann. Das Gesetz will des weitern *natürliche und juristische Personen* schützen, da beide durch eine Datenbearbeitung in ihren Rechten beeinträchtigt werden können. Umgekehrt sind auch die Informationsbearbeitungsvorschriften für natürliche und juristische Personen die selben. Schliesslich gilt der Entwurf sowohl für den privatrechtlichen wie für den öffentlich-rechtlichen Bereich.

Der Anwendbarkeit des allgemeinen Datenschutzgesetzes sind gleichwohl gewisse Grenzen gesetzt. Es soll unter anderem auf Rechtsprechungsverfahren vor richterlichen Behörden, auf Strafverfahren, auf Verwaltungsbeschwerdeverfahren, auf Rechtshilfeverfahren und auf das Registerrecht keine Anwendung finden. Der Grund liegt zur Hauptsache darin, dass die einschlägigen Prozessgesetze ihrerseits Garantien zum Schutze der Persönlichkeit vorsehen, welche nicht zusätzlich durch Datenschutzrecht, das zum Teil auch Verfahrensrecht ist, überlagert werden sollen. Bei den Vorarbeiten zum Gesetzesentwurf hat sich aber gezeigt, dass das im Bundesstrafprozess geregelte *gerichtspolizeiliche Ermittlungsverfahren* zusätzlicher Datenschutzgarantien bedarf. Im Anhang des Entwurfes sollen daher durch eine Änderung des Gesetzes über die Bundesstrafrechtspflege besondere Datenschutzbestimmungen erlassen werden. Im gleichen Zug werden durch eine Änderung des Bundesgesetzes über internationale Rechtshilfe in Strafsachen gesetzliche Grundlagen für den Datenaustausch im Rahmen der Internationalen Kriminalpolizeilichen Organisation (INTERPOL) und zugleich spezifisches Datenschutzrecht für diese kriminalpolizeiliche Informationstätigkeit geschaffen.

Der Vernehmlassungsentwurf von 1983 hatte vorgesehen, dass das Datenschutzgesetz des Bundes auch zur Anwendung käme, wenn ein Kanton beim Vollzug von Bundesrecht nicht über ausreichendes eigenes Datenschutzrecht verfügt. Mit einer solchen Regelung könnte eine Harmonisierung des schweizerischen Datenschutzrechts gefördert und das Entstehen von «Datenschutz-oasen» im Bereich des Vollzugs von Bundesrecht vermieden werden. Gleichwohl enthält

der vorliegende Entwurf keine entsprechende Regelung mehr. Der Grund liegt darin, dass die Bestimmung des «ausreichenden kantonalen Datenschutzrechts» erhebliche Probleme aufwerfen würde, vor allem wenn sie mit der gebotenen föderalistischen Rücksichtnahme durchgeführt wird. Würde der Bund allein auf das Vorhandensein eines kantonalen Gesetzes abstellen, könnte dies zu unbilligen Lösungen führen. Will er anderseits nicht jegliches Datenschutzrecht der Kantone unesehen akzeptieren, liefe dies auf eine neue Genehmigungspflicht für kantonale Erlasse hinaus, verbunden mit einer bundesrechtlichen Ersatzordnung für all jene Fälle, in denen das kantonale Recht nicht ausreicht. Es wäre dann möglich, dass im gleichen Kanton unterschiedliches Datenschutzrecht für den Vollzug von Bundesrecht und für den autonomen kantonalen Bereich gelten würde. Der Bundesrat ist deshalb der Auffassung, das Bundesdatenschutzgesetz sollte keine Anwendung auf den Vollzug von Bundesrecht durch die Kantone finden.

213 Allgemeines Datenschutzgesetz

213.1 Materielle und organisatorische Grundprinzipien des Datenschutzes

Die wichtigsten Leitideen und organisatorischen Voraussetzungen für einen wirkungsvollen Datenschutz sind in den *Allgemeinen Bestimmungen* des ersten Abschnittes verankert. Sie gelten sowohl für private Datenbearbeiter wie für Organe des Bundes. Im Grundsatzartikel 4 wird festgehalten, dass die Beschaffung von Personendaten nur mit *rechtmässigen Mitteln* und *nicht gegen Treu und Glauben* erfolgen darf. Bei der Bearbeitung von Daten ist auf deren *Richtigkeit* zu achten. Die Datenbearbeitung muss zudem *verhältnismässig* sein. Der dem Betroffenen bei der Datenbeschaffung angegebene oder für ihn erkennbare *Bearbeitungszweck soll später nicht geändert* werden, es sei denn, ein Gesetz sehe dies vor. Wer Daten bearbeitet, hat diese mit geeigneten technischen oder organisatorischen Mitteln *gegen Eingriffe unbefugter Dritter zu schützen*. – Diese Bestimmungen bilden zusammen mit dem Grundsatz für die Bekanntgabe von Daten ins Ausland (vgl. Ziff. 213.5) den *materiellen Kerngehalt* des Datenschutzes.

Damit aber die genannten Grundsätze in der Rechtswirklichkeit auch durchgesetzt werden können, müssen geeignete organisatorische und verfahrensmässige Voraussetzungen geschaffen werden. Sie sollen gewährleisten, dass die Datenbearbeitung für die betroffenen Personen in einem gewissen Umfang einsehbar wird. Zu diesem Zweck werden Inhaber von Datensammlungen verpflichtet, *einer Person auf deren Verlangen mitzuteilen, ob über sie in der Datensammlung Angaben vorhanden sind und wie die Datensammlung verwendet wird*. Da aber das *Auskunftsrecht* nur wahrnehmen kann, wer von der Existenz einer Datensammlung Kenntnis hat, sind alle Bundesstellen verpflichtet, ihre Datensammlungen beim Datenschutzbeauftragten registrieren zu lassen. Für Privatpersonen geht die Registrierpflicht weniger weit; sie müssen nur solche Sammlungen melden, bei denen eine erhebliche Gefahr einer Persönlichkeitsverletzung besteht. Schliesslich sind Datenbekanntgaben ins Ausland unter bestimmten Voraussetzungen ebenfalls meldepflichtig (vgl. Ziff. 213.5).

213.2 Datenschutz im Bereich des Privatrechts

Der zweite Abschnitt des Entwurfes ist auf vier Artikel beschränkt und enthält Bearbeitungsvorschriften für natürliche und juristische Personen, die im Rahmen des Privatrechts handeln. Ein Regelungsvorschlag für diesen Bereich war bereits bei der Vorbereitung der am 16. Dezember 1983 beschlossenen Revision von Artikel 28 des Zivilgesetzbuches und 49 des Obligationenrechts diskutiert, in der Folge aber zugunsten einer eingehenderen Bearbeitung im Rahmen der Datenschutzgesetzgebung zurückgestellt worden. In seinem privatrechtlichen Teil soll das Datenschutzrecht eine Ergänzung und Konkretisierung des Persönlichkeitsrechtes des Zivilgesetzbuches sein. Im Entwurf sind Terminologie und Systematik deshalb aus dem Zivilgesetzbuch übernommen worden. Das neue Gesetz soll Datenbearbeitern und Richtern Anhaltspunkte geben, in welchen Fällen durch Datenbearbeitung die Persönlichkeit einer Person widerrechtlich verletzt sein kann. Bestimmte Informationstätigkeiten, vor allem solche, die gegen die allgemeinen Bearbeitungsgrundsätze des Gesetzes verstossen, werden demnach im Entwurf als widerrechtliche Persönlichkeitsverletzungen qualifiziert. Der Entwurf gibt aber auf der andern Seite auch an, unter welchen Voraussetzungen ein Interesse an der Informationstätigkeit bestehen kann, das selbst eine Persönlichkeitsverletzung zu rechtfertigen vermag. Dabei wird insbesondere berücksichtigt, dass die Informationsbeschaffung und -bearbeitung im wirtschaftlichen Wettbewerb von zentraler Bedeutung ist. Unter gewissen Voraussetzungen kann das Interesse an Informationen über die Konkurrenz oder an Daten im Zusammenhang mit Vertragsverhandlungen oder Kreditüberprüfungen derart gewichtig sein, dass die betroffene Person eine Beeinträchtigung ihrer Persönlichkeitsrechte in Kauf nehmen muss. Die vielfach kritisierten komplizierten Fiktionen, Vermutungen und Gegenvermutungen des Vernehmlassungsentwurfs wurden fallengelassen zugunsten eines flexibleren Systems, das es erlaubt, den Eigenheiten des Einzelfalls Rechnung zu tragen. Für den Rechtsschutz verweist der Entwurf im wesentlichen auf die in den Artikeln 28–28f des Zivilgesetzbuches vorgesehenen Rechtsbehelfe.

213.3 Datenschutz im öffentlich-rechtlichen Bereich

Der Entwurf regelt im öffentlich-rechtlichen Abschnitt die Datenbearbeitung in der gesamten Bundesverwaltung sowie bei Personen und Organisationen, die mit öffentlichen Aufgaben des Bundes betraut sind. Er geht davon aus, dass die Verwaltung beim Bearbeiten von Personendaten grundsätzlich – wenn auch mit ganz unterschiedlicher Intensität – die Grundrechte der betroffenen Personen beeinträchtigen kann. Deshalb soll das künftige Datenschutzrecht sicherstellen, dass auch bei der Datenbearbeitung das Gesetzmässigkeits- und Verhältnismässigkeitsprinzip beachtet werden. Organe des Bundes dürfen demgemäss Personendaten nur bearbeiten, wenn dafür eine Rechtsgrundlage besteht. Für die Bearbeitung besonders schützenswerter Daten und für die Erstellung von Persönlichkeitsprofilen werden zudem qualifizierte Anforderungen an die Rechtsgrundlage gestellt beziehungsweise eine Bewilligung des Bundesrates oder die Einwilligung der betroffenen Personen verlangt. Des weitern werden den Bun-

desorganen *Handlungsanweisungen* für bestimmte Bearbeitungsformen gegeben, namentlich für das Beschaffen, die Bekanntgabe, das Anonymisieren und Vernichten der Daten. Für Datenbearbeitungen im Bereich der Statistik, Forschung und Planung sind Erleichterungen vorgesehen, sofern in diesen Fällen der Bearbeitungszweck nicht personenbezogen ist. Schliesslich wird der Bundesrat ermächtigt, im Bereich des Staatsschutzes und der militärischen Sicherheit von den Grundsätzen dieses Gesetzes abweichende Bearbeitungsregeln zu erlassen. Der Entwurf enthält zudem verfahrensrechtliche Bestimmungen, die zum Teil der Klärung des geltenden Rechts dienen, zum Teil aber auch Neuerungen enthalten, so etwa die Möglichkeit, einen Bestreitungsvermerk bei den Daten anzubringen, wenn deren Richtigkeit vom Betroffenen in Abrede gestellt wird.

213.4 Organisations- und Strafbestimmungen

Für die Einhaltung des Gesetzes sollen nach dem Entwurf ein Datenschutzbeauftragter und eine Datenschutzkommission besorgt sein.

Der *Datenschutzbeauftragte* amtet vorab als Vermittlungsperson zwischen Datenbearbeitern und betroffenen Personen. Er kann bei heiklen Datenbearbeitungen Abklärungen vornehmen. Dabei sind seine Kontrollbefugnisse im öffentlich-rechtlichen Bereich umfassend. Im privaten Bereich hingegen soll in erster Linie die betroffene Person ihre datenschutzrechtlichen Ansprüche vor dem Zivilrichter geltend machen; der Datenschutzbeauftragte darf sich hier nur einschalten, wenn durch bestimmte Bearbeitungsmethoden oder -systeme für eine Vielzahl von Personen eine erhebliche Gefahr einer Persönlichkeitsverletzung besteht. Stellt er Missstände fest, so kann er die betroffenen Organe und Privaten rechtlich nicht verpflichten, diese zu beheben, sondern er darf nur Empfehlungen abgeben. Werden diese nicht beachtet, kann er die Angelegenheit aber der Eidgenössischen Datenschutzkommission zum Entscheid unterbreiten.

Die *Eidgenössische Datenschutzkommission* soll im öffentlich-rechtlichen Bereich einen umfassenden Rechtsschutz gewährleisten; auf privatrechtlichem Gebiet kann aber auch die Kommission nur bei solchen Datenbearbeitungen eingreifen, die eine erhebliche Gefahr für eine Vielzahl von Personen darstellen. Sie entscheidet erstinstanzlich über Empfehlungen des Datenschutzbeauftragten und behandelt Beschwerden gegen Verfügungen von Organen des Bundes in Datenschutzfragen und Rekurse gegen letztinstanzliche kantonale Entscheide, die sich auf öffentlich-rechtliche Datenschutzvorschriften des Bundes stützen. Die Entscheidungen der Datenschutzkommission können ans Bundesgericht weitergezogen werden.

Das Schutzdispositiv des Gesetzes wird weiter durch *Strafbestimmungen* verstärkt. Unter Strafe gestellt werden das unbefugte Beschaffen von Personendaten sowie die Bekanntgabe von geheimen Personendaten, von denen jemand bei der Ausübung seines Berufs Kenntnis erhalten hat. Ebenfalls strafbar macht sich der Private, der als Inhaber einer Datensammlung seine Auskunftspflicht gegenüber der betroffenen Person verletzt, eine registrierpflichtige Sammlung nicht meldet oder bei Abklärungen des Datenschutzbeauftragten seine Mitwirkungspflichten nicht erfüllt.

213.5 Grenzüberschreitender Datenschutz

Im Gegensatz zum Informationsverkehr zwischen Bundesverwaltung und Kantonen soll der Datenaustausch von der Schweiz ins Ausland speziell geregelt werden. Die überragende Bedeutung der grenzüberschreitenden Datenflüsse muss auch im Datenschutzrecht ihren Niederschlag finden. Bereitet es schon im Landesrecht Mühe, den Schutzbedürfnissen der betroffenen Personen zu entsprechen, so werden die Schwierigkeiten bei Datenbearbeitungen über die Landesgrenzen hinweg fast unüberwindlich, wenn der Gesetzgeber nicht besondere Vorkehren trifft. Die Schutzmassnahmen müssen ihrerseits aber so ausgestaltet werden, dass internationale Informationsflüsse grundsätzlich unbehindert bleiben.

Der Entwurf sieht für den Datenverkehr mit dem Ausland dreierlei vor: Zum einen statuiert er den für private Bearbeiter wie öffentliche Organe geltenden Grundsatz, dass Personendaten nicht ins Ausland bekanntgegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet wird. Eine solche Gefährdung kann bei heiklen Daten namentlich bestehen, wenn der ausländische Staat keinen dem schweizerischen Recht vergleichbaren gesetzlichen Datenschutz kennt. Für Organe des Bundes gelten sodann bei Datentransfers ins Ausland die allgemeinen Bekanntgaberegeln. Das bedeutet zur Hauptsache, dass Daten nur ins Ausland weitergegeben werden dürfen, wenn eine Rechtsgrundlage besteht oder der Empfänger im Ausland die Daten zur Erfüllung seiner gesetzlichen Aufgaben benötigt. Schliesslich müssen private und öffentliche Bearbeiter, die ohne Wissen der Betroffenen Personendaten regelmässig oder in grosser Zahl ins Ausland liefern, den Datenschutzbeauftragten darüber informieren, damit dieser nötigenfalls auf besondere Gefährdungen hinweisen kann.

214 Datenschutz in der medizinischen Forschung

Eine Offenbarung des Berufsgeheimnisses zu Zwecken der medizinischen Forschung soll nicht nur mit der Einwilligung des Betroffenen, sondern auch mit Bewilligung einer vom Bundesrat eingesetzten Sachverständigenkommission erfolgen können. Die Kommission darf eine Bewilligung aber nur erteilen, wenn die Forschung nicht mit anonymisierten Daten durchgeführt werden kann und es für den Forscher unverhältnismässig schwierig wäre, den Entscheid der Betroffenen einzuholen. Voraussetzung für eine Bewilligung der Kommission ist zudem, dass die Forschungsinteressen gegenüber den Geheimhaltungsinteressen der betroffenen Personen, namentlich der Patienten, überwiegen. Damit werden hohe qualitative Anforderungen an das Forschungsprojekt gestellt, zu dessen Gunsten ein Berufsgeheimnis aufgehoben werden soll. In bestimmten Fällen soll allerdings das Bewilligungsverfahren vereinfacht werden können. So soll die Sachverständigenkommission einer Klinik oder einem Institut für die interne Forschung, für medizinische Dissertationen, medizinische Register usw. eine generelle Bewilligung erteilen können. Solche Vereinfachungen sind aber nur möglich, wenn keine schutzwürdigen Interessen der Betroffenen gefährdet sind und die Personendaten zu Beginn der Forschung anonymisiert werden.

Unabhängig von einer Kommissionsbewilligung hat zudem jeder Betroffene die Möglichkeit, die Weitergabe seiner Daten zu untersagen.

Bei der Kommission handelt es sich um eine eidgenössische Behörde, die weisungsunabhängig ist. Sie wird vom Datenschutzbeauftragten beraten. Dieser wacht auch über die Einhaltung der Bewilligungen. Er kann die Entscheide der Sachverständigenkommission an die allgemeine Datenschutzkommission weiterziehen.

Die nun vorgesehene Offenbarung des Berufsgeheimnisses für die medizinische Forschung bedingt vor allem eine Revision des Strafgesetzbuches (Art. 321 StGB). Der Datenschutz in der medizinischen Forschung soll deshalb direkt im Strafgesetzbuch und im Datenschutzgesetz geregelt werden. Auf die Schaffung eines besonderen Gesetzes wurde mit Rücksicht auf die Vernehmlassungsergebnisse verzichtet.

215 Revision des Bundesstrafprozesses und des Rechtshilfegesetzes

Der Bundesstrafprozess untersteht dem Datenschutzgesetz nicht. Damit würden aber auch für das gerichtspolizeiliche Ermittlungsverfahren Datenbearbeitungsgrundsätze weitgehend fehlen. Diese Lücke soll mit der Revision des Bundesgesetzes über die Bundesstrafrechtspflege geschlossen werden. Dabei geht es darum, bei der Beschaffung von Informationen durch die gerichtliche Polizei und für die Aufbewahrung von Polizeidaten einen Ausgleich zwischen dem Anspruch der Betroffenen auf Wahrung ihrer Privatsphäre und den Interessen der Strafverfolgung zu finden. Eine besondere Regelung ist für *Bildaufzeichnungen* der gerichtlichen Polizei bei *öffentlichen Kundgebungen* vorgesehen. Weil Teilnehmer an solchen Manifestationen sich grundsätzlich auf die Meinungsäusserungsfreiheit berufen können, darf die Polizei von ihnen nur Aufnahmen machen, wenn Hinweise bestehen, dass im Zusammenhang mit der Kundgebung Verbrechen oder Vergehen geplant sind, deren Schwere und Eigenart diese Massnahmen rechtfertigen. Des weitem wird das *Auskunfts- und Berichtigungsrecht* der betroffenen Personen bezüglich Polizeiakten sowie die Bekanntgabe von Daten aus den Ermittlungsverfahren an andere Behörden geregelt. Verweigern die gerichtspolizeilichen Organe eine Auskunft, so kann der Betroffene den Datenschutzbeauftragten einschalten, welcher gegenüber dem Bundesanwalt als dem Leiter der gerichtlichen Polizei eine Empfehlung abgibt. Einigen sich Bundesanwalt und Datenschutzbeauftragter nicht, so können sie die Angelegenheit der Anklagekammer des Bundesgerichts zum Entscheid vorlegen. Diese Lösung wurde gewählt, weil die Anklagekammer bereits heute bei der Telefonüberwachung eine vergleichbare Aufgabe erfüllt.

Des weitem werden gesetzliche Grundlagen für die Durchsuchung, Untersuchung und erkennungsdienstliche Behandlungen von Personen geschaffen. Bei diesen Bestimmungen handelt es sich zwar nicht um eigentliche Datenschutzbestimmungen, doch kann die Persönlichkeit der Betroffenen durch solche Amtshandlungen der gerichtspolizeilichen Organe ebenso stark wie durch Informationsbearbeitungen beeinträchtigt werden, weshalb sich eine Regelung auch dieser Fragen aufdrängt.

Im Bundesgesetz über internationale Rechtshilfe in Strafsachen wird die Rechtsgrundlage für den Informationsaustausch zwischen der Bundesanwaltschaft und der Internationalen Kriminalpolizeilichen Organisation INTERPOL geschaffen. Der Datenschutz richtet sich auf diesem Gebiet grundsätzlich nach den Statuten und Reglementen von INTERPOL, soweit diese vom Bundesrat als anwendbar erklärt werden. Der Datenschutzbeauftragte kann die zuständigen Verwaltungsstellen in Datenschutzfragen beraten. Er kann aber eine Angelegenheit nicht an die Datenschutzkommission weiterziehen. Hingegen ist er befugt, dort, wo über INTERPOL Informationen nicht kriminalpolizeilicher Natur vermittelt werden – etwa bei der Suche nach Vermissten oder der Identifizierung von Unbekannten –, alle ihm aufgrund des allgemeinen Datenschutzgesetzes zustehenden Rechte ausüben.

22 Erläuterungen zu den einzelnen Artikeln

22.1 Allgemeines Datenschutzgesetz

22.1.1 Erster Abschnitt: Zweck, Geltungsbereich und Begriffe

Artikel 1 Zweck

Der erste Artikel des Entwurfs verweist auf die Bezugspunkte und Quellen allen Datenschutzrechts. Es sind dies beim Informationsaustausch zwischen Privaten der Persönlichkeitsschutz, bei der Datenbearbeitung durch staatliche Behörden die Grundrechte, vor allem das ungeschriebene Verfassungsrecht der persönlichen Freiheit. Zweck des Datenschutzes ist es, die Bedeutung dieser Rechtsgüter im Zusammenhang mit der Informationsbearbeitung genauer zu umschreiben und sie gegen Verletzungen durch bestimmte Arten der Datenbearbeitung zu schützen. Der Zweckartikel soll als Leitlinie für die Auslegung der einzelnen Datenschutzbestimmungen den Bezug zum Persönlichkeitsschutz und zu den Grundrechten hervorheben.

Einen Anspruch auf Datenschutz im Sinne dieses Gesetzes haben sowohl *natürliche* wie *juristische* Personen. Zu den juristischen Personen gehören nach den Regeln des Persönlichkeitsrechts des Zivilgesetzbuches nicht nur die juristischen Personen des Privatrechts und jene des öffentlichen Rechtes des Bundes und der Kantone, sondern auch ausländische juristische Personen des öffentlichen Rechtes, wenn ihnen Zivilrechtsfähigkeit zuerkannt wird. Nicht geschützt sind jedoch, ebenfalls in Analogie zum Persönlichkeitsrecht des Privatrechts, Personenverbindungen, die nach schweizerischem Zivilrecht keine Rechtspersönlichkeit haben. Personengesellschaften allerdings, die, ohne dass es sich bei ihnen um juristische Personen handelt, bereits aufgrund des geltenden Rechts gegen aussen rechtsfähig sind, so etwa Kollektiv- und Kommanditgesellschaften, können den Schutz des Gesetzes beanspruchen. Hingegen gilt dies nicht für Personenverbindungen, die nach schweizerischem Recht keinerlei Elemente einer Rechtspersönlichkeit aufweisen, etwa ethnische Gruppen oder einfache Gesellschaften, über die Daten bearbeitet werden. Zwar ist durchaus vorstellbar, dass auch solche Personengruppen ein Bedürfnis nach Datenschutz haben, und ihre Unterstellung unter das Gesetz liesse sich aus diesem Grund sachlich rechtfertigen. Gegen eine solche Lösung spricht aber letztlich, dass mit dem Daten-

schutzgesetz, das in seinem privatrechtlichen Teil als Ergänzung zum Zivilgesetzbuch konzipiert ist, nicht für bestimmte Einzelfälle neue Formen von juristischen Personen geschaffen werden sollen. Deshalb müssen in diesen Fällen Abwehransprüche von einzelnen Gruppenangehörigen in ihrem eigenen Namen geltend gemacht werden.

Bei der Vorbereitung des Entwurfes und namentlich im Vernehmlassungsverfahren war einlässlich darüber diskutiert worden, ob juristische Personen im Bereich des Privatrechts in gleichem Mass geschützt werden sollten wie natürliche Personen; es stellte sich auch die Frage, wie weit sie auf dem Gebiet des öffentlichen Rechts, wo Datenschutz eine Konkretisierung der Grundrechte darstellt, überhaupt fähig seien, einen entsprechenden Schutz in Anspruch zu nehmen. Verschiedentlich war verlangt worden, dass juristische Personen vom Schutz des Gesetzes ausgenommen werden sollten (wie etwa in der Bundesrepublik Deutschland und in Frankreich) oder wenigstens der Schutz für sie vermindert würde. Begründet wurde dies namentlich damit, dass bei juristischen Personen mit wirtschaftlicher Tätigkeit eine grössere Transparenz wünschenswert sei, vor allem wenn es darum gehe, die Interessen der Gläubiger zu wahren. In der Tat sehen sich Personen und Unternehmen, die am wirtschaftlichen Wettbewerb teilnehmen, einem stärkeren Publikumsinteresse ausgesetzt; sie müssen sich auch eine genauere Beobachtung durch weitere Wettbewerbsteilnehmer gefallen lassen als andere Privatpersonen. Auch bei öffentlich-rechtlichen Körperschaften oder Anstalten kann einem allfälligen Geheimhaltungsinteresse ein öffentliches Interesse an der Offenlegung ihrer Tätigkeit gegenüberstehen. Mit Blick auf solche Fälle liesse es sich allenfalls rechtfertigen, den juristischen Personen nicht alle Rechtsbehelfe des Datenschutzes zur Verfügung zu stellen. Eine (teilweise) Ausklammerung der juristischen Personen aus dem Schutzbereich des Datenschutzgesetzes bedeutete aber einen Bruch mit der schweizerischen Rechtstradition. Bereits aufgrund von Artikel 53 des Zivilgesetzbuches sind nämlich juristische Personen vor widerrechtlichen Informationstätigkeiten geschützt, namentlich wenn dabei ihre Ehre oder ihre (gerade im Wettbewerb wichtige) Geheimsphäre betroffen ist²⁵⁾. Aber auch in der Sache selbst würde eine Nichtunterstellung juristischer Personen zu unbefriedigenden Ergebnissen führen. Stossend wäre dies vor allem bei kleinen Unternehmen, bei denen Angaben über die juristische Person vielfach auch einen Bezug zu natürlichen Personen aufweisen. Auch könnten nichtwirtschaftlich tätige juristische Personen, wie Parteien, karitative Organisationen oder Kirchen keinen Datenschutz beanspruchen. Wollte man aber nur die juristischen Personen, die wirtschaftlich tätig sind, vom Gesetz freistellen, so hätte dies eine *Privilegierung der natürlichen Personen*, die in wirtschaftlichem Wettbewerb stehen, zur Folge. Aus diesen Gründen soll das Datenschutzgesetz im privaten Bereich natürlichen und juristischen Personen *den gleichen Schutz* gewähren. Auch gegenüber behördlicher Datenbearbeitung soll den juristischen Personen der Datenschutz in vollem Umfang zugute kommen, wiewohl juristische Personen sich nach vorherrschender Lehre nicht auf alle für den Datenschutz im öffentlichen Bereich massgeblichen Grundrechte berufen können, namentlich nicht auf die persönliche Freiheit²⁶⁾. Weil aber im Bereich des Datenschutzes natürliche und juristische Personen sehr ähnliche Schutzbedürfnisse haben, muss sich eine juristische

Person im Zusammenhang mit der Datenbearbeitung auch auf die persönliche Freiheit berufen können. Da zudem andere für den Datenschutz massgebliche verfassungsrechtliche Maximen wie das Gesetzmässigkeits- und das Verhältnismässigkeitsprinzip unbestrittenermassen auch juristische Personen schützen, drängt sich insgesamt eine differenzierte Regelung für natürliche und juristische Personen auch im öffentlichen Bereich nicht auf.

Keine Anwendung findet das Gesetz hingegen auf internationale Organisationen. Diese können als Subjekte des Völkerrechts nicht ohne weiteres dem innerstaatlichen Recht unterstellt werden. Datenschutzrechtliche Regelungen für diese Organisationen müssen in den betreffenden Sitzabkommen vorgesehen werden. Das gleiche gilt auch für das Internationale Komitee des Roten Kreuzes (IKRK). Zwar handelt es sich beim IKRK um einen Verein im Sinne des Zivilgesetzbuches. Dennoch wird das IKRK in der Praxis zunehmend als Subjekt des Völkerrechts anerkannt und den internationalen Organisationen gleichgestellt²⁷⁾. Diese Praxis erscheint auch mit Blick auf die Datenschutzgesetzgebung sinnvoll. Das IKRK kann seine Aufgabe nur erfüllen, wenn es bei seiner Tätigkeit durch keine staatliche Behörde, auch nicht durch einen Datenschutzbeauftragten im Sinne dieses Gesetzes, kontrolliert wird. Das IKRK hat aber selber seinen Zentralen Suchdienst strengen datenschutzrechtlichen Regeln unterstellt.

Artikel 2 Geltungsbereich

Nach Absatz 1 nimmt das Gesetz zwei Kategorien von Datenbearbeitern in die Pflicht, nämlich die sogenannten privaten Personen und die Bundesorgane. *Private Personen* (Bst. a) sind solche, die Daten im Rahmen eines Sachverhaltes bearbeiten, der seinerseits durch das Privatrecht geregelt wird. Zu den *Bundesorganen* (Bst. b) gehören vorab jene Verwaltungseinheiten des Bundes, die einen bestimmten Aufgabenbereich selbständig bearbeiten, aber auch Personen, die mit öffentlichen Aufgaben betraut sind (vgl. Art. 3 Bst. c und d und die entsprechenden Erläuterungen).

Die Frage, ob ein Datenbearbeiter als private Person oder öffentliches Organ behandelt werden muss, wird im konkreten Fall nicht immer leicht zu beantworten sein. Ausschlaggebend wird sein, ob die der Datenbearbeitung zugrunde liegende Tätigkeit vorwiegend durch das öffentliche oder das Privatrecht geprägt ist. So sind z. B. selbständige Anstalten wie die SUVA, aber auch die privaten Verbandsausgleichskassen, die Aufgaben in der Alters- und Hinterlassenenversicherung und der Arbeitslosenversicherung wahrnehmen, öffentliche Organe, da ihre Tätigkeit weitestgehend durch das Bundesverwaltungsrecht geregelt ist. Schwieriger zu beurteilen ist die Zuordnung der Krankenkassen. Soweit sie dem Krankenversicherungsgesetz unterstellt sind, vom Bund anerkannt werden und hoheitlich verfügen können, sind auch sie mit der Erfüllung einer öffentlichen Aufgabe des Bundes betraut und unterstehen den Vorschriften für Bundesorgane. Die Unterscheidung ist darum wichtig, weil für öffentliche Organe strengere und detailliertere Datenschutzregelungen gelten als für private Personen.

Absatz 2 sieht verschiedene Einschränkungen des Geltungsbereichs vor:

Buchstabe a Bearbeitung zu ausschliesslich persönlichem Gebrauch

Die gesetzlichen Pflichten, die beim Umgang mit Personendaten zu beachten sind, wie auch die Rechte der betroffenen Personen müssen eine Grenze im engsten Persönlichkeitsbereich der datenbearbeitenden Person selbst finden. Dort, wo eine *natürliche Person* Daten zu ihrem *ausschliesslich persönlichen Gebrauch* bearbeitet, kann das Datenschutzgesetz ohnehin kaum mehr Geltung beanspruchen. Der Gedanke, dass der private persönliche Gebrauch eines Datums zu respektieren sei, findet sich übrigens auch im Urheberrecht²⁸⁾. Mit dem ausschliesslich persönlichen Gebrauch ist vor allem eine Verwendung der Informationen im engeren Privat- und Familienleben gemeint. Niemand soll beispielsweise verpflichtet werden, Einsicht in sein privates Notizbuch zu gewähren. Ebenso müssen Privatgespräche im Familien- und Freundeskreis, private Briefsammlungen und ähnliches dem Datenschutzgesetz entzogen bleiben. Auch Notizen, die jemand zwar bei der Ausübung seines Berufs, aber nur als Arbeitshilfe zum persönlichen Gebrauch macht, etwa zur Gedächtnisstütze, fallen nicht unter das Gesetz. Kommt es im Rahmen der Datenbearbeitung zum persönlichen Gebrauch doch zu Persönlichkeitsverletzungen – etwa wenn ein persönlicher Brief liegen geblieben und Dritten zur Kenntnis gelangt ist –, so kann der Verletzte immer noch die ihm aufgrund des allgemeinen Persönlichkeitssschutzes von Artikel 28 des Zivilgesetzbuches zustehenden Rechtsansprüche geltend machen. Im übrigen wird es Sache der Gerichtspraxis sein, dafür zu sorgen, dass sich Datenbearbeiter nicht missbräuchlich auf die vorliegende Bestimmung berufen, etwa um ihrer Auskunftspflicht zu entgehen.

Buchstabe b Ausnahme für die Medien

Mit der Revision von Artikel 28 des Zivilgesetzbuches vom 16. Dezember 1983 ist der Persönlichkeitsschutz gegenüber den Medien ganz wesentlich verbessert worden. Soweit Informationen in periodisch erscheinenden Medien, namentlich Presse, Radio und Fernsehen, veröffentlicht werden, kann ein Betroffener aufgrund von Artikel 28g ff. des Zivilgesetzbuches eine Gegendarstellung verlangen. Dieses auf die Besonderheiten einer durch die Medien zugefügten Persönlichkeitsverletzung ausgerichtete Schutzinstrument muss nicht noch mit allgemeinen Datenschutzvorschriften ergänzt werden; das Gesetz soll deshalb in diesem Bereich keine Anwendung finden. Hingegen gelten seine Bestimmungen auch für periodisch erscheinende Medien so lange, *als noch keine Veröffentlichung der Daten stattfindet*. Für Datenbearbeitungen in diesem *Vorfeld der Publikation* sind nach dem Entwurf jedoch gewisse Erleichterungen möglich (vgl. dazu Art. 10 Abs. 2 Bst. d).

Buchstabe c Bundesversammlung

Ausgenommen vom Geltungsbereich des Datenschutzgesetzes sind auch die *Geschäfte der Bundesversammlung*. Das Parlament könnte seine verfassungsrechtlich vorgesehene Oberaufsicht über Verwaltung und Rechtspflege (Art. 85 Ziff. 11 BV) nicht richtig wahrnehmen, wenn es in jedem Fall die Datenschutzgrundsätze, insbesondere die Bestimmung über die Weitergabe von Personendaten, beachten müsste. Dazu kommt, dass für die Beratungen der eidgenössi-

schen Räte von Verfassungen wegen das Öffentlichkeitsprinzip gilt (Art. 94 BV). Des weitem enthalten das Geschäftsverkehrsgesetz und die Reglemente der beiden Räte sowie die Kommissionsreglemente zum Teil recht detaillierte Bestimmungen über die Informationsbearbeitung des Parlaments im Vorverfahren der Gesetzgebung²⁹⁾. So können zum Beispiel die Geschäftsprüfungskommissionen der eidgenössischen Räte gestützt auf Artikel 47^{quater} des Geschäftsverkehrsgesetzes (SR 171.11) von allen Behörden und Amtsstellen ohne Rücksicht auf das Amtsgeheimnis zweckdienliche Auskünfte verlangen, wobei der Bundesrat, unter anderem zur Wahrung schutzwürdiger persönlicher Interessen, anstelle der Herausgabe der Akten einen besonderen Bericht erstatten kann. Auch in diesem Bereich könnte es mithin – würde das Datenschutzgesetz für anwendbar erklärt – zu unübersichtlichen Zuständen kommen, weil nicht immer klar wäre, welcher Erlass nun anzuwenden wäre. Die Ausnahmeklausel bezieht sich auf die gesamte parlamentarische Tätigkeit und erstreckt sich auch auf die parlamentarischen Dienste, soweit diese unmittelbar für die Bundesversammlung tätig sind. Datenbearbeitungen, die in keinem direkten Zusammenhang mit dem Parlament stehen, etwa die Führung der Personalakten der Mitarbeiter dieser Dienste, sollen jedoch dem Gesetz unterstehen.

Im Gegensatz zum Entwurf von 1983 bleiben die *Regierungsobliegenheiten des Bundesrates* dem Gesetz unterstellt. Auch der Bundesrat hält sich bei seiner Tätigkeit an die Grundsätze des vorliegenden Gesetzes. Die Beratungen im Bundesrat sollen jedoch nach wie vor geheim bleiben, damit der Bundesrat seine Regierungsgeschäfte mit der nötigen Unbefangenheit wahrnehmen kann. Zu diesem Zweck allein ist es jedoch nicht erforderlich, den Bundesrat vom Anwendungsbereich des Datenschutzgesetzes auszunehmen, denn Artikel 13 des Verwaltungsorganisationsgesetzes sieht bereits vor, dass die Verhandlungen des Bundesrates nicht öffentlich sind. Diese Bestimmung ist in dem Sinn zu interpretieren, dass auch ein Betroffener, ähnlich wie bei den Beratungen vieler Gerichte, keinen Anspruch hat, Einblick in die Beratungen des Bundesrates zu nehmen. Sie geht als Spezialnorm dem Datenschutzgesetz vor. Es handelt sich bei ihr um eine gesetzlich vorgesehene Einschränkung des Auskunftsrechts im Sinne von Artikel 6 dieses Entwurfes. Dass der Bundesrat nicht der Aufsicht des Datenschutzbeauftragten unterstellt ist, wird in Artikel 24 Absatz 1 klargestellt.

Buchstabe d Rechtsprechungsverfahren

Rechtsprechungsverfahren folgen genauen Regeln, die in den Prozessgesetzen festgehalten sind. Zweck verschiedener Prozessbestimmungen ist es dabei, die Persönlichkeit der in ein Verfahren Einbezogenen zu schützen. Dies gilt namentlich für die Bestimmungen über die Anhörungs-, Akteneinsichts- und Mitwirkungsrechte der Betroffenen. Prozessgesetze enthalten aber auch eigentliche Bestimmungen über die Informationsbearbeitung, indem sie etwa festlegen, wie der Prozessstoff gesammelt und gewürdigt wird. Im Prozessrecht werden auch die Interessen des Richters und der Parteien an einer Information gegenüber dem Geheimhaltungsinteresse derjenigen Person, welche die Angaben machen könnte, abgewogen, so bei der Regelung des Zeugnisverweigerungsrechts. Prozessrecht ist deshalb in einem gewissen Sinne immer auch Datenschutzrecht.

Fände nun das Datenschutzgesetz auch auf Rechtsprechungsverfahren Anwendung, so würden sich zwei Gesetze mit zum Teil gleicher Zielrichtung überlagern. Das aber würde zu Rechtsunsicherheiten, zu Koordinationsproblemen und schliesslich zu Verzögerungen führen. Die Ausnahmeklausel des vorliegenden Absatzes soll dies verhindern.

Ausgenommen vom Gesetz sind auch Verfahren vor dem Bundesgericht und den eidgenössischen Rekurs- oder Schiedskommissionen. Dabei kommt es nicht darauf an, ob es sich um ein erstinstanzliches oder ein Beschwerdeverfahren handelt. Die Ausnahmeklausel gilt allerdings nur während der Zeit, in der ein Verfahren *hängig* ist. Auf die Weiterverwendung der Daten oder die Weitergabe an Dritte nach Abschluss des Verfahrens ist das Gesetz wieder anwendbar, ebenso auf die Aufbewahrung und Vernichtung der Verfahrensakten. Auch die Datenbearbeitungen der *administrativen Dienste* der Gerichtsinstanzen (z. B. der Kanzleien) fallen unter das Gesetz.

Buchstabe e Strafverfahren

Aus den gleichen Gründen wie bei den Rechtsprechungsverfahren vor richterlichen Behörden (Bst. d) soll das Datenschutzgesetz auch in Strafverfahren, das heisst in Verfahren nach dem Bundesstrafprozess, dem Verwaltungsstrafrecht und dem Militärstrafprozess keine Anwendung finden. Diese Verfahren werden lediglich darum nicht im gleichen Zug mit dem Rechtsprechungsverfahren von Buchstabe d erwähnt, weil darin auch Bestimmungen über das Ermittlungsverfahren enthalten sind. Zwar ist der Bundesanwalt, welcher die Ermittlungen der gerichtlichen Polizei leitet, Organ der Rechtspflege; ihrer staatsrechtlichen Stellung nach ist die Bundesanwaltschaft jedoch eine administrative Behörde. Unter die Ausnahmeklausel fällt auch die Ermächtigung des EJPD zur Strafverfolgung von Beamten im Sinne von Artikel 15 des Verantwortlichkeitsgesetzes (SR 170.32).

Buchstabe f Internationale Rechtshilfeverfahren in Zivil- und Strafsachen

Das Datenschutzgesetz soll des weitem auch auf internationale Rechtshilfeverfahren in Zivil- und Strafsachen keine Anwendung finden. Der Grund liegt darin, dass der Ausgangspunkt für ein Rechtshilfegesuch immer ein Rechtsprechungs- oder Strafverfahren ist und dass das Rechtshilfegesetz in Strafsachen seinerseits gewisse Bestimmungen zum Schutze der Persönlichkeit enthält (vgl. dazu ausführlicher Ziff. 224). Die Rechtshilfe in Zivilsachen ist zudem weitgehend Angelegenheit der kantonalen Gerichte; dem Bund (Bundesamt für Polizeiwesen) kommt hier nur eine Übermittlungsfunktion zu.

Buchstabe g Beschwerdeverfahren im Staats- und Verwaltungsrecht

Verwaltungsbeschwerdeverfahren sind Rechtsprechungsverfahren der *Bundesverwaltung und des Bundesrates*. Sie sind im Verwaltungsverfahrensgesetz (SR 172.021) einlässlich geregelt, weshalb das Datenschutzgesetz auch hier keine Anwendung finden soll. Die Ausnahmeklausel gilt aber nur für *zweitinstanzliche Verwaltungsverfahren*. Würde auch die erstinstanzliche Verwaltungstätigkeit im Sinne des Verwaltungsverfahrensgesetzes dem Datenschutzgesetz nicht unterstellt, so bestünde die Gefahr, dass es in weiten Bereichen des Verwaltungshandelns für die Betroffenen keine Datenschutzgarantien gäbe. Das Verwal-

tungsverfahrensgesetz findet nämlich grundsätzlich Anwendung in allen Verwaltungssachen, die durch Verfügungen erledigt werden. Da die meisten Verwaltungstätigkeiten in eine Verfügung münden können, vermöchten sich die Organe des Bundes unter Umständen zu leicht ihren Datenschutzpflichten zu entziehen. – Aus analogen Gründen werden auch die seltenen Fälle einer staatsrechtlichen Beschwerde an den Bundesrat (Art. 73 des Verwaltungsverfahrensgesetzes) vom Datenschutzgesetz ausgenommen.

Buchstabe h Öffentliche Register

Ähnliche Überlegungen wie bei den Gesetzesvorschriften über die hängigen Rechtsprechungsverfahren haben auch zu einer Ausnahmeklausel für die öffentlichen Register des privatrechtlichen Rechtsverkehrs geführt. Zu diesen Registern gehören das Grundbuch, die Zivilstandsregister, das Güterrechtsregister, das Handelsregister, das Schiffsregister, das Luftfahrzeugbuch, die Register für Schuldbetreibung und Konkurs, das Register der Eigentumsvorbehalte sowie die Register über die Erfindungspatente, den Sortenschutz, die gewerblichen Muster und Modelle und die Fabrik- und Handelsmarken. Diese Register stellen im Grunde genommen staatlich getragene und gesicherte «Informationssysteme» dar, die bestimmte Angaben über die Begründung, den Bestand, die Änderung oder die Ausübung von privaten Rechten enthalten. Die Datenbearbeitung im Rahmen dieser Register läuft meist nach sehr detaillierten und formellen Vorschriften ab. Diese sollen, wiederum aus Gründen der Rechtssicherheit, nicht durch das Datenschutzgesetz modifiziert werden.

Neben den in den Buchstaben c–h erwähnten Fällen gibt es in vielen andern Erlassen ebenfalls spezifische Informationsbearbeitungs- und Datenschutzregelungen. Stehen diese im Widerspruch zum allgemeinen Datenschutzgesetz, muss der Rechtsanwender entscheiden, wie die betreffende Normenkonkurrenz aufzulösen ist. Dabei hat er nach den allgemeinen Auslegungsregeln vorzugehen. Im allgemeinen wird dies bedeuten, dass das Datenschutzgesetz Vorrang vor andern Datenbearbeitungsvorschriften hat, weil es als «Querschnittsgesetz» grundsätzlich für alle privaten und öffentlichen Informationstätigkeiten gilt. Wenn aber das Spezialrecht strengere Datenschutznormen oder eine in sich geschlossene Datenschutzkonzeption enthält, gehen diese Bestimmungen ausnahmsweise jenen des allgemeinen Datenschutzgesetzes vor.

Artikel 3 Begriffe

Buchstabe a Personendaten

Personendaten (Daten) sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. Personendaten gibt es in der Form des Wortes, Bildes oder Zeichens. Eine Person ist *bestimmt*, wenn sich aus den Angaben ergibt, dass sie sich auf diese Person und nur auf diese beziehen (z. B. bei einem Personalausweis). *Bestimmbar* ist die Person, wenn sie zwar allein durch die Daten nicht eindeutig identifiziert wird, aus den Umständen, das heisst dem Kontext einer Information aber auf sie geschlossen werden kann (z. B. wenn aus Angaben über Liegenschaften der Eigentümer ausfindig gemacht werden kann). Für die Bestimmbarkeit genügt allerdings nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand für die Bestim-

mung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird (etwa durch eine komplizierte Analyse einer Statistik), liegt keine Bestimmbarkeit vor³⁰⁾.

Buchstabe b Betroffene Personen

Als betroffene Person wird jemand bezeichnet, über den Daten bearbeitet werden. Die betroffenen Personen sind diejenigen, zu deren Schutz das Gesetz geschaffen werden soll. Betroffene Person kann jede natürliche und jede juristische Person des Privatrechts und des öffentlichen Rechts sein (vgl. dazu die Ausführungen zu Art. 1).

Buchstabe c Private Personen

Private Personen im Sinne dieses Gesetzes sind in erster Linie die Daten bearbeitenden natürlichen und juristischen Personen des Privatrechts. Als private Personen gelten aber auch Personen des öffentlichen Rechts, soweit sie sich im Rahmen des Privatrechts bewegen.

Bei *Organen*, die im Privatrecht verankert sind, kommt es darauf an, ob ihre Rechtstellung in materieller Hinsicht als eine privatrechtliche oder öffentlich-rechtliche angesehen werden muss. Ist das betreffende Amt im wesentlichen als öffentlich-rechtliches ausgestaltet, so untersteht der Amtsträger nicht dem privatrechtlichen Teil des Datenschutzgesetzes, sondern allenfalls vorhandenem kantonalem Datenschutzrecht. Dies trifft insbesondere für den Vormund zu. Seine Aufgaben sind zwar im Zivilgesetzbuch geregelt, so dass er in Anlehnung an die bundesgerichtliche Praxis³¹⁾ auch als Privatperson betrachtet werden könnte. Da aber sein Verhältnis zum Mündel im wesentlichen ein hoheitliches ist, er einer staatlichen Aufsicht untersteht und seine Anordnungen mit Beschwerde angefochten werden können, muss er unter dem Gesichtspunkt des Datenschutzgesetzes als öffentliches Organ betrachtet werden³²⁾. Er soll deshalb dem Datenschutzrecht jenes Kantons unterstehen, der auch sonst seine Rechtstellung festlegt. Der Bund könnte zwar gestützt auf seine Privatrechtskompetenz den Datenschutz im Vormundenschaftswesen einheitlich regeln. Wie weit dies opportun ist, soll jedoch im Rahmen der Revision des Vormundschaftsrechts geprüft werden.

Buchstabe d Bundesorgane

Zu den Bundesorganen zählen vorab die Departemente und Bundesämter sowie deren Abteilungen und Sektionen. Des weitern fallen die eidgenössischen Anstalten und Betriebe (namentlich SBB und PTT) sowie die militärischen Kommandos darunter. Bundesorgane sind aber auch alle natürlichen und juristischen Personen, vor allem wirtschaftliche Organisationen und öffentlich-rechtliche Körperschaften, die bei der Erfüllung öffentlich-rechtlicher Aufgaben für den Bund Daten bearbeiten. Organe der Kantone und Gemeinden sind nach schweizerischem Staatsrecht hingegen keine Organe des Bundes, auch wenn sie Bundesaufgaben wahrnehmen.

Buchstabe e Besonders schützenswerte Personendaten

Ob eine Bearbeitung von Daten die Persönlichkeit und die Grundrechte einer Person beeinträchtigt, hängt nicht nur von Zweck, Umfang und Art der Bearbeitung ab, sondern auch von der Qualität der bearbeiteten Informationen. Es gibt gewisse Daten, die als solche die Persönlichkeit der betroffenen Personen besonders stark berühren, vor allem wenn sie aus dem Geheimbereich oder dem Privatleben stammen oder wenn sie Ansehen und soziale Geltung einer Person wesentlich beeinflussen können. Der Gesetzesentwurf sieht für diese Arten der Daten deshalb zum Teil besondere Vorschriften vor (vgl. Art. 7 Abs. 2, 9 Abs. 2, 14 Abs. 2, 16 Abs. 1, 29).

Ziffer 1 umfasst nicht nur die religiösen, weltanschaulichen, politischen oder gesellschaftlichen Ansichten und Tätigkeiten als solche, sondern bezieht sich auch auf die Mitgliedschaft in entsprechenden Vereinigungen. In *Ziffer 2* werden Angaben über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit als besonders schützenswert erklärt. Mit der Verwendung des Begriffs «*Gesundheit*» wird der Kreis der besonders schützenswerten Daten etwas enger gezogen als im Vernehmlassungsentwurf von 1983, gemäss welchem jede Angabe über den *körperlichen Zustand* besonders schützenswert gewesen wäre. Der «*körperliche Zustand*» hätte aber beispielsweise auch Körpergrösse, Haar- und Augenfarbe umfasst, während mit dem etwas engeren Begriff der «*Gesundheit*» im vorliegenden Entwurf medizinische Befunde gemeint sind, welche sich für die Betroffenen negativ auswirken können. Die *Intimsphäre* ist im Sinn der französischen «*sphère intime*» oder der italienischen «*sfera intima*» zu verstehen; sie umfasst Daten, die eine Person nur wenigen Auserwählten mitteilt und die für sie von grosser emotionaler Bedeutung sind. Die Intimsphäre beinhaltet mehr als das Sexualleben, erstreckt sich aber beispielsweise nicht auf die finanziellen Verhältnisse. Die Aufnahme der *Rassenzugehörigkeit* in den Kreis besonders schützenswerter Daten geschah hauptsächlich mit Rücksicht auf die Konvention des Europarates bzw. im Hinblick auf den internationalen Datenaustausch. Mit den in *Ziffer 3* erwähnten *Massnahmen der sozialen Hilfe* sind Sozialversicherungsleistungen im Zusammenhang mit Krankheit und Unfall sowie Vormundschafts- und Fürsorgemassnahmen gemeint. Zu den *administrativen und strafrechtlichen Verfolgungen und Sanktionen* von *Ziffer 4* gehören neben den Verfolgungen und Verurteilungen nach gemeinem Strafrecht auch etwa Disziplinarverfahren, Führerausweisentzüge und Strafvollzugsmassnahmen.

In aller Regel betreffen die Angaben nach den Ziffern 1–3 nur natürliche Personen. Eine Ausnahme stellt aber beispielsweise die Angabe über ein weltanschaulich ausgerichtetes Unternehmen oder über die Bestrafung einer juristischen Person dar³³⁾.

Die Aufzählung der besonders schützenswerten Daten ist abschliessend.

Buchstabe f Persönlichkeitsprofil

Ein besonderer Schutz muss auch gewährt werden, wenn Persönlichkeitsprofile erstellt, ausgewertet oder an Dritte bekanntgegeben werden. Ein Persönlichkeitsprofil ist eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch die ausserberuflichen Beziehungen und Tätigkeiten, die ein *Gesamtbild* oder ein

wesentliches Teilbild der betreffenden Person ergibt. Persönlichkeitsprofile können zum Beispiel bei Sicherheitsüberprüfungen oder im Rahmen eines Anstellungsverhältnisses entstehen. Aber auch Datensammlungen über das Konsumverhalten oder über schulische und berufliche Qualifikationen sind geeignet, mindestens ein Teilbild der betroffenen Personen zu ergeben. Entscheidend ist, dass auch durch die systematische Zusammenstellung von an sich nicht besonders schützenswerten Daten (z. B. über Lesegewohnheiten, Reise- und Freizeitaktivitäten) sensitive Bereiche einer Person, z. B. ihre Weltanschauung, erschlossen werden können. Durch die Auswertungsmöglichkeiten der automatischen Datenverarbeitung und durch die Verknüpfung automatisierter Datenbestände ist die Erstellung von Persönlichkeitsprofilen leichter und häufiger geworden. Die Betroffenen haben oft keine Kenntnis vom Bestehen eines Profils und können so dessen Richtigkeit und Verwendung nicht kontrollieren. Einmal erstellt, können aber Persönlichkeitsprofile den Betroffenen der Freiheit berauben, sich so darzustellen, wie er will. Sie vermögen mithin die Entfaltung der Persönlichkeit ganz wesentlich zu beeinträchtigen. Deshalb sollen sie, gleich wie besonders schützenswerte Daten, nur unter bestimmten Voraussetzungen erstellt und bearbeitet werden dürfen.

Buchstaben g und h Bearbeiten und Bekanntgeben

Der Begriff des Bearbeitens ist umfassend: *Jeder Umgang mit Daten und alle Phasen der Bearbeitung fallen darunter.* Der Begriff umfasst selbst das bloße Aufbewahren oder Archivieren der Daten, weil auch in diesem Bearbeitungsstadium, etwa durch Mängel bei der Datensicherung, noch Persönlichkeitsverletzungen möglich sind. Soweit die Akten allerdings im Bundesarchiv archiviert sind, können für sie besondere Regelungen vorgesehen werden (vgl. Art. 30 Abs. 2). In Buchstabe h wird das *Bekanntgeben* der Daten als Unterbegriff des Bearbeitens besonders definiert, weil es sich dabei um die wohl heikelste Bearbeitungsphase handelt und sich das Bekanntgeben in sehr unterschiedlichen Formen vollziehen kann. Daten gibt bekannt, wer Einsicht in die Akten gibt, z. B. den Online-Zugriff auf eine Datensammlung gestattet, wer Magnetbänder überspielen lässt oder einfach Angaben aus einer Datensammlung macht. Der Entwurf sieht für die Bekanntgabe zusätzliche Vorschriften vor (vgl. Art. 7 Abs. 2 Bst. b, 8 und 16). Wo er nur von Bearbeiten spricht, ist die Bekanntgabe immer auch miteingeschlossen. Der Begriff des Bearbeitens wird im übrigen nicht nur für die automatische, sondern auch für die manuelle Datenverarbeitung verwendet sowie für alle Zwischenformen.

Buchstabe i Datensammlung

In Datensammlungen konzentrieren sich in der Regel die bearbeiteten Personendaten, und in Datensammlungen werden sie meistens längerfristig aufbewahrt. Aus diesen Gründen knüpfen spezifische Schutzbestimmungen des Datenschutzes, das Auskunftsrecht und die Registrierpflicht (Art. 5 und 7), an der Existenz einer Datensammlung an.

Eine Datensammlung im Sinne des Gesetzes ist ein Bestand von Daten, der auf mehr als eine Person Bezug nimmt. Sie kann ganz unterschiedlich organisiert und aufgebaut sein. Datenschutzrechtlich entscheidend ist, dass die zu einer be-

stimmten Person gehörenden Daten auffindbar sind. Bei den automatisch geführten Datensammlungen mit ihren vielfältigen Abfragemöglichkeiten trifft dies fast unbeschränkt zu, unabhängig davon, ob Personennamen als eigentliche Suchbegriffe vorgesehen sind oder nicht. Bei den manuell geführten Beständen von Personendaten fallen nicht nur jene Karteien oder Sammlungen unter den Begriff der Datensammlung, die nach den betroffenen Personen gegliedert sind, sondern auch solche, bei denen nur mittelbar, über eine Hilfsdatensammlung (z. B. ein Suchregister), ein personenbezogener Zugriff möglich ist. Keine Datensammlung stellen aber Datenbestände dar, wenn darin zwar noch Personendaten gefunden werden können, der damit verbundene Aufwand aber übermässig gross wäre. Dies ist etwa der Fall bei den Millionen von Zolldeklarationen, die bei sämtlichen Zollämtern der Schweiz zwar eine gewisse Zeit aufbewahrt, aber nicht nach Namen abgelegt sind.

Buchstabe k Inhaber der Datensammlung

Der Begriff bezeichnet eine natürliche oder juristische Person oder ein Bundesorgan, die aus datenschutzrechtlicher Sicht für die Bearbeitung der Personendaten aus einer Datensammlung verantwortlich sind und insbesondere der Auskunfts- und Registrierpflicht unterstehen. Inhaber der Datensammlung ist, wer, ohne dass er notwendigerweise über die einzelnen Daten selbst verfügt, den Zweck der Sammlung festlegt und die Bearbeitungsmittel und -methoden (z. B. Hard- und Software) bestimmt.

Das Gesetz bezeichnet im *privatrechtlichen Bereich* neben den natürlichen Personen auch die juristischen Personen als Inhaber der Datensammlung. Darunter fallen auch grosse, stark gegliederte Unternehmen. Bei diesen dürfte es nicht immer leicht sein, den *faktischen* Inhaber der Datensammlung zu bestimmen. Grosse Unternehmen müssen deshalb sicherstellen, dass ein Betroffener gleichwohl Auskunft über alle über ihn gespeicherten Daten erhalten kann. Aus Praktikabilitätsgründen werden sie aber zum Teil zurückfragen müssen, ob der Gestuchsteller sich auf eine bestimmte Filiale oder einen bestimmten Unternehmensbereich beschränken wolle. Bei den Organen des Bundes stellt sich das Problem nicht auf diese Weise, weil sie verpflichtet sind, alle Datensammlungen registrieren zu lassen. Bei der Anmeldung zur Registrierung können sie auch bekanntgeben, an wen sich ein Betroffener mit seinem Auskunftsbegehren richten muss. Gleiches gilt auch bei den registrierpflichtigen privatrechtlichen Datensammlungen.

Wenn jemand Daten durch Dritte bearbeiten lässt, kommt sowohl er selber wie der Dritte als Inhaber der Datensammlung in Frage. Ausschlaggebend ist, wer von beiden letztlich die Verantwortung für die Datenbearbeitung übernehmen kann. Dies ist in der Regel derjenige, der das Datenmaterial bereitstellt. Beschränkt sich etwa die Aufgabe eines Rechenzentrums darauf, für eine genau umschriebene Datenbearbeitung an einem vorgegebenen Bestand von Daten die technische Infrastruktur zur Verfügung zu stellen, so bleibt der Auftraggeber Inhaber der Datensammlung. Ebenso dürfte es sich verhalten, wenn ein Arzt seine Rechnungen durch eine Inkassostelle ausfertigen lässt. Wenn aber ein Institut für den Hersteller eines Produktes Marktforschung betreibt, wird es für die Daten verantwortlich sein. Gleiches gilt für den Privatdetektiv, der den Auftrag

hat, Informationen über eine bestimmte Person zu sammeln, denn sein Auftraggeber verfügt nicht selber über die Daten.

Buchstabe l Beteiligte an der Datensammlung

Beteiligte an der Datensammlung sind jene Personen und Organe des Bundes, die zwar nicht über Bestand und Zweck einer Datensammlung insgesamt entscheiden können, die aber das Recht haben, einzelne Daten aus der Sammlung selbständig zu bearbeiten. Als Beispiel sei etwa das Zentrale Ausländerregister erwähnt, für welches das Bundesamt für Ausländerfragen die Verantwortung trägt, bei welchem aber Einwohner- und Fremdenpolizeibehörden im Online-Betrieb selbständig Daten verändern können. Von der Kategorie der Beteiligten ist jene der *Empfänger der Daten* zu unterscheiden, welche lediglich Daten zur Kenntnis nehmen, diese aber weder verändern noch löschen können.

221.2 Zweiter Abschnitt: Allgemeine Datenschutzbestimmungen

Artikel 4 Grundsätze

Artikel 4 fasst in knapper Form die wichtigsten materiellen Grundsätze des Datenschutzes zusammen; es handelt sich hier um die *eigentlichen* Leitideen des Gesetzes. Der Artikel gilt sowohl für die privaten Datenbearbeiter wie auch die öffentlichen Organe. Verletzt der *private Datenbearbeiter* die Grundsätze und kann er hiefür nicht einen Rechtfertigungsgrund geltend machen, so begeht er eine Persönlichkeitsverletzung (vgl. Art. 9 Abs. 2 Bst. a). Die Grundsätze besagen mithin, unter welchen Voraussetzungen eine Datenbearbeitung privater Personen zur Persönlichkeitsverletzung wird. Für die *öffentlichen Organe* wirken die Grundsätze noch direkter; sie stellen unmittelbar anwendbares Verhaltensrecht dar, dessen Verletzung der Betroffene auf dem Beschwerdeweg rügen kann.

Absatz 1 Art des Beschaffens

Private Datenbearbeiter oder Organe des Bundes dürfen Daten erheben, wenn und soweit dies in einem völkerrechtlichen Vertrag, einem Gesetz, einem allgemein verbindlichen Bundesbeschluss oder allenfalls einer Verordnung vorgesehen ist. Im privatrechtlichen Bereich ist das Beschaffen der Personendaten im allgemeinen nicht weiter umschrieben. Hier ist deshalb neben den allgemeinen Verbotsnormen, die zur Anwendung gelangen können, der Grundsatz, dass Personendaten nicht wider Treu und Glauben behandelt werden dürfen, von besonderer Bedeutung. Daten sollen nicht in einer Art erhoben werden, mit der die betroffene Person nicht rechnen musste und sie nicht einverstanden gewesen wäre. Wider Treu und Glauben handelt namentlich, wer Daten durch absichtliche Täuschung beschafft (vgl. dazu Art. 28 OR), weil er beispielsweise die betroffene Person über seine Identität oder den Zweck seiner Bearbeitung falsch informiert. Gegen den Grundsatz von Treu und Glauben verstösst, sofern sie nicht schon einen Straftatbestand erfüllt, auch die *geheime* Datenbeschaffung, z. B. durch Abhören von Gesprächen oder Beobachten des Betroffenen³⁴⁾, oder die versteckte Erhebung durch Programmanipulationen bei interaktiven Kommunikationssystemen (Videotex). Klar rechtswidrig, weil gegen Normen

des Strafgesetzbuches verstossend, ist das Beschaffen von Daten sodann, wenn es mit Gewalt, Arglist oder Drohung gegenüber der betroffenen Person geschieht.

Für die *Organe des Bundes* wird im vierten Abschnitt des Gesetzes zusätzlich noch festgehalten, dass die Datenerhebung für den Betroffenen grundsätzlich erkennbar sein muss (Art. 15).

Absatz 2 Richtigkeit der Daten

Wenn unrichtige Daten bearbeitet werden, so kann dies zu erheblichen Beeinträchtigungen der betroffenen Personen führen. Dabei können an sich geringfügige Fehler bereits bedeutsame Auswirkungen haben. Wenn beispielsweise jemand von einem Inkassobüro zu Unrecht bedrängt wird, weil an der gleichen Strasse eine Person mit demselben Namen wohnt, die Inkassostelle aber die falsche Hausnummer notiert hat, wird er dies als äusserst unangenehm empfinden. Richtigkeit im Sinne dieses Gesetzes bedeutet allerdings nicht nur, dass Daten keine Falschaussagen enthalten dürfen, sondern auch, dass sie, soweit in einem bestimmten Sachzusammenhang erforderlich, nachgeführt und vollständig sein müssen. Dass beispielsweise ein Personalchef, der aufgrund eines veralteten Arztzeugnisses einen Arbeitnehmer versetzt oder entlässt, dessen Persönlichkeit beeinträchtigen kann, liegt auf der Hand. Eine Kreditüberprüfung führt zu falschen Schlüssen, wenn daraus zwar hervorgeht, dass jemandem in einem Scheidungsurteil Unterhaltszahlungen auferlegt worden sind, jedoch der Hinweis fehlt, dass die Unterstützungspflicht des Betreffenden infolge Wiederverheiratung seines früheren Ehegatten entfallen sei. Die Beispiele zeigen, dass die Frage, ob ein Datum richtig sei, nicht abstrakt, sondern jeweils nur im konkreten Anwendungsfall beantwortet werden kann.

Absatz 3 Verhältnismässigkeit der Datenbearbeitung

Mit dem in diesem Absatz statuierten Verhältnismässigkeitsgebot wird das im öffentlich-rechtlichen Bereich ohnehin geltende Verhältnismässigkeitsprinzip auch für den privaten Bereich als anwendbar erklärt. Der Datenbearbeiter ist demnach gehalten, nur diejenigen Daten zu erheben und weiter zu bearbeiten, die für einen bestimmten Zweck geeignet sind und die er tatsächlich benötigt. Wer z. B. Autos vermietet, darf zwar die Personalien des Mieters erheben; übermässig wäre es aber, wenn der Mieter zusätzlich Auskünfte über seine Familienverhältnisse oder seine Beziehungen zu weiteren Drittpersonen geben müsste. Bei Kreditauskünften können neben Angaben über Vermögensverhältnisse und Zahlungsmoral auch die Familienverhältnisse wesentlich sein; übermässig wären aber Auskünfte über die Religionszugehörigkeit oder politische Auffassungen der überprüften Person.

Des weitem muss aber auch zwischen dem Bearbeitungszweck und der mit Blick darauf nötigen Persönlichkeitsbeeinträchtigung ein vernünftiges Verhältnis bestehen. So ist es etwa unzulässig, im Hinblick auf einen Wahlkampf das Privatleben eines politischen Gegners umfassend und systematisch auszuforschen.

Absatz 4 Zweckänderung

Die Gefahr, dass Daten zu andern als den ursprünglich vorgesehenen Zwecken verwendet werden, ist angesichts der multifunktionalen Nutzungs- und Mitteilungsmöglichkeiten moderner Informationssysteme stark gestiegen. Der Grundsatz von Treu und Glauben im Rechtsverkehr verlangt nun aber, dass die von der Informationsbearbeitung betroffenen Personen wissen, wozu ihre Daten bearbeitet werden. Sie haben ihre Angaben in vielen Fällen nicht voraussetzungslos, sondern mit Blick auf einen bestimmten Bearbeitungszweck und möglicherweise nur für diesen geliefert. Deshalb sollen die Daten grundsätzlich nur zu dem Zweck verwendet werden, der bei der Beschaffung angegeben wird oder aus den Umständen ersichtlich ist. Das bedeutet, dass beispielsweise Adressen, die im Zusammenhang mit einer Initiative gesammelt wurden, von den Initianten nachher nicht zu kommerziellen Zwecken, etwa für einen Werbeversand verwendet werden dürfen. Ebenso wäre es nicht zulässig, dass Personaldienste der Bundesverwaltung Adressen von Bundesbeamten mit einem bestimmten Einkommen an Verkaufsorganisationen vermitteln. Unrechtmässig wäre es auch, wenn aufgrund von Videotextdaten Konsumgewohnheiten oder sonstige Interessen von Personen systematisch erforscht würden.

Eine Zweckänderung ist immerhin dann erlaubt, wenn sie in einem *Rechtssatz vorgesehen* ist. So kann etwa eine Behörde durch Rechtssatz ermächtigt werden, auf den Datenbestand einer andern Behörde Zugriff zu nehmen. Diese Ausnahme erscheint gerechtfertigt, weil ihr erstens ein Entscheid eines demokratisch legitimierten Gesetzgebers zugrunde liegt und zweitens die betroffene Person wegen der Öffentlichkeit der Gesetzestexte von einer solchen Zweckänderung grundsätzlich Kenntnis hat.

Absatz 5 Datenbekanntgabe ins Ausland

Daten, deren Bearbeitung im Inland problemlos ist, können für die betroffenen Personen gefährlich werden, wenn sie ins Ausland bekanntgegeben werden. Zu denken ist etwa an Informationen an ausländische Staaten über Ausländer in der Schweiz, wenn die Regierung im Heimatstaat des betreffenden Ausländers die Menschenrechte nicht respektiert. Aber auch Personalinformationen von schweizerischen Unternehmen an ausländische Filialen können dem Betroffenen zum Nachteil gereichen, etwa wenn bekannt wird, dass er einer im Ausland nicht genehmen Religionsgemeinschaft angehört³⁵⁾. Wer Daten ins Ausland transferiert, soll sich dieser Gefahren bewusst sein und sich entsprechend verhalten. Ähnliche Vorsicht kann unter Umständen auch bei Mitteilungen an *internationale Organisationen* angebracht sein. Allerdings dürfte eine Einschätzung der Gefahrenlage für den Datenbearbeiter in vielen Fällen recht schwierig sein. Deshalb sind nur solche Datenbekanntgaben unzulässig, die eine *schwerwiegende* Persönlichkeitsverletzung zur Folge haben können. Mit dieser Umschreibung wird sichergestellt, dass der Datenaustausch über die Landesgrenzen hinweg einerseits nicht über Gebühr beeinträchtigt wird und andererseits vor allem keine solche Mitteilungen umfasst, die einen vorwiegend persönlichen oder familiären Charakter haben.

Eine schwerwiegende Persönlichkeitsverletzung ist vor allem vorstellbar bei Datentransfers in Länder, die keinen dem schweizerischen Recht vergleichbaren

Schutz gewährleisten. Ein vergleichbarer Schutz besteht namentlich dann, wenn im betreffenden Staat die materiellen Grundsätze im Sinne von Artikel 4 dieses Gesetzes beachtet werden und der Betroffene Auskunft über seine Daten verlangen und diese allenfalls berichtigen oder löschen lassen kann. Dies dürfte bei Staaten mit Datenschutzgesetzen und solchen, welche die Konvention Nr. 108 des Europarates ratifiziert haben, praktisch immer zutreffen. Doch kann, da die überwiegende Mehrzahl aller Staaten keine Datenschutzgesetzgebung hat, nicht allein auf dieses Kriterium abgestellt werden. In vielen Fällen werden die Rechtsordnung und -praxis sowie die Verwaltungsorganisation des betreffenden Staates insgesamt gewürdigt werden müssen. In Fällen, in denen die ausländische staatliche Ordnung keine genügenden Datenschutzgarantien bietet, bleibt den Datenbearbeitern die Möglichkeit, auf vertraglichem Wege die nötigen Schutzvorkehrungen zu treffen.

Absatz 6 Datensicherung

Gewisse Datenschutzprobleme können im voraus vermieden werden, wenn die Datenbearbeiter die nötigen Sicherheitsvorkehrungen treffen. Darunter fallen, namentlich bei modernen Informatiksystemen, *bauliche* Massnahmen, die sicherstellen, dass unbefugte Dritte keinen Zutritt zum Computer haben. Bei gewissen Datenbearbeitungen sind *technische* Vorkehrungen nötig, die verhindern, dass im Falle einer Panne (z. B. Betriebsunterbruch infolge Stromausfalls) die Daten unwiederbringlich verlorengehen. Ferner kann mit *organisatorischen* Massnahmen (Benutzeridentifikation, periodische Evaluation der Sicherheitsmassnahmen, Ernennung eines Datenschutzbeauftragten im Betrieb) sichergestellt werden, dass die Daten nicht beliebigen Personen zur Verfügung stehen und die Datenschutzgrundsätze beachtet werden.

Das Gesetz verzichtet darauf, die Sicherheitsmassnahmen im Detail zu regeln. Angesichts der unüberblickbaren Vielfalt von Datenbearbeitungsarten obliegt es den Bearbeitern oder ihren Berufs- und Fachverbänden, für ihren Bereich die Sicherheitsbedürfnisse zu definieren und die nötigen Sicherheitsmassnahmen anzuordnen. Sollten sich dabei Schwierigkeiten ergeben, kann der Bundesrat gestützt auf die Ausführungsgesetzgebungskompetenz (Art. 30 Abs. 1) einige Minimalanforderungen aufstellen. In der Bundesverwaltung wird er bereichsspezifisch Datensicherungsvorschriften erlassen.

Artikel 5 Auskunftsrecht

Das Auskunftsrecht ist das bedeutendste Institut des Datenschutzgesetzes. Es erlaubt es der betroffenen Person überhaupt erst, ihre datenschutzrechtlichen Ansprüche durchzusetzen. Nur wer weiss, ob und welche Daten über ihn bearbeitet werden, kann diese nötigenfalls berichtigen oder vernichten lassen oder wenigstens deren Richtigkeit bestreiten (vgl. Art. 12 und 22).

Berechtigt, ein Auskunftsbegehren zu stellen, ist nach *Absatz 1* jede Person. Beim Auskunftsrecht handelt es sich um ein subjektives, höchstpersönliches Recht. Auch eine urteilsfähige unmündige oder entmündigte Person kann deshalb das Auskunftsrecht selber, ohne Zustimmung des gesetzlichen Vertreters, ausüben (vgl. Art. 19 Abs. 2 ZGB). Aus dem Charakter des höchstpersönlichen Rechts folgt auch, dass nicht von vornherein auf das Auskunftsrecht verzichtet

werden kann (Abs. 6). *Adressat* des Auskunftsbegehrens ist nicht jeder, der Daten bearbeitet, sondern der *Inhaber einer Datensammlung*. Weil dieser seine Daten systematisch geordnet hat, sind die Möglichkeiten einer Persönlichkeitsverletzung bei ihm wesentlich grösser als bei jemandem, dessen Daten nicht nach den betroffenen Personen erschliessbar sind. Auch wäre eine generelle Auskunftspflicht über jede Datenbearbeitung, die nicht im Rahmen einer Datensammlung geschieht, nicht praktikabel, weil der Datenbearbeiter dann oft aufwendige Recherchen durchführen müsste, um die Daten überhaupt noch zu finden. Eine Person kann nur über ihre *eigenen* Daten Auskunft verlangen; könnte sie auch Daten Dritter einsehen, würde damit gerade wieder die Möglichkeit neuer Persönlichkeitsverletzungen geschaffen.

Absatz 2 bestimmt, worin die Auskunft bestehen muss. Der Inhaber der Datensammlung wird vorerst feststellen, ob sich überhaupt Daten vom Gesuchsteller in seiner Sammlung befinden. Trifft dies nicht zu, so teilt er es dem Gesuchsteller mit, und die Angelegenheit ist erledigt. Existieren Daten, so muss der Inhaber dem Gesuchsteller deren Inhalt mitteilen (Bst. a). Dabei muss er dafür besorgt sein, dass die Auskunft *vollständig* und *richtig* ist. Eine teilweise Auskunft ist nur zulässig, wenn das Gesetz eine Ausnahme bzw. eine Beschränkung der Auskunft vorsieht (vgl. Art. 6) oder wenn der Betroffene ausdrücklich nur eine Teilauskunft verlangt hat. Dem Gesuchsteller muss des weitern Aufschluss über den *Bearbeitungszweck* gegeben werden, weil er nur so allfällige Risiken, die sich aus der Datenbearbeitung ergeben können, richtig einzuschätzen vermag. Zudem soll ihm die *gesetzliche Grundlage* der Bearbeitung bekanntgegeben werden. Diese letztere Bestimmung richtet sich in erster Linie an Bundesorgane; sie kann aber auch für Private von Bedeutung sein, da auch sie zum Teil aufgrund gesetzlicher Verpflichtungen Datenbearbeitungen vornehmen (der Arbeitgeber z. B. bearbeitet Arbeitnehmerdaten für die Abrechnung mit der AHV). Des weitern sollen dem Gesuchsteller die *Kategorien der bearbeiteten Daten*, der an der *Sammlung Beteiligten* und der *Empfänger der Daten* mitgeteilt werden (Bst. b). Hingegen werden die Inhaber der Datensammlung nicht verpflichtet, die *Beteiligten und Empfänger einzeln* zu nennen. Dies würde zu einem unverhältnismässigen Aufwand führen und könnte Privatpersonen zwingen, ihr Geschäftsgeheimnis offenzulegen und ihre Geschäftspartner bekanntzugeben. Auch eine Verpflichtung des Inhabers der Datensammlung, die *Herkunft* der Daten bekanntzugeben, wurde nicht in den Entwurf aufgenommen. Die Erfahrung zeigt, dass eine Bekanntgabe der Herkunft in vielen Fällen entweder mit sehr grossem Aufwand verbunden oder aber nur wenig aussagekräftig ist. Eine solche Verpflichtung wäre aber auch für die Medien problematisch, weil auf diese Weise Journalisten bereits vor einer Veröffentlichung gezwungen werden könnten, Aufschluss über ihre Informanten zu geben. Das bedeutet allerdings nicht, dass ein Betroffener die Herkunft der Daten überhaupt nicht erfahren kann. Nach der Rechtsprechung des Bundesgerichts kann er – allerdings nur gegenüber staatlichen Organen, nicht gegenüber Privaten – gestützt auf Artikel 4 BV nicht nur in einem hängigen Verfahren, sondern grundsätzlich auch ausserhalb eines formellen Verfahrens Akteneinsicht verlangen, sofern nicht öffentliche Interessen des Staates oder berechnete Geheimhaltungsinteressen eines Dritten entgegenstehen³⁶⁾.

In *Absatz 3* geht es um den sogenannten *Aufklärungsschaden*. Den Begriff des Aufklärungsschadens kennt man vor allem in der Medizin. Ein Aufklärungsschaden liegt vor, wenn ein Patient unvorbereitet mit einem medizinischen Befund konfrontiert wird und sich in der Folge sein Gesundheitszustand deswegen verschlechtert. An sich geht der Entwurf davon aus, dass nicht der Inhaber einer Datensammlung entscheiden soll, ob eine Auskunft sich für den Betroffenen nachteilig auswirken kann oder nicht. Der Gesuchsteller soll die allfälligen Risiken einer Auskunft selber abwägen. Für Auskünfte über den Gesundheitszustand ist aber eine Ausnahme angezeigt. Der Inhaber einer Datensammlung, etwa eine Krankenversicherung, soll zwar auch in solchen Fällen nicht unter Berufung auf einen möglichen Aufklärungsschaden die Auskunft verweigern können. Er soll aber die Auskunft über einen Arzt erteilen lassen können, weil dieser aufgrund seiner Ausbildung und Erfahrung eher in der Lage ist, den Betroffenen so zu orientieren, dass dieser nicht noch zusätzlichen Schaden nimmt. Absatz 3 ist mithin eine Persönlichkeitsschutzbestimmung zugunsten der betroffenen Person. Datenschutzrechtlich gesehen handelt es sich dabei, soweit der Inhaber der Datensammlung ein Bundesorgan ist, um eine Sonderregelung im Vergleich zu den Bekanntgaberegeln von Artikel 16.

Mit *Absatz 4* soll sichergestellt werden, dass sich ein Inhaber einer Datensammlung seiner Auskunftspflichten nicht entledigen kann, indem er die Sammlung durch einen Dritten bearbeiten lässt. Es ist ihm jedoch unbenommen, die Auskunft durch den Dritten, z. B. ein Rechenzentrum, erteilen zu lassen. Der Dritte seinerseits ist zur Auskunft verpflichtet, wenn er den Inhaber der Datensammlung nicht bekanntgibt oder dieser im Ausland Wohnsitz hat. Damit wird sichergestellt, dass immer jemand über eine Datensammlung Auskunft geben muss. Der Betroffene, der Auskunft über seine Daten in einer Datensammlung haben will, soll nicht lange Recherchen über die Identität des Inhabers der Datensammlung anstellen oder im Ausland klagen müssen.

Nach *Absatz 5* ist die Auskunft schriftlich und kostenlos zu erteilen. In der Ausführungsverordnung kann der Bundesrat jedoch Ausnahmen vom Grundsatz der Schriftlichkeit und der Unentgeltlichkeit vorsehen. So ist namentlich denkbar, dass in bestimmten Fällen der Gesuchsteller direkt auf einem Bildschirm Einblick in seine Daten nehmen kann. Unter gewissen Umständen kann es auch angezeigt sein, dem Betroffenen Einsicht in ein ganzes Dossier zu gewähren. Um eine übermässige Beanspruchung der Inhaber von Datensammlungen zu verhindern, wird die Verordnung voraussichtlich vorsehen, dass derjenige, der in einem bestimmten Zeitraum, zum Beispiel in einem Jahr, mehr als eine Auskunft einholt, dafür bezahlen muss. Ein Entgelt wird der Inhaber möglicherweise auch verlangen können, wenn sein Aufwand aus anderen Gründen ein übermässiger ist, etwa weil er die Akten bereits archiviert hat.

Artikel 6 Einschränkungen des Auskunftsrechts

So wichtig und unabdingbar das Auskunftsrecht für den Persönlichkeits- und Datenschutz auch ist, so kann es doch nicht uneingeschränkt beansprucht werden. Überwiegende öffentliche Interessen sowie Schutzinteressen eines Dritten oder der datenbearbeitenden Person selbst können einer Auskunftserteilung entgegenstehen. Weil es sich beim vorliegenden Artikel aber um eine Ausnah-

meregel handelt, mit welcher das höchstpersönliche Auskunftsrecht eingeschränkt wird, ist die Aufzählung der Einschränkungsründe abschliessend. Entsprechend soll die Bestimmung auch restriktiv ausgelegt und die Auskunft nur soweit beschränkt werden, als dies wirklich unerlässlich ist. Die Art der Auskunftsbeschränkung kann im übrigen ganz unterschiedlich sein. Es ist möglich, die Auskunft ganz oder teilweise zu verweigern oder sie auf einen spätern Zeitpunkt zu verschieben. Wenn verschiedene Möglichkeiten offenstehen, ist die für den Betroffenen günstigere Lösung zu wählen. Die Bestimmung im vorliegenden Entwurf lehnt sich im übrigen zu einem wesentlichen Teil an die Regelung des Akteneinsichtsverweigerungsrechts im Verwaltungsverfahrensgesetz (Art. 27, SR 172.021) an.

Zu den einzelnen Verweigerungsgründen von *Absatz 1* ist folgendes zu bemerken:

In einem formellen Gesetz (das heisst in einem völkerrechtlichen Vertrag oder einem referendumspflichtigen Bundesbeschluss) vorgesehene *Befugnisse* des Inhabers der Datensammlung zur Auskunftsverweigerung (Bst. a) sind in erster Linie im öffentlich-rechtlichen Bereich denkbar. Zu erwähnen in diesem Zusammenhang ist insbesondere Artikel 13 des Verwaltungsorganisationsgesetzes (SR 172.010), gemäss welcher Bestimmung die Verhandlungen des Bundesrates nicht öffentlich sind. Aufgrund dieser Bestimmung hat der Bundesrat die Möglichkeit, ein Auskunftsbegehren, mit welchem Einsicht in die Verhandlungsprotokolle verlangt wird, abschlägig zu beantworten. Im privaten Bereich dürften solche Befugnisse des Inhabers der Datensammlung zur Auskunftsverweigerung, wenn überhaupt, nur ganz selten vorkommen.

Überwiegende öffentliche Interessen, die eine Auskunftseinschränkung rechtfertigen (Bst. b), sind namentlich im Bereich der inneren oder äusseren Sicherheit denkbar, wobei der Begriff der äusseren Sicherheit nebst der Beachtung der völkerrechtlichen Verpflichtungen auch die Pflege guter Beziehungen zum Ausland einschliesst. Eine Auskunftsverweigerung ist etwa möglich, wenn Personen Einblick in Datensammlungen der Bundesanwaltschaft nehmen wollen und mit der Erteilung der Auskunft Ermittlungsergebnisse und -methoden aufgedeckt würden. Sie ist auch denkbar bei Datensammlungen des Eidgenössischen Departementes für auswärtige Angelegenheiten, wenn mit der Auskunft Einblick in Verhandlungen mit andern Staaten ermöglicht würde oder Informationen über Personen preisgegeben würden, deren Schutz die Schweiz aufgrund des Völkerrechts übernommen hat.

Eine Auskunft soll auch dann verweigert werden dürfen, wenn sie dazu führen würde, dass *der Zweck einer Strafuntersuchung oder eines andern amtlichen Untersuchungsverfahrens*, z. B. eines Disziplinarverfahrens, in Frage gestellt würde (Bst. c). Die Bestimmung dürfte keine allzu grosse Bedeutung erlangen, da ja das Gesetz insgesamt keine Anwendung auf Verfahren findet, die in Prozessgesetzen geregelt sind (vgl. Art. 2). Immerhin ist vorstellbar, dass auch Auskünfte, die ausserhalb eines Untersuchungsverfahrens erteilt werden, dieses negativ beeinflussen könnten, etwa wenn ein Beschuldigter bei jener Person, die gegen ihn Strafanzeige erstattet hat, Einblick in die Datensammlung nehmen will.

Auch *überwiegende Interessen des Inhabers der Datensammlung* können eine Einschränkung der Auskunft rechtfertigen (Bst. d). Im Vordergrund stehen dabei vor allem Fälle aus dem privatrechtlichen Bereich. So darf etwa ein Warenhaus, das eine Sammlung von des Diebstahls verdächtigen Personen führt, die Auskunft verweigern. Eine Einschränkung ist auch zulässig, wenn der Inhaber der Sammlung befürchten muss, dass der Gesuchsteller Wirtschaftsspionage betreiben will.

Einschränkungen der Auskunft sind schliesslich auch zulässig, wenn befürchtet werden muss, dass der Gesuchsteller beim Einblick in seine Daten zugleich auch Informationen über Drittpersonen erhält und dadurch die *Interessen dieser Drittpersonen verletzt werden können* (Bst. e). So ist etwa denkbar, dass ein Versicherungsnehmer ein Interesse daran hat, dass ein im Versicherungsvertrag begünstigter Dritter von der Begünstigung nichts erfährt.

Jede Verweigerung, Einschränkung und jeder Aufschub einer Auskunft ist gemäss *Absatz 2* zu begründen. Die Bundesorgane müssen dies nach den Grundsätzen des Verwaltungsverfahrensrechts in Form einer anfechtbaren Verfügung tun. Für die privaten *Bearbeiter* gelten keine Formvorschriften, doch wird es von Vorteil sein, wenn sie dem Gesuchsteller die Gründe für die Einschränkung der Auskunft schriftlich mitteilen. Die Begründung soll so gehalten sein, dass der Betroffene in der Lage ist zu beurteilen, ob die Einschränkung der Auskunft zu Recht erfolgte. In bestimmten Fällen, etwa im Bereich der inneren oder äusseren Sicherheit, können jedoch an die Begründungspflicht nicht allzu hohe Anforderungen gestellt werden, weil sonst das zuständige Bundesorgan gerade das preisgeben müsste, was mit der Auskunftsverweigerung verschwiegen werden soll.

Artikel 7 Register der Datensammlungen

Das Register der Datensammlungen ist der Schlüssel für die Ausübung des Auskunftsrechts. Es wird gemäss *Absatz 1* vom Datenschutzbeauftragten geführt und kann von jedermann eingesehen werden.

Nach *Absatz 2* gibt das Register unterschiedlich Aufschluss über die Datensammlungen des öffentlich-rechtlichen und des privatrechtlichen Bereichs. Sammlungen, die von Bundesorganen geführt werden, müssen grundsätzlich alle gemeldet werden. Ausgenommen sind allenfalls Datensammlungen im Bereiche des Staatsschutzes und der militärischen Sicherheit (Art. 21). Im privaten Bereich hingegen besteht grundsätzlich keine Registrierpflicht für Datensammlungen. Eine Ausnahme gilt aber für solche Sammlungen, in welchen besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeitet werden (Bst. a) oder aus denen Daten an Dritte bekanntgegeben werden (Bst. b). Aber selbst diese – unter dem Gesichtspunkt des Persönlichkeitsschutzes heiklen – Datensammlungen unterstehen der Registrierpflicht nur, wenn der Inhaber der Sammlung nicht aufgrund eines Gesetzes dazu verpflichtet ist, sie zu führen, oder wenn die betroffenen Personen davon keine Kenntnis haben. Der Arbeitgeber etwa, der aufgrund der AHV-Gesetzgebung eine Datei über den Lohn seiner Angestellten führt und aufgrund dieser Sammlung Mitteilungen an die AHV macht, ist der Registrierpflicht nicht unterstellt. In welcher Weise die betroffenen Personen Kenntnis erhalten müssen, dass eine Datensammlung mit

sensitiven Daten über sie geführt wird oder dass Daten an Dritte bekanntgegeben werden, lässt sich nicht abschliessend umschreiben. Es wird nicht in jedem Fall erforderlich sein, dass der Inhaber einer Datensammlung alle Personen, die darin aufgeführt sind, persönlich orientiert. Wenn es sich um Datensammlungen eines Unternehmens über seine Arbeitnehmer handelt, kann ein Rundschreiben oder eine Mitteilung am Anschlagbrett genügen. Vorstellbar ist auch eine entsprechende Aufklärung der Mitarbeiter bei der Anstellung. Die Mitteilung soll aber in jedem Fall für den Betroffenen klar erkennbar sein. Meldepflichtig sind zudem nur *regelmässige* Bearbeitungen und Bekanntgaben, d. h. solche, die sich periodisch wiederholen. Aufgrund der vorgeschlagenen Regelung kann der private Inhaber einer Datensammlung frei entscheiden, ob er eine Datensammlung registrieren lassen oder ob er statt dessen lieber die Betroffenen über seine Sammlung orientieren will. Grosse Sammlungen allerdings, etwa solche von Organisationen der Direktwerbung oder von Auskunfteien, müssen in der Regel registriert werden, da eine Orientierung aller Betroffenen nicht möglich sein dürfte.

Nach *Absatz 3* müssen Datensammlungen angemeldet werden, bevor sie eröffnet werden. Dies erlaubt es dem Datenschutzbeauftragten, den Bearbeiter am Anfang der Informationstätigkeit auf allfällige Probleme aufmerksam zu machen.

Absatz 4 hält fest, dass der Bundesrat in einer Ausführungsverordnung die Einzelheiten der Registrierung regelt. Er wird insbesondere vorsehen müssen, welche Angaben für die Registrierung im einzelnen zu machen sind. Es dürfte sich dabei im wesentlichen um die gleichen handeln, die aufgrund von Artikel 5 Absatz 2 Buchstabe b bei einem Auskunftsbegehren bekanntgegeben werden müssen. Des weitern wird der Bundesrat festlegen, in welcher Weise das Register veröffentlicht wird bzw. wie Einsicht in dieses genommen werden kann. Die Verordnung wird ferner vorsehen, dass das Register periodisch bereinigt werden muss. Der Bundesrat kann sodann für Datensammlungen, bei deren Bearbeitung keine Nachteile für die betroffenen Personen zu befürchten sind, vereinfachte Meldeverfahren oder Ausnahmen von der Melde- oder der Registrierpflicht vorsehen.

Schliesslich ist darauf hinzuweisen, dass private Personen, die registrierpflichtige Datensammlungen nicht melden, sich gemäss Artikel 28 des Entwurfs strafbar machen.

Artikel 8 Bekanntgeben ins Ausland

Wie bereits weiter oben dargestellt wurde (vgl. die Erläuterungen zu Art. 4 Abs. 5), kann die Datenbekanntgabe ins Ausland mit erhöhten Risiken einer Persönlichkeitsverletzung verbunden sein. *Absatz 1* sieht deshalb vor, dass gewisse *Datentransfers* ins Ausland dem Datenschutzbeauftragten gemeldet werden müssen, damit dieser, gestützt auf Artikel 24, in heiklen Fällen allenfalls nähere Abklärungen vornehmen kann. Als Ausland im Sinne dieser Bestimmung gelten nicht nur andere Staaten, sondern auch internationale Organisationen. Massgeblich ist, ob die Daten einer ausländischen Rechtsordnung unterstellt werden. Auch ein Weitergeben von Daten innerhalb eines multinationalen Unternehmens stellt ein Bekanntgeben ins Ausland dar. Die Bekanntgabepflicht

für Datentransfers ist jedoch sehr eingeschränkt. Sie gilt nur, wenn die Bekanntgabe *regelmässig* erfolgt oder einen *bedeutenden Umfang* annimmt. Sie entfällt zudem in allen Fällen, in denen die Bekanntgabe gesetzlich vorgeschrieben ist (Bst. a) oder die betroffenen Personen Kenntnis davon haben (Bst. b). Ob die Betroffenen Kenntnis haben, beurteilt sich nach den gleichen Kriterien wie bei der Ausnahme von der Registrierpflicht (Art. 7).

Gemäss *Absatz 2* regelt der Bundesrat die Meldung im einzelnen. Er wird dabei insbesondere festlegen, wann die Bekanntgabe ins Ausland von bedeutendem Umfang ist. Dabei ist davon auszugehen, dass der Begriff «bedeutender Umfang» eine quantitative wie auch eine qualitative Komponente hat. In der Verordnung wird deshalb zwischen den besonders schützenswerten Personendaten und den übrigen Daten in der Weise unterschieden werden, dass bei der ersten Kategorie die Zahl, die eine Meldepflicht auslöst, kleiner ist als bei der zweiten. Des weitern kann der Bundesrat vereinfachte Meldungen vorsehen für Datentransfers, die, obwohl sie den Betroffenen nicht bekannt sind, deren Persönlichkeit nicht verletzen. Das kann etwa der Fall sein, wenn nicht besonders schützenswerte Personendaten zu Zwecken der nicht personenbezogenen Forschung und Statistik weitergegeben werden. Es mag dies auch zutreffen, wenn Daten innerhalb einer in verschiedenen Ländern tätigen Unternehmung, etwa einer Fluggesellschaft, bekanntgegeben werden. In solchen Fällen dürfte unter Umständen bereits eine Globalmeldung genügen.

Schliesslich ist darauf hinzuweisen, dass Private sich nach Artikel 28 strafbar machen, wenn sie die Meldepflicht vorsätzlich verletzen.

221.3 Dritter Abschnitt: Bearbeiten von Personendaten durch private Personen

Artikel 9 Persönlichkeitsverletzungen

In seinem privatrechtlichen Teil stellt das Datenschutzgesetz eine Ergänzung und Konkretisierung des Persönlichkeitsschutzes des Zivilgesetzbuches dar. Ausgangspunkt ist dabei die Bestimmung von Artikel 28 Absatz 1 des Zivilgesetzbuches, die unter anderem besagt, dass den Richter anrufen könne, wer in seiner Persönlichkeit widerrechtlich verletzt wird. Der dritte Abschnitt des Entwurfs konkretisiert nun diese Generalklausel für den Bereich der Datenbearbeitung. Artikel 9 als erste Bestimmung des Abschnittes nennt Tatbestände, d. h. Bearbeitungsarten, die als Persönlichkeitsverletzungen zu gelten haben und grundsätzlich widerrechtlich sind, wenn der Bearbeiter sich nicht auf einen Rechtfertigungsgrund berufen kann.

Absatz 1 stellt den Bezug zu Artikel 28 Absatz 1 des Zivilgesetzbuches her. Er macht auf diese Weise deutlich, dass das Datenschutzgesetz, soweit es sich auf private Datenbearbeiter bezieht, den Grundsätzen des Persönlichkeitsschutzes des Zivilgesetzbuches folgt. Beide Gesetze haben letztlich den gleichen Zweck, nämlich die Autonomie und Entscheidungsfreiheit der betroffenen Personen zu schützen.

In *Absatz 2* werden Datenbearbeitungen genannt, die zu Persönlichkeitsverletzungen führen. Eine Persönlichkeitsverletzung begeht, wer die allgemeinen *Da-*

tenschutzgrundsätze von Artikel 4 nicht beachtet (Bst. a). Die Grundsätze stellen das ethische und rechtspolitische Fundament des Datenschutzgesetzes dar, und es soll deshalb nicht ohne zwingenden Grund gegen sie verstossen werden können. Eine Persönlichkeitsverletzung liegt ferner vor, wenn sich der Bearbeiter über den *ausdrücklichen Willen der betroffenen Person hinwegsetzt* (Bst. b). Damit soll als eigentliche Neuerung im Privatrecht das Selbstbestimmungsrecht der betroffenen Person über ihre Daten garantiert und geschützt werden. Die betroffene Person kann das Bearbeiten voraussetzungslos, ohne Nachweis eines besonderen Interesses, untersagen. Sie kann aber die Datenbearbeitung nicht pauschal verbieten, sondern nur gegenüber bestimmten Bearbeitern und bezogen auf bestimmte Bearbeitungsarten. Eine Persönlichkeitsverletzung liegt zudem nur vor, wenn die betroffene Person die Datenbearbeitung *ausdrücklich* untersagt hat. Hat ein Datenbearbeiter es lediglich unterlassen abzuklären, ob eine Person mit der Bearbeitung der sie betreffenden Daten einverstanden ist, so soll dies noch nicht von Gesetzes wegen als Persönlichkeitsverletzung gelten. In diesem Zusammenhang sei erwähnt, dass bereits heute die Adresshändler mit der sogenannten «Robinson-Liste» die Möglichkeit geschaffen haben, sich durch eine ausdrückliche Willenserklärung gegen unerwünschte Datenbearbeitungen, vor allem gegen Werbesendungen, zu schützen. Im übrigen versteht sich von selbst, dass eine betroffene Person ihr Bearbeitungsverbot widerrufen kann, allenfalls auch durch eine stillschweigende Einwilligung zu einer Datenbearbeitung. Eine Persönlichkeitsverletzung liegt schliesslich vor, wenn *besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgegeben werden* (Bst. c). Diese Angaben können für den Betroffenen sehr nachteilig sein oder ihn umfassend beschreiben. Er muss deshalb von demjenigen, dem er die Daten offenbart hat oder der davon Kenntnis erlangt hat, Verschwiegenheit verlangen können. Derartige Daten sollen nicht ohne Rechtfertigungsgrund, zum Beispiel nicht ohne Einwilligung des Betroffenen, weitergegeben werden. Auch diese Bestimmung widerspiegelt, wie jene von Buchstabe b, die Leitidee des Gesetzes, dass die Betroffenen bei der Bearbeitung ihrer eigenen Daten mitbestimmen sollen.

Die Aufzählung der Persönlichkeitsverletzungen ist *nicht abschliessend*. Auch kann, sofern die entsprechenden Tatbestände erfüllt sind, eine betroffene Person zusätzlich nach anderen dem Persönlichkeitsschutz dienenden Gesetzen gegen widerrechtliche Datenbearbeitungen vorgehen, etwa nach dem Gesetz über den unlauteren Wettbewerb³⁷⁾.

Artikel 10 Rechtfertigungsgründe

Absatz 1 wiederholt der Klarheit halber den bereits in Artikel 28 Absatz 2 des Zivilgesetzbuches enthaltenen Grundsatz, dass eine Persönlichkeitsverletzung dann nicht widerrechtlich ist und keine rechtlichen Konsequenzen nach sich zieht, wenn der Verletzte dazu eingewilligt hat oder der Verletzer ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Bestimmung als Rechtfertigungsgrund geltend machen kann. Auch gegenüber Persönlichkeitsverletzungen, die durch Datenbearbeitungen begangen werden, ist mithin der Schutz nicht umfassend. Er hat namentlich dann zurückzutreten, wenn die – privaten oder öffentlichen – Interessen an der Datenbearbeitung das Informa-

tionsabwehrinteresse der betroffenen Person überwiegen. Anders als der Vorwurf verzichtet die jetzige Vorlage darauf, bereits eine Interessenabwägung in der Weise vorzunehmen, dass für bestimmte Datenbearbeitungsarten von Gesetzes wegen ein Rechtfertigungsgrund respektive die gesetzliche Vermutung eines Rechtfertigungsgrundes vorgesehen wird. Ein solches System erscheint zu starr und vermöchte dem Einzelfall zu wenig gerecht zu werden. Es ist auch im Vernehmlassungsverfahren als zu kompliziert kritisiert worden. Letztlich kann allein der Richter unter Berücksichtigung der konkreten Umstände entscheiden, ob eine Persönlichkeitsverletzung gerechtfertigt ist oder nicht.

In Absatz 2 werden dem Richter aber gewisse *Anhaltspunkte*, gleichsam *Gewichtssteine*, für die Interessenabwägung an die Hand gegeben. Der Gesetzgeber kann zwar dem Richter seine Verantwortung nicht abnehmen. Er ist jedoch in der Lage, ihm für bestimmte Bereiche, wo Datenbearbeitungs- und -schutzinteressen in einem besonderen Spannungsverhältnis stehen, Beurteilungselemente zu liefern. Die in Absatz 2 genannten Rechtfertigungsgründe können grundsätzlich bei allen in Artikel 9 vorgesehenen sowie weiteren im Entwurf nicht beschriebenen Persönlichkeitsverletzungen zur Anwendung kommen. Allerdings wird der Richter bei bestimmten Verletzungen das Bestehen eines Rechtfertigungsgrundes eher bejahen als bei andern. So ist etwa ein Beschaffen von Daten mit unrechtmässigen Mitteln nur selten und ein Beschaffen wider Treu und Glauben praktisch überhaupt nie zu rechtfertigen, während sich andererseits für eine Persönlichkeitsverletzung infolge unrichtiger Datenbearbeitung wohl eher ein Rechtfertigungsgrund finden lässt.

Der Entwurf sieht im wesentlichen drei Gruppen von Rechtfertigungsgründen vor, nämlich solche für bestimmte wirtschaftliche Tätigkeiten (Vertragsabschluss, wirtschaftlicher Wettbewerb, Kreditüberprüfung), für die Medien und für Datenbearbeitungen zu nicht personenbezogenen Zwecken:

Nach *Buchstabe a* kann eine Persönlichkeitsverletzung gerechtfertigt sein, wenn die betroffene Person *Vertragspartner* des Bearbeiters ist. Dabei kommen alle denkbaren Vertragsformen in Betracht. Die Wendung «in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages» erlaubt auch Informationstätigkeiten im Vorfeld einer Vereinbarung. So kommt zum Beispiel der Rechtfertigungsgrund in Betracht, wenn jemand im Hinblick auf Vertragsverhandlungen Referenzen über einen potentiellen Käufer oder einen möglichen Mieter einholt. Nicht mehr in unmittelbarem Zusammenhang mit dem Vertrag stehen aber Werbeaktionen, obwohl auch sie letzten Endes zu einem Vertragsabschluss führen sollen. Der Rechtfertigungsgrund gilt für jede Form des Bearbeitens, für das Beschaffen wie für das Auswerten der Daten. Auch bei Bekanntgaben an Dritte kann der Rechtfertigungsgrund angerufen werden, etwa wenn der Bearbeiter die Daten seiner Vertragspartner an eine Filiale, einen Lieferanten oder einen Spediteur weiterleitet.

Buchstabe b sieht einen Rechtfertigungsgrund im Bereich des *wirtschaftlichen Wettbewerbs* vor. Wer auf dem Markt bestehen will, muss seine Wirtschaftsdaten fortlaufend überarbeiten und sich namentlich über seine Konkurrenten informieren. Umgekehrt hat er hinzunehmen, dass seine Mitbewerber über ihn die verschiedensten Informationen einholen wollen. Für eine gewisse Publizität

im wirtschaftlichen Wettbewerb sorgt bereits das *Handelsregister*. Die im Register eingetragenen Personen tun kund, dass sie sich dem wirtschaftlichen Wettbewerb stellen; sie legen ihre Geschäftstätigkeit bis zu einem gewissen Grade offen, namentlich auch um vertrauens- und kreditwürdig zu sein. Wenn jemand über solche, in gewissem Sinn «öffentliche» Personen Daten bearbeitet, soll für allfällige Persönlichkeitsverletzungen ein Rechtfertigungsgrund in Betracht kommen. Zum Kreis dieser Personen gehören vor allem Kapitalgesellschaften und Genossenschaften sowie die eintragungspflichtigen Einzelfirmen und Personengesellschaften³⁸⁾. Nicht dazu gehören hingegen die natürlichen Personen, die in ihrer Eigenschaft als Organe juristischer Personen im Handelsregister eingetragen sind. Der Rechtfertigungsgrund von Buchstabe b fällt aber nur in Betracht, wenn die Daten ausschliesslich *intern* bearbeitet, d. h. nicht Dritten bekanntgegeben werden. Wieweit dabei der Informationsaustausch innerhalb eines Konzerns noch als interne Bearbeitung anzusehen ist, muss der Praxis überlassen werden. Ausschlaggebend wird sein, ob die in Frage stehende Bekanntgabe grundsätzlich auf eine Unternehmung als wirtschaftliche Einheit beschränkt bleibt. Der Rechtfertigungsgrund kann zudem nur angerufen werden, wenn die betreffenden Daten und die Art ihrer Bearbeitung für den wirtschaftlichen Wettbewerb relevant sind.

Aus ähnlichen Gründen wie bei den Wettbewerbsinformationstätigkeiten kommen nach *Buchstabe c* auch bei Datenbearbeitungen zur Prüfung der *Kreditwürdigkeit* eines kaufmännischen Unternehmens Rechtfertigungsgründe in Betracht. Die Wettbewerbswirtschaft ist wesentlich Kreditwirtschaft. Wer im Handelsregister eingetragen ist, muss sich auch Kreditüberprüfungen gefallen lassen und allfällige Persönlichkeitsverletzungen eher in Kauf nehmen als andere Personen. Der Rechtfertigungsgrund kann aber nur angerufen werden, wenn bei der Kreditüberprüfung nicht besonders schützenswerte Personendaten bearbeitet werden. Diese Einschränkung erscheint darum notwendig, weil anders als im Fall von Buchstabe b bei der Kreditüberprüfung die Daten in vielen Fällen Dritten bekanntgegeben werden. Dies geschieht etwa, wenn eine Kreditauskunftei die Bonität einer Unternehmung abgeklärt hat und ihrem Auftraggeber die Ergebnisse ihrer Nachforschungen bekanntgibt. Der Rechtfertigungsgrund findet des weitern nur Anwendung, wenn feststeht, dass die Kreditauskunft für den Abschluss oder die Abwicklung eines Vertrages tatsächlich benötigt wird. Ausgeschlossen werden damit pauschale, listenmässige Übermittlungen von Kreditwürdigkeitsinformationen oder Beantwortungen von allgemeinen, nicht anlassgebundenen Anfragen.

Nach *Buchstabe d* kann ein Rechtfertigungsgrund auch dann vorliegen, wenn Daten im Hinblick auf eine *Veröffentlichung in periodisch erscheinenden Medien* bearbeitet werden. Es handelt sich hier um eine Datenbearbeitung im *Vorfeld* der Publikation. Sind die Daten erst einmal veröffentlicht, so findet nach Artikel 2 Absatz 2 Buchstabe b nicht mehr das Datenschutzgesetz Anwendung, sondern gelten die Artikel 28 ff. des Zivilgesetzbuches. Mit der Regelung wird ein ausserordentlich heikles Spannungsfeld angesprochen. Die Informationstätigkeit der Medien, bei der es immer auch um personenbezogene Daten geht, kann unter Datenschutzgesichtspunkten in verschiedener Hinsicht problematisch sein. Medienschaffende und Medienunternehmen haben vielfältige Datenbe-

schaffungsmethoden. Sie wollen häufig gerade sensitive Angaben über bestimmte Personen ausfindig machen. Sie müssen oft unter Zeitdruck und gestützt auf unsichere Quellen arbeiten, weshalb sie die Datenrichtigkeit in diesem Stadium ihrer Tätigkeit bei aller journalistischen Sorgfalt nicht immer schon voll gewährleisten können. Sie sammeln Informationen häufig auf Vorrat, zum Teil in umfangreichen Datenbanken und über lange Zeit hinweg, um im geeigneten Moment das Material für die Publikation bereitzuhaben. – Andererseits ist für eine Demokratie das Funktionieren der Medien lebensnotwendig. Diese können jedoch ihre Aufgabe nur wahrnehmen, wenn sie auch bei der Bearbeitung heikler Daten eine gewisse Freiheit genießen und ihre Informationsquellen bis zu einem gewissen Grade geschützt bleiben. Deshalb kann das öffentliche Interesse an selbständigen und unabhängigen Medien in bestimmten Fällen höher sein als das Persönlichkeitsschutzinteresse eines einzelnen. Die vorliegende Bestimmung soll einen Ausgleich zwischen Persönlichkeitsschutz und Medienfreiheit schaffen. Auf den Rechtfertigungsgrund kann sich allerdings nur berufen, wer Daten für *periodisch erscheinende Medien* bearbeitet. Das Buch und der Film sind nicht geschützt. Die Beschränkung auf die periodischen Medien scheint angezeigt, weil diesen die wichtigste Rolle bei der öffentlichen Meinungsbildung zukommt. Zwar ist nicht zu verkennen, dass auch Filme und Bücher diesbezüglich wesentliche Beiträge leisten können. Der Einbezug auch dieser Medien in die vorliegende Regelung würde aber letztlich den Persönlichkeitsschutz über Gebühr beeinträchtigen, weil ein Datenbearbeiter im Falle einer Persönlichkeitsverletzung fast immer behaupten könnte, er sammle Daten und werte diese im Hinblick auf eine Publikation aus. Was alles periodisch erscheinende Medien sind, ergibt sich aus der Praxis zum zivilrechtlichen Persönlichkeitsschutz (Art. 28c Abs. 3 und 28g ZGB). Dazu zählen nicht nur die herkömmlichen Druckerzeugnisse, Radio und Fernsehen, sondern auch der Allgemeinheit zugängliche Informationsdatenbanken, wenn sie in regelmässiger Folge neue Personendaten für jedermann auf Abruf bereithalten. Der Rechtfertigungsgrund kann selbst dann zur Anwendung gelangen, wenn Daten, die im Hinblick auf eine Publikation bearbeitet werden, *Dritten bekanntgegeben* werden. Damit wird dem Umstand Rechnung getragen, dass der Journalist einem Verleger probeweise Entwürfe liefern können muss. Zudem gewährleistet diese Regelung eine Gleichstellung von Journalisten, welche für Radio und Fernsehen oder die Presse arbeiten, und solchen, die für Nachrichten- oder Bildagenturen tätig sind. Der Zweck solcher Agenturen besteht gerade darin, Informationen für Dritte, im wesentlichen für periodisch erscheinende Medien, bereitzustellen.

Buchstabe e sieht einen Rechtfertigungsgrund für Fälle vor, in denen zwar Personendaten bearbeitet werden, der Zweck des Bearbeitens aber in keinem Zusammenhang mit den betroffenen Personen steht. Der Entwurf nennt als wichtigste solcher Bearbeitungsarten, bei denen der Personenbezug fehlen kann, die *Forschung, die Planung und die Statistik*. Weitere derartige nicht personenbezogene Bearbeitungen sind denkbar, etwa wenn bei einem Test einer EDV-Anlage Personendaten verwendet werden. Der Grund für die Privilegierung liegt darin, dass Forschung, Statistik und Planung nicht nur wichtige Entscheidungsgrundlagen für die privatwirtschaftliche Tätigkeit liefern, sondern auch vielfältige so-

ziale und öffentliche Bedürfnisse erfüllen. Zudem erscheinen allfällige Persönlichkeitsverletzungen, etwa Verstösse gegen die Grundsätze von Artikel 4 des Entwurfes, im Kontext von Forschung, Planung und Statistik weniger schwerwiegend, weil diese Bearbeitungen keine direkten Konsequenzen für die betroffenen Personen haben. Das bedeutet umgekehrt jedoch, dass sich nicht auf den Rechtfertigungsgrund berufen kann, wer beispielsweise als Historiker oder Genealoge wirklich personenbezogene Forschung betreibt. Diese Forscher können allenfalls die allgemeinen Rechtfertigungsgründe von Artikel 10 Absatz 1 geltend machen. Der besondere Rechtfertigungsgrund von Buchstabe e fällt ferner nur in Betracht, wenn die Ergebnisse der Forschung so veröffentlicht werden, dass Rückschlüsse auf die betroffenen Personen praktisch nicht mehr möglich sind. Die Anrufung des Rechtfertigungsgrundes ist auch zulässig, wenn Daten zwischen Forschern oder Forschungsteams ausgetauscht werden. Damit wird dem Umstand Rechnung getragen, dass in der Forschung und teilweise auch in der Planung und Statistik eine vielfältige Zusammenarbeit, oftmals über die Landesgrenzen hinweg, besteht, die datenschutzrechtlich eine gewisse Privilegierung verdient. Schliesslich ist darauf hinzuweisen, dass allfällig bestehende Geheimhaltungsvorschriften auch im Bereich der Forschung, Statistik und Planung vollumfänglich Geltung haben; ein Forscher kann nicht gestützt auf Buchstabe e die Weitergabe geheimer Daten rechtfertigen.

Eine Persönlichkeitsverletzung kann nach *Buchstabe f* schliesslich gerechtfertigt sein, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht hat. Wer etwa Informationen über sich selbst, auch besonders schützenswerte, in einem Medium verbreitet, nimmt in Kauf, dass unbestimmt viele Personen davon Kenntnis nehmen und die entsprechenden Daten allenfalls weiterverwenden. Das gleiche gilt für Äusserungen, die jemand in der Öffentlichkeit macht, zum Beispiel in einer Gemeindeversammlung. Gäbe es für Persönlichkeitsverletzungen, die bei der Bearbeitung, insbesondere der Bekanntgabe solcher Informationen, begangen werden, keinen Rechtfertigungsgrund, würde die gesellschaftliche Kommunikation zu stark eingeschränkt.

Artikel 11 Datenbearbeitung durch Dritte

Die organisatorischen und technischen Möglichkeiten, Datenbearbeitungen an andere Personen zu übertragen, sind sehr gross. Sie entsprechen den vielfältigen Bedürfnissen nach Arbeitsteilung bei der Informationsverarbeitung und -übermittlung. In gewissen Fällen wird die Bearbeitung von Daten vollständig einem spezialisierten Dritten übertragen, etwa einem Meinungsforschungsinstitut oder einer Treuhandfirma. Diese Möglichkeiten will das Datenschutzgesetz nicht beschneiden.

Mit *Absatz 1* soll aber sichergestellt werden, dass durch die Übertragung der Datenbearbeitung an Dritte die Rechte der betroffenen Personen nicht geschmälert werden. Wer einem Dritten den Auftrag zur Datenbearbeitung gibt, muss deshalb dafür sorgen, dass dieser die datenschutzrechtlichen Schranken in gleicher Weise beachtet, wie er es selbst tun müsste (Bst. a). Dies gilt für jegliche Bearbeitungsart, von der Erhebung bis zur allfälligen Weitergabe der Daten. Bei der Übertragung der Bearbeitung an einen Dritten muss der Auftraggeber in Analogie zu Artikel 55 des Obligationenrechts alle gebotene Sorgfalt auf-

wenden, um Verstöße gegen das Datenschutzgesetz zu verhindern. Er muss den Auftragnehmer entsprechend auswählen, ihm die richtigen Instruktionen erteilen und ihn soweit als möglich auch überwachen. Die Übertragung der Datenbearbeitung an Dritte ist aber ausgeschlossen, wenn der Auftraggeber gesetzlich oder vertraglich zur Geheimhaltung der Daten verpflichtet ist (Bst. b). Das bedeutet zum Beispiel, dass ein Arzt, der seine Rechnungen durch eine fremde Inkassostelle ausfertigen lässt, aufgrund von Artikel 321 des Strafgesetzbuches dies nur mit Einwilligung des Betroffenen tun darf oder aber dafür sorgen muss, dass diese Stelle nicht Kenntnis von eigentlichen, dem Arztgeheimnis unterstellten Patientendaten erhält. Auch hier gehen die Geheimhaltungsvorschriften als die einschränkenderen Datenschutzbestimmungen dem allgemeinen Datenschutzgesetz vor.

Auf der anderen Seite kann der Dritte nach *Absatz 2* all diejenigen Rechtfertigungsgründe geltend machen, auf die sich auch der Auftraggeber berufen könnte. Diese Regelung ist darum notwendig, weil eine betroffene Person, die sich in ihren Persönlichkeitsrechten beeinträchtigt glaubt, aufgrund von Artikel 28 des Zivilgesetzbuches nicht nur gegen den Auftraggeber, sondern direkt auch gegen den Auftragnehmer klagen kann. In solchen Fällen scheint aber nach einem Teil der Lehre der beklagte Auftragnehmer nur Einreden geltend machen zu können, die in direktem Zusammenhang mit seiner eigenen Person stehen³⁹⁾. Der Entwurf will nun die Verteidigungsmittel desjenigen, der für einen andern Daten bearbeitet, ergänzen, damit bei einer allfälligen Auseinandersetzung zwischen ihm und der betroffenen Person alle datenschutzrechtlichen Fragen geklärt werden können.

Artikel 12 Klagen und Verfahren

Da das Datenschutzgesetz in seinem privatrechtlichen Teil eine Ergänzung und Konkretisierung des Zivilgesetzbuches darstellt, soll auch der Rechtsschutz der gleiche sein wie im Zivilrecht. Der Entwurf sieht allerdings einige Ergänzungen vor, die einerseits gewissen Eigenheiten der Datenbearbeitung Rechnung tragen und andererseits dazu bestimmt sind, das *Auskunftsrecht* als zentrales Institut des Datenschutzgesetzes auch prozessrechtlich zu verankern. Die Anlehnung an das Zivilgesetzbuch hat namentlich zur Folge, dass die *Klagelegitimation* zum grössten Teil die gleiche ist wie im allgemeinen Persönlichkeitsrecht. Dies gilt vollumfänglich für die *Passivlegitimation*. Die widerrechtlich verletzte Person kann ihre Schutzansprüche gegenüber jedermann geltend machen, «der an der Verletzung mitwirkt» (entsprechend Art. 28 Abs. 1 ZGB), das heisst *gegen jeden* vorgehen, von dem sie annimmt, dass mit einer Änderung von dessen Verhalten die Verletzung beseitigt oder verhindert werden kann oder gegenüber welchem sie die Unrechtmässigkeit seiner Datenbearbeitung festgestellt haben will. Dabei kommt es nicht darauf an, ob der Beklagte die Hauptverantwortung für die Persönlichkeitsverletzung trägt oder nur eine untergeordnete Rolle spielt⁴⁰⁾. Unter den Bedingungen der Informatik heisst dies, dass die verletzte Person nicht nur den Inhaber einer Datensammlung, sondern auch dessen Hilfspersonen und Beauftragte belangen kann. Sie mag beispielsweise die Betreiber eines Rechenzentrums oder eines Datenübermittlungsnetzes oder auch Personen, die Software oder Hardware für die verletzende Bearbeitung zur Verfügung gestellt

haben, ins Recht fassen, sofern deren Handeln oder Unterlassen für die Verletzung ursächlich ist. Allerdings ist derjenige, gegen den wegen Persönlichkeitsverletzung geklagt wird, nicht notwendigerweise identisch mit jenem, der Schadenersatz zu leisten hat. Schadenersatzansprüche beruhen auf besonderen Voraussetzungen; sie setzen in der Regel einen Verschuldensnachweis voraus.

Was die *aktive Klagelegitimation* angeht, so hat nicht jeder durch eine Informationstätigkeit Verletzte, sondern nur die Person, über die Daten bearbeitet werden, ein Klagerecht. Denn das Datenschutzgesetz schützt nach seinem Artikel 1 einzig diese Personen. Drittbetroffene haben nur soweit ein Klagerecht, als ihnen ein solches aufgrund des Zivilgesetzbuches zusteht⁴¹⁾.

Im Gegensatz zum Vorentwurf verzichtet die jetzige Vorlage auf eine ausdrückliche Regelung des *Klagerechts der Verbände*. Für das Verbandsklagerecht werden demnach im Bereich des Datenschutzgesetzes die gleichen Regeln gelten, wie sie vom Bundesgericht für das allgemeine Persönlichkeitsrecht entwickelt worden sind. Ein Verband wird einerseits klagen können, wenn er selber durch eine unrechtmässige Datenbearbeitung geschädigt oder gefährdet ist. Berufsverbände können zudem in eigenem Namen, aber für ihre Mitglieder klagen, wenn sie gemäss ihren Statuten entsprechende Interessen der Mitglieder wahrzunehmen haben und diese selber zur Klage berechtigt sind⁴²⁾.

Absatz 1 verweist in seinem ersten Satz lediglich auf die Rechtsbehelfe des Zivilgesetzbuches. Der betroffenen Person stehen demnach drei Klagearten zur Verfügung: mit der *Unterlassungsklage* will sie eine bevorstehende Persönlichkeitsverletzung verhindern, mit der *Beseitigungsklage* eine bereits eingetretene Beeinträchtigung rückgängig machen und mit der *Feststellungsklage* sich die Unrechtmässigkeit einer Datenbearbeitung richterlich bestätigen lassen. Sie kann im Rahmen der Unterlassungs- und Beseitigungsklage, wie im zweiten Satz präzisierend festgehalten ist, insbesondere die *Berichtigung oder Vernichtung* der Daten verlangen. Dies dürften die Hauptbegehren im Rahmen des datenschutzrechtlichen Persönlichkeitsschutzes sein. Die betroffene Person kann nach Massgabe von Artikel 28c des Zivilgesetzbuches auch *vorsorgliche Massnahmen* verlangen, für welche die rechtswidrige Persönlichkeitsverletzung bloss glaubhaft gemacht werden muss.

Ein besonderes Klagebegehren stellt die Möglichkeit des *Bestreitungsvermerks* von *Absatz 2* dar. Die Richtigkeit oder Unrichtigkeit von Tatsachenbehauptungen lässt sich, vor allem wenn diese mit Werturteilen verknüpft sind, nicht immer befriedigend beweisen. In solchen Fällen soll die betroffene Person verlangen können, dass bei den betreffenden Daten ein Bestreitungsvermerk angebracht wird. Auf diese Weise kann sie ihre eigene Beurteilung einer Information zur Geltung bringen, ohne die wesentlich einschränkendere und deshalb schwieriger durchsetzbare Berichtigung oder gar eine Vernichtung der Daten verlangen zu müssen. Die konkreten Voraussetzungen für die Gutheissung eines Begehrens um Aufnahme eines Vermerks wird die Praxis entwickeln müssen. Sie wird dabei namentlich Umfang und Inhalt des allfälligen Vermerks je nach den Umständen und nach der Zumutbarkeit für die datenbearbeitende Person festlegen. Ein Bestreitungsvermerk soll im übrigen auch im Rahmen einer vorsorglichen Massnahme im Sinne von Artikel 28c des Zivilgesetzbuches verlangt werden können.

Mit *Absatz 3* wird festgehalten, dass für Klagen zur Durchsetzung des *Auskunftsrechts* die gleiche Gerichtsstandsregelung gilt, wie sie in Artikel 28*b* des Zivilgesetzbuches für die Geltendmachung von Persönlichkeitsverletzungen im allgemeinen vorgesehen ist. Zudem wird für die Durchsetzung des Auskunftsrechts ein einfaches und rasches Verfahren vorgeschrieben. Ein solches Verfahren erscheint namentlich darum notwendig, weil der Entscheid bezüglich des Auskunftsrechts von ausschlaggebender Bedeutung für das Einreichen von Persönlichkeitsschutzklagen sein kann. Wie schon in Artikel 28*b* Absatz 1 des Zivilgesetzbuches ist auch hier eine verfahrensrechtliche Normierung durch den Bund nötig, um dem materiellen Recht zum Durchbruch zu verhelfen.

221.4 Vierter Abschnitt: Bearbeiten von Personendaten durch Bundesorgane

Artikel 13 Verantwortliches Organ

Im Bereich der öffentlichen Verwaltung bearbeiten eine Vielzahl von Behörden und Amtsstellen, aber auch private Personen oder Organisationen für verschiedenste gesetzliche Aufgaben Personendaten. *Absatz 1* sieht nun vor, dass all diese Bundesorgane im Rahmen ihrer durch Gesetz und Verordnung eingeräumten Zuständigkeiten auch die datenschutzrechtliche Verantwortung übernehmen müssen. Sie sind es, die namentlich Einblick in die Datensammlungen geben, die Weitergaberegeln beachten und Sicherheitsmassnahmen ergreifen müssen. Diese Zuordnung der Verantwortlichkeit ist notwendig, weil sinnvollerweise nicht der Bund als solcher oder der Bundesrat als oberste Vollzugsbehörde ins Recht gefasst werden kann, sondern nur jene Stelle, die auch faktisch in der Lage ist, die Datenschutzvorschriften anzuwenden. Welche Verwaltungseinheiten dies im einzelnen sind, ist nicht immer leicht auszumachen, weil die Organisationsvorschriften des Bundes im wesentlichen nur die Aufgaben der Ämter umschreiben. Je nach Sachbereich und Organisation eines Amtes müssen aber bestimmte Datenbearbeitungsarten von Verwaltungseinheiten unterer Stufe, zum Beispiel von einer Abteilung oder Sektion, verantwortet werden. Letztlich ist es Sache der Departemente und Ämter, die Verantwortlichkeiten zu regeln und diese gegen aussen bekanntzugeben. Bereits heute ist im Register der Sammlungen von Personendaten, welches vom Bundesamt für Justiz herausgegeben wird, für jede Datensammlung eine verantwortliche Stelle angegeben.

Absatz 2 räumt dem Bundesrat die Kompetenz ein, für Informationssysteme, an denen mehrere Bundesorgane oder neben Bundesorganen auch kantonale Organe und Private beteiligt sind, die Verantwortung besonders zu regeln. Diese Bestimmung ist vor allem für grosse, dezentralisierte Informationssysteme oder für sogenannte Verbundsysteme gedacht. *Dezentralisierte Systeme* zeichnen sich dadurch aus, dass die Daten nicht vom Systembetreiber selber, sondern von Aussenstellen des Systems, an der sogenannten Peripherie, erhoben werden. Dies ist beispielsweise der Fall beim Personalinformationssystem der Bundes-

verwaltung (PERIBU), das zwar vom Personalamt geführt wird, bei dem aber die Daten von den Personaldiensten der einzelnen Ämter eingegeben werden. *Verbundsysteme* kommen durch eine Verknüpfung von an sich selbständigen Rechneranlagen zustande und dürften mit der Verbreitung der Personalcomputer in naher Zukunft noch sehr stark zunehmen. Die Frage der Verantwortung stellt sich in besonderem Mass bei Systemen, die von *Bund und Kantonen gemeinsam geführt* werden. Gerade hier kann die Verantwortlichkeit zum Teil nur auf Bundesebene vernünftig geregelt werden. In materieller Hinsicht wird es vor allem darum gehen, die Ober- oder Hauptverantwortung für ein bestimmtes Informationssystem einem Organ zuzuordnen. Daneben werden auch die Zugriffsbefugnisse der einzelnen am System Beteiligten und deren Verantwortung für die Richtigkeit und die Sicherheit der Daten festgelegt werden müssen. Zudem muss bestimmt werden, wie im einzelnen den Auskunftersuchen der betroffenen Person zu entsprechen ist. Der Bundesrat kann die Regelung der Verantwortlichkeit an die Departemente delegieren für Fälle, in denen nur Verwaltungseinheiten innerhalb eines Departementes betroffen sind.

Artikel 14 Rechtsgrundlage

Absatz 1 hält fest, dass die Datenbearbeitung durch Bundesorgane wie jedes Verwaltungshandeln einer gesetzlichen Grundlage bedarf. Dies gilt für alle Formen und Phasen der Informationsbearbeitung, sofern nicht in den nachfolgenden Artikeln ausdrücklich eine Ausnahme vorgesehen ist. Bei der gesetzlichen Grundlage kann es sich um einen völkerrechtlichen Vertrag, um eine Verfassungs- oder eine Gesetzesbestimmung oder um eine gestützt darauf erlassene Verordnungsnorm handeln. Wie detailliert die gesetzliche Grundlage sein muss, ist nach allgemeinen Grundsätzen zu beurteilen. Massgeblich ist namentlich, ob und wie weit mit einer Datenbearbeitung in die Freiheitsrechte der Bürger eingegriffen wird, die Art der bearbeiteten Daten, der Kreis der betroffenen Personen, aber auch die Organisation des Informationssystems und der allfällige Einbezug kantonaler oder privater Stellen in die Bearbeitung. Grundsätzlich müssen in der Rechtsgrundlage Zweck, beteiligte Organe und Ausmass der Datenbearbeitung in den Grundzügen festgelegt sein. Angesichts der unendlichen Vielfalt von Datenbearbeitungsvorgängen in der Bundesverwaltung dürfen aber keine allzu strengen Anforderungen an die gesetzliche Grundlage gestellt werden. Vielfach muss es genügen, dass eine Informationsbearbeitung in einem einschichtigen sachlichen Zusammenhang mit der Aufgabe des betreffenden Bundesorgans steht. – Im übrigen müssen Bundesorgane, soweit nicht besondere gesetzliche Vorschriften entgegenstehen, bei der Datenbearbeitung immer auch die Grundsätze von Artikel 4 beachten.

Absatz 2 stellt qualifizierte Anforderungen an das Bearbeiten von *besonders schützenswerten Personendaten* und von *Persönlichkeitsprofilen*. Solche Daten sollen zum einen bearbeitet werden dürfen, wenn ein *Gesetz im formellen Sinn* es ausdrücklich vorsieht (Bst. a). Darunter fallen auch völkerrechtliche Verträge und alle referendumpflichtigen Bundesbeschlüsse. Da es aber kaum je möglich sein wird, für jegliche Bearbeitung sensibler Daten die nötige Bestimmung in einem Gesetz zu schaffen, sollen derartige Daten auch bearbeitet werden dürfen, wenn die Bearbeitung für eine in einem formellen Gesetz klar umschrie-

bene Aufgabe unentbehrlich ist (Bst. b). Hingegen rechtfertigt der Umstand, dass eine Aufgabe durch Verwendung von besonders schützenswerten Daten oder Persönlichkeitsprofilen noch besser erfüllt werden kann, für sich allein die Bearbeitung dieser Daten noch nicht. Um kurzfristig auftretenden Bedürfnissen Rechnung tragen zu können, soll ferner der Bundesrat im Einzelfall die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen bewilligen können. Er darf dies aber nur tun, wenn er sich zuvor vergewissert hat, dass die Rechte der betroffenen Personen dadurch nicht gefährdet werden (Bst. c). Eine Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen ist schliesslich zulässig, wenn die betroffene Person eingewilligt oder ihre Daten allgemein zugänglich gemacht hat (Bst. d). Die Einwilligung kann aber nicht pauschal erfolgen, sondern muss sich auf einen bestimmten Einzelfall beziehen; nur dann kann man von einer Zustimmung in Kenntnis der Konsequenzen ausgehen. Was die allgemeine Zugänglichkeit der Daten angeht, verweisen wir auf die Erläuterungen zu Artikel 10 Absatz 2 Buchstabe f. – Auch bei Bearbeitungen gemäss den Buchstaben c und d muss mindestens eine gesetzliche Grundlage im Sinne von Absatz 1 gegeben sein.

Artikel 15 Beschaffen von Personendaten

Die besonderen Vorschriften über das Beschaffen von Personendaten stellen eine *Ergänzung* zu den Grundsätzen von Artikel 4 und den allgemeinen Bearbeitungsvorschriften von Artikel 14 dar. Sie sollen Gewähr bieten, dass in einer Zeit, in welcher die Verwaltung auf immer mehr Informationen und namentlich auch auf Personendaten angewiesen ist, diese so beschafft werden, dass der Betroffene allenfalls dazu Stellung nehmen und sich gegen eine unzulässige Bearbeitung wehren kann.

Absatz 1 hält demgemäss fest, dass Daten so beschafft werden müssen, dass dies für die betroffenen Personen erkennbar ist. Diesem Gebot wird am besten nachgelebt, wenn die Daten *bei der betroffenen Person selber* erhoben werden. Aber auch eine Erhebung bei Dritten ist zulässig, sofern die betroffene Person ausreichend darüber informiert wird. Denn die Erhebung bei Dritten, die bereits über die benötigten Daten verfügen, stellt eine wichtige Rationalisierungsmöglichkeit für die Verwaltung dar, welche nicht grundsätzlich in Frage gestellt werden soll. Auch ist es zum Teil im Interesse des Bürgers, wenn er die gleichen Angaben nicht gegenüber verschiedenen Verwaltungsstellen wiederholen muss.

Für systematische Erhebungen, etwa mittels *Fragebogen*, sieht *Absatz 2* besondere *Orientierungspflichten* für das verantwortliche Bundesorgan vor, weil in solchen Fällen in grossem Umfang Daten beschafft werden. Wenn auch aufgrund einer Befragung nicht notwendigerweise eine Datensammlung im Sinne des Entwurfs entstehen muss, so sollen doch die Betroffenen in ähnlicher Weise orientiert werden wie bei Datensammlungen (vgl. Art. 5).

Auf eine Orientierung der Betroffenen soll gemäss *Absatz 3* jedoch in drei Fällen verzichtet werden können. Sie ist nicht obligatorisch, wenn die betroffene Person, z. B. in einem Buch, eigene Daten der Allgemeinheit zugänglich gemacht hat (Bst. a), wenn dadurch die Erfüllung der Aufgabe des Bundesorgans in Frage gestellt würde (Bst. b) oder wenn der Aufwand übermässig wäre

(Bst. c). Letzteres kann namentlich bei statistischen Untersuchungen der Fall sein.

Artikel 16 Bekanntgabe von Personendaten

Die Erfahrung zeigt, dass die Regelungen über die Bekanntgabe von Personendaten die wichtigste Rolle im öffentlich-rechtlichen Persönlichkeitsschutz spielen. Die im Entwurf vorgeschlagene Bestimmung geht davon aus, dass der moderne Sozial- und Leistungsstaat in umfassender Weise Informationsbearbeitung betreibt. Soweit es dabei um Personendaten geht, stehen diese Informationsbearbeitungen in einem Spannungsfeld zwischen den Erfordernissen einer koordinierten und rationellen Verwaltungstätigkeit und den Anliegen des Persönlichkeitsschutzes. Wenn auch unbestritten ist, dass die einzelnen Verwaltungsstellen in Sachfragen, die sie gemeinsam betreffen, zusammenarbeiten sollen, so muss andererseits doch sichergestellt sein, dass nicht jede Amtsstelle in alle Personendaten Einblick nehmen kann, die im Staat insgesamt bearbeitet werden. Eine gewisse Abschottung zwischen den Verwaltungseinheiten, eine Art «informationeller Gewaltenteilung» ist notwendig.

Im geltenden Recht finden sich erst ansatzweise Regelungen für den Informationsaustausch zwischen den einzelnen Verwaltungsstellen. So verbietet es das in verschiedenen Beamtengesetzen verankerte Amtsgeheimnis einem Beamten unter anderem, geheimhaltungswürdige Tatsachen einer andern Behörde mitzuteilen⁴³⁾. Andererseits sehen die Vorschriften der Rechts- und Amtshilfe gegenseitige Informationspflichten der Behörden vor. Einschlägige Bestimmungen sind allerdings nicht sehr häufig⁴⁴⁾, und die Grundsätze der Rechts- und Amtshilfe sind in der Schweiz, abgesehen von einer spärlichen Praxis bezüglich der Rechtshilfe bei der Strafverfolgung⁴⁵⁾, noch kaum herausgebildet. Der vorliegende Artikel stellt deshalb eine *Art allgemeiner Amts- und Rechtshilfebestimmung und eine Ausführungsbestimmung zum allgemeinen Amtsgeheimnis* dar. Er legt fest, unter welchen Voraussetzungen Bundesorgane Personendaten weitergeben dürfen. Er sieht allerdings *keine Pflicht* zur Datenbekanntgabe vor, weil auch in Fällen, in denen die Voraussetzungen von Artikel 16 erfüllt sind, das zuständige Organ zusätzlich noch prüfen muss, ob mit der Bekanntgabe nicht gegen die Grundsätze von Artikel 4 verstossen wird. So dürfen Daten namentlich nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet wird (vgl. Art. 4 Abs. 5). Die Bekanntgaberegeln gelten sowohl für den Datenaustausch zwischen Bundesorganen wie auch für die Weitergabe von Daten an kantonale, kommunale und ausländische Behörden und an private Personen im In- und Ausland. Sie stellen eine *Ergänzung* zu Artikel 14 dar.

Nach *Absatz 1* ist die Bekanntgabe in fünf Fällen zulässig:

Daten dürfen einmal weitergegeben werden, wenn dafür eine *Rechtsgrundlage* besteht, das heisst wenn die Weitergabe in einem Gesetz, in einer Verordnung oder in einem Vertrag vorgesehen ist. Diese Rechtsgrundlage muss sich ausdrücklich auf den *Transfer der Daten als solchen* beziehen. Eine allgemeine Kompetenz zur Datenbearbeitung im Sinne von Artikel 14 genügt demnach nicht. Hingegen kommt es nicht darauf an, ob die Weitergabe der Daten als

Recht oder Pflicht der bekanntgebenden Behörde oder aber als Anspruch des Empfängers der Daten umschrieben ist.

Fehlt es an einer Rechtsgrundlage, so können Personendaten dennoch im Einzelfall bekanntgegeben werden, wenn der Empfänger sonst seine gesetzliche Aufgabe überhaupt nicht erfüllen könnte (Bst. a). Die Beschränkung auf den Einzelfall bedeutet, dass ohne gesetzliche Grundlage einem andern Organ oder einer Privatperson kein dauernder Zugriff auf eine Datensammlung gewährt werden darf, wie dies etwa in Form eines Online-Anschlusses oder durch periodisches Zustellen von Computer-Ausdrucken möglich wäre. Ein Einzelfall im Sinne von Buchstabe a liegt vor, wenn die Daten für einen *einmaligen Zweck* bekanntgegeben werden. Dabei kommt es nicht darauf an, ob es sich um die Daten einer einzigen Person oder einer Mehrzahl von Personen handelt.

Die fehlende Rechtsgrundlage kann auch durch die Einwilligung der betroffenen Person ersetzt werden (Bst. b), wobei die Zustimmung eine ausdrückliche oder stillschweigende sein kann. Sie muss für den betreffenden Einzelfall vorliegen; Globalermächtigungen genügen nicht. Das bedeutet allerdings nicht, dass die Einwilligung nur gültig ist, wenn sie sich auf eine einzige Bekanntgabe bezieht. Der Betroffene kann seine Einwilligung auch für mehrere Bekanntgaben erteilen, wenn die Umstände, unter denen die Bekanntgabe stattfinden darf, klar feststehen. So ist etwa denkbar, dass jemand seinen bisherigen Arbeitgeber generell ermächtigt, anderen Arbeitgebern Auskünfte über seine Qualifikationen zu geben (vgl. auch den neu vorgeschlagenen Art. 328b OR, Ziff. 221.1). Kann eine Einwilligung nicht oder nur mit unzumutbarem Aufwand eingeholt werden, so genügt es, wenn nach den Umständen eindeutig hervorgeht, dass die betroffene Person der Datenbekanntgabe zugestimmt hätte.

Eine Weitergabe von Personendaten ist auch dann zulässig, wenn die betroffene Person ihre Daten ohnehin schon der Öffentlichkeit zugänglich gemacht hat, etwa durch Veröffentlichung in einem Buch oder einer Zeitschrift (Bst. c).

Schliesslich soll die Bekanntgabe auch ohne Rechtsgrundlage und ohne Einwilligung der betroffenen Person möglich sein, wenn diese in rechtsmissbräuchlicher Art Angaben über sich selber verweigern will (Bst. d). In der Praxis geht es dabei vor allem um die Geltendmachung familienrechtlicher Ansprüche, etwa wenn ein Elternteil, der zu Alimenten verpflichtet ist, sich ins Ausland absetzt und der anspruchsberechtigte Elternteil oder das Kind seine Adresse bei der Botschaft erfahren möchte. Die Bestimmung kann auch im Bereich der Sozialversicherung Bedeutung erlangen, wenn sich ein Arbeitnehmer darüber informieren will, ob der Arbeitgeber seine Beiträge einbezahlt hat. Bevor die Daten bekanntgegeben werden, soll sich die betroffene Person im Sinne des rechtlichen Gehörs grundsätzlich dazu äussern können. Dieses Recht ist indes kein absolutes; das Bundesorgan kann auf die Einholung einer Stellungnahme namentlich verzichten, wenn sonst die Gefahr besteht, dass Rechtsansprüche oder wichtige Interessen von Dritten beeinträchtigt würden oder wenn der Betroffene innert Frist nicht reagiert oder nicht auffindbar ist.

Für die Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen müssen, wie auch sonst bei deren Bearbeitung, besondere Voraussetzungen erfüllt sein. Hat die betroffene Person nicht in die Bekanntgabe

eingewilligt oder ihre Daten der Öffentlichkeit nicht zugänglich gemacht, so muss die Bekanntgabe entweder im Gesetz ausdrücklich vorgesehen oder für eine gesetzlich klar umschriebene Aufgabe unentbehrlich sein. Fehlt es an diesen Voraussetzungen, so besteht die Möglichkeit, dass der Bundesrat die Datenbekanntgabe bewilligt (vgl. Art. 14 Abs. 2).

Absatz 2 gibt Bundesorganen die Möglichkeit, die Personalien (Name, Vorname), die Adresse sowie das Geburtsdatum einer Person auf Anfrage einem andern öffentlichen Organ oder interessierten Privatpersonen bekanntzugeben. Damit wird ein wichtiges Begehren aus der Vernehmlassung erfüllt. Gewisse Grundangaben zur Identifizierung einer Person, die ohnehin mehr oder weniger bekannt sind, sollen auf einfachem Weg in Erfahrung gebracht werden können. Da aber Absatz 2 keine Bekanntgabepflicht statuiert, muss das Bundesorgan auch bei dieser Art von Datenweitergabe allfälligen Schutzbedürfnissen einer betroffenen Person Rechnung tragen. Es kann etwa eine Auskunft verweigern, wenn allein schon die Tatsache, dass ein Organ über die Personalien verfügt, Aufschluss über die betroffene Person geben kann. Dies gilt namentlich für Bekanntgaben durch Strafverfolgungsbehörden des Bundes. Der Bundesrat kann allenfalls die Stellen bezeichnen, die Personalien bekanntgeben dürfen.

Absatz 3 nennt schliesslich Fälle, in denen Bundesorgane eine nach diesem Gesetz grundsätzlich zulässige Bekanntgabe einschränken können oder müssen. Dies trifft zu, wenn *wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen* einer betroffenen Person es verlangen (Bst. a). Es handelt sich bei dieser Bestimmung um eine Art «ordre public»-Vorbehalt, der gegenüber jedem Empfänger gilt. Wesentliche öffentliche Interessen sind namentlich solche des Staatsschutzes oder der militärischen Sicherheit. Bei offensichtlich schutzwürdigen Interessen einer betroffenen Person kann es sich beispielsweise um das Geheimhaltungsbedürfnis einer Person handeln, welche in eine amtliche Untersuchung einbezogen ist. Des weitern bleiben *gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften* vorbehalten (Bst. b). In verschiedenen Bereichen, namentlich im Sozialversicherungsrecht, gelten spezielle Geheimhaltungspflichten, die eine Bekanntgabe von Personendaten nur in vom Bundesrat bezeichneten Fällen ausnahmsweise zulassen⁴⁶⁾. Ebenso gibt es eine Anzahl bereichsspezifischer Datenschutzbestimmungen, die den zulässigen Empfängerkreis und zum Teil auch die Art der Daten, die übermittelt werden, festlegen⁴⁷⁾. Solche Bestimmungen gehen als Spezialnormen Artikel 16 des Entwurfes vor.

Bei dieser Ausgestaltung der Bekanntgaberegeln (und der Beschaffungsregeln) erübrigt es sich im Gegensatz zum Vorentwurf, die *Datenbekanntgabe an Steuerbehörden eigens zu regeln*. Die Praxis der Auskunftserteilung an Steuerbehörden kann im wesentlichen gleichwohl im bisherigen Umfang weitergeführt werden. Steuergesetze sehen in der Regel ausdrücklich Amtshilfepflichten vor⁴⁸⁾, so dass eine Rechtsgrundlage für die Datenweitergabe, zuweilen auch für die Weitergabe von besonders schützenswerten Daten, gegeben ist. Wo eine solche fehlt, kann der Steuerbehörde gemäss Artikel 16 Absatz 1 Buchstabe a immer noch im Einzelfall Auskunft erteilt werden, sofern die Behörde diese Information für die Erfüllung ihrer Aufgaben unbedingt benötigt. Eine solche Datenbekanntgabe stellt auch keinen Verstoß gegen das Zweckvereinbarkeitsgebot

von Artikel 4 Absatz 4 dar, solange der Steuerbehörde nur solche Informationen bekanntgegeben werden, die diese zur Steuerveranlagung tatsächlich benötigt. Nach Artikel 15 des Entwurfes muss die Steuerbehörde der betroffenen Person in diesen Fällen allerdings Mitteilung machen, wenn sie Auskünfte nicht direkt bei ihr beschafft. Die bestehenden Auskunftspflichten gegenüber den Steuerbehörden sind im übrigen deshalb gerechtfertigt, weil diese durchwegs dem Steuergeheimnis unterstehen, das heisst einer qualifizierten Schweigepflicht, welche die Steuerbehörden gegenüber Dritten, seien es Private oder andere Behörden, zu Stillschweigen verpflichtet.

Artikel 17 Sperrung der Bekanntgabe

Die Bestimmung sieht ein *beschränktes Abwehrrecht* der betroffenen Personen bei an sich zulässigen Bekanntgaben von Personendaten vor. Die Möglichkeit der Sperrung ist vor allem bei Datenweitergaben ins Ausland und an private Personen von Bedeutung. Bei solchen Bekanntgaben kann das verantwortliche Bundesorgan nicht alle möglichen negativen Auswirkungen voraussehen. Deshalb soll die betroffene Person ihre Interessen direkt geltend machen können. Die Sperre gilt grundsätzlich aber auch für Bekanntgaben gegenüber anderen Behörden, doch dürfte sie hier eher von untergeordneter Bedeutung sein, weil in vielen Fällen die Ausnahmebestimmung von Absatz 2 zur Anwendung kommt. Das Sperrecht kann nicht in pauschaler Weise geltend gemacht werden; die betroffene Person muss sich vielmehr an die zuständigen Organe wenden und die Daten, welche der Sperrung unterliegen sollen, genau bezeichnen.

Eine Sperrung der Bekanntgabe kann gemäss *Absatz 1* nicht jedermann verlangen, sondern nur eine betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht. Ein solches ist beispielsweise gegeben, wenn die betroffene Person durch die Datenbekanntgabe Belästigungen, Pressionen oder gar Verfolgungen durch die Empfängerkreise ausgesetzt würde.

Nach *Absatz 2* ist die Wirkung einer Sperre zudem beschränkt. Wo eine Rechtspflicht zur Bekanntgabe von Personendaten besteht, muss das verantwortliche Organ die Daten trotz Sperrung bekanntgeben (Bst. a). Die Sperrung ist auch unbeachtlich, wenn das Bundesorgan dadurch gehindert würde, seine Aufgabenerfüllung gemäss zu erfüllen (Bst. b).

Artikel 18 Anonymisieren und Vernichten von Personendaten

Die modernen Kopiertechniken und die durch die automatische Datenverarbeitung bedingten Sicherheitsmassnahmen führen zu einer grossen Menge von Datenbeständen. Viele dieser Bestände sind nach kurzer Zeit nicht mehr von praktischem Interesse. Weil sie aber gleichwohl bezüglich möglicher Persönlichkeitsverletzungen ein gewisses Risiko darstellen können, hält die Bestimmung als Grundsatz fest, dass solche Daten vernichtet oder wenigstens anonymisiert werden sollen. Eine solche Vorschrift entspricht dem Gebot einer verhältnismässigen Datenbearbeitung, wie es in Artikel 4 Absatz 3 des Entwurfes festgehalten ist. Andererseits trägt der Artikel dem Umstand Rechnung, dass bestimmte Daten, auch wenn sie für die ordentliche Verwaltungstätigkeit nicht mehr benötigt werden, gleichwohl nicht vernichtet oder anonymisiert werden können. Es sind dies zum einen jene Akten, die, etwa im Hinblick auf ein mögliches Revisionsver-

fahren, Beweis- oder Sicherungszwecken dienen (Bst. a). Zum andern handelt es sich um Dokumente, die namentlich für die Geschichtswissenschaft von Interesse sind. Welche Akten dies im einzelnen sind, ist in den Bestimmungen über das Bundesarchiv festgelegt. Diese sollen als Spezialnorm Artikel 18 des Entwurfs vorgehen (Bst. b).

Im Gegensatz zum Vorentwurf wird auf die Spezialregelung der *Archivierung von Daten* verzichtet. Archiviert im Sinne dieses Entwurfes (vgl. Art. 3 Bst. g) sind Dokumente, die von den ständig benötigten Akten getrennt werden und zu denen der Zugang infolge räumlicher Distanz oder organisatorischer Massnahmen beschränkt ist (z. B. wenn die Akten in abgeschlossenen Schränken oder Zimmern gelagert werden, die nur bestimmten Personen zugänglich sind, oder wenn bei automatisierter Bearbeitung der Zugang nur über einen zusätzlichen Code möglich ist). Mit einer konsequenten Archivierung kann zwar vielfältigen Anliegen des Datenschutzes entsprochen werden. Doch wie diese im einzelnen durchzuführen ist, lässt sich nicht in einer allgemeinen Regel festhalten. Zu unterschiedlich sind die diesbezüglichen organisatorischen und räumlichen Voraussetzungen bei den einzelnen Dienststellen der Bundesverwaltung und den Organisationen, die Aufgaben des Bundes übernehmen. Zu vielfältig sind auch die Abstufungen zwischen Daten, die täglich benötigt werden, solchen für den gelegentlichen Gebrauch und solchen, die nur noch selten benutzt werden. Hier müssen bereichsspezifisch die nötigen Zugriffsbeschränkungen festgelegt werden.

Artikel 19 Bearbeiten für Forschung, Planung und Statistik

Das öffentliche Interesse an Forschung, Planung und Statistik, aber auch der Umstand, dass Datenbearbeitungen in diesem Zusammenhang, soweit nicht personenbezogen, etwas weniger heikel erscheinen, erfordern auch im öffentlichrechtlichen Bereich eine Sonderregelung. Artikel 19 sieht demzufolge verschiedene Abweichungen von allgemeinen Grundsätzen des Entwurfs vor. Die Bestimmung gilt sowohl, wenn ein verantwortliches Organ eigene Daten zu nicht personenbezogenen Zwecken bearbeitet, wie auch, wenn es die Daten zu nicht personenbezogenen Forschungs-, Planungs- oder Statistikzwecken andern Organen des Bundes oder der Kantone oder Privatpersonen bekanntgibt. Im letzteren Fall bleiben allerdings besondere Geheimhaltungsvorschriften vorbehalten.

Absatz 1 nennt die *Voraussetzungen*, die kumulativ erfüllt sein müssen, wenn sich ein Bundesorgan auf das Forschungsprivileg berufen will. Erste Bedingung ist, dass das Organ, welches mit personenbezogenen Daten Forschung, Planung oder Statistik betreibt, die Daten anonymisiert, sobald dies der Bearbeitungszweck zulässt (Bst. a). Unter Anonymisierung ist dabei jede Massnahme zu verstehen, die bewirkt, dass die Identität der betroffenen Personen nicht mehr oder nur noch mit ausserordentlichem Aufwand festgestellt werden kann. In der Praxis kommt es häufig vor, dass ein Forscher, Planer oder Statistiker zwar in der Regel nicht mehr auf die Personenkennzeichnung der einzelnen Daten angewiesen ist, dass er aber gleichwohl noch nicht endgültig anonymisieren kann, weil er ausnahmsweise die Möglichkeit haben muss, die Identität einer Person festzustellen. In derartigen Situationen soll er mit Verschlüsselungen oder Kennzif-

fern arbeiten. Er kann beispielsweise die persönlichen Kennzeichen von den übrigen Daten so trennen, dass allein aufgrund einer Referenznummer noch feststellbar ist, welche Daten zu welcher Person gehören. Diese Praxis ist bereits heute recht verbreitet. Gibt ein Bundesorgan Daten für die Bearbeitung zu (nicht personenbezogenen) Forschungs-, Planungs- und Statistikzwecken bekannt, so muss es zudem durch Auflagen auf dem Vertrags- oder Verfügungswege sicherstellen, dass die betreffenden Bundesorgane oder Privaten die Daten ihrerseits nur mit seiner Zustimmung an Dritte bekanntgeben (Bst. b). Dabei wird vorausgesetzt, dass dieser Dritte die Daten wiederum zu Forschungs-, Planungs- oder Statistikzwecken oder für einen sonstigen nicht personenbezogenen Bearbeitungszweck verwendet. Schliesslich gelten die Erleichterungen von Artikel 19 nur, wenn die Ergebnisse der Bearbeitung so veröffentlicht werden, dass nach der allgemeinen Lebenserfahrung keine Rückschlüsse mehr auf die betroffenen Personen möglich sind (Bst. c).

Absatz 2 zählt abschliessend auf, welche datenschutzrechtlichen Bestimmungen bei nicht personenbezogenen Datenbearbeitungen unbeachtlich sind. Es ist dies einmal das Gebot der Zweckvereinbarkeit von Artikel 4 Absatz 4. Weil Forschungs-, Planungs- und Statistkarbeiten im Sinne dieser Bestimmung auf die betroffenen Personen keine direkten Auswirkungen haben, sollen auch Daten verwendet werden dürfen, die unter Umständen in einem ganz andern Sachzusammenhang erhoben worden sind (Bst. a). Aus demselben Grund sollen Bundesorgane im Rahmen von Forschung, Planung und Statistik und allenfalls weiteren nicht personenbezogenen Zwecken auch besonders schützenswerte Personendaten und Persönlichkeitsprofile (wobei letztere kaum eine Rolle spielen dürften) bearbeiten können, selbst wenn sie sich bei dieser Tätigkeit nur auf eine allgemeine Rechtsgrundlage im Sinne von Artikel 14 Absatz 1 stützen können und die qualifizierten Anforderungen von Artikel 14 Absatz 2 nicht erfüllt sind (Bst. b). Ferner gelten bei der Weitergabe von Daten zu nicht personenbezogenen Zwecken die allgemeinen Bekanntgaberegeln nicht (Bst. c). So ist für die Datenweitergabe als solche zu nicht personenbezogenen Zwecken keine zusätzliche Rechtsgrundlage nötig. Die Weitergabe kann auch erfolgen, ohne dass der Empfänger die Daten zur Erfüllung einer gesetzlichen Aufgabe unbedingt benötigt und ohne dass die betroffene Person im Einzelfall eingewilligt hat. Hingegen muss das Bundesorgan, von welchem die Daten stammen, aufgrund von Absatz 1 Buchstabe b der Weitergabe zustimmen.

Artikel 20 Privatrechtliche Tätigkeit von Bundesorganen

Gewisse Verwaltungseinheiten des Bundes, namentlich SBB und PTT, aber auch die Einkaufsstellen der Bundesverwaltung, nehmen bei ihrer Tätigkeit am wirtschaftlichen Wettbewerb teil. Nach *Absatz 1* sollen sie dabei den privaten Mitkonkurrenten gleichgestellt sein, sofern sie sich wie diese dem Privatrecht unterstellen. Dies ist dann der Fall, wenn sie nicht hoheitlich handeln, das heisst ihre Rechtsbeziehungen zu Dritten nicht in Form von Verfügungen, sondern mit privatrechtlichen Vereinbarungen gestalten. Unter diesen Voraussetzungen sollen für sie die weniger strengen datenschutzrechtlichen Auflagen des dritten Abschnittes des Gesetzes gelten. Das bedeutet in der Praxis zum Beispiel, dass sie Auskunftsbegehren mit dem Hinweis darauf, dass sie im wirt-

schaftlichen Wettbewerb stehen, allenfalls abschlägig beantworten können (vgl. Art. 6 Abs. 1 Bst. d); auch sind die Bearbeitungsregeln des vierten Abschnittes nicht beachtlich.

Der Umstand, dass Bundesorgane im wirtschaftlichen Wettbewerb stehen und privatrechtlich handeln, führt nach *Absatz 2 nicht auch zu einer Lockerung der datenschutzrechtlichen Aufsicht*. Der Datenschutzbeauftragte soll die privatrechtliche Tätigkeit von Bundesorganen in gleichem Umfang wie ihr hoheitliches Handeln überprüfen können. Das bedeutet, dass Bundesorgane im wirtschaftlichen Wettbewerb die gleichen Registrier- und Meldepflichten (Art. 7 und 8) haben, wie andere Bundesorgane.

Artikel 21 Staatsschutz und militärische Sicherheit

Die Organe des Staatsschutzes und der militärischen Sicherheit – das sind insbesondere die Bundespolizei und militärische Abwehr- und Nachrichtendienste – üben ihre Aufgaben hauptsächlich durch Bearbeiten von Personendaten aus. Dabei sind sie darauf angewiesen, Informationen aus den verschiedensten Quellen zu beziehen. Die Bearbeitung erheischt ein grosses Mass an Geheimhaltung, so auch zum Schutze der Mitarbeiter dieser Dienste. Andererseits stellt die Zusammenarbeit mit Staatsschutz- oder militärischen Sicherheitsbehörden fremder Staaten ebenfalls eine Notwendigkeit dar. Unter diesen Umständen ist es schwierig, allgemeine Regeln für die Informationstätigkeit von Staatsschutzbehörden festzulegen: Die Notwendigkeit eines wirksamen Datenschutzes ist zwar gerade in diesem Bereich offensichtlich, doch kann dieser mit Rücksicht auf höhere Interessen des Staates zum Teil nur ein beschränkter sein. Die vorliegende Bestimmung gibt deshalb dem Bundesrat die Kompetenz, im Bereich des Staatsschutzes und der militärischen Sicherheit Abweichungen vom allgemeinen Datenschutzgesetz vorzusehen. Diese Ausnahmen kann der Bundesrat in einer Verordnung regeln oder im Einzelfall bewilligen.

In *Absatz 1* ist abschliessend aufgezählt, von welchen Bestimmungen dieses Gesetzes Abweichungen zulässig sind. So kann der Bundesrat für die Organe des Staatsschutzes und der militärischen Sicherheit Ausnahmen vom Grundsatz der Zweckvereinbarkeit (Art. 4 Abs. 4) und von den Anforderungen an die Bekanntgabe von Daten ins Ausland (Art. 4 Abs. 5) vorsehen (Bst. a). Es liegt in der Natur der Tätigkeit von Staatsschutzbehörden, dass sie auch auf solche Daten angewiesen sind, die ursprünglich nicht für Staatsschutzzwecke erhoben worden sind. Beim Datenaustausch mit ausländischen Staatsschutzbehörden kommt es zudem vor, dass im höheren Staatsinteresse Informationen über Personen auch dann bekanntgegeben werden, wenn nicht auszuschliessen ist, dass diesen dadurch ein Nachteil erwächst. Die Ausnahme von Artikel 4 Absatz 5 soll ermöglichen, dass die Auskunftserteilung an ausländische Behörden im Interesse der inneren und äusseren Sicherheit weiterhin in dem Umfange möglich bleibt, wie das heute der Bundesratsbeschluss sowie die Vorschriften des EJPD betreffend den Polizeidienst der Bundesanwaltschaft erlauben⁴⁹⁾. Staatsschutzbehörden sind ferner häufig auf besonders schützenswerte Personendaten angewiesen. Der Bundesrat soll die Bearbeitung solcher Daten zulassen können, auch wenn die sonst im Datenschutzgesetz vorgesehenen qualifizierten Voraussetzungen nicht erfüllt sind (Bst. b). Aus Gründen der Geheimhaltung sollen Staatsschutz-

behörden sodann unter bestimmten Voraussetzungen von der Pflicht entbunden werden können, ihre Datensammlungen und ihre Datenbekanntgaben ins Ausland dem Datenschutzbeauftragten zu melden (Bst. c). Der Bundesrat kann auch vorsehen, dass eine Datensammlung zwar dem Datenschutzbeauftragten gemeldet wird, dieser sie aber nicht im Register der Datensammlungen publiziert. Schliesslich soll die Möglichkeit geschaffen werden, die Zusammenarbeit zwischen Behörden des Staatsschutzes und der militärischen Sicherheit auf der einen und dem Datenschutzbeauftragten auf der andern Seite abweichend von den allgemeinen Grundsätzen zu regeln (Bst. d). Der Bundesrat wird dabei vor allem entscheiden müssen, ob die Auskunftspflichten gegenüber dem Datenschutzbeauftragten und dessen Akteneinsichtsrecht (vgl. Art. 24 Abs. 3) eingeschränkt werden sollen.

Absatz 2 hält der Klarheit halber fest, dass auch zugunsten des Staatsschutzes und der militärischen Sicherheit das Stimm-, Petitions- und Statistikgeheimnis in keinem Fall durchbrochen werden darf.

Um den Kreis der Geheimnisträger in Staatsschutzangelegenheiten kleinzuhalten, sieht *Absatz 3* vor, dass datenschutzrechtliche Meinungsverschiedenheiten zwischen den Staatsschutzbehörden auf der einen sowie den betroffenen Personen und dem Datenschutzbeauftragten auf der andern Seite nicht von der Datenschutzkommission bzw. von ihrem Präsidenten, sondern vom übergeordneten Departement (EJPD oder EMD) entschieden werden. Im Falle eines Weiterzugs des Departementsentscheids durch die betroffene Person oder bei Meinungsverschiedenheiten zwischen Staatsschutzbehörden und Datenschutzbeauftragtem entscheidet der Bundesrat. Dieser Rechtsweg an den Bundesrat entspricht auch der allgemeinen Regelung der Organisation der Bundesrechtspflege in Angelegenheiten des Staatsschutzes (Art. 100 Bst. a OG; SR 173.110).

Artikel 22 Ansprüche und Verfahren

Dass sich Bundesorgane beim Umgang mit Personendaten an die Vorschriften dieses Gesetzes halten, liegt nicht nur im öffentlichen Interesse, sondern ebenso im Interesse der jeweils betroffenen Personen. Diesen räumt Artikel 22 einen *Rechtsanspruch* auf eine gesetzmässige Datenbearbeitung ein. Zudem regelt er die prozessrechtlichen Modalitäten für die Durchsetzung solcher Ansprüche. Das vorgeschlagene Rechtsschutzsystem orientiert sich einerseits an den privatrechtlichen Klagen nach Artikel 12 des Entwurfes bzw. Artikel 28a des Zivilgesetzbuches und fügt sich andererseits in das geltende Verwaltungsverfahrenrecht ein.

Nach *Absatz 1* kann gegenüber dem jeweils verantwortlichen Bundesorgan datenschutzrechtliche Ansprüche geltend machen, wer sich über ein *schutzwürdiges Interesse* ausweist. Nach der geltenden verwaltungsrechtlichen Praxis ist demnach nicht nur die betroffene Person legitimiert, sondern unter Umständen auch ein Dritter, dessen eigene Personendaten nicht zur Diskussion stehen. Damit ist der Kreis der Berechtigten etwas grösser als im privatrechtlichen Teil des Gesetzes, wobei allerdings berücksichtigt werden muss, dass sich gestützt auf den allgemeinen Persönlichkeitsschutz des Zivilgesetzbuches unter Umständen auch Dritte gegen Datenbearbeitungen wehren können, die ihre eigene Person nicht direkt betreffen. Auch die Legitimation der *Verbände* richtet sich nach all-

gemeinen verwaltungsrechtlichen Grundsätzen. Verbände können datenschutzrechtliche Ansprüche geltend machen, wenn sie ein *eigenes Interesse* nachweisen; sie sind zudem legitimiert, *die Interessen eines Mitgliedes zu verteidigen*, wenn sie dartun, dass dies nach den Statuten zu ihren Aufgaben gehört, dass die Interessenwahrung im Sinne einer Mehrheit oder einer grossen Anzahl der Mitglieder ist und dass diese selber zur Geltendmachung entsprechender Begehren befugt wären⁵⁰). Die Begehren können, wie im privatrechtlichen Bereich, auf die *Unterlassung* einer widerrechtlichen Bearbeitung (Bst. a), die *Beseitigung* der Folgen einer solchen Bearbeitung (Bst. b) oder auf die *Feststellung der Widerrechtlichkeit* einer Datenbearbeitung (Bst. c) lauten. Im Rahmen des bereits erwähnten, unmittelbar aus Artikel 4 BV fliessenden allgemeinen Akteneinsichtsrechts kann zudem unter bestimmten Umständen auch Aufschluss über die *Herkunft* der Daten verlangt werden (vgl. dazu die Erläuterungen zu Art. 5). Allfällige Schadenersatzansprüche richten sich nach dem Verantwortlichkeitsgesetz des Bundes.

Absatz 2 weist darauf hin, dass im Rahmen von Unterlassungs- und Beseitigungsklagen insbesondere die *Berichtigung* oder *Vernichtung* der Daten verlangt werden kann (Bst. a). Zudem sieht er in Analogie zu Artikel 28a Absatz 2 des Zivilgesetzbuches die Möglichkeit vor, dass ein Entscheid, der in einer datenschutzrechtlichen Angelegenheit ergeht (z. B. die Feststellung, dass eine Bearbeitung widerrechtlich war, oder die Berichtigung von Daten), Dritten mitgeteilt oder veröffentlicht wird (Bst. b).

Nach *Absatz 3* ist auch im öffentlich-rechtlichen Bereich die Möglichkeit eines *Bestreitungsvermerks* vorgesehen. Dieser stellt eine besondere Art von *Beweislastregel* dar. Da im Verwaltungsrecht die *Offizialmaxime* gilt, muss ein Bundesorgan, das sich mit einem datenschutzrechtlichen Begehren konfrontiert sieht, den Sachverhalt von Amtes wegen abklären. Dabei sind die Parteien allerdings verpflichtet, an der Feststellung des Sachverhalts mitzuwirken. Wenn nun die Richtigkeit oder Falschheit eines Datums im Rahmen der amtlichen Untersuchung nicht eindeutig festgestellt werden und die Behörde auf die umstrittene Angabe nicht einfach verzichten kann, besteht die Möglichkeit, einen Bestreitungsvermerk anzubringen. Damit wird dargetan, dass der Betroffene mit der Darstellung eines Sachverhaltes in behördlichen Akten nicht einverstanden ist. Wie der Bestreitungsvermerk genau auszugestalten ist, ob als einfache Kennzeichnung oder eher als eine Art von Gegendarstellung, soll die Praxis entscheiden.

Absatz 4 hält ausdrücklich fest, dass datenschutzrechtliche Begehren im Sinne des vorliegenden Artikels nach den Grundsätzen des Verwaltungsverfahrensgesetzes zu behandeln sind. Dies gilt auch in Sachbereichen, in denen das Verwaltungsverfahrensgesetz nach seinen Artikeln 2 und 3 nicht anwendbar ist. Denn die Gründe für diese Ausnahmeregelung – bereits bestehendes Spezialverfahrensrecht, Notwendigkeit eines raschen Entscheides u. ä. – gelten für den Datenschutz nicht. Die Anwendbarkeit des Verwaltungsverfahrensgesetzes bedeutet vor allem, dass über datenschutzrechtliche Begehren im Sinne der Absätze 1 und 2 in Form einer *Verfügung* entschieden werden muss. Ob diese im Zusammenhang mit einem andern Verfahren (z. B. Steuerverfahren) ergeht oder von diesem losgetrennt wird, bleibt der entscheidenden Behörde überlassen. Auch die Verweigerung und Beschränkung einer Auskunft muss verfügt werden.

Absatz 5 sieht einen besonderen *Rechtsweg* bei Entscheidungen in Datenschutzangelegenheiten vor. Entsprechende Verfügungen sind nicht an die Aufsichtsbehörde, sondern an die Eidgenössische Datenschutzkommission weiterziehbar (vgl. dazu Art. 27).

221.5 Fünfter Abschnitt: Eidgenössischer Datenschutzbeauftragter

Artikel 23 Wahl und Stellung

Mit Verhaltensnormen allein kann kein wirkungsvoller Datenschutz geschaffen werden. Damit die datenschutzrechtlichen Grundsätze des Entwurfes in der Rechtswirklichkeit tatsächlich beachtet werden, ist eine Aufsicht und vor allem auch eine Beratung durch ein kompetentes Organ notwendig. Die Notwendigkeit einer Kontrolle wurde auch im Vernehmlassungsverfahren nicht grundsätzlich in Frage gestellt, wenngleich über deren konkrete Ausgestaltung die Meinungen zum Teil auseinandergingen. Der vorliegende Entwurf versucht nun, die datenschutzrechtliche Aufsicht zwar wirksam, doch zugleich einfach und bürgerfreundlich zu gestalten. Anstelle der etwas schwerfälligen, mit einem umfassenden Pflichtenheft ausgestatteten 13köpfigen Datenschutzkommission des Vorentwurfs soll nun die Aufsicht zur Hauptsache einem *Datenschutzbeauftragten* übertragen werden. Daneben soll eine *Datenschutzkommission* als Schieds- und Rekurskommission im Sinne der Revisionsvorlage zum Bundesgesetz über die Organisation der Bundesrechtspflege in datenschutzrechtlichen Streitfällen entscheiden. Die Befugnisse des Datenschutzbeauftragten und der Kommission sind im öffentlich-rechtlichen Bereich umfassend, auf privatrechtlichem Gebiet hingegen auf solche Datenbearbeitungen beschränkt, die besonders schwere Risiken in sich bergen.

Nach *Absatz 1* wird der Datenschutzbeauftragte vom Bundesrat gewählt. Dieser wird die Anstellungsbedingungen in einer Verordnung oder im Einzelfall genauer regeln. Dabei wird er für den Datenschutzbeauftragten in der Regel den Beamtenstatus vorsehen und ihn in jedem Fall dem Amtsgeheimnis unterstellen.

Nach *Absatz 2* soll der Datenschutzbeauftragte seine Aufgaben selbständig erfüllen können. Er ist administrativ dem Eidgenössischen Justiz- und Polizeidepartement zugeordnet. Für die Eingliederung in dieses Departement spricht der Umstand, dass der Datenschutzbeauftragte, wie das EJPD auch, in erster Linie *Rechtsfragen* behandelt.

Der Beauftragte verfügt nach *Absatz 3* über ein eigenes Sekretariat, für welches der Bundesrat die nötigen Mittel jeweils mit dem Budget beantragt.

Artikel 24 Aufsicht

Die Bestimmung regelt die Arbeitsweise des Datenschutzbeauftragten und umschreibt seine Befugnisse. Seine wichtigsten Kompetenzen bestehen darin, dass er von sich aus bei Datenbearbeitungen, bei denen er Persönlichkeitsverletzungen vermutet, *Abklärungen* vornehmen und *Empfehlungen* an die Datenbearbeiter richten oder die betroffenen Personen, die sich an ihn gewendet haben, orientieren kann. Hingegen darf er keine rechtsverbindlichen Anordnungen treffen.

Nach *Absatz 1* hat der Datenschutzbeauftragte nicht nur die Einhaltung dieses Gesetzes, sondern auch aller weiteren datenschutzrechtlichen Erlasse des Bundes zu überwachen. Damit sind bereits bestehendes und künftiges Spezialdatenschutzrecht, aber auch völkerrechtliche Verträge gemeint. Von der Aufsicht durch den Datenschutzbeauftragten ausgenommen ist allerdings der Bundesrat. Der Datenschutzbeauftragte kann nicht Kontrollorgan seiner eigenen Aufsichtsbehörde sein. Das heisst aber nicht, dass sich der Bundesrat grundsätzlich nicht auch nach den datenschutzrechtlichen Bestimmungen richten will.

Nach *Absatz 2* kann der Datenschutzbeauftragte von sich aus oder aufgrund von Anzeigen die ihm nötig erscheinenden Abklärungen vornehmen. Da er niemals in der Lage sein wird, alle datenschutzrechtlich problematischen Bearbeitungen zu untersuchen, wird er sich auf Fälle mit besonderer Tragweite und grosser Präjudizwirkung beschränken. Entsprechend besteht auch für Personen, die eine tatsächliche oder vermeintliche Verletzung von Datenschutzvorschriften anzeigen, kein Erledigungsanspruch. Bei Datenbearbeitungen durch Private kann der Datenschutzbeauftragte zudem nur ausnahmsweise Abklärungen vornehmen. Denn entsprechend der im Zivilrecht geltenden Privatautonomie soll es grundsätzlich Sache der Betroffenen und nicht einer staatlichen Behörde sein, sich gegen Persönlichkeitsverletzungen durch Datenbearbeitungen zu wehren. Diesbezügliche Ansprüche sollen vor dem Zivilrichter durchgesetzt werden. Eine Ausnahme gilt lediglich in drei Fällen: Der Datenschutzbeauftragte soll auch im privaten Bereich intervenieren können, wenn bestimmte Bearbeitungsmethoden die Gefahr in sich bergen, dass die Persönlichkeit einer grösseren Anzahl von Personen verletzt wird (Bst. a). Man kann in diesem Zusammenhang von *Fehlern bei der Konzeption eines Informationssystems* sprechen, die sich mit den Mitteln des Zivilprozessrechts nicht mehr angemessen beheben lassen. Hier soll der Datenschutzbeauftragte gleichsam im öffentlichen Interesse Abklärungen vornehmen können. Die gleichen Befugnisse hat er auch bei *registrierpflichtigen Datensammlungen und meldepflichtigen Bekanntgaben ins Ausland* (Bst. b und c). Auch in diesen Fällen sind die Risiken einer Persönlichkeitsverletzung stark erhöht. Wenn der Beauftragte bei der Meldung solcher Datenbearbeitungen auf mögliche Persönlichkeitsgefährdungen stösst, soll er Massnahmen ergreifen können, da ansonsten Registrier- und Meldepflicht keine Wirkungen entfalten würden. Weil aber die Registrierpflicht für private Datenbearbeiter eine sehr eingeschränkte ist, sind auf diesem Gebiet auch der Tätigkeit des Datenschutzbeauftragten enge Grenzen gesetzt. Bei den Bundesorganen hingegen kann der Datenschutzbeauftragte jederzeit alle ihm nützlich erscheinenden Abklärungen vornehmen (Bst. d). Der Grundsatz der gesetzmässigen Verwaltung gilt absolut, weshalb auch die Kontrolle umfassend sein soll.

Absatz 3 räumt dem Datenschutzbeauftragten die für seine Abklärungen nötigen *Informationsbeschaffungsrechte* ein. Er hat das Recht, Akten herauszuverlangen, wobei ihn vor allem die Informatikkonzepte interessieren dürften. Er kann sich aber auch vor Ort Datenbearbeitungen vorführen lassen um festzustellen, welche Bearbeitungsmöglichkeiten effektiv bestehen. Daneben muss er Auskünfte einholen können, und zwar nicht nur bei den hauptverantwortlichen Datenbearbeitern oder den Inhabern von Datensammlungen, sondern auch bei deren Hilfspersonen. Die in eine Abklärung einbezogenen Personen müssen den Da-

tenschutzbeauftragten unterstützen; sie haben eine ähnliche Mitwirkungspflicht, wie sie in Artikel 13 des Verwaltungsverfahrensgesetzes (SR 172.021) vorgesehen ist. Die Mitwirkungspflicht soll andererseits nicht zur Folge haben, dass private Bearbeiter oder Organe des Bundes sich selber belasten müssen. Absatz 3 sieht deshalb vor, dass eine vom Datenschutzbeauftragten einvernommene Person sich sinngemäss auf das Zeugnisverweigerungsrecht von Artikel 16 des Verwaltungsverfahrensgesetzes und damit zum Teil auch auf Artikel 42 Absätze 1 und 3 der Bundeszivilprozessordnung (SR 273) berufen kann. Der Datenbearbeiter oder eine Drittperson können demnach die Aussage namentlich verweigern, wenn sie dadurch sich selber oder nahe Verwandte der strafrechtlichen Verfolgung aussetzen würden. Als Straftatbestände fallen dabei vor allem die Artikel 28 und 29 des Entwurfs in Betracht. Die Befragten können dem Datenschutzbeauftragten auch ein Berufsgeheimnis entgegenhalten, jedoch nur solange sie die betroffene Person, in deren Interesse der Datenschutzbeauftragte ermittelt, nicht davon entbindet. Das Amtsgeheimnis hingegen gilt gegenüber dem Datenschutzbeauftragten nicht.

Kommt der Datenschutzbeauftragte im Rahmen seiner Abklärungen zum Schluss, dass eine Bearbeitungsart gegen die Vorschriften dieses Gesetzes verstösst, so erlässt er nach *Absatz 4* eine *Empfehlung*. Dabei wird er den Datenbearbeiter in der Regel auffordern, künftig seine Praxis zu ändern, ohne dass er aber auf Einzelfälle Bezug nimmt. Denkbar ist auch, dass der Beauftragte eine Empfehlung im Hinblick auf eine bestimmte betroffene Person oder Personengruppe macht. Die Empfehlung ist weder für private Datenbearbeiter noch für die Bundesorgane verbindlich. Es handelt sich dabei insbesondere *nicht* um eine *Verfügung*, die mit den Mitteln des Verwaltungszwanges durchgesetzt werden könnte. Private Datenbearbeiter und Bundesorgane sind deshalb frei, ob sie sich an die Empfehlung halten wollen oder nicht. Im letzteren Fall gehen sie allerdings das Risiko ein, dass im Rahmen eines privatrechtlichen Klage- oder eines öffentlich-rechtlichen Beschwerdeverfahrens die Unrechtmässigkeit ihrer Datenbearbeitung festgestellt wird und sie allenfalls auch straf- und haftpflichtrechtlich belangt werden. Zudem müssen sie damit rechnen, dass der Datenschutzbeauftragte die Angelegenheit der Datenschutzkommission unterbreitet, welche dann in einer *rechtsverbindlichen Entscheidung* festlegt, ob die entsprechende Bearbeitung zulässig ist.

Wenn der Datenschutzbeauftragte eine Empfehlung erlassen hat, wird er den Adressaten ersuchen, sich innert einer bestimmten Frist darüber auszusprechen, ob er sich daran halten werde. Verneint dies der betreffende Datenbearbeiter, antwortet er überhaupt nicht oder stellt der Datenschutzbeauftragte fest, dass trotz Annahme der Empfehlung die beanstandete Datenbearbeitung fortgesetzt wird, so kann er nach *Absatz 5* die Angelegenheit der Datenschutzkommission unterbreiten (Bst. a). Er wird vor allem dann einen Entscheid der Kommission verlangen, wenn wesentliche öffentliche Interessen auf dem Spiel stehen und wenn es um Fragen von präjudizieller Bedeutung geht. In Fällen, in denen nur eine einzige oder wenige Personen von einer unrechtmässigen Datenbearbeitung und keine öffentlichen Interessen betroffen sind, kann er auf die Anrufung der Datenschutzkommission verzichten, dafür aber die Personen, die ihm Meldung gemacht haben, auf den ordentlichen Rechtsweg verweisen (Bst. b). Es ist

dann Sache der betroffenen Personen, sich gegenüber privaten Datenbearbeitern mit zivilrechtlicher Klage gemäss Artikel 12 oder gegenüber Bundesorganen mit Beschwerde gemäss Artikel 22 zur Wehr zu setzen. Wird die Angelegenheit der Datenschutzkommission vorgelegt, so prüft sie die umstrittene Frage neu und erlässt eine Verfügung. Da die Empfehlung des Datenschutzbeauftragten in der Regel allgemein gehalten sein wird, werden die betroffenen Personen selber selten in dieses Verfahren einbezogen werden.

Artikel 25 Information

Die ausländischen Erfahrungen zeigen, dass das datenschutzrechtliche Bewusstsein vor allem durch die Öffentlichkeitsarbeit der Datenschutzverantwortlichen gestärkt werden kann. Nach *Absatz 1* soll deshalb der Datenschutzbeauftragte dem Bundesrat periodisch und nach Bedarf Bericht erstatten. Bei den periodischen Berichten handelt es sich um Tätigkeitsberichte, die stets veröffentlicht werden sollen. Bei Berichten über einzelne Vorkommnisse entscheidet der Bundesrat von Fall zu Fall über die Publikation.

Nach *Absatz 2* hat der Datenschutzbeauftragte zusätzlich die Möglichkeit, sich in Fällen von allgemeinem Interesse direkt an die Öffentlichkeit zu wenden. Dies wird er beispielsweise tun, wenn er eine Empfehlung zu einem Informationssystem von gesamtschweizerischer Bedeutung abgibt. Bei seiner Öffentlichkeitsarbeit darf er aber Informationen, die dem Amtsgeheimnis unterstehen, nur mit Zustimmung der zuständigen Behörde bekanntgeben. Damit aber diese nicht ohne weiteres verhindern kann, dass Missstände aufgedeckt und in der Öffentlichkeit bekanntgemacht werden, entscheidet bei Meinungsverschiedenheiten zwischen ihr und dem Datenschutzbeauftragten der Präsident der Eidgenössischen Datenschutzkommission. Sein Entscheid ist endgültig.

Artikel 26 Weitere Aufgaben

Neben der Aufsicht nach Artikel 24, welche das Schwergewicht in der Tätigkeit des Datenschutzbeauftragten bildet, hat dieser weitere Aufgaben wahrzunehmen, welche in *Absatz 1* festgehalten sind. So soll er, weil er auf dem Gebiet des Datenschutzes über die grössten Kenntnisse und die grösste Erfahrung verfügt, private Personen, aber auch Organe von Bund und Kantonen in Datenschutzfragen informieren und beraten können und allenfalls auch als Vermittler wirken (Bst. a). Mit diesen Tätigkeiten kann er wesentlich dazu beitragen, dass es gar nicht erst zu datenschutzrechtlichen Konflikten kommt. Des weitem hat er bei der Vorbereitung von Bundeserlassen und weiteren Massnahmen des Bundes, die datenschutzrechtlich von Bedeutung sind, Stellung zu nehmen (Bst. b). Der Datenschutzbeauftragte soll ferner mit in- und ausländischen Datenschutzbehörden zusammenarbeiten (Bst. c). Er kann dabei namentlich den Informationsaustausch zwischen den Datenschutzverantwortlichen des Bundes und der Kantone fördern. Die genannten Aufgaben werden zum Teil bereits heute vom Dienst für Datenschutz des Bundesamtes für Justiz wahrgenommen. Der Datenschutzbeauftragte leistet aber auch Amtshilfe im Sinne der Artikel 13 ff. des Übereinkommens Nr. 108 des Europarates zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Er orientiert auf Wunsch ausländische Behörden über die Rechts- und Verwaltungspra-

xis im Bereich des schweizerischen Datenschutzrechts oder gibt ihnen Sachauskünfte über bestimmte Datenbearbeitungen in der Schweiz. Schliesslich ist er am ehesten in der Lage zu beurteilen, in welchem Mass der Datenschutz in einem andern Staat gewährleistet ist. Er kann deshalb von Privaten oder Behörden um Gutachten ersucht werden, wenn sich die Frage stellt, ob durch einen Datentransfer ins Ausland die Persönlichkeit einer betroffenen Person im Sinne von Artikel 4 Absatz 5 schwerwiegend gefährdet wird (Bst. d).

Datenschutzprobleme stellen sich aber auch ausserhalb des Anwendungsbereiches dieses Gesetzes. Die Organe der Bundesverwaltung haben nach *Absatz 2* die Möglichkeit, sich auch dort vom Datenschutzbeauftragten beraten zu lassen. Der Datenschutzbeauftragte seinerseits kann um Einblick in derartige Datenbearbeitungen nachsuchen, etwa bei den Registerbehörden, im polizeilichen Ermittlungsverfahren, im Rechtshilfe- und im Verwaltungsstrafverfahren sowie bei den Verwaltungsbeschwerdeinstanzen, die nach Artikel 2 nicht zur Anwendung des Datenschutzgesetzes verpflichtet sind. Damit er sich ein genaues Bild von den anstehenden Problemen machen kann, ist es den Behörden gestattet, ihm Einblick in ihre Geschäfte gewähren. Bei Absatz 2 handelt es sich demnach um eine weitere Ausnahmebestimmung zum Gebot der Amtsverschwiegenheit nach Artikel 27 und zur Regelung der Zeugnispflicht nach Artikel 28 des Beamtengesetzes.

Absatz 3 regelt die Aufgaben des Datenschutzbeauftragten im Zusammenhang mit der Tätigkeit der Kommission für das Berufsgeheimnis in der medizinischen Forschung (vgl. dazu Ziff. 222.43).

221.6 Sechster Abschnitt: Eidgenössische Datenschutzkommission

Artikel 27

Mit der Einsetzung der *Eidgenössischen Datenschutzkommission* wird im öffentlich-rechtlichen Datenschutz ein umfassender Rechtsschutz gewährleistet. Gemäss *Absatz 1* handelt es sich bei der Datenschutzkommission um eine Schieds- und Rekurskommission, wie sie bei der laufenden Revision des Bundesgesetzes über die Bundesrechtspflege neu im Verwaltungsverfahrensgesetz verankert wird³¹⁾. Auch im Bereich des Datenschutzes soll das im Rahmen der Reorganisation der Bundesrechtspflege vorgesehene Konzept einer Verkürzung des verwaltungsinternen Beschwerdeverfahrens und einer Entlastung des Bundesgerichts durch die Schaffung spezieller verwaltungsgerichtlicher Behörden verwirklicht werden. Für die Datenschutzkommission werden demnach die neuen Regelungen des Verwaltungsverfahrensgesetzes gelten. Sie wird sieben Mitglieder umfassen, wobei der Bundesrat in der Ausführungsverordnung zu diesem Gesetz oder in einer speziellen Organisationsverordnung für die Kommission vorsehen kann, dass diese für den öffentlich-rechtlichen und den privaten Bereich je eine Abteilung bildet. Nach den allgemeinen Regeln für Schieds- und Rekurskommissionen wird die Datenschutzkommission Rechtsfragen von grundsätzlicher Bedeutung in der Besetzung von fünf und die übrigen Fragen in der Besetzung von drei Mitgliedern entscheiden.

Absatz 2 umschreibt die *Aufgaben* der Kommission. Die Kommission befindet erstinstanzlich über Empfehlungen, die der Datenschutzbeauftragte im Rahmen seiner Abklärungen (vgl. Art. 24) erlassen hat und die er ihr in der Folge zum Entscheid unterbreitet (Bst. a). In zweiter Instanz entscheidet die Kommission über Beschwerden gegen Verfügungen von Bundesorganen in Datenschutzfragen (Bst. b). Dabei kann es sich beispielsweise um Verfügungen betreffend das Auskunftsrecht oder um Entscheide über Berichtigungs- oder Vernichtungsbegehren im Sinne von Artikel 22 handeln. Ausgenommen bleiben allerdings Verfügungen des Bundesrates. Ebenfalls in zweiter Instanz beurteilt die Datenschutzkommission Beschwerden gegen Verfügungen der Kommission für das Berufsgeheimnis in der medizinischen Forschung (Bst. c; vgl. dazu ausführlicher Ziff. 222.43). Schliesslich können auch letztinstanzliche kantonale Entscheide, die sich auf öffentlich-rechtliche Vorschriften des Bundes über den Datenschutz stützen, bei der Datenschutzkommission angefochten werden (Bst. d). Das Gesetz findet zwar keine Anwendung auf die Datenbearbeitungen kantonalen Organe. Doch gelten auch für diese gewisse Spezialdatenschutzvorschriften des Bundes (z. B. im Sozialversicherungs- oder im Ausländerrecht).

Die Regelungen von Buchstaben b und d haben zur Folge, dass über datenschutzrechtliche Ansprüche, die sich allein auf das vorliegende Gesetz stützen, nicht diejenigen Instanzen entscheiden, die sonst für Beschwerden im betreffenden Sachgebiet zuständig sind. Weil es aber gerade in den Anfängen des Datenschutzgesetzes sehr wichtig ist, dass sich in Datenschutzfragen eine einheitliche Rechtsprechung herausbildet, kann diese Verzweigung des Rechtsweges in Kauf genommen werden. Da Entscheide der Datenschutzkommission mit verwaltungsgerichtlicher Beschwerde ans Bundesgericht weitergezogen werden können, ist zudem gewährleistet, dass das oberste Gericht unabhängig vom jeweiligen Kontext die Anwendung des Gesetzes überprüfen kann. Es kann nun allerdings Fälle geben, wo eine betroffene Person zusammen mit einem datenschutzrechtlichen Begehren auch Ansprüche geltend macht, die nicht im Datenschutzgesetz begründet sind. So ist beispielsweise vorstellbar, dass jemand bei den Organen der Invalidenversicherung eine Berichtigung seiner Gesundheitsdaten verlangt (vgl. Art. 22 Abs. 2 Bst. a), um auf diese Weise einen Anspruch auf eine höhere Invalidenrente zu begründen. Das Hauptbegehren ist hier nicht datenschutzrechtlicher Natur, sondern zielt auf eine Versicherungsleistung. Ein solches Begehren muss im ordentlichen Verfahren, auf dem dafür vorgesehenen Instanzenweg behandelt werden. Weil es sich bei den Datenschutzfragen nur um Vorfragen für die Geltendmachung von Leistungsansprüchen handelt, wird die Datenschutzkommission darauf nicht eintreten.

Es ist denkbar, dass der Datenschutzbeauftragte im Rahmen seiner Abklärungen auf Bearbeitungen stösst, die, wenn sie nicht sofort aufgegeben oder geändert werden, einer Person schweren Schaden zufügen, der nachher kaum mehr behoben werden kann. In solchen Fällen soll nach *Absatz 3* der Beauftragte beim Präsidenten der Datenschutzkommission *vorsorgliche Massnahmen* verlangen können. Den betroffenen Personen selber stehen für den privatrechtlichen Bereich gestützt auf Artikel 28c des Zivilgesetzbuches und für den öffentlich-rechtlichen Bereich aufgrund von Artikel 56 des Verwaltungsverfahrensgesetzes entsprechende Rechtsbehelfe zur Verfügung.

221.7 Siebenter Abschnitt: Strafbestimmungen

Verstösse gegen die Bestimmungen des Datenschutzgesetzes sollen grundsätzlich nicht mit strafrechtlichen, sondern mit zivil- und verwaltungsrechtlichen Sanktionen geahndet werden. Von diesem Prinzip sieht der Entwurf drei Ausnahmen vor. Strafbar ist einmal die Verletzung der Auskunft-, Melde- und Mitwirkungspflichten durch Private (Art. 28), weil diese Pflichten *eine gewisse Transparenz* der Datenbearbeitung garantieren. Werden sie nicht beachtet, so bleibt das Datenschutzgesetz zu einem wesentlichen Teil ohne Wirkung. Strafbar ist ferner, wer im Rahmen seiner Berufstätigkeit mit geheimen, besonders schützenswerten Personendaten zu tun hat und diese unbefugterweise bekanntgibt (Art. 29). Hier soll das Vertrauen der betroffenen Person, die einen Berufstätigen wegen seiner Fachkenntnisse in Anspruch nimmt und ihm dabei heikle Daten preisgibt, besonders geschützt werden. Schliesslich soll das unbefugte Beschaffen von Daten unter Strafe gestellt werden (Art. 179^{novies} StGB). Die ersten beiden Tatbestände sind als blosse Übertretungsdelikte im Datenschutzgesetz selbst geregelt. Der dritte Tatbestand wird, weil es sich bei ihm um ein Vergehen handelt, das zudem eine gewisse Verwandtschaft zum Dritten Titel des Strafgesetzbuches aufweist, ins Strafgesetzbuch eingefügt. Die Strafverfolgung ist bei allen drei Delikten Sache der Kantone.

Artikel 28 Verletzung der Auskunft-, Melde- und Mitwirkungspflichten

Nach *Absatz 1* wird der private Inhaber einer Datensammlung mit Haft oder mit Busse bestraft, wenn er seiner Auskunftspflicht nach Artikel 5 nicht nachkommt bzw. die Verweigerung nicht im Sinne von Artikel 6 Absatz 2 begründet. Unter Strafe gestellt ist die falsche Auskunft, worunter auch die unvollständige Auskunft fällt, sofern der Bearbeiter den Anschein erweckt, diese sei umfassend. Nicht bestraft wird hingegen, wer behauptet, er sei aufgrund von Artikel 6 nicht zur Auskunft verpflichtet. In solchen Fällen muss im zivilrechtlichen Klageverfahren entschieden werden, ob die Auskunftsverweigerung oder -einschränkung zu Recht erfolgt ist. Strafbar macht sich hingegen, wer fälschlicherweise behauptet, er habe keine Informationen über die um Auskunft ersuchende Person. *Vorsätzlich* handelt der Datenbearbeiter, wenn er um die Unrichtigkeit oder Unvollständigkeit seiner Auskunft weiss. Erteilt der Bearbeiter ohne nähere Prüfung eine Auskunft, obschon er weiss, dass diese möglicherweise falsch ist, handelt er *eventualvorsätzlich*. Die Verletzung der Auskunftspflicht ist ein Antragsdelikt; der Täter wird nur verfolgt, wenn derjenige, der um Auskunft ersucht hat, einen Strafantrag gestellt hat.

Von Amts wegen verfolgt werden nach *Absatz 2* Private, die dem Datenschutzbeauftragten registrierpflichtige Datensammlungen und meldepflichtige Datentransfers ins Ausland nicht bekanntgeben oder dabei unrichtige oder unvollständige Angaben machen (Bst. a). Der Vorsatz des Täters muss darin bestehen, die Meldepflicht zu umgehen. Kennt er die diesbezüglichen Vorschriften nicht, so kann er sich auf Gebotsirrtum berufen. Der Richter wird in diesem Fall die Strafe mildern oder von einer Bestrafung Umgang nehmen⁵²⁾. Schliesslich soll der Private bestraft werden, der bei Abklärungen des Datenschutzbeauftragten diesem unrichtige Auskünfte erteilt oder die Mitwirkung verweigert (Bst. b). Die

Bestimmung soll gewährleisten, dass der Datenschutzbeauftragte bei seinen Abklärungen alle nötigen Informationen einholen kann.

Auf eine Unterstellung der Bundesorgane unter diese Strafbestimmung wurde verzichtet, weil in der Verwaltung eine Dienstaufsicht besteht und der fehlbare Beamte anders als der Private mit disziplinarrechtlichen Massnahmen zur Rechenschaft gezogen werden kann. Zudem ist die Aufsicht des Datenschutzbeauftragten im öffentlich-rechtlichen Bereich sehr viel umfassender als gegenüber privaten Datenbearbeitern. Auch wäre es ungewöhnlich, dass im Fall, wo ein Beamter beziehungsweise das betreffende Amt einer andern Bundesbehörde keine Angaben macht, mithin keine Amtshilfe leistet, die ersuchende Behörde, das heisst der Datenschutzbeauftragte, direkt Strafanzeige machen kann. In solchen Streitigkeiten soll vielmehr die übergeordnete Behörde, das heisst letztlich der Bundesrat, entscheiden, ob Amtshilfe geleistet werden muss.

Artikel 29 Verletzung der beruflichen Schweigepflicht

Durch die zunehmende berufliche Spezialisierung, aber auch durch die neuen Informationsbearbeitungsmethoden ist der strafrechtliche Schutz des Berufsgeheimnisses nach Artikel 321 des Strafgesetzbuches lückenhaft geworden. Diese Bestimmung gilt nur für Geistliche, Rechtsanwälte, Verteidiger, Notare, Revisoren und Medizinalpersonen sowie ihr Personal. Die vorliegende Bestimmung will nun in weiteren Berufsbereichen, in denen der Schutz der Vertraulichkeit ebenfalls unerlässlich, aber Artikel 321 des Strafgesetzbuches nicht anwendbar ist, die Schweigepflicht regeln. Von einer Ausdehnung des Anwendungsbereiches des Artikels 321 des Strafgesetzbuches durch die Aufzählung weiterer Berufskategorien wurde im Rahmen dieses Entwurfes abgesehen, denn für die in Artikel 321 des Strafgesetzbuches erwähnten Berufe sehen die kantonalen und eidgenössischen Verfahrensgesetze in der Regel ein Zeugnisverweigerungsrecht vor, das im Rahmen der Datenschutzgesetzgebung nicht ausgedehnt werden soll. Eine Neufassung von Artikel 321 des Strafgesetzbuches wird aber bei der Revision des Allgemeinen Teils des Strafgesetzbuches geprüft.

Nach *Absatz 1* kommen als Täter nur Personen in Frage, die einen Beruf ausüben, bei dem die Kenntnis geheimer und besonders schützenswerter Personendaten unerlässlich ist. Dies trifft beispielsweise auf den Psychologen, den Sozialarbeiter oder den Ehevermittler, nicht aber auf den Coiffeur zu. Letzterem können bei der Ausübung seines Berufs zwar durchaus geheime und sensible Personendaten zur Kenntnis gelangen, darauf angewiesen ist er aber nicht. Da die Strafnorm nicht auf jedermann, sondern nur auf Angehörige bestimmter Berufsgruppen anwendbar ist, handelt es sich beim entsprechenden Tatbestand um ein *echtes Sonderdelikt*. Gegenstand der Tathandlung sind *geheime Personendaten*, die zudem *besonders schützenswert* im Sinne von Artikel 3 Buchstabe e sind. Nach Lehre und Rechtsprechung, die sich namentlich im Zusammenhang mit den Artikeln 162 (Verletzung des Fabrikations- oder Geschäftsgeheimnisses) und 321 (Verletzung des Berufsgeheimnisses) des Strafgesetzbuches herausgebildet haben, sind Daten geheim, wenn sie relativ unbekannt, das heisst weder offenkundig noch allgemein zugänglich sind und die betroffene Person sie aus berechtigtem Interesse geheimhalten will. Nur die vorsätzliche Begehung der Tat ist strafbar. Wer nicht um seine Geheimhaltungspflicht weiss, be-

findet sich in einem Verbotsirrtum im Sinne von Artikel 20 des Strafgesetzbuches. Die Strafe ist Haft oder Busse. Die Verfolgung geschieht nur auf Antrag.

Nach *Absatz 2* wird gleich bestraft, wer als Hilfsperson, das heisst als Angestellter oder Lehrling eines nach Absatz 1 zur Verschwiegenheit Verpflichteten vorsätzlich geheime, besonders schützenswerte Personendaten unbefugt offenbart.

Nach *Absatz 3* dauert der strafrechtliche Schutz auch an, wenn die zur Geheimhaltung Verpflichteten ihren Beruf aufgegeben oder die entsprechende Ausbildung beendet haben.

221.8 Achter Abschnitt: Schlussbestimmungen

Artikel 30 Vollzug

Absatz 1 weist auf die bereits von Verfassung wegen bestehende allgemeine Vollzugsverordnungs-kompetenz des Bundesrates hin.

Die folgenden Absätze sehen zudem Ermächtigungen an den Bundesrat vor, die nicht schon in der allgemeinen Vollzugskompetenz enthalten sind. So hat der Bundesrat nach *Absatz 2* besondere Bestimmungen für die Bearbeitung von Personendaten, die im Bundesarchiv archiviert sind, zu erlassen. Er kann dabei Abweichungen von den Bestimmungen über das Auskunftsrecht (Art. 5 und 6) und über die Bearbeitung besonders schützenswerter Personendaten (Art. 14 Abs. 2 und 16 Abs. 1) vorsehen. Derartige Ausnahmebestimmungen können nötig werden, weil mit der Archivierung der Akten im Bundesarchiv deren Zugänglichkeit vermindert wird. Die riesigen Datenbestände des Bundesarchivs können in der Regel zwar noch nach Personen erschlossen werden, doch ist der hierfür erforderliche Aufwand in vielen Fällen ausserordentlich gross. Im Bundesarchiv befinden sich zudem besonders schützenswerte Daten in grosser Zahl. Für deren Bearbeitung nach Ablauf der in den Archivvorschriften festgelegten Sperrfristen soll nicht in jedem Fall eine ausdrückliche Grundlage in einem formellen Gesetz oder eine vorgängige Bewilligung des Bundesrates notwendig sein.

Nach *Absatz 3* kann der Bundesrat auch für diplomatische und konsularische Vertretungen der Schweiz im Ausland Abweichungen von den Regeln über das Auskunftsrecht vorsehen. Der Grund liegt darin, dass Auskünfte von schweizerischen Vertretungen im Ausland an Ausländer über ihre Daten besondere Empfindlichkeiten wecken und damit das Verhältnis der Schweiz zum betreffenden Staat belasten können.

Absatz 4 enthält drei weitere Rechtsetzungsdelegationen an den Bundesrat. So soll er jene Datensammlungen bestimmen können, die eine *Bearbeitungsordnung* benötigen (Bst. a). Damit wird bei wichtigen Datensammlungen, insbesondere bei Verbundsystemen, die mehreren Zwecken gleichzeitig dienen, sichergestellt, dass die Grundsätze dieses Gesetzes mit Blick auf ein bestimmtes System in die Praxis umgesetzt werden. Bearbeitungsordnungen schaffen zusätzliche Transparenz und damit Überprüfbarkeit der Datenbearbeitungsprozesse. Bei der Bestimmung der Datensammlungen kann sich der Bundesrat auf das bereits bestehende Register der Datensammlungen in der Bundesverwaltung stützen.

Des weitem kann der Bundesrat festlegen, unter welchen Voraussetzungen *Dritte*, namentlich Private, *Daten für Bundesorgane bearbeiten dürfen* und wann ein Bundesorgan für eine andere Verwaltungsstelle oder für Private eine Bearbeitung durchführen darf (Bst. b). Dabei wird er abwägen müssen, wie weit im Rahmen einer öffentlich-rechtlichen Aufgabe Private mit der Bearbeitung von Personendaten betraut werden dürfen und ob mit dem Beizug von Aussenstehenden besondere Datensicherheitsprobleme auftreten können. Schliesslich kann der Bundesrat auch bestimmen, wie Mittel zur Kennzeichnung und Identifikation von Personen verwendet werden dürfen (Bst. c). Mit der stets schneller um sich greifenden Verbreitung der automatischen Datenverarbeitung werden auch die Datensicherheitsmassnahmen, insbesondere die Zugangskontrollen zu den Systemen, immer umfassender. Dabei spielt die Identifikation der zugangsberechtigten Personen eine zentrale Rolle. Die verwendeten Identifikationsmittel werden immer vielfältiger. Die Identität einer Person kann heute nicht mehr nur mit Passwörtern, Badges, Fingerabdrücken, sondern auch etwa aufgrund der Netzhaut oder der Haarqualität festgestellt werden. Derartige Identifikationsprozeduren stellen immer auch einen Eingriff in die Persönlichkeit dar, weshalb der Bundesrat die Befugnis haben soll, sie genauer zu regeln. Des weitem soll auch die Verwendung herkömmlicher Personenkennzeichnungen, wie etwa der AHV-Nummer, eingegrenzt werden können. Die AHV-Nummer wird heute in derart vielen Bereichen eingesetzt, dass, würden die entsprechenden Informationen verknüpft, umfassende Persönlichkeitsbilder entstünden.

In *Absatz 5* wird dem Bundesrat die Kompetenz eingeräumt, in Datenschutzangelegenheiten *völkerrechtliche Verträge* abzuschliessen, sofern diese den Grundsätzen des vorliegenden Entwurfs entsprechen. Für den Abschluss von Verträgen, die vom allgemeinen Datenschutzgesetz abweichen, bleibt die Bundesversammlung zuständig.

Nach *Absatz 6* hat der Bundesrat im Rahmen der Massnahmen für die Gesamtverteidigung auch vorsorglich den Schutz und die Sicherung von Datensammlungen zu regeln. Gewisse Datensammlungen, etwa die Mitgliederverzeichnisse der politischen Parteien, dürfen nicht in die Hände eines Angreifers fallen, weil sonst die betroffenen Personen ernsten Gefahren ausgesetzt sein können.

Artikel 31 Übergangsbestimmungen

Nach *Absatz 1* haben private Datenbearbeiter und Bundesorgane registrierpflichtige Datensammlungen dem Datenschutzbeauftragten innert eines Jahres zu melden.

Sie müssen gemäss *Absatz 2* zudem innert der gleichen Frist die nötigen Vorkehren treffen, damit sie die Auskünfte nach Artikel 5 erteilen können. Effektiv steht den Datenbearbeitern aber mehr als ein Jahr für die Vorbereitung auf dieses Gesetz zur Verfügung, da sie zusätzlich die Zeit zwischen der Verabschiedung und dem Inkrafttreten des Gesetzes nutzen können.

Absatz 3 erlaubt es den Bundesorganen, Sammlungen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen noch während fünf Jahren zu bearbeiten, auch wenn die strengen Anforderungen an die Rechtsgrundlagen nach diesem Gesetz (Art. 14 Abs. 2) nicht erfüllt sind. Der Grund liegt darin,

dass diese Rechtsgrundlagen nicht von einem Tag auf den andern geschaffen werden können.

222 Anhang: Änderung von Bundesgesetzen

222.1 Datenschutz im Arbeitsverhältnis

Artikel 328b (neu) und 362 OR

Mit der Einfügung von *Artikel 328b* in das Obligationenrecht soll der Persönlichkeitsschutz des *Arbeitsvertrags* mit einer spezifischen Datenschutzvorschrift ergänzt werden. Entsprechend ist auch in *Artikel 362* des Obligationenrechts die Liste derjenigen Artikel zu erweitern, die nicht zuungunsten des Arbeitnehmers abgeändert werden dürfen. Die Anpassung des Arbeitsvertragsrechts drängt sich auf, weil wohl kaum ein anderes Rechtsverhältnis Anlass gibt, personenbezogene Daten verschiedenster Art in solch grossem Umfang und während so langer Zeit zu erheben und zu bearbeiten, wie das Arbeitsverhältnis. Auch bedarf der Arbeitnehmer wegen seiner rechtlichen und tatsächlichen Abhängigkeit vom Arbeitgeber eines besonderen Schutzes. Der neue Artikel 328b des Obligationenrechts regelt deshalb in Ergänzung zum Datenschutzgesetz Inhalt und Umfang von Personalinformationen, die Einsichtnahme des Arbeitnehmers in Personaldaten sowie die Auskünfte von Arbeitgebern an Dritte über ihre Arbeitnehmer.

Artikel 328b Absatz 1 beschränkt die Zulässigkeit der Bearbeitung von Personaldaten auf Informationen, die sich auf die Eignung des Arbeitnehmers für das jeweilige Arbeitsverhältnis beziehen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Er stellt damit eine Konkretisierung des Verhältnismässigkeitsgebots von Artikel 4 Absatz 3 des allgemeinen Datenschutzgesetzes dar. Moderne Datenverarbeitungsmethoden können zwar durchaus zu einer Objektivierung von Personalentscheiden und zu einem besseren Schutz der Persönlichkeit des Arbeitnehmers führen. Sie bergen andererseits aber die Gefahr einer weitreichenden Erfassung des Personals bis hin zu einer beinahe vollständigen Durchleuchtung des Arbeitnehmers in sich. Solch umfassende Datenbearbeitungen lassen sich auch durch allfällige Vorteile für die Unternehmung nicht rechtfertigen.

Artikel 328b Absatz 2 legt fest, dass der Arbeitgeber Dritten nur Auskünfte über den Arbeitnehmer erteilen darf, wenn dies gesetzlich vorgesehen ist oder der Arbeitnehmer zugestimmt hat. Im geltenden Arbeitsrecht ist die Schweigepflicht des Arbeitgebers nicht ausdrücklich geregelt. Zwar kann man aus der Regelung über das Arbeitszeugnis auf eine solche Pflicht schliessen, weil der Arbeitnehmer, wenn er mit einem für ihn nachteiligen Arbeitszeugnis rechnet, eine blossе Arbeitsbestätigung verlangen kann (Art. 330a Abs. 2 OR)⁵³. In der Praxis jedoch decken die Arbeitgeber ihre Informationsbedürfnisse durch informelle Rückfragen bei ehemaligen Arbeitgebern. Die gesetzgeberischen Überlegungen bezüglich der Arbeitsbestätigung haben mithin keinen Niederschlag gefunden, und dem Selbstbestimmungsrecht des Arbeitnehmers über seine Personendaten wird nicht genügend Rechnung getragen. Deshalb soll nun im Arbeitsvertragsrecht eine klare Regelung geschaffen werden.

Absatz 3 verweist bezüglich des Auskunftsrechts auf das Datenschutzgesetz und räumt dem Arbeitnehmer zudem das Recht ein, *Einsicht* in seine Personalakten zu verlangen. Die Einblicknahme in ein Personaldossier ist in vielen Fällen einfacher als eine Auskunftserteilung durch den Arbeitgeber und gewährleistet die Vollständigkeit der Auskunft. Entzieht sich der Arbeitgeber der Pflicht zur Einsichtsgewährung, indem er zum Beispiel ein «graues» Personaldossier führt, so erfüllt er den Tatbestand von Artikel 28 Absatz 1 des Datenschutzgesetzes. Hingegen ist der Arbeitgeber berechtigt, aus den in Artikel 6 angeführten Gründen die Auskunft einzuschränken.

222.2 Internationales Privatrecht: Zuständigkeit und anwendbares Recht

Artikel 130 Absatz 3 und 139 Absatz 3 IPRG

Die im Bundesgesetz über das internationale Privatrecht vorgesehenen Kollisionsnormen genügen nicht, um alle Fragen der Zuständigkeit und der Rechtswahl im Zusammenhang mit internationalen privaten datenschutzrechtlichen Auseinandersetzungen befriedigend zu lösen. Das Bundesgesetz über das internationale Privatrecht⁵⁴⁾ muss daher um zwei Datenschutzbestimmungen ergänzt werden, welche *die Zuständigkeit schweizerischer Gerichte* für die Beurteilung von Klagen zur Durchsetzung des Auskunftsrechts und die Frage des *anwendbaren Rechts* betreffen.

Nach *Artikel 130 Absatz 3* können Klagen zur Durchsetzung des Auskunftsrechts gegen den Inhaber einer Datensammlung bei den schweizerischen Gerichten am Wohnsitz des Inhabers der Datensammlung und allenfalls an seinem Aufenthalts- oder Niederlassungsort eingereicht werden. Weil aber jemandem, der Einblick in eine Datensammlung nehmen will, deren Inhaber sich im Ausland aufhält, nicht zugemutet werden kann, sein Auskunftsrecht bei einem fremden Richter durchzusetzen, soll er seine Klage auch beim schweizerischen Gericht am Ort, wo die Datensammlung geführt oder verwendet wird, einreichen können.

Nach *Artikel 139 Absatz 3* des Bundesgesetzes über das Internationale Privatrecht hat die betroffene Person auch die Wahl bezüglich des anwendbaren Rechts. Ansprüche aus einer Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten oder wegen einer Beeinträchtigung des Auskunftsrechts kann sie nach dem Recht, das an ihrem gewöhnlichen Aufenthaltsort gilt, oder nach dem Recht des Staates, in dem die verletzende Handlung ihre Wirkung entfaltet, geltend machen, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste. Die betroffene Person kann aber auch nach dem Recht jenes Staates vorgehen, in dem der Urheber der Verletzung seine Niederlassung oder seinen gewöhnlichen Aufenthalt hat. Dem Bearbeiter wird damit weitgehend die Möglichkeit genommen, sich durch die Wahl seines Domizils zulasten der betroffenen Personen datenschutzrechtliche Vorteile zu verschaffen. Andererseits schränken die Möglichkeiten der Rechtswahl die Voraussehbarkeit für den Bearbeiter ein. Dieses Problem stellt jedoch keine datenschutz-

rechtliche Besonderheit dar, sondern wird im Gefolge der Internationalisierung der Wirtschaft auch in vielen andern Bereichen immer akuter.

222.3 Unbefugtes Beschaffen von Personendaten

Artikel 179^{novies} (neu) Strafgesetzbuch

Der Sachverhalt dieses Artikels ähnelt demjenigen von Artikel 143 des Strafgesetzbuches, wie ihn die Expertenkommission im Vorentwurf über die Änderung der Vermögensdelikte im Strafgesetzbuch vorgeschlagen hat, welcher in den Jahren 1985 und 1986 in die Vernehmlassung gegangen ist. Der Entwurf zu einem Artikel 143 des Strafgesetzbuches schützt aber in erster Linie das Vermögen des Datenbearbeiters und nicht die Persönlichkeit der betroffenen Personen. Verschiedentlich wurde deshalb in der Vernehmlassung zum Vorentwurf über die Änderung der Vermögensdelikte verlangt, dass das unbefugte Beschaffen von Personendaten generell, d. h. namentlich auch unter Berücksichtigung des Persönlichkeitsschutzes, geregelt werden solle. Deshalb sollen nun mit der Schaffung des Datenschutzgesetzes zugleich die Bestimmungen des Strafgesetzbuches über die strafbaren Handlungen gegen die Geheim- oder Privatsphäre (Art. 179 ff.) um den Tatbestand des unbefugten Beschaffens von besonders schützenswerten Personendaten ergänzt werden.

Tatobjekt in Artikel 179^{novies} sind besonders schützenswerte Personendaten, die nicht frei zugänglich sind. Welche Daten besonders schützenswert sind, ergibt sich aus Artikel 3 Buchstabe e. Nicht frei zugänglich sind die Daten, wenn sich der Täter bei deren Beschaffung in Räumlichkeiten begibt oder sich an Anlagen zu schaffen macht, zu denen er keine Zutrittsberechtigung hat. Die Beschaffung ist in verschiedensten Formen möglich. Dazu gehört die Entnahme ganzer Dossiers oder von Teilen davon aus einer Aktenablage oder das Kenntnisnehmen von Daten aus automatischen Systemen durch Manipulationen an einer Dateneinstationsstation oder durch Anzapfen von Datenübertragungsleitungen. Nur die vorsätzliche Tat ist strafbar. Artikel 179^{novies} ist Antragsdelikt, wobei sowohl der Datenbearbeiter als auch die betroffene Person einen Strafantrag stellen können. Das unbefugte Beschaffen von Personendaten soll als Vergehen mit Gefängnis oder Busse bestraft werden.

222.4 Datenschutz in der medizinischen Forschung

222.41 Verfassungsrechtliche Rahmenbedingungen

Medizinische Forschung wird vor allem an Universitäten und an Spitälern (öffentlichen und privaten) betrieben; die Forschungstätigkeit des Bundes ist dagegen eher von untergeordneter Bedeutung. Das bestehende Verfassungsrecht erlaubt es nun aber nicht, die Datenbearbeitung in all diesen Forschungsbereichen umfassend zu regeln. Während sich datenschutzrechtliche Regelungen für die private Forschung und für jene des Bundes auf die Artikel 64 und 85 Ziffer 1 BV stützen lassen, hat der Bund keine Kompetenz, im Bereich des kantonalen öffentlichen Rechts – wozu auch Universitäten und kantonale sowie kom-

munale Spitäler gehören – umfassende Datenschutzregelungen zu erlassen. In diesen Fällen ist allenfalls vorhandenes kantonales Datenschutzrecht massgeblich. Daran ändert auch Artikel 27^{sexies} BV, der Forschungsartikel, nichts. Er verleiht dem Bund einzig die Befugnis, die wissenschaftliche Forschung zu fördern, hält jedoch an der Kompetenzverteilung im Hochschulwesen und im Forschungsbereich grundsätzlich fest. Das Hochschulwesen aber ist – abgesehen von den Technischen Hochschulen – der gestaltenden Einwirkung durch den Bund entzogen⁵⁵). Auch Artikel 69 BV, der dem Bund die Kompetenz zur Bekämpfung übertragbarer oder stark verbreiteter oder bösartiger Krankheiten erteilt, stellt keine ausreichende Verfassungsgrundlage für eine bundesrechtliche Datenschutzregelung im kantonalen Bereich dar. Von allen Forschungsvorhaben bezieht sich nur ein Teil auf diese Krankheitskategorien.

Eine für jegliche medizinische Forschungstätigkeit geltende Datenschutzregelung lässt sich allerdings zu einem wesentlichen Teil auf die Strafrechtskompetenz von Artikel 64^{bis} BV abstützen. Soweit nämlich nur die Datenweitergabe geregelt werden soll, besteht ein enger sachlicher Zusammenhang mit den Berufsgeheimnissen. Für die Regelung der Berufsgeheimnisse bzw. die Festlegung strafrechtlicher Sanktionen wegen deren Verletzung ist der Bund aufgrund von Artikel 64^{bis} BV zuständig. Mit dem Erlass von Artikel 321 des Strafgesetzbuches hat er von dieser Kompetenz Gebrauch gemacht. Wenn man die Berufsgeheimnisse unter datenschutzrechtlichen Gesichtspunkten eingehender regeln will, steht dem verfassungsrechtlich nichts entgegen. Deshalb erscheint es zulässig, für die Verletzung der Berufsgeheimnisse unter bestimmten Voraussetzungen einen neuen Rechtfertigungsgrund vorzusehen, der darin besteht, dass die entsprechenden Daten für die medizinische Forschung benötigt werden.

Anders verhält es sich in bezug auf eine allfällige Regelung der Datenbeschaffung und -bearbeitung. In diesen Fällen ist im Gegensatz zur Datenweitergabe das Berufsgeheimnis nicht notwendigerweise betroffen. Würden Datenbearbeitungsgrundsätze (z. B. Aufbewahrungsregeln) aufgestellt bzw. für Verstösse gegen Datenbearbeitungsgrundsätze strafrechtliche Tatbestände geschaffen, so würde eine neue Kategorie von Handlungen als prinzipiell strafwürdig erklärt. Angesichts der Verschiedenartigkeit der denkbaren Verletzungen sollen aber Verstösse gegen Datenbearbeitungsgrundsätze nicht generell pönalisiert werden, sondern nur, wo sie besonders schwerwiegend sind bzw. die Durchsetzung des Datenschutzes insgesamt in Frage stellen (vgl. Art. 28 und 29 DSGVO sowie Art. 179^{novies} StGB). Auf jeden Fall soll nicht die Strafrechtskompetenz der verfassungsrechtlich massgebliche Anknüpfungspunkt für die generelle Regelung der Datenbearbeitung in der medizinischen Forschung sein. Hingegen kann der Bund gestützt auf die Strafrechtskompetenz auch organisatorische Regelungen über eine Kommission erlassen, welche die Forschungsvorhaben unter datenschutzrechtlichen Gesichtspunkten zu überprüfen hat. Zwar ist die Organisation der Strafrechtspflege grundsätzlich Sache der Kantone und ist bis anhin aufgrund der Strafrechtskompetenz des Bundes keine vergleichbare Instanz errichtet worden. Wo aber organisatorische Vorkehren notwendig sind, damit eine materielle Regelung des Strafrechts richtig und rechtsgleich angewendet wird, kann der Bund die entsprechenden Normen erlassen⁵⁶). Im übrigen erscheint die vorgeschlagene Regelung kompetenzrechtlich auch darum unbedenklich,

weil die Kommission nicht dazu berufen ist, als eigentliches Organ der Strafrechtspflege tätig zu sein, sondern allein über die Zulässigkeit einer Offenbarung eines Berufsgeheimnisses entscheiden muss.

222.42 Regelungskonzept im allgemeinen

Die verfassungsrechtlich gebotene Beschränkung der Regelung auf die Datenweitergabe ist vertretbar. Denn bei der Datenweitergabe muss entschieden werden, unter welchen Voraussetzungen ein Berufsgeheimnis über medizinische Personendaten gelüftet werden darf. Etwas weniger vordringlich, doch an sich ebenfalls erwünscht ist die Regelung der Bearbeitung von Medizinaldaten, die nicht über die Offenbarung von Berufsgeheimnissen, namentlich nicht durch die Weitergabe von Krankengeschichten durch behandelnde Ärzte erhoben werden. Dies vor allem auch darum, weil auf diese Datenbearbeitung, wenigstens soweit die Forschung von Institutionen des Bundes oder von privaten Forschungsstellen durchgeführt wird, die Grundsätze des Datenschutzgesetzes Anwendung finden werden. Für Universitäts- und Kantonsspitäler gilt allenfalls vorhandenes kantonales Datenschutzrecht. Die vorgeschlagene Regelung dürfte deshalb insgesamt zu einer wesentlichen Verbesserung des Schutzes von Gesundheitsdaten führen.

In Artikel 19 des Datenschutzgesetzes ist ein Forschungsprivileg vorgesehen. Diese Regelung soll der nicht personenbezogenen Forschung, Planung und Statistik einen privilegierten Umgang mit Personendaten ermöglichen: Personendaten dürfen unter weniger restriktiven Voraussetzungen an Dritte weitergegeben werden, wenn diese sie nicht zu personenbezogenen Zwecken, namentlich zu Forschungszwecken, verwenden. Allfällige Geheimhaltungspflichten bleiben jedoch vorbehalten. Wo aber die Forschung mit einem Berufsgeheimnis in Konflikt gerät, kommen diese privilegierenden Sonderregelungen des Datenschutzgesetzes nicht zur Anwendung. Solche Fälle werden allein von Artikel 321^{bis} des Strafgesetzbuches erfasst.

222.43 Erläuterungen zu Artikel 321^{bis} des Strafgesetzbuches sowie den Artikeln 26 Absatz 3 und 27 Absatz 1 Buchstabe c des Datenschutzgesetzes

Artikel 321^{bis} StGB Berufsgeheimnis in der medizinischen Forschung

Absatz 1 Neuer Rechtfertigungsgrund für die Offenbarung eines Berufsgeheimnisses

Die Bestimmung erweitert die in Artikel 321 des Strafgesetzbuches erwähnten Rechtfertigungsgründe für die Verletzung der Berufsgeheimnisse. Als neuer Rechtfertigungsgrund wird die Bewilligung zur Offenbarung des Berufsgeheimnisses einer Sachverständigenkommission vorgesehen. Diese Bewilligung für eine straflose Verletzung eines Berufsgeheimnisses soll sich jedoch nur auf die Forschung im Bereich der Medizin oder des Gesundheitswesens beziehen können. Im Vordergrund steht dabei die Forschung für eine wirksamere Bekämpfung

fung schwerer oder häufiger Leiden. Aber auch im öffentlichen Gesundheitswesens werden Forschungsvorhaben durchgeführt, an denen ein grosses öffentliches Interesse besteht. So gehören beispielsweise Erhebungen über den Gesundheitszustand der Bevölkerung zu den unentbehrlichen Grundlagen einer sinnvollen Spitalplanung. Auch für wissenschaftliche Untersuchungen über Nebenwirkungen von Medikamenten oder für wissenschaftliche Dokumentationen und Statistiken über Langzeiterfolge bestimmter Therapien kann die Kommission eine Bewilligung erteilen. Hingegen soll sie für reine Marktforschungszwecke die Schweigepflicht nicht aufheben können.

Die Zweckdefinition steckt lediglich den Rahmen für eine zulässige Aufhebung der Berufsgeheimnisse ab. Die Schaffung genauerer Kriterien wird Aufgabe der Sachverständigenkommission sein. Der neue Rechtfertigungsgrund wird vor allem für Ärzte und Zahnärzte sowie ihre Hilfspersonen von Bedeutung sein, in Einzelfällen auch für Apotheker und Hebammen, kaum jedoch für die anderen nach Artikel 321 StGB einer Schweigepflicht unterworfenen Berufsgruppen.

Eine Schweigepflicht im Sinne von Artikel 321 des Strafgesetzbuches besteht grundsätzlich auch über den Tod des Geheimnisherrn hinaus⁵⁷⁾. Verletzt der Geheimnispflichtige das Berufsgeheimnis erst nach dem Tode des Geheimnisherrn, so bleibt er mangels Strafantrag aber zumeist straflos (Art. 28 StGB). Die Bewilligung der Sachverständigenkommission einer Offenbarung des Berufsgeheimnisses kann gleichwohl auch im Zusammenhang mit Daten von Verstorbenen von Bedeutung sein, da eine rechtswidrige Verletzung etwa des Arztgeheimnisses auch disziplinar- oder zivilrechtliche und in Ausnahmefällen selbst strafrechtliche Folgen haben kann⁵⁸⁾.

Die Erlaubnis zur Offenbarung eines Berufsgeheimnisses zu Zwecken der medizinischen Forschung kann neben dem Berechtigten allein die Kommission erteilen. Die Bestimmung bringt für diese Forschungstätigkeit eine abschliessende bundesrechtliche Regelung, die als Spezialregelung Artikel 321 Ziffer 2 des Strafgesetzbuches vorgeht, wonach die vorgesetzte Behörde oder Aufsichtsbehörde eine Bewilligung zur Offenbarung des Berufsgeheimnisses erteilen kann.

Auch in Fällen, in denen die Kommission eine Bewilligung erteilen könnte oder diese bereits erteilt hat, ist ein Widerspruch des Betroffenen zu respektieren. Ein Berufsgeheimnis, namentlich das Arztgeheimnis, soll in keinem Fall gegen seinen ausdrücklichen Willen offenbart werden. Hat ein Arzt aufgrund einer Kommissionsbewilligung bereits Daten bekanntgegeben und untersagt der Betroffene nachträglich diese Bekanntgabe, so dürfen die Forscher nicht weiter mit den entsprechenden Personendaten arbeiten.

Nach Artikel 29 des Datenschutzgesetzes soll bestraft werden, wer einen Beruf ausübt, der die Kenntnis geheimer, besonders schützenswerter Personendaten erfordert, und solche Daten unbefugt bekannt gibt. Wer solche Daten aber aufgrund einer Bewilligung der Sachverständigenkommission offenbart, macht sich, gleich wie wenn er mit Einwilligung des Betroffenen handelt, nicht strafbar.

Absatz 2 Voraussetzungen für eine Bewilligung der Sachverständigenkommission

Für eine Bewilligung der Sachverständigenkommission müssen bestimmte Voraussetzungen kumulativ erfüllt sein.

Die Bewilligung darf nur erteilt werden, wenn die Forschung nicht mit anonymisierten Daten durchgeführt werden kann (Bst. a). Soweit ein Forschungsprojekt demnach nicht auf Angaben angewiesen ist, aufgrund derer sich die betroffenen Personen identifizieren lassen, soll die Sachverständigenkommission keine Offenbarung des Berufsgeheimnisses bewilligen. Eine Bewilligung durch die Kommission setzt zudem voraus, dass es unmöglich oder unverhältnismässig schwierig wäre, den Entscheid der Betroffenen einzuholen (Bst. b). Schwierigkeiten dürften vor allem bei retrospektiven Untersuchungen auftreten, wenn die entsprechenden Patienten nicht mehr leben oder nicht auffindbar sind oder wenn sie sich, etwa bei Forschungsvorhaben einer grösseren Klinik, auf ein weites, womöglich die Landesgrenzen überschreitendes Einzugsgebiet verteilen. Die Hinderungsgründe müssen nicht absolut zwingend sein: Es genügt, dass der Versuch, die Einwilligung der Betroffenen zu erlangen, einen unverhältnismässig grossen Aufwand erfordern würde, der das Forschungsvorhaben scheitern liesse. Auch hier wird es Sache der Kommission sein, die Grenzen genauer abzustechen. Schliesslich müssen die Forschungsinteressen gegenüber den Geheimhaltungsinteressen überwiegen (Bst. c).

Damit werden qualitative Anforderungen an das Forschungsprojekt gestellt, zu dessen Gunsten ein Berufsgeheimnis durchbrochen werden soll. Die Kommission wird die konkreten Umstände des Einzelfalls abschätzen und gewichten müssen. Sie wird etwa darauf abstellen, in welchem Mass der Forscher auf die Daten angewiesen ist, welche Behandlungschancen und medizinischen Fortschritte das Forschungsprojekt eröffnet, für wieviele Personen die Forschungsergebnisse von Nutzen sein können, welchen Stellenwert das Forschungsprojekt für das öffentliche Gesundheitswesen hat. Weitergehende generelle Regeln lassen sich hier nicht aufstellen. Sicherlich erfüllen aber Forschungsprojekte, die vorwiegend Selbstzweck sind oder mit denen ausschliesslich Gewinninteressen verfolgt werden, diese Voraussetzung nicht.

Absatz 3 Auflagen und Veröffentlichung der Bewilligung

Die Sachverständigenkommission wird den Bewilligungsentscheid mit Auflagen zur Sicherung des Datenschutzes verbinden. Die Ausführungsverordnung des Bundesrates (Abs. 5) wird die möglichen Auflagen umschreiben müssen. In Frage kommen etwa Auflagen betreffend den Zweck, zu dem die Daten weitergegeben werden dürfen, Art und Umfang der Daten, die Personen, welche vom Berufsgeheimnis entbunden werden, die Art der Datenauswertung sowie den Kreis der Personen, die Zugang zu den Daten erhalten.

Mit der Veröffentlichung der Kommissionsbewilligung sollen Betroffene auf die geplante Datenweitergabe aufmerksam gemacht werden. Der Einzelne hat aufgrund dieser Mitteilung nochmals die Möglichkeit, z. B. seinem Arzt kundzutun, dass er eine Weitergabe seiner Patientendaten untersage.

Absatz 4 Generelle Bewilligungen oder andere Vereinfachungen

In Fällen, in denen die schutzwürdigen Interessen der betroffenen Personen nicht gefährdet sind und die Personendaten zu Beginn der Forschung anonymisiert werden, soll die Sachverständigenkommission *generelle Bewilligungen* erteilen können. Im Vordergrund stehen das Bedürfnis der Kliniken und medizinischen Universitätsinstitute, zu Behandlungszwecken erhobene Daten auch für die interne Forschung zu verwenden, namentlich bei der Aus- und Weiterbildung des Personals. Dem medizinischen Personal soll deshalb auch Einsicht in Krankengeschichten gewährt werden können, die Patienten anderer Spitalabteilungen betreffen. Für solche Fälle, in denen das Berufsgeheimnis von Artikel 321 des Strafgesetzbuches grundsätzlich ebenfalls gilt, soll die Sachverständigenkommission nicht den eigentlichen Geheimnispflichtigen, sondern der Klinik- oder Institutsleitung eine generelle Bewilligung erteilen können. Die Einzelheiten sollen vom Bundesrat in einer Verordnung geregelt werden. Wo aber die Identität der betroffenen Personen nicht nur bei der Datenbeschaffung erkennbar ist, sondern auch für die weitere Bearbeitung der Daten benötigt wird, muss eine ordentliche Bewilligung der Sachverständigenkommission eingeholt werden.

Die bundesrätliche Verordnung kann darüber hinaus vorsehen, dass solch generelle Klinik- und Institutsbewilligungen nicht nur für interne Forscher, sondern auch für *Doktoranden* gelten. Damit kann Doktoranden unter den genannten Voraussetzungen - keine Gefährdung der Interessen der Betroffenen und sofortige Anonymisierung - ohne rechtswidrige Verletzung der ärztlichen Schweigepflicht Einsicht in Krankengeschichten gewährt werden. Möglicherweise muss die generelle Bewilligung mit einer Pflicht zur Meldung der einzelnen Forschungsvorhaben ergänzt werden, damit die Kommission prüfen kann, ob der Rahmen der generellen Bewilligung respektiert wird.

Eine Vereinfachung des Bewilligungsverfahrens drängt sich zudem im Zusammenhang mit medizinischen *Registern*, namentlich den Krebsregistern auf. Der Bundesrat kann aufgrund von Absatz 4 auch für diese Fälle eine generelle Bewilligung vorsehen. So kann für die Weitergabe von nicht anonymisierten Daten an ein Register der für das Register zuständigen Stelle im voraus eine generelle Bewilligung erteilt werden. Die Sachverständigenkommission muss diese Bewilligung mit Auflagen insbesondere betreffend die Verschlüsselung und die Aufbewahrung der nicht anonymisierten Daten verbinden sowie den Kreis der Personen festlegen, die Zugang zu diesen Daten erhalten sollen.

Auch für andere Fälle kann der Bundesrat gestützt auf Absatz 4 Vereinfachungen vorsehen. So ist etwa denkbar, dass eindeutige Fälle mit Präsidialentscheid oder von einem Ausschuss der Kommission entschieden werden.

Bewusst werden auf Gesetzesstufe die Vereinfachungsmöglichkeiten nicht abschliessend festgelegt. Da schwer abzuschätzen ist, wie viele Gesuche bei der Sachverständigenkommission jährlich eingehen und welcher Art sie sein werden, müssen flexible Lösungen möglich sein. Während der ersten Jahre muss die Kommission in einer Versuchsphase die zweckmässigste Organisationsform testen können.

Absatz 5 Organisation der Sachverständigenkommission und Verfahren

Die Sachverständigenkommission wird vom Bundesrat eingesetzt. Es handelt sich bei ihr um eine *eigenössische Behörde*. Der Entwurf verzichtet darauf, kantonale Bewilligungsinstanzen vorzusehen. Eine solche Lösung würde zwar mit der föderalistischen Struktur des Landes in Einklang stehen, sie wäre aber in der Praxis kaum zu verwirklichen oder mit schwerwiegenden Nachteilen verbunden. So könnte die Zuständigkeit für die Bewilligung nicht allein bei demjenigen Kanton liegen, in dem die Forschungstätigkeit stattfinden soll, sondern sie müsste sich auch auf diejenigen Kantone erstrecken, in denen die Daten erhoben werden sollen oder in denen die Berechtigten ihren Wohnsitz haben. Dasselbe Forschungsprojekt, etwa einer Universitätsklinik mit grossem Einzugsgebiet, müsste unter Umständen einer Vielzahl von kantonalen Kommissionen zur Bewilligung unterbreitet werden. Das wäre auch dann unpraktikabel, wenn jeder Kanton über die personellen Ressourcen verfügte, deren es für die Bildung der genannten Kommission bedarf. Überdies ist nicht auszuschliessen, dass verschiedene Kommissionen, mindestens was die Modalitäten der Bewilligung anbelangt, zu unterschiedlichen Ergebnissen kämen. Dies würde die Forschungsarbeit behindern und zu Rechtsunsicherheiten führen. Die vorgeschlagene Regelung lässt jedoch die Möglichkeit offen, die Sachverständigenkommission in Unterkommissionen mit regionaler Zuständigkeit für einzelne Landesteile oder Sprachgebiete aufzugliedern. Die praktischen Erfahrungen der Kommission werden zeigen, ob die Vorzüge einer föderalistischen Lösung auf diese Weise realisiert werden sollen.

Eine Bewilligung der Sachverständigenkommission soll unabhängig von eventuellen anderen Verfahren im Zusammenhang mit einem Forschungsprojekt, wie etwa vor dem Nationalfonds oder einer Ethischen Kommission, eingeholt werden können. Ein Bewilligungsverfahren vor der Sachverständigenkommission muss gleichzeitig mit solchen Verfahren laufen können, damit keine unerwünschten Verzögerungen entstehen.

Die *Organisation* der Kommission soll in einer Verordnung des Bundesrates geregelt werden. Von besonderer Bedeutung wird dabei die personelle Zusammensetzung der Kommission sein. Sie soll aus unabhängigen Mitgliedern bestehen, und die Interessen der medizinischen Forschung, der Patienten und der behandelnden Ärzte müssen darin in gleicher Weise vertreten sein. Zudem werden Kommissionsmitglieder mit richterlicher Erfahrung nötig sein.

Das Verfahren vor der Sachverständigenkommission richtet sich grundsätzlich nach dem Bundesgesetz über das Verwaltungsverfahren. Die Ausführungsverordnung des Bundesrates wird zusätzlich etwa vorsehen, welche Angaben ein Bewilligungsgesuch zu enthalten hat.

Die Kommission ist weisungsunabhängig. Administrativ wird sie dem Eidgenössischen Departement des Innern zugeordnet werden. Das Sekretariat soll dem Bundesamt für Gesundheitswesen übertragen werden.

Absatz 6 Forschungsgeheimnis

Jeder, der für die Forschung im Bereich der Medizin oder des Gesundheitswesens Berufsgeheimnisse bearbeitet, soll seinerseits einer Schweigepflicht unter-

stehen. Deshalb wird auch Forschern und ihren Hilfspersonen, soweit sie von behandelnden Ärzten oder allenfalls andern der beruflichen Geheimhaltungspflicht unterstehenden Personen unter Offenbarung des Berufsgeheimnisses Personendaten erhalten haben, eine Schweigepflicht auferlegt. Wenn schon durch den Entscheid einer Behörde die Offenbarung eines Geheimnisses unabhängig von der Einwilligung des Berechtigten zugunsten des Forschers zugelassen wird, so muss andererseits sichergestellt werden, dass die unbefugte Mitteilung an weitere Dritte unterbleibt. Bei der Schweigepflicht für die Forscher soll nicht unterschieden werden zwischen Angaben, welche die Ärzte aufgrund einer Bewilligung durch die Sachverständigenkommission weitergegeben haben, und solchen, die sie mit Einwilligung der Berechtigten offenbart haben. In beiden Fällen steigt durch die Verwendung der Personendaten in der Forschung das Risiko ihrer weiteren Verbreitung erheblich. Zudem wäre eine solche Differenzierung in der Praxis kaum durchführbar.

Damit erweitert Absatz 6 den Personenkreis, für den die Strafdrohung von Artikel 321 des Strafgesetzbuches gilt. Zugleich findet der vorgeschlagene Rechtfertigungsgrund aber auch auf diese neuen Träger eines Berufsgeheimnisses, die Forscher, Anwendung. Sie können mit Einwilligung der betroffenen Person oder mit Bewilligung der Sachverständigenkommission Gesundheitsdaten weiteren Forschern bekanntgeben.

Soweit Forscher die Daten für ihre Forschungsvorhaben aber direkt bei den Berechtigten und unabhängig etwa von einer ärztlichen Behandlung erheben, erscheint es nicht gerechtfertigt, sie einem entsprechenden Berufsgeheimnis zu unterstellen. Zwischen dem Forscher und seiner Auskunftsperson besteht nicht das gleiche Vertrauensverhältnis wie etwa zwischen Arzt und Patient. Hier wird der Straftatbestand der Verletzung der beruflichen Schweigepflicht (Art. 29 DSG) zur Anwendung kommen.

Artikel 26 Absatz 3 DSG Datenschutzbeauftragter

Als Hauptverantwortlicher für die Verwirklichung des Datenschutzes ist der Datenschutzbeauftragte in besonderem Mass prädestiniert, die Kommission zu beraten. Er kann auch auf eine gewisse «*unité de doctrine*» zwischen allgemeinem Datenschutzrecht und dem Datenschutz in der medizinischen Forschung hinwirken. Zudem soll er auch hier eine Kontrollfunktion übernehmen. Der Datenschutzbeauftragte hat für seine Beratungs- und Kontrolltätigkeit dieselben Informationsbeschaffungsrechte wie für seine Aufsichtstätigkeit nach Artikel 24 Absatz 3 des Datenschutzgesetzes. Im übrigen werden die Kontrollmassnahmen in der Ausführungsverordnung des Bundesrates näher zu regeln sein. Vor allem muss die Zusammenarbeit zwischen der Sachverständigenkommission und dem Datenschutzbeauftragten geordnet werden: Die Sachverständigenkommission wird den Datenschutzbeauftragten über ihre Bewilligungen und die darin gemachten Auflagen informieren. Stellt der Datenschutzbeauftragte fest, dass Auflagen nicht eingehalten werden, so hat er seinerseits die Kommission darauf aufmerksam zu machen. Weiter kann in der Ausführungsverordnung vorgesehen werden, dass der Präsident den Gesuchsteller in solchen Fällen nochmals auffordert, sich an die Auflagen des Bewilligungsentscheides zu halten, und ihm gleichzeitig den Widerruf der Bewilligung androht. Zudem besteht die

Möglichkeit, eine entsprechende Verfügung mit einer Strafandrohung zu versehen (Art. 292 StGB).

Schliesslich soll der Datenschutzbeauftragte Verfügungen der Sachverständigenkommission mit Beschwerde bei der Datenschutzkommission anfechten können. Der Datenschutzbeauftragte kann sich so auch vor der Datenschutzkommission nochmals für die Interessen der Betroffenen einsetzen. Hingegen erscheint es nicht nötig, dem Datenschutzbeauftragten auch die Legitimation für die Verwaltungsgerichtsbeschwerde vor dem Bundesgericht zuzuerkennen.

Artikel 27 Absatz 1 Buchstabe c DSG Rechtsmittel

Gegen die Entscheide der Sachverständigenkommission soll nicht direkt die Verwaltungsgerichtsbeschwerde zulässig sein, sondern dem Bundesgericht eine Rekurskommission vorgeschaltet werden. Dies entspricht dem bei der Revision des Bundesgesetzes über die Organisation der Bundesrechtspflege vorgesehenen Konzept für die Entlastung des Bundesgerichts. Dieser Rechtsmittelweg drängt sich umso mehr auf, als mit dem allgemeinen Datenschutzgesetz eine besondere Rekurskommission für Fragen des Datenschutzes eingesetzt wird.

222.5 Änderung des Bundesgesetzes über die Bundesstrafrechtspflege

Nach seinem Artikel 2 Absatz 2 Buchstabe e findet das Datenschutzgesetz keine Anwendung auf Strafverfahren, mithin auch nicht auf Verfahren nach dem Bundesgesetz vom 15. Juni 1934 über die Bundesstrafrechtspflege (BStP). Der Grund liegt, wie bereits erwähnt, darin, dass der Bundesstrafprozess selbst schon gewisse Garantien betreffend die Erhebung, Verwendung und Weitergabe der Personendaten vorsieht (z. B. die Bestimmungen über die Vernehmung des Beschuldigten, Art. 39 ff.). Auch müssen die Informationsrechte der an einem Bundesstrafverfahren beteiligten Personen in den einzelnen Verfahrensstadien notwendigerweise verschieden ausgestaltet sein. Eine zusätzliche Anwendung der allgemeinen Datenschutzregeln würde unter diesen Umständen das strafprozessuale Verfahren erschweren und unübersichtlich machen.

Der Bundesstrafprozess ist zwar in den letzten Jahren verschiedentlich revidiert worden. Dabei wurde namentlich die richterliche Kontrolle strafprozessualer Handlungen ausgebaut. Die materiellen Grundsätze des Strafprozessrechts sind jedoch in den letzten 50 Jahren dieselben geblieben. Das bedeutet unter anderem, dass für das gerichtspolizeiliche Ermittlungsverfahren eigentliche Normen über die Datenbearbeitung bis heute fehlen. Da polizeiliche Informationen häufig besonders schützenswerte Personendaten enthalten, soll diese Lücke nun geschlossen werden. Der Bundesstrafprozess wird demzufolge mit Bestimmungen über die Rechtshilfe, die Erhebung polizeilicher Daten, deren Weitergabe und Vernichtung ergänzt; zudem wird ein Auskunftsrecht für die betroffenen Personen vorgesehen.

Zu diesen datenschutzrechtlichen Bestimmungen kommen einige Vorschriften über *polizeiliche Zwangsmassnahmen* dazu, das heisst Vorschriften über die Durchsuchung und Untersuchung von Personen sowie die erkennungsdienstliche Behandlung. Weil diese Untersuchungshandlungen die Persönlichkeits-

rechte der Betroffenen ebenfalls beeinträchtigen können, sollen die Voraussetzungen für ihre Anwendung gesetzlich umschrieben und ihre Überprüfung durch die Anklagekammer des Bundesgerichts ermöglicht werden. Wenn man bei den Datenbearbeitungen strengen Legalitätsmassstäben folgt, müssen diese auch für die Zwangsmassnahmen gelten. Die vorgeschlagenen Bestimmungen lehnen sich an kantonale Vorbilder an.

Damit werden alle schweren Eingriffe in die persönliche Freiheit abschliessend aufgezählt und gesetzlich verankert. Hingegen können leichtere Eingriffe im Ermittlungsverfahren nach wie vor auf die Generalklausel von Artikel 102 abgestützt werden. Vorbehalten bleibt der polizeiliche Schusswaffengebrauch, für den besondere Regeln gelten⁵⁹⁾.

Auf eine entsprechende Änderung des Militärstrafprozesses wurde verzichtet; im Militärstrafverfahren hat die Ermittlungstätigkeit nicht die gleiche Bedeutung, da das Militärstrafverfahren fast von Anfang an ein Verfahren vor dem Untersuchungsrichter, das heisst ein gerichtliches Verfahren ist.

Artikel 26^{bis}

Die gerichtspolizeilichen Organe des Bundes sind für die Erfüllung ihrer Aufgaben in besonderem Masse auf die Mitwirkung anderer Verwaltungsstellen in Bund, Kantonen und Gemeinden angewiesen. Deshalb soll die Rechtshilfe für das gerichtspolizeiliche Ermittlungsverfahren ausdrücklich geregelt werden. Die Bestimmung ist in Anlehnung an Artikel 30 des Bundesgesetzes über das Verwaltungsstrafrecht konzipiert. Sie stellt für die Verwaltungsbehörden des Bundes eine Spezialnorm zu Artikel 16 des allgemeinen Datenschutzgesetzes dar und geht diesem vor.

In *Absatz 1* wird eine *generelle Rechtshilfepflicht* zugunsten der Strafverfolgungsbehörden des Bundes vorgesehen. Die Pflicht gilt für alle Organe des Bundes, der Kantone und der Gemeinden. Sie umfasst die Erteilung von Auskünften und die Gewährung von Akteneinsicht. Dazu gehört auch die Edition von Unterlagen oder Gegenständen, die als Beweismittel von Bedeutung sein können (vgl. Art. 65 BStP).

Die Pflicht zur Rechtshilfe ist indessen keine absolute. Nach *Absatz 2* kann ein Organ die Rechtshilfe verweigern oder einschränken, wenn wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person dies verlangen (Bst. a) oder ein Berufsgeheimnis es gebietet (Bst. b). Diese Bestimmung entspricht im wesentlichen der allgemeinen Regelung im Datenschutzgesetz (Art. 16 Abs. 3 DSG).

Entsprechend der Regelung im Verwaltungsstrafrecht gelten nach *Absatz 3* für die mit öffentlich-rechtlichen Aufgaben betrauten Organisationen die gleichen Rechtshilfepflichten wie für Behörden.

Nach *Absatz 4* sollen Meinungsverschiedenheiten über die Rechtshilfe innerhalb der Bundesverwaltung entweder vom übergeordneten Departement oder – wenn die betreffenden Behörden nicht im gleichen Departement eingegliedert sind – vom Bundesrat entschieden werden. Besteht die Meinungsverschiedenheit zwischen Bundes- und kantonalen Behörden, so soll die Anklagekammer des Bundesgerichts entscheiden, welche bereits für Anstände zwischen kantona-

len Behörden zuständig ist (Art. 357 StGB und Art. 252 BStP). In jenen seltenen Fällen schliesslich, wo sich gerichtliche Instanzen und Verwaltungsbehörden des Bundes über das Bestehen einer Rechtshilfepflicht uneins sind, soll eine Lösung auf dem Wege eines Meinungsaustausches zwischen Bundesrat und Bundesgericht gefunden werden.

Absatz 5 verweist auf weitere Rechtshilfebestimmungen im Strafgesetzbuch und im Gesetz über die Organisation der Bundesrechtspflege, die ergänzend Anwendung finden.

Artikel 52

Da im neu vorgeschlagenen Artikel 105^{bis} die Beschwerdemöglichkeiten gegen Zwangsmassnahmen insgesamt geregelt werden, ist der zweite Satz von Absatz 2 des Artikel 52 nicht mehr nötig und kann aufgehoben werden.

Artikel 64^{bis}

Die Bestimmung unterstellt die Tätigkeit der Bundesstrafbehörden einschliesslich der polizeilichen Organe datenschutzrechtlichen Grundsätzen. Geregelt werden die Beschaffung, die Berichtigung und die Vernichtung der Daten. Die Bestimmung erstreckt sich nicht nur auf die besonders schützenswerten, sondern auf alle persönlichen Daten. Im Rahmen einer Untersuchung zur Abklärung strafbarer Handlungen, vor allem bei Einvernahmen, ist es nämlich nicht möglich, zwischen besonders schützenswerten und anderen Daten zu unterscheiden.

Absatz 1 hält in Anlehnung an Artikel 15 des Datenschutzgesetzes fest, dass Personendaten bereits im gerichtspolizeilichen Ermittlungsverfahren bei der betroffenen Person selbst und für diese erkennbar beschafft werden sollen. Allerdings gilt diese Regel nicht absolut. Im Interesse einer wirkungsvollen Strafuntersuchung müssen die gerichtspolizeilichen Organe von diesen Grundsätzen abweichen dürfen. Zudem muss der kriminalpolizeilichen Notwendigkeit Rechnung getragen werden, jede Angabe einer betroffenen Person nach Möglichkeit durch weitere Aussagen Dritter und Sachbeweise zu überprüfen und zu erhärten. Darauf deutet die Wendung hin, Daten müssten «auch» bei der betroffenen Person beschafft werden.

In *Absatz 2* wird der datenschutzrechtliche Grundsatz, dass Daten richtig sein müssen (Art. 4 Abs. 2 DSGVO), näher ausgeführt. Danach soll der Inhaber einer Datensammlung oder das verantwortliche Organ jede Berichtigung oder Vernichtung von Daten an jene Behörden und Personen weitermelden, denen diese Daten früher bekanntgegeben worden sind. Mit der Aufnahme dieses Grundsatzes in den Abschnitt über die allgemeinen Bestimmungen wird deutlich gemacht, dass die Vorschrift auf *alle Verfahrensabschnitte des Bundesstrafprozesses* Anwendung findet.

Absatz 3 regelt die Behandlung der Daten, die für die Untersuchung nicht mehr benötigt werden. Die Regelung lehnt sich an die Bestimmung von Artikel 66 Absatz 1^{ter} des Bundesgesetzes über die Bundesstrafrechtspflege an, wonach die für die Untersuchung nicht benötigten Aufzeichnungen aus der Überwachung des Post-, Telefon- und Telegrafatenverkehrs nach Abschluss des Verfahrens zu

vernichten sind. Nicht vernichtet werden müssen jedoch jene Daten, die für die Durchführung anderer Untersuchungen notwendig sind. Die von der Rechtsprechung entwickelten Regeln sorgen in solchen Fällen für die rechtmässige Verwendung der Daten⁶⁰). Kommt es nach der Ermittlung zu einem förmlichen Verfahren, so werden die Ermittlungsakten nach Abschluss des eidgenössischen oder kantonalen Strafverfahrens vernichtet oder archiviert (vgl. dazu den neu vorgeschlagenen Art. 107^{bis}).

Artikel 72^{bis}

Dieser Artikel regelt die Überwachung von Kundgebungen. Die Frage, wieweit die Polizei rechtmässig durchgeführte Demonstrationen filmen oder fotografieren darf, ist seit längerem umstritten. Unter datenschutzrechtlichen Gesichtspunkten sind solche Aufnahmen insofern problematisch, als sie erlauben, die politische Tätigkeit von Demonstrationsteilnehmern festzustellen. Nach dem Entwurf soll die Polizei künftig rechtmässig durchgeführte Kundgebungen nur dann aufzeichnen dürfen, wenn es im Verlauf der Demonstration zu strafbaren Handlungen kommt oder konkrete Umstände darauf schliessen lassen, dass solche Handlungen vorbereitet werden. Letzteres ist etwa der Fall, wenn Kundgebungsteilnehmer Waffen oder gefährliche Werkzeuge mit sich führen oder wenn schon im Vorfeld der Kundgebung zu Gewalttätigkeiten aufgerufen wird.

Im vorliegenden Entwurf wird darauf verzichtet, die *akustische* Überwachung in vergleichbarer Weise zu regeln. Wer sich an einer Demonstration öffentlich äussert, nimmt in Kauf, dass seine Rede, auf welche Weise auch immer, zur Kenntnis genommen wird.

Des weitem wurde keine Bestimmung über die *traditionelle Überwachung und die Beschattung von Personen* in den Bundesstrafprozess aufgenommen. Es versteht sich, dass das Verhalten einer Person nur bei Vorliegen bestimmter Verdachtsgründe überwacht und aufgezeichnet wird. Die Befugnis der Polizei stützt sich dabei auf den allgemeinen Auftrag, Straftaten aufzudecken und zu verhindern. Dabei sind intensive Überwachungen mit einschneidenden Eingriffen in die Persönlichkeit selten und erfordern erfahrungsgemäss den Einsatz technischer Mittel. Technische Überwachungsgeräte dürfen aber nach den Artikeln 66 ff. des Bundesstrafprozesses nur mit Bewilligung des Präsidenten der Anklagekammer eingesetzt werden. Aus diesen Gründen erscheint es nicht nötig, in einer besonderen Norm die Überwachung und Beschattung von Personen zu regeln.

Artikel 73^{bis}

Die Durchsuchung von Personen wird im geltenden Recht nur im Zusammenhang mit der Hausdurchsuchung (Art. 67 Abs. 1 zweiter Satz BStP) erwähnt. Im übrigen muss sich die gerichtliche Polizei hiefür bis heute auf die Generalklausel von Artikel 102 BStP stützen, aufgrund welcher sie ermächtigt ist, Spuren der Vergehen festzustellen und zu sichern. Da eine Durchsuchung einen wesentlichen Eingriff in die Freiheit einer Person darstellen kann, soll hiefür nun eine ausdrückliche gesetzliche Grundlage geschaffen werden.

In *Absatz 1* werden die Voraussetzungen für eine polizeiliche Durchsuchung aufgezählt. Eine solche ist einmal zulässig, wenn die Voraussetzungen für eine

Festnahme erfüllt sind (Bst. a), d. h. bei Vorliegen eines Haftbefehls oder wenn eine vorläufige polizeiliche Festnahme sofort erfolgen muss (Art. 44 und 62 BStP). Eine Person kann ferner durchsucht werden, wenn der Verdacht besteht, dass sie Sachen bei sich trägt, die sicherzustellen sind (Bst. b). Sicherzustellende Gegenstände sind vorab solche, die der Einziehung oder Beschlagnahme unterliegen⁶¹). Die Durchsuchung kann schliesslich auch zur Feststellung der Identität (Bst. c) oder zum Schutze von Personen erfolgen, die nicht mehr voll zurechnungsfähig sind (Bst. d).

Nach *Absatz 2* ist eine Durchsuchung ferner zum Schutze von Polizeibeamten und Dritten zulässig. In diesem Zusammenhang ist vor allem auf die völkerrechtlich gebotenen Schutzmassnahmen für Staatsoberhäupter, Regierungsmitglieder und Diplomaten bei Staatsbesuchen oder internationalen Konferenzen hinzuweisen.

Schliesslich bestimmt *Absatz 3* in Anlehnung an Artikel 48 Absatz 2 des Gesetzes über das Verwaltungsstrafrecht (SR 313.0), dass eine Durchsuchung nur von einer Person gleichen Geschlechts oder einem Arzt vorgenommen werden darf. Ausnahmen sind zulässig, wenn sonst unwiderruflicher Schaden entstünde.

Artikel 73^{ter}

Der Artikel umschreibt die Voraussetzungen, unter welchen im Rahmen von Strafverfahren Untersuchungen von Personen vorgenommen werden dürfen. Solche Untersuchungen stellen in der Regel einen schweren Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Sie sind deshalb nach *Absatz 1* nur zulässig, wenn sie für die Feststellung des Sachverhaltes notwendig sind (Bst. a) oder wenn allein auf diese Weise die Zurechnungs-, Verhandlungs- oder Haftstellungsfähigkeit eines Beschuldigten abgeklärt werden kann (Bst. b).

Absatz 2 regelt die Zuständigkeit für die Anordnung einer Untersuchung. Im gerichtspolizeilichen Verfahren hat einzig der Bundesanwalt die entsprechende Befugnis.

Für die Untersuchung *nicht Beschuldigter* müssen nach *Absatz 3* zusätzliche Voraussetzungen erfüllt sein. Solche Personen dürfen gegen ihren Willen nur untersucht werden, wenn anders eine für die Abklärung der Straftat wesentliche Tatsache nicht festgestellt werden kann. Personen, die zur Zeugnisverweigerung berechtigt sind, steht in Anlehnung an die Regelung in einigen kantonalen Prozessordnungen ein sogenanntes *Untersuchungsverweigerungsrecht* zu.

Absatz 4 garantiert, dass die Untersuchungen nur von sachkundigen Personen durchgeführt werden. Zudem wird solchen Eingriffen eine absolute Schranke gesetzt: Sie sind nur zulässig, wenn keine Nachteile für die Betroffenen zu befürchten sind.

In *Absatz 5* schliesslich wird die polizeiliche Kompetenz zur Anordnung einer Blutprobe bei dringendem Tatverdacht verankert. Die Blutentnahme kann auch von sachkundigen Hilfskräften vorgenommen werden.

Artikel 73^{quater}

Die erkennungsdienstliche Behandlung von Beschuldigten und zu Vergleichszwecken gehört zu den klassischen polizeilichen Mitteln der Verbrechensbe-

kämpfung. Unter die Massnahmen des Erkennungsdienstes fallen alle Methoden, die der Identifikation von Personen dienen. Herkömmlicherweise versteht man darunter Finger- und Handballenabdrücke, Tatortspuren, Fotografien und Signalelemente⁶²⁾. Die erkennungsdienstlichen Massnahmen können sich jedoch je nach Stand der Wissenschaft und Kriminaltechnik ändern. So haben in neuerer Zeit Haar- und Stimmvergleiche an Bedeutung gewonnen.

Mit dem vorliegenden Artikel, der als Konkretisierung im Sinne von Artikel 30 Absatz 4 Buchstabe c DSG verstanden werden kann, soll die gesetzliche Grundlage für die Anwendung dieses wichtigen Fahndungsmittels geschaffen werden⁶³⁾. Erkennungsdienstlich behandelt werden können einerseits Beschuldigte, soweit es zur Beweiserhebung notwendig ist (Bst. a), und andererseits weitere Personen, wenn auf diese Weise die Herkunft von Spuren abgeklärt werden soll (Bst. b). Das Material von Freigesprochenen oder von Personen, die lediglich zur Feststellung ihrer Tatortberechtigung erkennungsdienstlich behandelt worden sind, wird nach den Bestimmungen der Verordnung über den Erkennungsdienst vernichtet.

Auch die übrigen erkennungsdienstlichen Daten werden nach Ablauf einer bestimmten Frist aus der Sammlung entfernt⁶⁴⁾. Die Erhebung von Schrift- und Stimmproben zu Vergleichszwecken bedarf keiner besonderen Regelung, da hier Zwangsmassnahmen ohnehin praktisch undurchführbar sind und sich folglich die Zulässigkeit dieser Massnahmen schon aus Artikel 102 des Bundesgesetzes über die Bundesstrafrechtspflege ergibt.

Artikel 101^{bis}

Förmliche Zeugeneinvernahmen werden erst vom Untersuchungsrichter durchgeführt. Im gerichtspolizeilichen Ermittlungsverfahren können jedoch Dritte als Auskunftspersonen einvernommen werden⁶⁵⁾. Dabei werden in der Praxis die Bestimmungen über das Recht zur Zeugnisverweigerung auch im Ermittlungsverfahren beachtet. Der vorliegende Artikel, der im übrigen Artikel 40 des Verwaltungsstrafrechts (SR 313.0) entspricht, ist die gesetzliche Umschreibung einer bereits geltenden Praxis. Ausdrücklich erwähnt wird zudem die Pflicht der gerichtlichen Polizei, jemanden, der in der eidgenössischen Voruntersuchung das Zeugnis verweigern darf, auch im gerichtspolizeilichen Ermittlungsverfahren auf dieses Recht aufmerksam zu machen.

Artikel 102^{bis}

Absatz 1 gibt – wie auch das allgemeine Datenschutzgesetz – jedermann das Recht, vom Bundesanwalt als Leiter der gerichtlichen Polizei Auskunft über die bei der gerichtlichen Polizei aufbewahrten Daten zu erhalten.

Die Auskunft kann nach *Absatz 2* eingeschränkt oder verweigert werden, wenn sie den Zweck des Ermittlungsverfahrens in Frage stellt (Bst. a) oder wenn überwiegende öffentliche Interessen, namentlich die innere oder äussere Sicherheit der Eidgenossenschaft (Bst. b) oder überwiegende Drittinteressen (Bst. c) entgegenstehen. Die Einschränkungen des Auskunftsrechts sind mithin fast die gleichen wie nach Artikel 6 des Datenschutzgesetzes. Das Auskunftsrecht soll nicht dazu führen, dass Delinquenten erfahren können, ob die Polizei ihnen be-

reits auf der Spur ist. Auch im Bereich des gerichtspolizeilichen Verfahrens muss sich ein Gesuchsteller aber nicht mit einer Auskunftsbeschränkung oder -verweigerung abfinden. Er kann in einem solchen Fall den Eidgenössischen Datenschutzbeauftragten anrufen (vgl. die Ausführungen zu Art. 102^{ter}).

In *Absatz 3* wird der Anspruch des Betroffenen, dass keine unrichtigen Daten über ihn gespeichert werden, gesetzlich verankert. Der Begriff «unrichtige Daten» ist aber nicht so zu verstehen, dass jedes Datum falsch sei, dessen materielle Wahrheit noch nicht feststeht. Alle Aussagen werden im Hinblick auf eine richterliche Beurteilung erhoben. Meist steht erst zu diesem Zeitpunkt endgültig fest, was als «falsch» oder als «richtig» zu gelten hat. Aus diesem Grund ist im gerichtspolizeilichen Ermittlungsverfahren eine Berichtigung von Daten im datenschutzrechtlichen Sinne nicht immer möglich. Ein Datum muss allerdings korrigiert werden, wenn es fälschlicherweise den Eindruck erweckt, es sei auch in materieller Hinsicht schon eindeutig bewiesen und es bestünden keine Zweifel mehr an seiner Richtigkeit. An die *Schutzwürdigkeit des Interesses* des Betroffenen für die Geltendmachung eines Berichtigungs- oder Vernichtungsanspruchs sollen in der Praxis keine allzu hohen Anforderungen gestellt werden. Immerhin muss der Betroffene ein eigenes Interesse glaubhaft machen können. Im übrigen versteht sich von selbst, dass Daten, bei denen sich herausstellt, dass sie unrichtig sind, von Amtes wegen korrigiert oder vernichtet werden sollen.

Weil der Betroffene in der Regel keinen direkten Beweis für die Unrichtigkeit einer Angabe erbringen kann, obliegt es nach *Absatz 4* der gerichtlichen Polizei, die Richtigkeit des Datums zu beweisen. Für den Fall, dass weder die Richtigkeit noch die Unrichtigkeit eines Datums bewiesen werden kann, ist die Möglichkeit des *Bestreitungsvermerks* vorgesehen. Eine ähnliche Lösung kennen bereits die Polizeigesetze der Kantone Waadt und Wallis. Sie entspricht auch allgemeinen strafprozessualen Grundsätzen.

Artikel 102^{ter}

Erteilt der Bundesanwalt keine oder nur eine eingeschränkte Auskunft, so kann der Betroffene nach *Absatz 1* seinen Fall dem Eidgenössischen Datenschutzbeauftragten zur Überprüfung vorlegen. Dieser kann den Bundesanwalt um Informationen ersuchen.

Gelangt der Datenschutzbeauftragte zu einem andern Ergebnis als der Bundesanwalt, so wird er diesem gestützt auf *Absatz 2* empfehlen, seine Verfügung in Wiedererwägung zu ziehen.

Ist der Bundesanwalt mit dieser Empfehlung nicht einverstanden, so können er oder der Datenschutzbeauftragte aufgrund von *Absatz 3* die Angelegenheit der Anklagekammer des Bundesgerichts unterbreiten. Diese Regelung rechtfertigt sich deshalb, weil das Bundesgericht im Bereich des Ermittlungsverfahrens bereits gewisse Aufgaben erfüllt (Haftrecht, amtliche Überwachung, Entsiegelung) und mit der vorliegenden Revision des Bundesstrafprozesses generell mehr Kompetenzen auf diesem Gebiet erhalten soll. Um den Untersuchungszweck nicht zu gefährden, stehen dem Betroffenen in diesem Verfahren aber keine Parteirechte zu. Hingegen kann die Anklagekammer, soweit es für ihren Entscheid notwendig ist, Einblick in die Akten der gerichtlichen Polizei nehmen.

Artikel 102^{quater}

Polizeilich erhobene Daten sind zu einem grossen Teil besonders schützenswert; ihre Weitergabe ist auf das Notwendige zu beschränken. In *Absatz 1* werden deshalb nach dem Vorbild verschiedener kantonaler Regelungen jene Behörden aufgezählt, denen die gerichtspolizeilichen Organe Daten bekanntgeben können.

Absatz 2 enthält einen Vorbehalt zugunsten weiterer Rechtshilfenvorschriften. Es handelt sich dabei insbesondere um die Artikel 352 ff. des Strafgesetzbuches, die vor allem das Rechtshilfeverfahren regeln, sowie die Artikel 19 und 30 des Verwaltungsstrafrechts, welche die Anzeigepflicht der Behörden und deren Verpflichtung zur Rechtshilfe regeln. Die Rechtshilfe gegenüber den Organen der militärischen Gerichtsbarkeit bestimmt sich nach den Artikeln 18 ff. des Militärstrafprozesses (SR 322.1).

Artikel 105^{bis}

Gegenwärtig unterstehen nur einzelne Massnahmen des Bundesanwaltes einer richterlichen Überprüfung, so die Abweisung eines Haftentlassungsgesuchs (Art. 52), die Überwachung des Post-, Telefon- und Telegrafatenverkehrs (Art. 66^{bis}) und die Durchsuchung von Papieren (Art. 69 Abs. 3 BStP). Für die übrigen Zwangsmassnahmen, wie Beschlagnahme und Durchsuchung ist bislang keine unmittelbare richterliche Kontrolle vorgesehen. Nach *Absatz 1* sollen die betroffenen Personen künftig wie im Verwaltungsstrafverfahren (vgl. Art. 26 Abs. 1 VStrR; SR 313.0) die Möglichkeit haben, jede Zwangsmassnahme von der Anklagekammer des Bundesgerichts überprüfen zu lassen. In Betracht fallen dabei namentlich folgende Massnahmen: Verhaftung, vorläufige Festnahme, Beschlagnahme, Untersuchung und Durchsuchung sowie die Einziehung. Dies bedeutet jedoch nicht, dass die Anklagekammer in das untersuchungsrichterliche Ermessen eingreifen oder jede Untersuchungshandlung auf ihre Angemessenheit prüfen soll. Eine Änderung der geltenden Praxis der Anklagekammer⁶⁶⁾ ist nicht beabsichtigt.

Andere polizeiliche Massnahmen, die nicht im gleichen Masse in die Persönlichkeitsrechte eingreifen, können weiterhin nur mit Aufsichtsbeschwerde beim Eidgenössischen Justiz- und Polizeidepartement angefochten werden (vgl. Art. 17 Abs. 1 BStP).

Artikel 107^{bis}

Nach *Absatz 1* soll die Bundesanwaltschaft die Akten nach Abschluss des eidgenössischen oder kantonalen Verfahrens vernichten oder archivieren. Akten des gerichtspolizeilichen Ermittlungsverfahrens können allerdings nur beschränkt vernichtet werden. Vielfach müssen sie im Hinblick auf allfällige Revisions- und Entschädigungsverfahren⁶⁷⁾ aufbewahrt werden. Zudem besteht zum Teil das Bedürfnis, sie zu statistischen Zwecken auszuwerten. Ferner müssen Erkenntnisse über erfahrungsgemäss langfristig angelegte nachrichtendienstliche Operationen, die teilweise in Ermittlungsverfahren nach dem Bundesstrafprozess gesammelt werden, lange aufbewahrt, bearbeitet und ausgewertet werden können. Gleiches gilt für die Terrorismusbekämpfung. Eine vorzeitige Vernichtung könnte die Aufrechterhaltung der inneren und äusseren Sicherheit der

Schweiz gefährden. Vorbehalten bleiben schliesslich gesetzliche Aufbewahrungsvorschriften. So hat der Bundesanwalt die Akten der eingestellten Untersuchungen aufzubewahren (Art. 124 BStP). Für all diese Fälle sieht Absatz 1 deshalb die Möglichkeit der *Archivierung* vor. In den Vorschriften über das Bundesarchiv können zudem Ablieferungspflichten zugunsten des Bundesarchivs vorgesehen werden.

Absatz 2 schränkt die Verwendung archivierter Akten ein. Sie dürfen nur im Zusammenhang mit einem andern Verfahren oder für nichtpersonenbezogene Zwecke, d. h. namentlich für Statistiken benutzt werden.

Nach *Absatz 3* wird der Bundesrat die Einzelheiten in der Verordnung regeln. Dabei wird er namentlich festlegen, wie die Archivierung organisiert werden muss.

222.6 Änderung des Bundesgesetzes über internationale Rechtshilfe in Strafsachen

222.61 Die Internationale Kriminalpolizeiliche Organisation INTERPOL

Die vorgeschlagene Gesetzesänderung hat zum Zweck, die polizeiliche Zusammenarbeit zwischen der Internationalen Kriminalpolizeilichen Organisation (INTERPOL) und unserem Lande zu regeln. Eine gesetzliche Ordnung des grenzüberschreitenden Informationsverkehrs in Polizeiangelegenheiten erscheint angezeigt, nachdem der Umfang dieses Datenaustausches zunehmend grösser wird. Im Jahre 1986 sind mehr als 100 000 Informationen durch das Nationale Zentralbüro der Schweiz, welches als Verbindungsstelle zwischen in- und ausländischen Polizeibehörden fungiert, vermittelt worden. Mit der vorgeschlagenen Ergänzung des Rechtshilfegesetzes sollen die Hauptelemente der Zusammenarbeit mit INTERPOL (Zuständigkeit und Aufgaben der beteiligten Bundesstelle) gesetzlich verankert und die aus heutiger Sicht notwendigen datenschutzrechtlichen Vorkehrungen getroffen werden. Die Aufgabenerfüllung und Effizienz von INTERPOL werden dadurch nicht beeinträchtigt.

1923 gegründet, vereinigt INTERPOL heute die Kriminalpolizeibehörden von 146 Staaten. Die Schweiz war seit jeher Mitglied der Organisation. INTERPOL verfolgt den Zweck, eine möglichst umfassende gegenseitige Unterstützung aller Kriminalpolizeibehörden im Rahmen internationaler Abkommen und der in den einzelnen Ländern geltenden Gesetze sicherzustellen und damit zur wirksamen Bekämpfung und Verhütung von Straftaten beizutragen.

Schwerpunkt der Tätigkeit von INTERPOL ist der polizeiliche Informationsaustausch zwischen den verschiedenen Mitgliedsländern (internationale Strafbefehle, Suchanzeigen, Gesuche um Überwachungen, Identifizierungen usw.). Dieser Informationsaustausch wickelt sich über die Nationalen Zentralbüros der Mitgliedstaaten ab. Sie sind Drehscheibe zwischen den nationalen Polizeibehörden und dem Generalsekretariat von INTERPOL bzw. den Nationalen Zentralbüros anderer Mitgliedstaaten. Der Grossteil des polizeilichen Informationsaustausches zwischen den einzelnen Nationalen Zentralbüros läuft über

das Generalsekretariat von INTERPOL; die Nationalen Zentralbüros verkehren aber auch direkt miteinander. Für den Informationsaustausch über das Generalsekretariat INTERPOL besteht ein «Reglement über die internationale polizeiliche Zusammenarbeit und die interne Kontrolle der Dateien von INTERPOL» aus dem Jahre 1984 (nachfolgend Reglement 84 genannt). Für den unmittelbaren Informationsaustausch zwischen den Nationalen Zentralbüros dagegen existiert heute noch keine Datenschutzregelung. Ein entsprechendes Reglement ist aber in Vorbereitung (vgl. Art. 11 des Reglementes 84; Anhang 2 der Verordnung vom 1. Dez. 1986 über das Nationale Zentralbüro INTERPOL Schweiz, IPVO; SR 172.213.56).

222.62 Notwendigkeit der Regelung

Heute ist der internationale polizeiliche Nachrichtenaustausch in den INTERPOL-Statuten geregelt, die allerdings die gesetzlichen Vorschriften der Mitgliedsländer vorbehalten. So darf kein Nationales Zentralbüro Informationen übermitteln, wenn dies einen Verstoß gegen Landesrecht darstellen würde. Die Statuten sind kürzlich aufgrund der Verordnung vom 1. Dezember 1986 über das Nationale Zentralbüro INTERPOL Schweiz ins innerstaatliche Recht aufgenommen worden, doch sind die gesetzlichen Grundlagen für die Verordnung ihrerseits noch nicht ausreichend.

Mit der vorliegenden Revision sollen die gesetzlichen Grundlagen für die Zusammenarbeit mit INTERPOL vervollständigt werden. So soll insbesondere die Weitergabe von polizeilichen Informationen zum Zwecke der *Verbrechensverhütung* näher geregelt werden. Anders als bei der *Verbrechensbekämpfung* kommen hier die Grundsätze des Bundesgesetzes über internationale Rechtshilfe in Strafsachen (IRSG; SR 351.1), die teilweise auch datenschutzrechtlichen Charakter haben (so etwa das Verbot der Rechtshilfe bei Strafverfolgungen wegen politischer Anschauungen, wegen Zugehörigkeit zu einer bestimmten Rasse, Religion oder einem Volksstamm; Art. 2 IRSG), nämlich nicht zur Anwendung. Ferner soll für den Datenaustausch zwischen der Bundesanwaltschaft in ihrer Eigenschaft als Nationales Zentralbüro und den Nationalen Zentralbüros anderer Staaten eine gesetzliche Regelung geschaffen werden, da für diese Art des Informationsaustausches ein INTERPOL-Reglement erst in Vorbereitung ist.

Mit der vorgeschlagenen Änderung des IRSG wird den Besonderheiten des polizeilichen Informationsaustausches Rechnung getragen. Der Datenaustausch zum Zwecke der Verbrechensverhütung soll nur dann erlaubt sein, wenn *aufgrund konkreter Umstände mit der Möglichkeit eines Verbrechens oder Vergehens zu rechnen ist*. Die Grundsätze des IRSG werden aber auch für den Informationsaustausch zu Präventionszwecken für anwendbar erklärt. Des weiteren wird sichergestellt, dass für den direkten Datenaustausch zwischen Nationalen Zentralbüros die Grundsätze des INTERPOL-Reglementes 84 und später allfällige weitere Reglemente von INTERPOL Geltung haben. Auf diese Weise werden Grundsätze des Datenschutzes beim Informationsaustausch über INTERPOL auch im schweizerischen Recht garantiert.

222.63 Standort der vorgeschlagenen Bestimmungen

Der internationale kriminalpolizeiliche Nachrichtenaustausch gehört rechtlich und faktisch zum Bereich der internationalen Rechts- und Amtshilfe in Strafsachen. Deshalb sollen die entsprechenden Bestimmungen ins IRSG und nicht etwa ins StGB eingefügt werden.

Die Regeln über die Zusammenarbeit im Rahmen von INTERPOL werden in einem neuen Abschnitt des IRSG zusammengefasst. Damit wird deutlich, dass sich die Bestimmungen nur auf die polizeiliche Informationsvermittlung beziehen. Mitteilungen im Rahmen eines Rechtshilfeverfahrens bleiben davon unberührt, auch wenn sie auf INTERPOL-Kanälen und damit durch das Nationale Zentralbüro übermittelt werden (vgl. Art. 29 Abs. 2 IRSG). Da für Rechtshilfegesuche strenge Verfahrensregeln gelten und ein ausgebauter Rechtsschutz besteht, findet das Datenschutzgesetz auf sie keine Anwendung (vgl. Art. 2 Abs. 2 Bst. f DSGVO).

222.64 Zu den einzelnen Bestimmungen

Artikel 81a Zuständigkeit

Nach Artikel 32 der Statuten von INTERPOL hat jedes Land ein Nationales Zentralbüro zu bezeichnen. Diese Dienststelle hat für die Verbindung zwischen den Strafverfolgungsbehörden des betreffenden Landes einerseits und den als Nationale Zentralbüros tätigen Dienststellen anderer Staaten sowie dem Generalsekretariat der Organisation andererseits zu sorgen. Art. 81a überträgt – entsprechend der bisherigen Regelung (Art. 1 der Verordnung über das Nationale Zentralbüro INTERPOL Schweiz) – der Bundesanwaltschaft die Aufgaben des Nationalen Zentralbüros.

Artikel 81b Aufgaben

Der Artikel bestimmt, zu welchen Zwecken und in welchem Masse die Bundesanwaltschaft mit dem Generalsekretariat von INTERPOL und deren Mitgliedstaaten zusammenarbeitet. Nach *Absatz 1* muss der Informationsaustausch im Zusammenhang mit der *Verfolgung* von Straftaten und zur *Vollstreckung von Strafen und Massnahmen* erfolgen. Nach *Absatz 2* sollen aber auch kriminalpolizeiliche Informationen zur *Verhütung* von Straftaten übermittelt werden können, allerdings nur in den Fällen, in denen aufgrund *konkreter Umstände* mit der nahen Möglichkeit eines Verbrechens oder Vergehens zu rechnen ist. In *Absatz 3* ist festgehalten, dass die Bundesanwaltschaft über INTERPOL auch Informationen zur Auffindung von Vermissten und zur Identifizierung von Unbekannten vermitteln kann. Unter diese Kategorie der *nichtkriminalpolizeilichen* Informationen fallen etwa dringliche Meldungen für die Alarmzentrale des Touring-Clubs der Schweiz. *Absatz 4* bildet die Grundlage für den *Informationsaustausch mit Privaten* zum Zwecke der Verbrechensaufklärung und -verhütung. Im Vordergrund stehen dabei Mitteilungen über gestohlene Gegenstände, gefälschte Schecks, Kreditkarten usw.

In ihrer Eigenschaft als Nationales Zentralbüro beschränkt sich die Bundesanwaltschaft auf die *Weitergabe* von Daten, worauf die Ausdrücke «vermitteln» und «übermitteln» hindeuten. Sie prüft dabei in jedem Fall die Zulässigkeit einer Anfrage oder Auskunft. Hingegen ist die Durchführung eigener Recherchen aufgrund der übermittelten Daten nicht Sache des Nationalen Zentralbüros.

Artikel 81c Datenschutz

Dieser Artikel enthält die eigentlichen Datenschutzbestimmungen für die Zusammenarbeit mit INTERPOL. Er begründet unterschiedliche Regelungen für den Austausch *kriminalpolizeilicher Informationen* und die Informationsvermittlung *zu administrativen Zwecken*. Im ersten Fall sind die allgemeinen Grundsätze des IRSG sowie die Statuten und Reglemente von INTERPOL anwendbar, im zweiten das Datenschutzgesetz. Diese Lösung rechtfertigt sich deshalb, weil im zweiten Fall die Daten häufig nicht in einem förmlichen Verfahren mitgeteilt werden und damit eine Ausnahme im Sinne von Artikel 2 Absatz 2 Buchstabe f des Datenschutzgesetzes nicht gerechtfertigt ist.

Absatz 1 unterstreicht, dass die Statuten und Reglemente von INTERPOL auch für unser Land Geltung haben, sofern sie vom Bundesrat für anwendbar erklärt worden sind. Da es sich bei den INTERPOL-Reglementen nicht um internationale Abkommen, sondern um Übereinkünfte zwischen den Polizeibehörden der Mitgliedstaaten handelt, unterliegen sie nicht der Genehmigung durch den Bundesrat und das Parlament. In Anbetracht ihrer grossen Bedeutung soll der Bundesrat aber ausdrücklich darüber entscheiden, ob und wie weit sie in unserem Land Anwendung finden. Hernach werden sie in der Amtlichen Sammlung publiziert und damit allgemeinverbindlich. Als Austausch *kriminalpolizeilicher Informationen* gelten auch Informationsvermittlungen, die nicht im Zusammenhang mit einem förmlichen Auslieferungsgesuch stehen. Auch auf solche Datenflüsse sollen künftig die allgemeinen Grundsätze des Rechtshilfegesetzes anwendbar sein. Der Datenschutzbeauftragte kann indes nur im Rahmen von Artikel 26 Absatz 2 des Datenschutzgesetzes, d. h. soweit die Bundesanwaltschaft einwilligt, prüfen, ob die Grundsätze des IRSG und die einschlägigen Datenschutzreglemente von INTERPOL beachtet werden. Stellt er Mängel fest, so kann er den Bundesanwalt orientieren und ihm Vorschläge für deren Behebung unterbreiten. Es steht ihm offen, nach Rücksprache mit dem Bundesanwalt in seinem Rechenschaftsbericht an die Bundesversammlung und den Bundesrat entsprechende Hinweise aufzunehmen. Hingegen kann er, da der polizeiliche Informationsaustausch in der Regel sehr schnell vor sich gehen muss, Fälle, in denen er mit dem Bundesanwalt kein Einvernehmen erzielt, nicht der Datenschutzkommission vorlegen.

Absatz 2 enthält die Grundlage für den Austausch von Informationen administrativer, nicht kriminalpolizeilicher Art. Dieser Datenaustausch wird, anders als jener zu kriminalpolizeilichen Zwecken, dem allgemeinen Datenschutzgesetz unterstellt. Entsprechend sind hier dem Datenschutzbeauftragten keine besonderen Beschränkungen auferlegt. Er kann insbesondere umstrittene Bearbeitungen der Datenschutzkommission vorlegen.

Absatz 3 regelt den direkten Informationsaustausch mit den Nationalen Zentralbüros anderer Staaten. Auch für diesen Datenverkehr gelten die oben erwähnten Grundsätze des IRSG. Darüber hinaus soll aber ein solcher Informationsaustausch nur zulässig sein, wenn die betroffenen Staaten auch für Daten, die sie nicht über die INTERPOL-Zentrale, sondern von einem andern Nationalen Zentralbüro direkt erhalten, datenschutzrechtlichen Schutz gewähren. Dieser soll dem Datenschutz entsprechen, welcher für Informationen besteht, die von der INTERPOL-Zentrale vermittelt werden. Das bedeutet insbesondere, dass der Empfängerstaat für die Richtigkeit und Aktualität der ihm mitgeteilten Daten sorgen muss; zudem muss die betroffene Person die Möglichkeit haben, falsche Daten berichtigen oder vernichten zu lassen. Es kann damit gerechnet werden, dass bis zum Inkrafttreten dieser Bestimmungen das entsprechende INTERPOL-Reglement erlassen ist. Der direkte Verkehr mit Nationalen Zentralbüros anderer Staaten ist dann zulässig, wenn diese dem INTERPOL-Reglement unterstehen.

Artikel 81d Finanzhilfen und Abgeltungen

Mit dieser Bestimmung wird eine ausdrücklich gesetzliche Grundlage für die Ausrichtung von finanziellen Beiträgen an INTERPOL geschaffen.

3 Personelle und finanzielle Auswirkungen

31 Auswirkungen für den Bund

Das Datenschutzgesetz wird einerseits gewisse Kosten verursachen, andererseits aber auch positive finanzielle Effekte zeitigen. Beide Auswirkungen können jedoch nicht frankenmässig exakt ermittelt werden. Sicherlich werden die Datenschutzvorschriften bei den datenbearbeitenden Organen zu Mehraufwendungen führen. Verursacht werden diese durch zusätzliche Kontrollen der Datenbearbeitung, strengere Datensicherungsmaßnahmen, die Erteilung von Auskünften über gespeicherte Personendaten sowie Änderungen von Computeranwendungen, die den gesetzlichen Anforderungen nicht entsprechen. In Einzelfällen kann deshalb die personelle Verstärkung einer Dienstseinheit nötig werden. Auf der anderen Seite werden aber die durch das Gesetz bewirkte grössere Transparenz der Verwaltungstätigkeit, die Verbesserung der Qualität der Daten, die Stärkung des Vertrauens der Öffentlichkeit in Informationssysteme der Bundesorgane positive finanzielle Folgen haben.

Von den finanziellen Auswirkungen auf die datenbearbeitenden Verwaltungsstellen sind die Folgen der Einrichtung der *Kontrollorgane* zu unterscheiden. Die vom Gesetz ausgelösten Ausgaben umfassen in erster Linie die Besoldungen für den Eidgenössischen Datenschutzbeauftragten und seine Mitarbeiter. Dabei wird allerdings das Sekretariat des Datenschutzbeauftragten keine erheblichen neuen Kosten verursachen, kann doch der bestehende Dienst für Datenschutz im Bundesamt für Justiz für die neue Aufgabe eingesetzt und etwas ausgebaut werden. Dieser durch die Datenschutz-Richtlinien des Bundesrates vom 16. März 1981 geschaffene Dienst hat gegenwärtig fünf Mitarbeiter (ohne Sekretariatspersonal), von denen etwa die Hälfte hauptsächlich mit Gesetzgebungsar-

beiten beschäftigt ist. Wenngleich diese Arbeiten wegfallen, so wird es für das Sekretariat des Datenschutzbeauftragten doch etwa zehn Leute brauchen, weil das Gesetz die Registrierung bestimmter privater Datensammlungen sowie verschiedene Kontrollen im privaten und im öffentlichen Bereich einführt. Die Ausgaben für eine Dienststelle mit zehn Personen liegen etwa bei 850 000 Franken im Jahr. Die Mitglieder der Datenschutzkommission und jene der Sachverständigenkommission für die medizinische Forschung werden nach den üblichen Ansätzen für Rekurskommissionen entschädigt. Für das Sekretariat der Datenschutzkommission sind voraussichtlich zwei, für jenes der Sachverständigenkommission in der medizinischen Forschung eine zusätzliche Stelle zu schaffen. Dazu kommen die Betriebskosten zweier Sekretariate. Da sich aber nicht voraussagen lässt, wieviele Entscheide die beiden Kommissionen jährlich fällen werden, können ihre Gesamtkosten nicht genau beziffert werden. Üblicherweise kostet die Erledigung eines Streitverfahrens durch eine im Milizsystem tätige Rekurskommission mindestens 1500 Franken. Eher niedriger dürften die Kosten für eine Bewilligung zur Aufhebung des Berufsgeheimnisses zu Zwecken der medizinischen Forschung sein.

32 Auswirkungen auf Private

Für die datenbearbeitenden privaten Personen können aus der Anwendung des Gesetzes gewisse Kosten resultieren. Zu denken ist namentlich an die Aufwendungen für die Anmeldungen von Datensammlungen zur Registrierung, für die Meldungen von Bekanntgaben von Personendaten ins Ausland sowie für die Erteilung von Auskünften über Daten an die betroffenen Personen. Gut organisierte Unternehmen und Betriebe werden jedoch kaum Schwierigkeiten haben, diese formellen Pflichten zu erfüllen. Die Kosten, insbesondere auch diejenigen für die Erteilung von Auskünften, dürfen im übrigen nicht überschätzt werden. Wie die ausländischen Erfahrungen zeigen, bewirkt das Institut des Auskunftswegs keineswegs unverhältnismässige Kosten, weil die Auskunftserteilung mit modernen EDV-Programmen leicht möglich ist und weil in aller Regel recht selten Auskunft verlangt wird.

4 Legislaturplanung

Die Vorlage ist im Bericht über die Legislaturplanung 1987–1991 angekündigt (BBl 1988 I 395, Ziff. 2.17).

5 Verfassungsmässigkeit

Die verfassungsrechtlichen Grundlagen für die Datenschutzgesetzgebung sind in den Ziffern 12 und 222.41 einlässlich geschildert worden, weshalb auf die dortigen Ausführungen verwiesen wird.

6 Delegation der Gesetzgebungskompetenz

In den Artikeln 5 Absatz 5, 7 Absatz 4, 8 Absatz 2, 13 Absatz 2, 21 Absatz 1 und 30 Absätze 2–6 sind Rechtsetzungsdelegationen an den Bundesrat vorgesehen, die über die allgemeine Vollzugsverordnungscompetenz hinausgehen. Vor allem wegen der raschen Entwicklung auf dem Gebiet der Informatik können für bestimmte Datenbearbeitungsarten weitere Regelungen notwendig werden, welche die Bestimmungen dieses Gesetzes näher ausführen oder allenfalls gewisse Ausnahmen davon vorsehen. Bei den noch zu erlassenden Normen wird es sich in den meisten Fällen um solche technischer oder administrativer Art handeln. Genauere Hinweise finden sich in den Erläuterungen zu den einschlägigen Artikeln.

7 Verhältnis zum europäischen Recht

Mit dem vorliegenden Gesetz würde im Privatbereich und im öffentlichen Recht des Bundes den Anforderungen der Konvention Nr. 108 des Europarates vom 28. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten Rechnung getragen. Um aber der Konvention beitreten zu können, müssten auch die Kantone ihren öffentlichen Bereich einem Datenschutzgesetz unterstellen. Solange die Kantone ihrerseits aber noch nicht alle Mindestanforderungen der Konvention erfüllen, kann ihr die Schweiz nicht beitreten⁶⁸⁾.

Anmerkungen

- 1) Vgl. Urteil des deutschen Bundesverfassungsgerichts vom 15. Dezember 1983 (Zensus-Urteil), BVerfGE 65, 43.
- 2) Vgl. BGE 44 II 319 ff. sowie BGE 107 Ia 148 ff., 109 Ia 273 ff.
- 3) Vgl. BGE 106 Ia 33 ff.
- 4) BGE 107 Ia 52 ff.; vgl. auch BGE 108 IV 158 ff.
- 5) Vgl. z. B. Verwaltungspraxis der Bundesbehörden 48/1984, Nr. 21, S. 143 ff.; Nr. 26, S. 157 ff.
- 6) Vgl. BVerfGE 65, 43.
- 7) Vgl. BGE 97 II 97 ff.
- 8) Botschaft des Bundesrates vom 5. Mai 1982 über die Änderung des Schweizerischen Zivilgesetzbuches, BBl 1982 II 636 ff. 658.
- 9) BGE 97 II 97 ff.; vgl. ferner BGE 109 II 353 ff., 62 II 101, 44 II 319.
- 10) Vgl. BGE 107 II 6, 111 II 209 ff.; vgl. auch BGE 84 II 573.
- 11) BGE 109 Ia 279 mit weiteren Hinweisen; vgl. auch BGE 106 Ia 280.
- 12) Vgl. Verwaltungspraxis der Bundesbehörden 48/1984, Nr. 25, S. 155 ff.; BGE 98 Ib 297.
- 13) Vgl. BGE 113 Ia 10, 101 Ia 18, 109 Ia 296 ff.
- 14) BBl 1981 I 1298, 1983 II 1177, 1986 III 1045.
- 15) Vgl. z. B. Verordnung vom 20. November 1985 über Stichprobenerhebungen bei der Bevölkerung (Mikrozensus; SR 431.116), Verordnung vom 8. Juli 1981 über Probeerhebungen für eine Strafvollzugsstatistik (SR 431.341), Verordnung des EDI vom 1. März 1984 über die Statistiken der Unfallversicherung (SR 431.835), Verordnung vom 18. April 1984 über die Führung eines Betriebs- und Unternehmensregisters (SR 431.903).
- 16) Vgl. etwa Jörg Paul Müller/Stefan Müller, Grundrechte, Besonderer Teil, Bern 1985, S. 25; Charles-Albert Morand, Problèmes constitutionnels relatifs à la protection de la personnalité à l'égard des banques de données électroniques, in: Informatique et protection de la personnalité, Fribourg 1981, S. 15 ff.
- 17) Vgl. immerhin BGE 110 Ia 83 ff., 95 I 103 ff.
- 18) Vgl. Jürg Boll, Die Entbindung vom Arzt- und Anwaltsgeheimnis, Diss. Zürich 1983, S. 3; René Russek, Das ärztliche Berufsgeheimnis, Diss. Zürich 1954, S. 42.
- 19) Vgl. Peter Schäfer, Ärztliche Schweigepflicht und Elektronische Datenverarbeitung, Diss. Zürich 1978, S. 29.
- 20) Zum folgenden vgl. besonders: Conseil de l'Europe, Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg 1981; Organisation de Coopération et de Développement Economiques (OCDE), Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, exposé de motifs, Paris 1980.
- 21) Vgl. Hans Huber, Berner Kommentar, Bd. I, N. 105 ff. zu Art. 6 ZGB; Raymond Disenheim, La notion du droit civil fédéral, contribution à l'étude de l'art. 64 de la Constitution fédérale, Diss. Lausanne 1973, S. 200 ff.
- 22) Amtl. Bull. N 1972 II, S. 2127 ff.
- 23) Amtl. Bull. N 1972 II, S. 2131.
- 24) Vgl. etwa die Datenschutzgesetze der USA, von Kanada, Israel, Norwegen, der Bundesrepublik Deutschland und (bedingt) von Frankreich.
- 25) Zum Schutz der Geheimsphäre vgl. BGE 97 II 100; Jean Nicolas Druey, Geheimsphäre des Unternehmens, Basel und Stuttgart 1977, S. 163 f.; Pierre Tercier, Le nou-

- veau droit de la personnalité, Zürich 1984, S. 75 ff. Erinntert sei auch an den strafrechtlichen Schutz, insbesondere durch Art. 162 (Verletzung des Fabrikations- oder Geschäftsgeheimnisses) und Art. 273 (Wirtschaftlicher Nachrichtendienst) StGB (SR 311.0), sowie an den Schutz gegen unlauteren Wettbewerb mittels Geheimnisverletzungen durch Art. 4 Bst. c und Art. 6 UWG vom 19. Dezember 1986 (BBl 1987 I 27).
- ²⁶⁾ Jörg Paul Müller/Stefan Müller (FN 16), S. 14; Ulrich Häfelin/Walter Haller, Schweizerisches Bundesstaatsrecht, Zürich 1984, S. 350.
- ²⁷⁾ Vgl. etwa Christian Dominicé, La personnalité juridique internationale du CICR, in: Etudes en l'honneur de Jean Pictet, Genève/La Haye 1984, S. 666; Paul Reuter, La personnalité juridique internationale du Comité international de la Croix rouge, ebenda, S. 782; vgl. auch BBl 1987 I 369 ff., 381.
- ²⁸⁾ Vgl. Art. 22 des Bundesgesetzes vom 7. Dezember 1922 betreffend das Urheberrecht an Werken der Literatur und Kunst (SR 231.1).
- ²⁹⁾ Vgl. etwa Art. 42 des Bundesgesetzes vom 23. März 1962 über den Geschäftsverkehr der Bundesversammlung sowie über die Form, die Bekanntmachung und das Inkrafttreten ihrer Erlasse (Geschäftsverkehrsgesetz; SR 171.11); Art. 22 ff. Geschäftsreglement des Nationalrates (SR 171.13) und Art. 17 und 20 f. Geschäftsreglement des Ständerates (SR 171.14).
- ³⁰⁾ Vgl. Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden 1978, NN. 19 ff. zu § 2.
- ³¹⁾ BGE 100 Ib 114.
- ³²⁾ Vgl. Schnyder/Murer, Berner Kommentar, Bd. II, 3. Abt., System. Teil, N. 54.
- ³³⁾ Art. 7 Verwaltungsstrafrecht (SR 313.0).
- ³⁴⁾ BGE 44 II 319 ff.; vgl. auch Art. 179^{bis} StGB (SR 311.0).
- ³⁵⁾ ZR 43/1944, Nr. 217.
- ³⁶⁾ BGE 112 Ia 100, 110 Ia 85, 103 Ia 492, 100 Ia 10.
- ³⁷⁾ Ebenso Botschaft (FN 8), S. 659.
- ³⁸⁾ Vgl. Art. 934 ff. OR (SR 220) und die Verordnung vom 7. Juni 1937 über das Handelsregister (SR 221.411).
- ³⁹⁾ Tercier (FN 25), N. 682.
- ⁴⁰⁾ Botschaft (FN 8), S. 656/687; Tercier (FN 25), N. 840 ff.
- ⁴¹⁾ Vgl. Tercier (FN 25), N. 799 ff.
- ⁴²⁾ BGE 103 II 294, 86 II 18 ff., 73 II 65.
- ⁴³⁾ Erich Richner, Umfang und Grenzen der Freiheitsrechte der Beamten nach schweizerischem Recht, Aarau 1954, S. 129; Paul Reichlin, Die Schweigepflicht des Verwaltungsbeamten, Zürich 1953, S. 21.
- ⁴⁴⁾ Vgl. aber Art. 30 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (SR 313.0).
- ⁴⁵⁾ Vgl. BGE 108 Ib 231, 96 IV 183, 87 IV 141, 86 IV 136.
- ⁴⁶⁾ Vgl. etwa Art. 50 AHVG (SR 831.10), Art. 102 UVG (SR 832.20), Art. 97 Arbeitslosenversicherungsgesetz (SR 837.0) sowie Art. 125 der Verordnung über die Unfallversicherung (SR 832.202) und Art. 125 der Arbeitslosenversicherungsverordnung (SR 837.02).
- ⁴⁷⁾ Vgl. etwa die Verordnung über das Zentrale Ausländerregister (SR 142.215).
- ⁴⁸⁾ Vgl. etwa Art. 90 des Bundesratsbeschlusses vom 9. Dezember 1940 über die Erhebung einer direkten Bundessteuer (SR 642.11), Art. 32 des Bundesgesetzes vom 27. Juni über die Stempelabgaben (SR 641.10), Art. 36 des Bundesgesetzes vom 13. Oktober 1965 über die Verrechnungssteuer (SR 642.21), Art. 4 Abs. 2 Bst. c und Art. 7 Abs. 2 des Bundesratsbeschlusses vom 29. Juli 1941 über die Warenumsatzsteuer (SR 641.20).

- 49) Bundesratsbeschluss vom 29. April 1958 über den Polizeidienst der Bundesanwaltschaft (SR 172.213.52) und Vorschriften des EJPd vom 29. April 1958 (BBl 1958 II 704 f.).
- 50) BGE 104 Ib 384, 101 Ib 110; Fritz Gygi, Bundesverwaltungsrechtspflege, 2. überarbeitete Auflage, Bern 1983, S. 160 f.
- 51) BBl 1985 II 737 ff., 956 f.
- 52) Vgl. Art. 20 des Strafgesetzbuches (SR 311.0); BGE 107 IV 193 ff., 207 E. 3.
- 53) Urs Ch. Nef, Aktuelle Probleme des Personaldatenschutzes im arbeitsrechtlichen Rechtsverhältnis, Zeitschrift für schweizerisches Recht, 92 (I) 1973, S. 357 ff.; Bernhard Frei, Der Persönlichkeitsschutz des Arbeitnehmers nach OR Art. 328 Abs. 1. Unter besonderer Berücksichtigung des Personaldatenschutzes, Bern 1982, S. 48 ff.; Verwaltungspraxis der Bundesbehörden 48/1984, Nr. 33, S. 198 ff.
- 54) BBl 1988 I 5.
- 55) BBl 1972 I 416.
- 56) Vgl. auch den Entwurf zu einem Bundesgesetz über den Schutz der Schwangerschaft und die Strafbarkeit des Schwangerschaftsabbruches, BBl 1977 III 91 ff.
- 57) Vgl. Günter Stratenwerth, Schweizerisches Strafrecht, Besonderer Teil I, 3. neubearbeitete Auflage, Bern 1983, S. 150; Schäfer, (FN 19), S. 30 ff.
- 58) Zum Antragsrecht der Eltern vgl. BGE 87 IV 105.
- 59) Vgl. BGE 94 IV 7 E. 1.
- 60) BGE 109 Ia 244 ff.
- 61) BGE 74 IV 213.
- 62) Vgl. Art. 1 der Verordnung über den Erkennungsdienst der Bundesanwaltschaft (SR 172.213.57).
- 63) Vgl. auch BGE 109 Ia 156.
- 64) Vgl. Art. 9 und 17 der Verordnung über den Erkennungsdienst der Bundesanwaltschaft.
- 65) Markus Peter, Ermittlungen nach Bundesstrafprozess, Kriminalistik 1973, S. 565; Robert Hauser, Zeitschrift für Schweiz. Strafrecht 1972, S. 137 ff.
- 66) Vgl. BGE 96 IV 141, 95 IV 47.
- 67) Vgl. BGE 109 IV 63.
- 68) Vgl. Art. 4 der Konvention Nr. 108 und Ziff. 117 der Botschaft.

Bundesgesetz über den Datenschutz (DSG)

Entwurf

vom

*Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 31^{bis} Absatz 2, 64 und 85 Ziffer 1 der Bundesverfassung,
nach Einsicht in eine Botschaft des Bundesrates vom 23. März 1988¹⁾,
beschliesst:*

1. Abschnitt: Zweck, Geltungsbereich und Begriffe

Art. 1 Zweck

Dieses Gesetz soll die Persönlichkeit und die Grundrechte von Personen schützen, über die Personendaten bearbeitet werden.

Art. 2 Geltungsbereich

¹ Dieses Gesetz gilt für das Bearbeiten von Personendaten durch:

- a. private Personen;
- b. Bundesorgane.

² Es ist nicht anwendbar auf:

- a. Daten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet;
- b. Daten, die in periodisch erscheinenden Medien wie Presse, Radio und Fernsehen veröffentlicht werden;
- c. die Geschäfte der Bundesversammlung;
- d. Rechtsprechungsverfahren vor richterlichen Behörden;
- e. Strafverfahren;
- f. internationale Rechtshilfeverfahren in Zivil- und Strafsachen;
- g. Beschwerdeverfahren im Staats- und Verwaltungsrecht;
- h. die öffentlichen Register des Privatrechtsverkehrs.

Art. 3 Begriffe

Die folgenden Ausdrücke bedeuten:

- a. *Personendaten (Daten)*: alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;

¹⁾ BBl 1988 II 413

- b. *betroffene Personen*: natürliche oder juristische Personen, über die Daten bearbeitet werden;
- c. *private Personen*: natürliche und juristische Personen, die dem Privatrecht unterstehen;
- d. *Bundesorgane*: Behörden und Dienststellen des Bundes sowie Personen, die mit öffentlichen Aufgaben des Bundes betraut sind;
- e. *besonders schützenswerte Personendaten*: Daten über:
 - 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
 - 2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
 - 3. Massnahmen der sozialen Hilfe,
 - 4. administrative oder strafrechtliche Verfolgungen und Sanktionen;
- f. *Persönlichkeitsprofil*: eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;
- g. *Bearbeiten*: jeder Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten;
- h. *Bekanntgeben*: das Zugänglichmachen von Daten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen;
- i. *Datensammlung*: jeder Bestand von Daten, der so aufgebaut ist, dass die Daten nach den betroffenen Personen erschliessbar sind;
- k. *Inhaber der Datensammlung*: private Personen oder Bundesorgane, die über den Zweck und den Inhalt einer Datensammlung entscheiden;
- l. *Beteiligte*: private Personen oder Bundesorgane, die Daten in eine Datensammlung eingeben oder darin verändern dürfen.

2. Abschnitt: Allgemeine Datenschutzbestimmungen

Art. 4 Grundsätze

¹ Personendaten dürfen nur mit rechtmässigen Mitteln und nicht wider Treu und Glauben beschafft werden.

² Daten müssen richtig sein.

³ Das Bearbeiten von Daten muss verhältnismässig sein.

⁴ Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich ist oder der gesetzlich vorgesehen wird.

⁵ Daten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet wird, namentlich weil ein Datenschutz fehlt, der mit dem schweizerischen vergleichbar ist.

⁶ Daten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

Art. 5 Auskunftrecht

¹ Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

² Der Inhaber der Datensammlung muss ihr mitteilen:

- a. alle über sie in der Datensammlung vorhandenen Daten; und
- b. den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens, die Kategorien der bearbeiteten Daten sowie der an der Sammlung Beteiligten und der Empfänger der Daten.

³ Daten über die Gesundheit kann der Inhaber der Datensammlung der betroffenen Person über einen Arzt mitteilen lassen.

⁴ Lässt der Inhaber der Datensammlung Daten durch einen Dritten bearbeiten, so bleibt er auskunftspflichtig. Der Dritte ist auskunftspflichtig, wenn er den Inhaber nicht bekanntgibt oder dieser keinen Wohnsitz in der Schweiz hat.

⁵ Die Auskunft ist in der Regel schriftlich und kostenlos zu erteilen. Der Bundesrat regelt die Ausnahmen. Er kann ein Entgelt namentlich vorsehen, wenn die Auskunft einen übermässigen Aufwand erfordert.

⁶ Niemand kann im voraus auf das Auskunftsrecht verzichten.

Art. 6 Einschränkungen des Auskunftsrechts

¹ Der Inhaber der Datensammlung kann die Auskunft verweigern, einschränken oder aufschieben, soweit:

- a. ein formelles Gesetz es vorsieht;
- b. es wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich ist;
- c. die Auskunft den Zweck einer Strafuntersuchung oder eines anderen amtlichen Untersuchungsverfahrens in Frage stellen würde;
- d. es wegen überwiegender Interessen des Inhabers der Datensammlung erforderlich ist und dieser die Daten Dritten nicht bekanntgibt; oder
- e. es wegen überwiegender Interessen eines Dritten erforderlich ist.

² Der Inhaber der Datensammlung muss angeben, aus welchem Grund er die Auskunft verweigert.

Art. 7 Register der Datensammlungen

¹ Der Eidgenössische Datenschutzbeauftragte führt ein Register der Datensammlungen. Jede Person kann das Register einsehen.

² Bundesorgane müssen sämtliche Datensammlungen beim Datenschutzbeauftragten zur Registrierung anmelden. Private Personen müssen Sammlungen nur anmelden, wenn sie, ohne gesetzliche Pflicht und ohne dass die betroffenen Personen davon Kenntnis haben, regelmässig:

- a. besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeiten; oder
- b. Daten an Dritte bekanntgeben.

³ Die Datensammlungen müssen angemeldet werden, bevor sie eröffnet werden.

⁴ Der Bundesrat regelt die Anmeldung der Datensammlungen sowie die Führung und die Veröffentlichung des Registers. Er kann für bestimmte Arten von Datensammlungen Ausnahmen von der Meldepflicht oder der Registrierung vorsehen, wenn das Bearbeiten die Persönlichkeit der betroffenen Personen nicht gefährdet.

Art. 8 Bekanntgeben ins Ausland

¹ Wer Personendaten regelmässig oder in bedeutendem Umfang ins Ausland bekanntgeben will, muss dies dem Eidgenössischen Datenschutzbeauftragten vorher melden, wenn:

- a. dafür keine gesetzliche Pflicht besteht; oder
- b. die betroffenen Personen davon keine Kenntnis haben.

² Der Bundesrat regelt die Meldung im einzelnen. Er kann vereinfachte Meldungen oder Ausnahmen von der Meldepflicht vorsehen, wenn das Bearbeiten die Persönlichkeit der betroffenen Personen nicht gefährdet.

3. Abschnitt: Bearbeiten von Personendaten durch private Personen

Art. 9 Persönlichkeitsverletzungen

¹ Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

² Er darf insbesondere nicht ohne Rechtfertigungsgrund:

- a. Daten entgegen den Grundsätzen von Artikel 4 bearbeiten;
- b. Daten gegen den ausdrücklichen Willen der betroffenen Person bearbeiten;
- c. besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben.

Art. 10 Rechtfertigungsgründe

¹ Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

² Ein überwiegendes Interesse des Bearbeiters kann insbesondere vorliegen, wenn dieser:

- a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über seinen Vertragspartner bearbeitet;
- b. mit einer Person, deren Firma im Handelsregister eingetragen ist, in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Daten bearbeitet, ohne diese Dritten bekanntzugeben;
- c. zur Prüfung der Kreditwürdigkeit einer Person, deren Firma im Handelsregister eingetragen ist, nicht besonders schützenswerte Daten bearbeitet und sie nur Dritten bekanntgibt, die sie für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen;
- d. Daten für die Veröffentlichung in periodisch erscheinenden Medien bearbeitet;
- e. Daten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind;
- f. Daten bearbeitet, welche die betroffene Person allgemein zugänglich gemacht hat.

Art. 11 Datenbearbeitung durch Dritte

¹ Das Bearbeiten von Personendaten kann einem Dritten übertragen werden, wenn:

- a. der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte; und
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

² Der Dritte kann dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.

Art. 12 Klagen und Verfahren

¹ Für Klagen und vorsorgliche Massnahmen zum Schutz der Persönlichkeit gelten die Artikel 28–28f des Zivilgesetzbuches¹⁾. Der Kläger kann insbesondere verlangen, dass die Personendaten berichtigt oder vernichtet werden.

² Kann weder die Richtigkeit noch die Unrichtigkeit von Daten bewiesen werden, so kann der Kläger verlangen, dass bei den Daten ein entsprechender Vermerk angebracht wird.

³ Klagen zur Durchsetzung des Auskunftsrechts können am Wohnsitz des Klägers oder des Beklagten eingereicht werden. Der Richter entscheidet in einem einfachen und raschen Verfahren.

¹⁾ SR 210

4. Abschnitt: Bearbeiten von Personendaten durch Bundesorgane

Art. 13 Verantwortliches Organ

¹ Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt.

² Bearbeiten Bundesorgane Daten zusammen mit anderen Bundesorganen, kantonalen Organen oder Privaten, so kann der Bundesrat die Verantwortung für den Datenschutz besonders regeln.

Art. 14 Rechtsgrundlagen

¹ Organe des Bundes dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.

² Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen sie nur bearbeiten, wenn zudem:

- a. ein formelles Gesetz es ausdrücklich vorsieht;
- b. es für eine in einem formellen Gesetz klar umschriebene Aufgabe unentbehrlich ist;
- c. der Bundesrat es bewilligt, weil die Rechte der betroffenen Personen nicht gefährdet sind; oder
- d. die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht hat.

Art. 15 Beschaffen von Personendaten

¹ Das Beschaffen von Personendaten muss für die betroffenen Personen erkennbar sein.

² Bei systematischen Erhebungen, namentlich mit Fragebogen, gibt das Bundesorgan den Zweck und die Rechtsgrundlage des Bearbeitens, die Kategorien der an der Datensammlung Beteiligten und der Empfänger der Daten bekannt.

³ Diese Anforderungen müssen nicht erfüllt sein, wenn:

- a. die betroffene Person ihre Daten allgemein zugänglich gemacht hat;
- b. die Erfüllung der Aufgabe des Bundesorgans in Frage gestellt würde; oder
- c. ein übermässiger Aufwand verursacht würde.

Art. 16 Bekanntgabe von Personendaten

¹ Bundesorgane dürfen Personendaten bekanntgeben, wenn dafür Rechtsgrundlagen im Sinne von Artikel 14 bestehen, oder wenn:

- a. die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind;
- b. die betroffene Person im Einzelfall eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf;
- c. die betroffene Person ihre Daten allgemein zugänglich gemacht hat; oder

- d. der Empfänger glaubhaft macht, 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; der betroffenen Person ist vorher wenn möglich Gelegenheit zur Stellungnahme zu geben.

² Bundesorgane dürfen in jedem Fall auf Anfrage Name, Vorname, Adresse und Geburtsdatum einer Person bekanntgeben.

³ Das Bundesorgan lehnt die Bekanntgabe ab, schränkt sie ein oder verbindet sie mit Auflagen, wenn:

- a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person es verlangen; oder
- b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.

Art. 17 Sperrung der Bekanntgabe

¹ Eine betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann vom verantwortlichen Bundesorgan verlangen, dass es die Bekanntgabe von bestimmten Personendaten sperrt.

² Das Bundesorgan hebt die Sperre auf, wenn:

- a. eine Rechtspflicht zur Bekanntgabe besteht; oder
- b. die Erfüllung seiner Aufgabe sonst gefährdet wäre.

Art. 18 Anonymisieren und Vernichten von Personendaten

Bundesorgane müssen Personendaten, die sie nicht mehr benötigen, anonymisieren oder vernichten, soweit die Daten nicht:

- a. Beweis- oder Sicherungszwecken dienen;
- b. dem Bundesarchiv abzuliefern sind.

Art. 19 Bearbeiten für Forschung, Planung und Statistik

¹ Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke insbesondere für Forschung, Planung und Statistik selbst bearbeiten und Dritten bekanntgeben, wenn:

- a. die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt;
- b. der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und
- c. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

² Die Anforderungen der folgenden Bestimmungen müssen nicht erfüllt sein:

- a. Artikel 4 Absatz 4 über den Zweck des Bearbeitens;
- b. Artikel 14 Absatz 2 über die Rechtsgrundlagen für die Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen und
- c. Artikel 16 Absatz 1 über die Bekanntgabe von Daten.

Art. 20 Privatrechtliche Tätigkeit von Bundesorganen

¹ Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für das Bearbeiten von Personendaten durch private Personen.

² Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.

Art. 21 Staatsschutz und militärische Sicherheit

¹ Für das Bearbeiten von Personendaten durch Organe des Staatsschutzes oder der militärischen Sicherheit kann der Bundesrat:

- a. Ausnahmen von den Bestimmungen über den Zweck des Bearbeitens (Art. 4 Abs. 4) und die Bekanntgabe ins Ausland (Art. 4 Abs. 5) vorsehen;
- b. das Bearbeiten von besonders schützenswerten Daten und Persönlichkeitsprofilen bewilligen, auch wenn die Voraussetzungen von Artikel 14 Absatz 2 und 16 Absatz 1 nicht erfüllt sind;
- c. die Pflicht zur Meldung und zur Registrierung (Art. 7 und 8) aufheben;
- d. die Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten abweichend von Artikel 24 Absatz 3 regeln.

² Das Stimm-, das Petitions- und das Statistikgeheimnis bleiben gewahrt.

³ Das übergeordnete Departement entscheidet an Stelle der Datenschutzkommission (Art. 27 Abs. 2) oder ihres Präsidenten (Art. 25 Abs. 2 und 27 Abs. 3). Es hört den Datenschutzbeauftragten an. An die Stelle der Beschwerde an das Bundesgericht tritt die Beschwerde an den Bundesrat.

Art. 22 Ansprüche und Verfahren

¹ Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es:

- a. das widerrechtliche Bearbeiten von Personendaten unterlässt;
- b. die Folgen eines widerrechtlichen Bearbeitens beseitigt;
- c. die Widerrechtlichkeit des Bearbeitens feststellt.

² Er kann insbesondere verlangen, dass das Bundesorgan:

- a. Daten berichtigt oder vernichtet;
- b. den Entscheid oder die Berichtigung Dritten mitteilt oder veröffentlicht.

³ Kann weder die Richtigkeit noch die Unrichtigkeit von Daten bewiesen werden, so muss das Bundesorgan bei den Daten einen entsprechenden Vermerk anbringen.

⁴ Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz¹⁾. Die Ausnahmen von Artikel 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.

⁵ Die Verfügungen des Bundesorgans können mit Beschwerde bei der Eidgenössischen Datenschutzkommission angefochten werden.

5. Abschnitt: Eidgenössischer Datenschutzbeauftragter

Art. 23 Wahl und Stellung

¹ Der Eidgenössische Datenschutzbeauftragte wird vom Bundesrat gewählt.

² Er erfüllt seine Aufgaben selbständig und ist dem Eidgenössischen Justiz- und Polizeidepartement administrativ zugeordnet.

³ Er verfügt über ein ständiges Sekretariat.

Art. 24 Aufsicht

¹ Der Datenschutzbeauftragte überwacht die Einhaltung dieses Gesetzes und der übrigen Datenschutzvorschriften des Bundes. Der Bundesrat ist von dieser Aufsicht ausgenommen.

² Er kann von sich aus oder aufgrund von Meldungen Dritter den Sachverhalt näher abklären, wenn:

- a. Bearbeitungsmethoden privater Personen geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen;
- b. Datensammlungen registriert werden müssen (Art. 7);
- c. Bekanntgaben ins Ausland gemeldet werden müssen (Art. 8);
- d. Daten durch Bundesorgane bearbeitet werden.

³ Bei der Abklärung kann er Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Die in die Abklärung einbezogenen Personen müssen an der Feststellung des Sachverhaltes mitwirken. Das Zeugnisverweigerungsrecht nach Artikel 16 des Verwaltungsverfahrensgesetzes¹⁾ gilt sinngemäss.

⁴ Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, so empfiehlt der Beauftragte, das Bearbeiten zu ändern oder zu unterlassen.

⁵ Wird eine Empfehlung des Datenschutzbeauftragten nicht befolgt oder abgelehnt, so kann er:

- a. die Angelegenheit der Eidgenössischen Datenschutzkommission vorlegen, welche mit Verfügung entscheidet; oder
- b. das Ergebnis der betroffenen Person, die sich an ihn gewendet hat, mitteilen und diese auf den ordentlichen Rechtsweg (Art. 12 und 22) verweisen.

¹⁾ SR 172.021

Art. 25 Information

¹ Der Datenschutzbeauftragte erstattet dem Bundesrat periodisch und nach Bedarf Bericht. Die periodischen Berichte werden veröffentlicht.

² In Fällen von allgemeinem Interesse kann er die Öffentlichkeit über seine Feststellungen und Empfehlungen informieren. Daten, die dem Amtsgeheimnis unterstehen, darf er nur mit Zustimmung der zuständigen Behörde veröffentlichen. Verweigert diese die Zustimmung, so entscheidet der Präsident der Eidgenössischen Datenschutzkommission endgültig.

Art. 26 Weitere Aufgaben

¹ Der Datenschutzbeauftragte hat insbesondere folgende weitere Aufgaben:

- a. er unterstützt private Personen sowie Organe des Bundes und der Kantone durch Orientierung, Beratung und Vermittlung;
- b. er nimmt Stellung zu Erlassen und Massnahmen des Bundes, die für den Datenschutz erheblich sind;
- c. er arbeitet mit in- und ausländischen Datenschutzbehörden zusammen;
- d. er begutachtet, wieweit der Datenschutz im Ausland mit dem schweizerischen vergleichbar ist.

² Auch wenn dieses Gesetz nach Artikel 2 Absatz 2 Buchstaben e–h nicht anwendbar ist, kann der Datenschutzbeauftragte Organe der Bundesverwaltung in Datenschutzfragen beraten. Diese können ihm Einblick in ihre Geschäfte gewähren.

³ Der Datenschutzbeauftragte berät die Sachverständigenkommission für das Berufsgeheimnis in der medizinischen Forschung (Art. 321^{bis} StGB¹⁾). Hat die Kommission die Offenbarung des Berufsgeheimnisses bewilligt, überwacht er die Einhaltung der damit verbundenen Auflagen. Er kann dazu Abklärungen nach Artikel 24 Absatz 3 vornehmen. Er kann Kommissionsentscheide mit Beschwerde bei der Eidgenössischen Datenschutzkommission anfechten.

6. Abschnitt: Eidgenössische Datenschutzkommission

Art. 27

¹ Die Eidgenössische Datenschutzkommission ist eine Schieds- und Rekurskommission im Sinne von Artikel 71a–c des Bundesgesetzes über das Verwaltungsverfahren²⁾.

² Sie entscheidet über:

- a. Empfehlungen des Datenschutzbeauftragten, die ihr vorgelegt werden (Art. 24 Abs. 5 Bst. a);

¹⁾ SR 311.0

²⁾ SR 172.021

- b. Beschwerden gegen Verfügungen von Bundesorganen in Datenschutzfragen, ausgenommen solche des Bundesrates;
- c. Beschwerden gegen Verfügungen der Kommission für das Berufsgeheimnis in der medizinischen Forschung (Art. 321^{bis} StGB¹⁾);
- d. Beschwerden gegen letztinstanzliche kantonale Entscheide, die sich auf öffentlich-rechtliche Vorschriften des Bundes über den Datenschutz stützen.

³ Stellt der Datenschutzbeauftragte bei einer Sachverhaltsabklärung nach Artikel 24 Absatz 2 fest, dass den betroffenen Personen ein nicht leicht wiedergutmachender Nachteil droht, so kann er dem Präsidenten der Datenschutzkommission vorsorgliche Massnahmen beantragen. Das Verfahren richtet sich sinngemäss nach den Artikeln 79–84 des Bundesgesetzes über den Bundeszivilprozess²⁾.

7. Abschnitt: Strafbestimmungen

Art. 28 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten

¹ Private, die vorsätzlich eine Auskunft, zu der sie nach den Artikeln 5 und 6 verpflichtet sind, falsch erteilen, werden auf Antrag mit Haft oder mit Busse bestraft.

² Mit Haft oder mit Busse werden Private bestraft, die vorsätzlich:

- a. Datensammlungen nach Artikel 7 oder Datenbekanntgaben ins Ausland nach Artikel 8 nicht melden oder bei der Meldung falsche Angaben machen;
- b. dem Datenschutzbeauftragten bei der Abklärung eines Sachverhaltes (Art. 24 Abs. 3) falsche Auskünfte erteilen oder die Mitwirkung verweigern.

Art. 29 Verletzung der beruflichen Schweigepflicht

¹ Wer vorsätzlich geheime, besonders schützenswerte Personendaten unbefugt bekanntgibt, die er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat, wird auf Antrag mit Haft oder mit Busse bestraft.

² Gleich wird bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten unbefugt bekanntgibt, die er bei seiner Tätigkeit für den Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.

³ Das unbefugte Bekanntgeben geheimer, besonders schützenswerter Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

¹⁾ SR 311.0

²⁾ SR 273

8. Abschnitt: Schlussbestimmungen

Art. 30 Vollzug

¹ Der Bundesrat erlässt die Ausführungsbestimmungen.

² Er regelt die Bearbeitung von Daten, die im Bundesarchiv archiviert sind. Dabei kann er Abweichungen von den Artikeln 5 und 6 über die Auskunft sowie von den Artikeln 14 Absatz 2 und 16 Absatz 1 über die Bearbeitung besonders schützenswerter Daten vorsehen.

³ Er kann für die Auskunftserteilung durch diplomatische und konsularische Vertretungen der Schweiz im Ausland Abweichungen von den Artikeln 5 und 6 vorsehen.

⁴ Er kann ferner bestimmen:

- a. welche Datensammlungen eine Bearbeitungsordnung benötigen;
- b. unter welchen Voraussetzungen ein Bundesorgan Personendaten durch einen Dritten bearbeiten lassen oder für Dritte bearbeiten darf;
- c. wie die Mittel zur Kennzeichnung und Identifikation von Personen verwendet werden dürfen.

⁵ Er kann völkerrechtliche Verträge über den Datenschutz abschliessen, wenn sie den Grundsätzen dieses Gesetzes entsprechen.

⁶ Er regelt, wie Datensammlungen zu sichern sind, deren Daten im Kriegs- oder Krisenfall zu einer Gefährdung von Leib und Leben der betroffenen Personen führen können.

Art. 31 Übergangsbestimmungen

¹ Die Inhaber von Datensammlungen müssen bestehende Datensammlungen, die nach Artikel 7 zu registrieren sind, spätestens ein Jahr nach Inkrafttreten dieses Gesetzes anmelden.

² Sie müssen innert einem Jahr nach Inkrafttreten dieses Gesetzes die notwendigen Vorkehren treffen, damit sie die Auskünfte nach Artikel 5 erteilen können.

³ Bundesorgane dürfen eine bestehende Datensammlung mit besonders schützenswerten Daten oder mit Persönlichkeitsprofilen noch während fünf Jahren nach Inkrafttreten dieses Gesetzes benutzen, ohne dass die Voraussetzungen von Artikel 14 Absatz 2 erfüllt sind.

Art. 32 Referendum und Inkrafttreten

¹ Dieses Gesetz untersteht dem fakultativen Referendum.

² Der Bundesrat bestimmt das Inkrafttreten.

Änderung von Bundesgesetzen

1. Das Obligationenrecht¹⁾ wird wie folgt geändert:

Art. 328b (neu)

3. Bei der
Bearbeitung
von Personen-
daten

¹ Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.

² Er darf Dritten Auskünfte über den Arbeitnehmer nur erteilen, wenn eine gesetzliche Vorschrift dies erlaubt oder der Arbeitnehmer zugestimmt hat.

³ Hat der Arbeitnehmer ein Auskunftsrecht nach den Artikeln 5 und 6 des Bundesgesetzes vom ...²⁾ über den Datenschutz, so muss ihm der Arbeitgeber auf Verlangen Einsicht in die Daten gewähren.

Art. 362

...

Artikel 328b (Schutz der Persönlichkeit bei der Bearbeitung von Personendaten)

...

2. Das Bundesgesetz vom 18. Dezember 1987³⁾ über das Internationale Privatrecht (IPRG) wird wie folgt geändert:

Art. 130 Abs. 3 (neu)

³ Klagen zur Durchsetzung des Auskunftsrechts gegen den Inhaber einer Datensammlung können bei den in Artikel 129 genannten Gerichten oder bei den schweizerischen Gerichten am Ort, wo die Datensammlung geführt oder verwendet wird, eingereicht werden.

Art. 139 Abs. 3 (neu)

³ Absatz 1 ist auch anwendbar auf Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten.

¹⁾ SR 220

²⁾ AS ...

³⁾ BBl 1988 I 5; AS ...

3. Das Schweizerische Strafgesetzbuch¹⁾ wird wie folgt geändert:

Art. 179^{novies} (neu)

Unbefugtes
Beschaffen
von Personen-
daten

Wer unbefugt besonders schützenswerte Personendaten, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Gefängnis oder mit Busse bestraft.

Art. 321^{bis} (neu)

Berufsgeheimnis
in der
medizinischen
Forschung

¹ Berufsgeheimnisse dürfen für die Forschung im Bereich der Medizin oder des Gesundheitswesens offenbart werden, wenn eine Sachverständigenkommission dies bewilligt und der Berechtigte es nicht ausdrücklich untersagt hat.

² Die Kommission erteilt die Bewilligung, wenn:

- a. die Forschung nicht mit anonymisierten Daten durchgeführt werden kann;
- b. es unmöglich oder unverhältnismässig schwierig wäre, die Einwilligung des Berechtigten einzuholen und
- c. die Forschungsinteressen gegenüber den Geheimhaltungsinteressen überwiegen.

³ Die Kommission verbindet die Bewilligung mit Auflagen zur Sicherung des Datenschutzes. Sie veröffentlicht die Bewilligung.

⁴ Sind die schutzwürdigen Interessen der Berechtigten nicht gefährdet und werden die Personendaten zu Beginn der Forschung anonymisiert, so kann die Kommission generelle Bewilligungen erteilen oder andere Vereinfachungen vorsehen. Der Bundesrat regelt die Einzelheiten.

⁵ Der Bundesrat setzt die Kommission ein. Er ordnet ihre Organisation und das Verfahren. Die Kommission ist an keine Weisung gebunden.

⁶ Wer ein Berufsgeheimnis offenbart, das er durch seine Tätigkeit für die Forschung im Bereich der Medizin oder des Gesundheitswesens erfahren hat, wird nach Artikel 321 bestraft.

4. Das Bundesgesetz über die Bundesstrafrechtspflege²⁾ wird wie folgt geändert:

IV. Rechtshilfe (neu)

Art. 26^{bis}

¹ Die Behörden des Bundes, der Kantone und der Gemeinden haben den mit

¹⁾ SR 311.0

²⁾ SR 312.0

der Verfolgung und Beurteilung von Bundesstrafsachen betrauten Behörden in der Erfüllung ihrer Aufgabe Rechtshilfe zu leisten; sie haben ihnen insbesondere die benötigten Auskünfte zu erteilen und Einsicht zu gewähren in amtliche Akten, die für die Strafverfolgung von Bedeutung sein können.

² Die Rechtshilfe kann verweigert, eingeschränkt oder mit Auflagen versehen werden, wenn:

- a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person es verlangen; oder
- b. Berufsgeheimnisse (Art. 77) entgegenstehen.

³ Die mit öffentlich-rechtlichen Aufgaben betrauten Organisationen sind im Rahmen dieser Aufgaben gleich den Behörden zur Rechtshilfe verpflichtet.

⁴ Anstände innerhalb der Bundesverwaltung entscheidet das übergeordnete Departement oder der Bundesrat, Anstände zwischen Bund und Kantonen die Anklagekammer des Bundesgerichts.

⁵ Im übrigen sind für die Rechtshilfe die Artikel 352 ff. des Strafgesetzbuches¹⁾ und Artikel 18 des Bundesgesetzes über die Organisation der Bundesrechtspflege²⁾ anwendbar.

Art. 52 Abs. 2 zweiter Satz

Aufgehoben

IX. Bearbeiten von Personendaten, Beschlagnahme, Durchsuchung, Einziehung und Überwachung (*neu*)

*Art. 64^{bis} (*neu*)*

¹ Die Personendaten werden auch bei der betroffenen Person und für diese erkennbar beschafft, ausser wenn die Untersuchung dadurch gefährdet wird oder ein unverhältnismässiger Aufwand verursacht würde.

² Werden Personendaten berichtet oder vernichtet oder ist ihre Richtigkeit nicht bewiesen (Art. 102^{bis} Abs. 3 und 4), so informieren die zuständigen Organe unverzüglich die Behörden und Organe, denen diese Daten mitgeteilt worden sind.

³ Erweisen sich Personendaten für eine Untersuchung als unnötig, so müssen sie spätestens bei deren Abschluss vernichtet werden. Sie können jedoch soweit erforderlich für andere Verfahren verwendet werden.

Gliederungstitel vor Art. 65

Aufgehoben

¹⁾ SR 311.0

²⁾ SR 173.110

Art. 72^{bis} (neu)

Die Polizei kann auch Teilnehmer einer rechtmässig durchgeführten Kundgebung fotografieren oder filmen, wenn konkrete Umstände darauf schliessen lassen, dass Teilnehmer ein Verbrechen oder Vergehen beabsichtigen, dessen Schwere oder Eigenart den Eingriff rechtfertigt.

IX.^{bis} Durchsuchung, Untersuchung, erkennungsdienstliche Behandlung von Personen (neu)

Art. 73^{bis} (neu)

¹ Die gerichtliche Polizei kann eine Person durchsuchen, wenn:

- a. die Voraussetzungen für eine Festnahme erfüllt sind;
- b. Verdacht besteht, dass die Person Sachen bei sich hat, die sicherzustellen sind;
- c. es zur Feststellung der Identität erforderlich ist; oder
- d. die Person sich erkennbar in einem Zustand befindet, der die freie Willensbetätigung ausschliesst, und die Durchsuchung zu ihrem Schutz erforderlich ist.

² Die gerichtliche Polizei kann eine Person nach Waffen, gefährlichen Werkzeugen und Explosivstoffen durchsuchen, wenn dies nach den Umständen zum Schutz von Polizeibeamten oder Dritten erforderlich ist.

³ Die Durchsuchung muss von einer Person gleichen Geschlechts oder einem Arzt vorgenommen werden, ausser wenn sie nicht aufgeschoben werden kann.

Art. 73^{ter} (neu)

¹ Der Richter kann anordnen, dass der körperliche oder geistige Zustand des Beschuldigten untersucht wird, wenn dies nötig ist, um:

- a. den Sachverhalt festzustellen; oder
- b. die Zurechnungs-, Verhandlungs- oder Hafterstehungsfähigkeit bzw. die Notwendigkeit einer Massnahme abzuklären.

² Vor Einleitung der Voruntersuchung ist der Bundesanwalt für die Anordnung solcher Untersuchungen zuständig.

³ Eine nicht beschuldigte Person darf gegen ihren Willen nur untersucht werden, wenn dadurch eine erhebliche, auf andere Weise nicht zu ermittelnde Tatsache festgestellt werden kann. Wer zur Zeugnisverweigerung berechtigt ist, darf nicht gegen seinen Willen untersucht werden.

⁴ Die Untersuchung muss von einem Arzt oder einer andern sachkundigen Person durchgeführt werden. Eingriffe in die körperliche Unversehrtheit dürfen nur vorgenommen werden, wenn dadurch keine Nachteile zu befürchten sind.

⁵ Die gerichtliche Polizei kann bei dringendem Tatverdacht eine Blutprobe anordnen.

Art. 73^{quater} (neu)

Die gerichtliche Polizei kann erkennungsdienstlich behandeln:

- a. Beschuldigte, soweit es zur Beweiserhebung notwendig ist;
- b. andere Personen, um die Herkunft von Spuren zu klären.

Art. 101^{bis} (neu)

Die gerichtliche Polizei kann mündliche und schriftliche Auskünfte einholen sowie Auskunftspersonen einvernehmen. Wer zur Zeugnisverweigerung berechtigt ist, muss vorher darauf aufmerksam gemacht werden, dass er die Aussage verweigern darf.

Art. 102^{bis} (neu)

¹ Jede Person kann von der Bundesanwaltschaft Auskunft darüber verlangen, welche Daten die gerichtliche Polizei über sie bearbeitet.

² Der Bundesanwalt kann die Auskunft verweigern, wenn:

- a. diese den Zweck des Ermittlungsverfahrens in Frage stellen würde;
- b. es wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Schweiz erforderlich ist; oder
- c. es wegen überwiegender Interessen eines Dritten erforderlich ist.

³ Wer ein schutzwürdiges Interesse hat, kann verlangen, dass die gerichtliche Polizei unrichtige Daten berichtigt oder vernichtet.

⁴ Den Beweis für die Richtigkeit von Daten muss die gerichtliche Polizei erbringen. Lässt sich weder die Richtigkeit noch die Unrichtigkeit beweisen, so wird dies in den Akten vermerkt.

Art. 102^{ter} (neu)

¹ Lehnt der Bundesanwalt ein Gesuch um Auskunft, Berichtigung oder Vernichtung ab, so kann der Gesuchsteller vom Eidgenössischen Datenschutzbeauftragten verlangen, dass er die Angelegenheit überprüft.

² Der Datenschutzbeauftragte empfiehlt dem Bundesanwalt, welche Auskunft er dem Gesuchsteller erteilen oder ob er dem Gesuch um Berichtigung oder Vernichtung entsprechen soll.

³ Sind sich der Bundesanwalt und der Datenschutzbeauftragte nicht einig, so können beide die Sache der Anklagekammer des Bundesgerichts zum Entscheid vorlegen.

Art. 102^{quater} (neu)

¹ Vor Einleitung der Voruntersuchung dürfen Daten aus dem gerichtspolizeilichen Ermittlungsverfahren folgenden Behörden und Organen bekanntgegeben werden:

- a. dem Bundesrat;
- b. den gerichtspolizeilichen Organen und den Gerichtsbehörden des Bundes und der Kantone, wenn sie die Daten für ein Verfahren benötigen;
- c. den Organen des Staatsschutzes und der militärischen Sicherheit;
- d. den gerichtspolizeilichen Organen und anderen mit Polizeiaufgaben betrauten Verwaltungsstellen ausländischer Staaten im Rahmen von Artikel 16 des Bundesgesetzes vom ...¹⁾ über den Datenschutz;
- e. dem Eidgenössischen Datenschutzbeauftragten;
- f. dem Bundesamt für Polizeiwesen, soweit dieses die Daten zur Erfüllung seiner Aufgaben im Rahmen der Bundesgesetze über die Rechtshilfe in Strafsachen benötigt oder Daten ins automatisierte Fahndungsregister RI-POL aufgenommen werden sollen;
- g. dem Eidgenössischen Justiz- und Polizeidepartement, wenn für die Strafverfolgung eines Beamten seine Ermächtigung nötig ist, sowie der dem Beamten vorgesetzten Behörde, die zur Ermächtigung Stellung nehmen muss.

² Vorbehalten bleiben weitere Rechtshilfenvorschriften.

Art. 105^{bis} (neu)

¹ Zwangsmassnahmen, die der Bundesanwalt angeordnet oder bestätigt hat, können innert zehn Tagen mit Beschwerde bei der Anklagekammer des Bundesgerichts angefochten werden.

² Für Haftbeschwerden gelten die Verfahrensvorschriften der Artikel 215–219 sinngemäss.

Art. 107^{bis} (neu)

¹ Nach Abschluss des eidgenössischen oder kantonalen Verfahrens werden Akten von der Bundesanwaltschaft vernichtet oder archiviert, soweit sie nicht dem Bundesarchiv abzuliefern sind.

² Bei der Bundesanwaltschaft oder im Bundesarchiv archivierte Akten können für ein anderes Verfahren und für nicht personenbezogene Zwecke verwendet werden.

³ Der Bundesrat regelt die Einzelheiten.

5. Das Bundesgesetz vom 20. März 1981²⁾ über internationale Rechtshilfe in Strafsachen (IRSG) wird wie folgt geändert:

2.^{bis} Abschnitt: Zusammenarbeit mit INTERPOL (neu)

Art. 81a Zuständigkeit

¹ Die Bundesanwaltschaft nimmt die Aufgaben eines Nationalen Zentralbüros

¹⁾ AS ...

²⁾ SR 351.1

im Sinne der Statuten der Internationalen Kriminalpolizeilichen Organisation (INTERPOL) wahr.

² Sie ist zuständig für die Informationsvermittlung zwischen den Strafverfolgungsbehörden von Bund und Kantonen einerseits sowie den Nationalen Zentralbüros anderer Staaten und dem Generalsekretariat von INTERPOL anderseits.

Art. 81b Aufgaben

¹ Die Bundesanwaltschaft vermittelt kriminalpolizeiliche Informationen zur Verfolgung von Straftaten und zur Vollstreckung von Strafen und Massnahmen.

² Sie kann kriminalpolizeiliche Informationen zur Verhütung von Straftaten übermitteln, wenn aufgrund konkreter Umstände mit der nahen Möglichkeit eines Verbrechens oder Vergehens zu rechnen ist.

³ Sie kann Informationen zur Suche nach Vermissten und zur Identifizierung von Unbekannten vermitteln.

⁴ Zur Verhinderung und Aufklärung von Straftaten kann die Bundesanwaltschaft von Privaten Informationen entgegennehmen und Private orientieren, wenn dies im Interesse der betroffenen Person ist und deren Zustimmung vorliegt oder nach den Umständen vorausgesetzt werden kann.

Art. 81c Datenschutz

¹ Der Austausch kriminalpolizeilicher Informationen richtet sich nach den Grundsätzen dieses Gesetzes sowie nach den vom Bundesrat anwendbar erklärten Statuten und Reglementen von INTERPOL.

² Für den Austausch von Informationen zur Suche nach Vermissten, zur Identifizierung von Unbekannten und zu administrativen Zwecken gilt das Bundesgesetz vom ...¹⁾ über den Datenschutz.

³ Die Bundesanwaltschaft kann den Zentralbüros anderer Staaten Informationen direkt vermitteln, wenn der Empfängerstaat den datenschutzrechtlichen Vorschriften von INTERPOL untersteht.

Art. 81d Finanzhilfen und Abgeltungen

Der Bund kann Finanzhilfen und Abgeltungen an INTERPOL ausrichten.

¹⁾ AS ...

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988

In	Bundesblatt
Dans	Feuille fédérale
In	Foglio federale
Jahr	1988
Année	
Anno	
Band	2
Volume	
Volume	
Heft	18
Cahier	
Numero	
Geschäftsnummer	88.032
Numéro d'affaire	
Numero dell'oggetto	
Datum	10.05.1988
Date	
Data	
Seite	413-534
Page	
Pagina	
Ref. No	10 050 713

Das Dokument wurde durch das Schweizerische Bundesarchiv digitalisiert.
Le document a été digitalisé par les. Archives Fédérales Suisses.
Il documento è stato digitalizzato dell'Archivio federale svizzero.