03.016

Botschaft

zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung

vom 19. Februar 2003

Sehr geehrte Herren Präsidenten,
sehr geehrte Damen und Herren,

mit dieser Botschaft unterbreiten wir Ihnen einen Entwurf zur Änderung des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz und einen Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 23. Mai 2002 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung mit dem Antrag auf Zustimmung.

Gleichzeitig beantragen wir Ihnen, die folgenden parlamentarischen Vorstösse abzuschreiben:

2000	M	00.3000	Erhöhte Transparenz bei der Erhebung von Personendaten (S 7.3. 00, Kommission für Rechtsfragen SR 99.067; N 5.10.00)
1999	M	98.3529	Erhöhter Schutz für Personendaten bei Online-Verbindungen (S 16.3. 99, Geschäftsprüfungskommission SR; N 21.12.99)

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

19. Februar 2003

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Pascal Couchepin
Die Bundeskanzlerin: Annemarie Huber-Hotz

Übersicht

Die vorliegende Revision bezweckt in erster Linie die Verbesserung der Information der Personen, deren Daten bearbeitet werden, die Festlegung eines minimalen Schutzstandards bei der Verarbeitung von Daten durch kantonale Behörden beim Vollzug von Bundesrecht und die Übernahme der Grundsätze des Zusatzprotokolls vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung ins schweizerische Recht.

Ausgangslage und Ziel der Vorlage

Auslöser für die vorliegende Revision sind zwei im Jahre 1999 bzw. 2000 von den Eidg. Räten angenommene Motionen, die einerseits eine Verstärkung der Transparenz beim Beschaffen von Daten verlangen und andrerseits eine formelle gesetzliche Grundlage für Online-Verbindungen zu Datenbanken des Bundes sowie einen Mindestschutz bei der Bearbeitung von Daten durch die Kantone beim Vollzug von Bundesrecht. Ausserdem müssen einige Bestimmungen des Datenschutzgesetzes angepasst werden, damit die Schweiz dem Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung beitreten kann.

Die Erfahrungen bezüglich Datenschutz haben gezeigt, dass die Anwendung des Datenschutzgesetzes im Allgemeinen befriedigt, auch wenn das Gesetz einzelne punktuelle Mängel aufweist, insbesondere was die Mittel betrifft, die den betroffenen Personen zur Verfügung stehen, um sich gegen die Verarbeitung sie betreffender Daten zu wehren.

Inhalt der Vorlage

Die Vorlage sieht für private Datenbearbeiter und Bundesorgane die Verpflichtung zur aktiven Information der betroffenen Person vor, wenn besonders schützenswerte Daten und Persönlichkeitsprofile beschafft werden. Die betroffene Person muss mindestens über die Identität des Inhabers der Datensammlung informiert werden, über den Zweck des Bearbeitens und über die Kategorien von Datenempfängern, wenn eine Bekanntgabe der Daten vorgesehen ist. Bei Personendaten, die nicht besonders schützenswert sind und auch kein Persönlichkeitsprofil darstellen, muss für die betroffene Person zumindest erkennbar sein, dass Daten beschafft werden.

Die Revision umfasst ausserdem gewisse Änderungen hinsichtlich der Pflicht zur Meldung von Datensammlungen und sie stärkt die Position von Personen, die sich einer Bearbeitung der sie betreffenden Daten widersetzen. Sie legt ausserdem die Mindestanforderungen fest, denen die Kantone im Bereich des Datenschutzes genügen müssen, wenn sie Bundesrecht vollziehen, und sie verstärkt die Kontrollmöglichkeiten, wenn beim Vollzug von Bundesrecht Personendaten bearbeitet werden.

Die Revision soll es dem Bundesrat ermöglichen, während einer zeitlich beschränkten Versuchsphase die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen im Rahmen von Pilotversuchen zu bewilligen. Unter bestimmten Voraussetzungen sollen neue Systeme getestet werden können, bevor die formellgesetzliche Grundlage für die betreffende automatisierte Datenbearbeitung in Kraft tritt.

Der Revisionsentwurf passt das schweizerische Recht an das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung an. Die Vorlage legt gestützt auf dieses Zusatzprotokoll die Kriterien für eine rechtmässige grenzüberschreitende Bekanntgabe von Daten fest und gewährt dem Eidgenössischen Datenschutzbeauftragten ein Beschwerderecht im Rahmen der Aufsicht über Bundesorgane.

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage

1.1.1 Geltendes Recht

1.1.1.1 Auf eidgenössischer Ebene

Auf eidgenössischer Ebene wird der Datenschutz heute durch das Bundesgesetz vom 19. Juni 1992[1] über den Datenschutz (DSG), in Kraft seit dem 1. Juli 1993, geregelt. Es gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch Privatpersonen und Bundesorgane (Art. 2).

Das DSG legt die Grundsätze fest, die es bei der Bearbeitung von Personendaten zu beachten gilt. Insbesondere dürfen Personendaten nur rechtmässig beschafft werden (Art. 4 Abs. 1). Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein (Art. 4 Abs. 2). Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde und der gesetzlich vorgesehen oder aus den Umständen ersichtlich ist (Art. 4 Abs. 3). Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern (Art. 5).

Das DSG regelt die Bekanntgabe der Daten ins Ausland (Art. 6) sowie das Auskunftsrecht (Art. 8). Es untersagt den Privatpersonen, die Personendaten bearbeiten, die Persönlichkeit der betroffenen Personen widerrechtlich zu verletzen (Art. 12 Abs. 1) und insbesondere Daten einer Person gegen deren ausdrücklichen Willen zu bearbeiten, wenn kein Rechtfertigungsgrund vorliegt (Art. 12 Abs. 2 Bst. b). Es regelt die Rechtsansprüche, welche die in ihren Persönlichkeitsrechten verletzten Personen geltend machen können, sowie das Verfahren (Art. 15).

Die Artikel 16 bis 25 DSG regeln die Bearbeitung von Personendaten durch Bundesorgane. Bundesorgane dürfen Personendaten nur bearbeiten, wenn eine gesetzliche Grundlage besteht (Art. 17 Abs. 1). Für die Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen wird grundsätzlich eine formellgesetzliche Grundlage verlangt (Art. 17 Abs. 2). Die Bekanntgabe von Personendaten an Dritte ist ebenfalls an das Vorliegen einer Rechtsgrundlage geknüpft, dies unter Vorbehalt der in Artikel 19 Absatz 1 DSG vorgesehenen Ausnahmen. Personendaten dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich vorgesehen ist (Art. 19 Abs. 3). Die Anforderungen sind noch strenger für besonders schützenswerte Personendaten und für Persönlichkeitsprofile, welche nur durch ein Abrufverfahren zugänglich gemacht werden dürfen, wenn ein formelles Gesetz es ausdrücklich vorsieht (Art. 19 Abs. 3).

Das DSG regelt die Aufgaben und Zuständigkeiten des Eidgenössischen Datenschutzbeauftragten (Art. 26 bis 32). Er überwacht die Einhaltung des Gesetzes durch die Bundesorgane und berät Privatpersonen. Er hat die Kompetenz, Abklärungen durchzuführen und Empfehlungen abzugeben. Wird eine Empfehlung im Privatrechtsbereich nicht befolgt, kann er die Angelegenheit der Eidgenössischen Daten-

[1] SR **235.1**

schutzkommission zum Entscheid vorlegen (Art. 29 Abs. 4). Im öffentlichen Bereich kann er die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen (Art. 27 Abs. 5). Der Datenschutzbeauftragte ist gegenüber Verfügungen der Departemente und der Bundeskanzlei nicht zur Beschwerde befugt[2].

1.1.1.2 Auf kantonaler Ebene

Die Bearbeitung von Personendaten durch kantonale Behörden wird grundsätzlich durch das kantonale Recht geregelt (Art. 2 Abs. 1 DSG). Es spielt dabei keine Rolle, ob die bearbeiteten Daten direkt von den Kantonen erhoben oder ob sie ihnen durch den Online-Zugang zu einer vom Bund geführten Datenbank übermittelt worden sind. Verschiedene Bestimmungen des Bundesrechts schränken allerdings die kantonale Hoheit im Bereich des Datenschutzes ein[3]. Darüber hinaus gelten gemäss Artikel 37 Absatz 1 DSG für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht verschiedene Bestimmungen des DSG, soweit keine kantonalen Datenschutzvorschriften bestehen. Die Mehrzahl der Kantone hat ein Datenschutzgesetz (im formellen Sinn) erlassen, andere stützen sich aber auf Verordnungen oder gar auf Weisungen, die nicht immer veröffentlicht sind.

Artikel 37 Absatz 2 DSG verpflichtet ferner die Kantone zur Bestimmung eines Kontrollorgans, welches für die Einhaltung des Datenschutzes sorgt. Diese Verpflichtung wurde in unterschiedlichem Ausmass erfüllt. Rechtsstellung, Befugnisse und Handlungsinstrumente der Kontrollorgane können sich vom einen Kanton zum andern erheblich unterscheiden.

1.1.2 Parlamentarische Vorstösse, die zur Revision geführt haben

1.1.2.1 Motion «Online-Verbindungen»

Eine Teilrevision des DSG wurde durch die Annahme einer Motion der Geschäftsprüfungskommission des Ständerats am 21. Dezember 1999 erforderlich (Motion 98.3529 vom 17.11.1998. Online-Verbindungen. Erhöhter Schutz für Personendaten; nachstehend: Motion «Online-Verbindungen»). Die Motion beauftragt den Bundesrat, den Eidgenössischen Räten eine Revision des DSG zu unterbreiten, die zum Ziel hat, für sämtliche Online-Verbindungen, selbst für Pilotprojekte, gesetzliche Grundlagen zu schaffen. Für die Einrichtung von Online-Zugängen zu Informationssystemen des Bundes sollen Mindeststandards vorgesehen werden, die es erlauben, die Zusammenarbeit zwischen Bund und Kantonen zu verbessern.

In seiner Antwort beantragte der Bundesrat, die Motion in ein Postulat umzuwandeln. Hinsichtlich des ersten Punkts der Motion erinnerte er daran, dass es bereits nach dem geltenden Recht einer ausdrücklichen gesetzlichen Grundlage bedarf, um ein Abrufverfahren einzurichten, das den Online-Zugang zu einer durch ein Bundesorgan geführten Datenbank erlaubt (Art. 19 Abs. 3 erster Satz DSG). Eine ausdrück-

2 BGE **123** II 542.
3 Vgl. Art. 16 Abs. 2 und 37 Abs. 1 DSG; Art. 16 Abs. 3 BWIS (SR **120**); Art. 16 Abs. 1 und 17 Abs. 1 BStatG (RS **431.01**).

liche Grundlage in einem formellen Gesetz ist sodann erforderlich, wenn in einem Abrufverfahren besonders schützenswerte Personendaten oder Persönlichkeitsprofile zugänglich gemacht werden (Art. 19 Abs. 3, zweiter Satz DSG). Nach Ansicht des Bundesrates gilt diese Anforderung auch während der Pilotphase; es ist somit nicht erforderlich, das Gesetz in diesem Punkt zu revidieren. Dennoch erklärte sich der Bundesrat bereit, eine Revision des DSG zur Einführung einer spezifischen Regelung für die Pilotphase eines Projekts vorzuschlagen. Diese soll dann anwendbar sein, wenn ein wichtiges öffentliches Interesse die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen vor dem Inkrafttreten der formellgesetzlichen Grundlage unbedingt erfordert. Können nämlich die geplanten Online-Verbindungen nicht unter realistischen Bedingungen erprobt werden, ist es schwierig, den Kreis der Bundesbehörden und kantonalen Instanzen, und in gewissen Fällen auch der Privatpersonen, präzise zu umschreiben, für den der Zugang erforderlich ist. Können dagegen während der Pilotphase die Zugänge zu Datenbanken, namentlich mittels Online-Verbindungen, erprobt werden, erleichtert dies die Festlegung der Zugangsbedürfnisse im Rahmen der Ausarbeitung der formellgesetzlichen Grundlage.

Hinsichtlich des zweiten Punkts der Motion erklärte sich der Bundesrat bereit, auf Bundesebene Standards für den Zugriff, die Benutzung, den Schutz und die Kontrolle von Datenbanken des Bundes festzulegen. Er hat die Frage offen gelassen, ob für die Festlegung dieser Standards eine für die Kantone direkt anwendbare Bundesregelung erlassen werden oder ob eine subsidiäre Regelung getroffen werden sollte, die dann anwendbar wäre, wenn entsprechende kantonale Regelungen fehlen.

Bei der Annahme der Motion hat der Vertreter der Bundesrates verlauten lassen, dass dieser sich der Motion anschliessen könnte, wenn ihm ein ausreichender Handlungsspielraum eingeräumt werde, um die Motion im Sinne seiner Antwort verwirklichen zu können[4].

1.1.2.2 Motion «Erhöhte Transparenz»

Am 5. Oktober 2000 hiessen die Eidgenössischen Räte eine zweite Motion gut, welche den Bundesrat ersucht, den Eidgenössischen Räten eine Revision des DSG zu unterbreiten. Es handelt sich um eine Motion der Kommission für Rechtsfragen des Ständerats (Motion 00.3000 vom 28.1.2000. Erhöhte Transparenz bei der Erhebung von Personendaten; nachstehend: Motion «Erhöhte Transparenz»). Sie verlangt, Privatpersonen und Bundesorgane zu verpflichten, die Betroffenen bei der Erhebung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen zu informieren. Die Motion sieht vor, dass insbesondere anzugeben ist, wer der Inhaber der Datensammlung ist und zu welchem Zweck die erhobenen Daten bearbeitet werden. Zusätzlich sind sämtliche weiteren Angaben zu machen, die nach dem Grundsatz von Treu und Glauben und dem Grundsatz der Verhältnismässigkeit erforderlich sind. Die Informationspflicht hätte sowohl für die Datenerhebung bei den betroffenen Personen als auch bei Dritten zu gelten. Ausnahmen wären vorzusehen, um überwiegende öffentliche oder private Interessen zu schützen.

4 AB **1999** S 212 und N 2599.

1.2 Tragweite und Ziele der Revision

Nach Annahme der beiden Motionen arbeitete die Bundesverwaltung unter Federführung des Bundesamtes für Justiz in Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten einen ersten Revisionsentwurf aus. Dabei stellte sich die Grundsatzfrage, ob die Revision auf diejenigen Bereiche zu beschränken sei, deren Neuregelung durch die erwähnten Motionen angestrebt wird, oder ob sie auf weitere Punkte auszudehnen bzw. als Totalrevision durchzuführen sei. Insbesondere stellte sich die Frage, ob nicht die Gelegenheit ergriffen werden sollte, das DSG mit dem Gemeinschaftsrecht in Übereinstimmung zu bringen, insbesondere mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[5] (Richtlinie 95/46/EG).

Um die Ansichten von Fachleuten zusammenzutragen, bildete das Bundesamt für Justiz eine informelle Arbeitsgruppe von Datenschutzspezialisten des öffentlichen und privaten Sektors, denen der Vorentwurf unterbreitet wurde[6]. Dabei zeigte sich, dass die Mehrheit dieser Fachleute der Ansicht ist, dass sich das DSG insgesamt bewährt hat, und dass eine Totalrevision des Gesetzes zum gegenwärtigen Zeitpunkt verfrüht wäre. Das Gesetz weist gewisse punktuelle Mängel auf, die im Rahmen einer Teilrevision behoben werden können, und es wäre falsch, die materiellen Grundsätze des Datenschutzes anzutasten. Die Revision soll sich deshalb auf diejenigen Punkte beschränken, für welche das dringende Bedürfnis nach einer Neuregelung festgestellt wurde, oder für die sich ein Anpassungsbedarf aus der Umsetzung der beiden oben erwähnten Motionen ergibt. Die materiellen Bestimmungen sollen nicht in Frage gestellt werden. Dagegen wird eine Verbesserung der Instrumente angestrebt, mit denen die betroffenen Personen ihre Rechte geltend machen können. Damit wird die mit der Motion 00.3000 verlangte Erhöhung der Transparenz wirksam ergänzt. Der eidgenössische Datenschutzbeauftragte hätte allerdings – ohne die grundsätzlichen Prinzipien des Gesetzes in Frage stellen zu wollen – eine weitergehende Revision befürwortet. Insbesondere sollten aus seiner Sicht die Harmonisierung des schweizerischen mit dem Gemeinschaftsrecht angestrebt werden sowie die Untersuchungs-, Beratungs- und Mediationskompetenzen des Datenschutzbeauftragten verstärkt werden.

Eine Totalrevision wird mittelfristig unumgänglich, wenn die Schweiz sich im Rahmen der bilateralen Verhandlungen II mit der EU betreffend die Liberalisierung des Dienstleistungsverkehrs sowie den Beitritt der Schweiz zu den Abkommen von Schengen und Dublin auf die Übernahme der Richtlinie 95/46/EG verpflichtet. Zum gegenwärtigen Zeitpunkt erscheint es indessen nicht als zwingend, über eine Teilre-

5 ABl L 281 vom 23. November 1995, S. 31.

6 Diese informelle Arbeitsgruppe setzte sich wie folgt zusammen:
- Prof. Dr. iur. Rainer J. Schweizer, Professor an der Universität St.Gallen, Präsident der eidgenössischen Datenschutzkommission;
- Urs Belser, Fürsprecher, Bern;
- Ursula Uttinger, lic. iur., Präsidentin des Datenschutzforums Schweiz;
- Markus Siegenthaler, Fürsprecher, Datenschutzbeauftragter des Kantons Bern;
- Gérald Page, Docteur en droit, Advokat und Lehrbeauftragter an der Universität Genf.

vision hinauszugehen (vgl. Ziff. 1.2.3.2). Nötigenfalls wird der Bundesrat dem Parlament eine Zusatzbotschaft unterbreiten.

Die Teilrevision wird darüber hinaus der Schweiz erlauben, das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung STE 108 (Zusatzprotokoll), umzusetzen. Der Bundesrat hat aufgrund der positiven Vernehmlassungsergebnisse am 30. September 2002 die Unterzeichnung des Zusatzprotokolls – unter Vorbehalt der parlamentarischen Genehmigung bzw. der Ratifikation – beschlossen (vgl. Ziff. 1.2.3.1.2).

1.2.1 Die Grundzüge der Revision

Die Revisionsarbeiten waren vom Bemühen getragen, den Persönlichkeitsschutz zu verstärken, ohne indessen die Tätigkeiten der Inhaber der Datensammlungen unnötig zu erschweren. So können sich zwar für die Privatpersonen durch die Einführung einer Informationspflicht zusätzliche Anforderungen ergeben; diese werden aber mit Erleichterungen bei der Kontrolle zumindest teilweise kompensiert. Insbesondere wird die mit dem vorliegenden Gesetzesentwurf geschaffene Transparenz dazu führen, dass bezüglich der Pflicht zur Registrierung von Datensammlungen (Art. 11 DSG) Erleichterungen möglich werden. Ebenso wird die Meldepflicht für die Bekanntgabe von Daten ins Ausland (Art. 6 DSG) aufgehoben und durch eine bloss noch punktuelle Informationspflicht ersetzt und zwar sowohl für Private als auch für Bundesorgane.

Der Entwurf weicht nicht vom bislang geltenden Konzept ab, wonach es grundsätzlich der betroffenen Person anheim gestellt ist, ob sie ihre Rechte wahrnehmen will oder nicht. Der Datenschutzbeauftragte als Kontrollorgan kann weiterhin von sich aus tätig werden, indem er Sachverhaltsfeststellungen vornimmt und Empfehlungen erlässt; seine Kompetenzen werden nur geringfügig erweitert.

Es wird somit davon ausgegangen, dass die betroffene Person selbst die ihr zustehenden Rechte ausüben kann, wenn sie über die Datenbeschaffung informiert ist, und dass bezüglich der Kontrollfunktion des Datenschutzbeauftragten keine weitergehenden Massnahmen erforderlich sind. Dieses Konzept hat den Vorteil, dass die Beschränkungen, denen die Inhaber der Datensammlungen – insbesondere Private – unterworfen sind, minimal bleiben. Den betroffenen Personen ist der Entscheid, bis zu welchem Punkt sie Beeinträchtigungen ihrer Privatsphäre zulassen wollen, weitgehend selbst überlassen. Andererseits soll auch die Informationspflicht der Inhaber der Datensammlungen auf das unbedingt Notwendige beschränkt werden. Die betroffenen Personen sollen nicht mit Informationen überschwemmt werden. Dies wäre aus Sicht der Betroffenen – vor allem bei gängigen Transaktionen – mit Sicherheit nicht erwünscht.

Die Selbstverantwortung soll auch auf Seiten der Inhaber der Datensammlungen gestärkt werden. Deshalb wird mit dem vorliegenden Entwurf angestrebt, Selbstregulierungsmechanismen – namentlich die Vergabe von Datenschutz-Qualitätszeichen bzw. – Zertifizierungen durch unabhängige Stellen – zu fördern.

Sodann strebt der Entwurf eine klarere Umschreibung der Verantwortlichkeiten und der Kontrolle bei der Delegation der Bearbeitung an Dritte an. Er auferlegt den Inhabern der Datensammlungen eine Sorgfaltspflicht; gleichzeitig überlässt er ihnen einen erheblichen Handlungsspielraum bezüglich der Wahl der Mittel zu deren Erfüllung. Der Inhaber der Datensammlung muss sich bei der Bekanntgabe von Daten ins Ausland vergewissern, dass beim Empfänger ein angemessenes Schutzniveau gewährleistet ist. Der Entwurf schreibt indessen nicht vor, welche Vorkehrungen er dazu zu treffen hat. Das erforderliche angemessene Schutzniveau kann sich insbesondere aus gesetzlichen oder vertraglichen Bestimmungen sowie aus internationalen Abkommen ergeben. Desgleichen ist der Inhaber der Datensammlung in der Wahl der Mittel frei, durch die er eine Datenbeschaffung erkennbar macht. Er trägt jedoch die Verantwortung für allfällige den durch die Beschaffung Betroffenen zugefügte Nachteile.

Der Entwurf überträgt dem Bundesrat die Befugnis, während einer befristeten Zeitdauer die automatisierte Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen im Rahmen von Pilotversuchen vor dem Inkrafttreten einer formellgesetzlichen Grundlage zu bewilligen.

Für die Bearbeitung von Daten des Bundes durch kantonale Organe im Rahmen des Vollzugs von Bundesrecht werden die durch die Kantone zu erfüllenden Anforderungen angehoben und die Kontrollmöglichkeiten erweitert. Soweit Daten des Bundes bearbeitet werden, verfügt die Eidgenossenschaft über eine ausreichende verfassungsmässige Kompetenzgrundlage, um den Kantonen Mindeststandards aufzuerlegen (vgl. Ziff. 5.1).

Als Ergänzung zur Informationspflicht wird vorgeschlagen, die Rechte derjenigen Personen zu stärken, welche die Bearbeitung der sie betreffenden Daten untersagen wollen. Erfahrungsgemäss befindet sich eine Person, die eine Verletzung ihrer Persönlichkeitsrechte erleidet, oft in einer Position, die es ihr nicht erlaubt, mit den ihr zustehenden Rechtsmitteln wirksam dagegen vorzugehen. Vielfach ist die Verletzung, wenn die Justiz eingreift, bereits erfolgt und kann nicht mehr verhindert werden. Oft liefert der Inhaber der Datensammlung auch nicht die nötigen Angaben (z.B. über die Rechtfertigungsgründe, auf die er eine bestimmte Bearbeitung stützt), die es der betroffenen Person erlauben würden, ihre allfälligen Ansprüche geltend zu machen. Die an die Datenerhebung geknüpfte Informationspflicht erscheint nur dann sinnvoll, wenn sie für die betroffene Person mit der Möglichkeit verbunden ist, sich der Datenbearbeitung wirksam zu widersetzen. Deshalb sieht der Entwurf für den Fall einer Untersagung der Datenbearbeitung durch die betroffene Person vor, dass der Inhaber der Datensammlung die Bearbeitung sofort vorübergehend einzustellen und ihr die Rechtfertigungsgründe mitzuteilen hat. Der Inhaber der Datensammlung kann jedoch mit der Datenbearbeitung fortfahren, wenn diese gesetzlich vorgesehen ist.

Weitere Massnahmen zur Verstärkung der Position der Betroffenen im Prozess sind denkbar. So wurde angeregt, nach dem Beispiel des Artikel 13*a* des Bundesgesetzes gegen den unlauteren Wettbewerb[7] eine Beweislastumkehr einzuführen, da der Beweis der Unrechtmässigkeit einer Verletzung von Persönlichkeitsrechten oder der Tragweite der erlittenen Beeinträchigung, beispielsweise im Fall einer grenzüberschreitenden Datenübermittlung, in der Regel schwierig ist. Die Ausnahmen von den

7 SR **241**

allgemein geltenden Beweisregeln sollen indessen nicht weiter ausgebaut werden. Auch ohne Erleichterungen bei der Beweislast muss es aber bereits heute dem Inhaber der Datensammlung obliegen, diejenigen Tatsachen zu beweisen, welche in seinem Einflussbereich liegen (z.B. das Vorliegen von Gründen, die eine Datenbearbeitung rechtfertigen). Weiter wurde auch die Frage aufgeworfen, ob der Ausgleich für unrechtmässige Beeinträchtigungen – insbesondere bei grenzüberschreitenden Datenübermittlungen – durch die allgemeinen Haftungsregeln ausreichend sichergestellt sei. Ein Ausgleich mittels der Einführung neuer Sanktionen, beispielsweise in Form einer Entschädigung, die unabhängig vom Ausmass der Beeinträchtigung zu leisten wäre (ähnlich wie dies im Arbeitsrecht im Fall einer missbräuchlichen Kündigung vorgesehen ist), wurde nach eingehender Prüfung verworfen. Diese Art der Sanktion wäre im schweizerischen Recht ein Fremdkörper, zumal das Datenschutzrecht nicht nur Beziehungen vertraglicher Natur erfasst.

Die Revision erlaubt in gewissen Punkten die Annäherung des schweizerischen Rechts an das Recht der Europäischen Union, doch hat der Entwurf nicht zum Ziel, unser Recht in allen Punkten demjenigen der EU anzugleichen. Anerkanntermassen entspricht das Schutzniveau des DSG annähernd demjenigen des EU-Rechts. Die EU zählt daher die Schweiz zu den Ländern, die ein angemessenes Datenschutzniveau aufweisen, womit der Datentransfer aus den EU-Mitgliedstaaten in unser Land erlaubt ist. Sollte sich im Rahmen der Bilateralen II (Liberalisierung des Dienstleistungsverkehrs sowie Übereinkommen von Schengen und Dublin) die Notwendigkeit der Übernahme des Gemeinschaftsrechts im Datenschutzbereich ergeben, würde eine umfangreichere Revision des DSG notwendig werden. Dies könnte in einer nächsten Revisionsphase geschehen; allenfalls könnte dem Parlament auch eine Zusatzbotschaft vorgelegt werden.

Schliesslich wären bezüglich der im DSG verwendeten Terminologie verschiedene Änderungen denkbar. Die Neudefinition gewisser Begriffe (z.B. «Dritte» oder «Abrufverfahren») könnte gewisse Vorteile bringen; darüber hinaus entspricht der Ausdruck «Inhaber der Datensammlung» nicht der Begrifflichkeit der Richtlinie 95/46/EG. Aufgrund der weitreichenden Auswirkungen auf den gesamten Gesetzestext, welche neue Legaldefinitionen nach sich ziehen, soll indessen auf eine Neufassung oder Ergänzung der heute geltenden Begriffsdefinitionen (Art. 3 DSG) im Rahmen der Teilrevision verzichtet werden.

1.2.2 Die wesentlichen Neuerungen

1.2.2.1 Die Informationspflicht bei der Erhebung von Personendaten

Eine der hauptsächlichen Neuerungen des Gesetzesentwurfs ergibt sich aus der Umsetzung der Motion «Erhöhte Transparenz»: Es wird eine verhältnismässig detaillierte Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen eingeführt (Art. 7*a* des Entwurfs). Beim Beschaffen von Daten, die nicht besonders schützenswert sind und keine Persönlichkeitsprofile darstellen, wird die Informationspflicht hingegen relativiert. Artikel 4 Absatz 4 des Entwurfs beschränkt sich für diese Art von Daten auf den Grundsatz, dass die Beschaffung und insbesondere der Zweck der Bearbeitung erkennbar sein müssen. Dieser Grundsatz ist nicht neu, denn er gilt heute schon für die Beschaffung

von Personendaten durch Bundesorgane (Art. 18 Abs. 2 DSG). Er soll künftig auch für den privaten Sektor Anwendung finden. Der Umfang dieser Verpflichtung wird von den Umständen der Beschaffung abhängen. Sind Beschaffung und Zweck der Bearbeitung nach den konkreten Umständen für die betroffene Person offensichtlich erkennbar, ist keinerlei zusätzliche Information seitens der die Daten beschaffenden Person erforderlich. Sind Beschaffung und Zweck der Bearbeitung nach den Umständen hingegen nicht oder nicht deutlich erkennbar, wird von der Person, welche die Daten beschafft, mehr Information erwartet.

1.2.2.2 Vereinfachung der Meldepflicht

Die für Privatpersonen und Bundesorgane geltende Verpflichtung, die Übermittlung von Daten ins Ausland vorgängig dem Eidgenössischen Datenschutzbeauftragten zu melden (Art. 6 DSG), wird durch eine Sorgfaltspflicht ersetzt, die nur noch eine eng begrenzte Informationspflicht umfasst. Die Verpflichtung der Privatpersonen, die regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder regelmässig Personendaten an Dritte bekannt geben, ihre Datensammlungen beim Datenschutzbeauftragten anzumelden (Art. 11 DSG) wird mit dem neuen Artikel 11*a* beibehalten. Der im Vernehmlassungsentwurf enthaltene Vorschlag, die Meldepflicht abzuschaffen, hat keinen ungeteilten Anklang gefunden; zudem scheint es zum gegenwärtigen Zeitpunkt nicht mehr gleichermassen wahrscheinlich, dass die EU ihre Richtlinie in diesem Punkt revidieren wird, wie dies zum Zeitpunkt der Ausarbeitung des Vernehmlassungsentwurfs der Fall war. Die Meldepflicht wird nun beibehalten, aber differenzierter geregelt; die Meldung selbst soll administrativ vereinfacht werden.

1.2.2.3 Untersagung der Datenbearbeitung

Das Recht der betroffenen Person, sich der Bearbeitung von sie betreffenden Personendaten zu widersetzen ist bereits in Artikel 12 Absatz 2 Buchstabe b und Artikel 20 DSG geregelt. Artikel 15 DSG umschreibt das Verfahren, wenn gegen eine Bearbeitung durch private Personen vorgegangen werden soll. Der Gesetzesentwurf sieht mit Artikel 15*a* eine diesbezügliche Neuerung vor. Private werden verpflichtet, die Bearbeitung unverzüglich einzustellen, wenn die betroffene Person die Bearbeitung untersagt; es sei denn, für die Bearbeitung bestehe eine gesetzliche Pflicht. Der Inhaber der Datensammlung muss daraufhin innert zehn Tagen einen Rechtfertigungsgrund geltend machen. Tut er dies, so können die Betroffenen noch innert einer Frist von zehn Tagen vom Richter verlangen, dass er die Bearbeitung gemäss Artikel 15 Absatz 1 DSG provisorisch oder definitiv untersagt. Diese Massnahme ergibt sich indirekt aus der Motion «Erhöhte Transparenz». Das Recht auf Information hätte keinerlei praktischen Nutzen, wenn die betroffene Person sich der Bearbeitung nicht wirksam widersetzen könnte.

1.2.2.4 Förderung der Selbstregulierung durch Zertifizierung

Mit dem Entwurf soll die Selbstregulierung im Bereich des Datenschutzes gefördert werden. Deshalb sieht er mit dem neuen Artikel 11 eine Bestimmung vor, die darauf abzielt, die Verbreitung von Datenschutzzertifizierungen und – Qualitätszeichen zu begünstigen. Der Bundesrat wird ermächtigt, die Zertifizierungsverfahren und die Anerkennung der zertifizierenden Stellen so weit wie nötig zu regeln. Ebenfalls ist vorgesehen, dass zertifizierte Unternehmen von der Meldepflicht nach Artikel 11*a* entbunden werden können.

1.2.2.5 Automatisierte Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen im Rahmen von Pilotversuchen

In seiner Antwort auf die Motion «Online-Verbindungen» hat der Bundesrat dargelegt, dass im Rahmen einer Revision des DSG die Anforderungen an die gesetzliche Grundlage im Lichte der Bedürfnisse der Praxis anzupassen seien. Der Entwurf sieht daher einen neuen Artikel 17*a* vor, der es dem Bundesrat erlaubt, für eine zeitlich beschränkte Dauer die automatisierte Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen im Rahmen von Pilotversuchen zu bewilligen, bevor die entsprechende formellgesetzliche Grundlage in Kraft getreten ist. Das Gesetz sieht Kriterien vor, die umschreiben, in welchen Fällen die Notwendigkeit zur Durchführung eines Pilotversuches gegeben ist. Die Aufgaben, welche die betreffende Datenbearbeitung erfordern, müssen indessen wie bisher in einem formellen Gesetz umschrieben sein.

1.2.2.6 Gemeinsame Bearbeitung von Personendaten durch Bundesorgane und Dritte

Es kommt vor, dass Bundesorgane Daten zusammen mit kantonalen Behörden oder Privatpersonen bearbeiten, welche ihrerseits die Bearbeitung teilweise oder vollumfänglich Dritten anvertrauen können. Somit stellt sich die Frage, wie das Bundesorgan weiterhin seine Verantwortung zum Schutz dieser Daten wahrnehmen kann. Der Gesetzesentwurf bringt diesbezüglich Verbesserungen, denn er erlaubt dem Bundesorgan, bei dem Dritten, der die Daten bearbeitet, Kontrollen durchzuführen oder durchführen zu lassen (Art. 16 Abs. 3 und 4 des Entwurfs). Die Kompetenz, bei den Kantonen oder Dritten Kontrollen durchzuführen, ergibt sich bereits aus dem Begriff des Inhabers der Datensammmlung. Sie ergibt sich auch aufgrund der allgemeinen Regeln über die Bundesaufsicht.

1.2.2.7 Mindeststandard in den Kantonen

Der Gesetzesentwurf verstärkt den Schutz der Daten, die von kantonalen Organen beim Vollzug von Bundesrecht bearbeitet werden, indem er (im Einklang mit den Forderungen der Motion «Online-Verbindungen») einen Mindeststandard festlegt. Das Regelungskonzept von Artikel 37 Absatz 1 des Entwurfs lehnt sich an das für die grenzüberschreitende Datenübermittlung vorgesehene System an: Gewährleisten die kantonalen Datenschutzbestimmungen kein angemessenes Schutzniveau, kommen die Bestimmungen des Bundesrechts ergänzend zur Anwendung.

1.2.3 Das internationale Umfeld

1.2.3.1 Europarat

1.2.3.1.1 Geltendes Recht

Angesichts des Informationsflusses, der letztlich keine Grenzen kennt, drängt sich eine internationale Zusammenarbeit auf, um ein möglichst hohes Datenschutzniveau bei gleichzeitiger Gewährleistung des freien grenzüberschreitenden Informationsaustausches sicherzustellen. Mit dieser Zielsetzung hat der Europarat das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen STE 108) vom 28. Januar 1981[8] beschlossen. Dieses Übereinkommen trat für die Schweiz am 1. Februar 1998[9] in Kraft.

Zweck des Übereinkommens ist es, im privaten und im öffentlichen Sektor den Rechtsschutz des Einzelnen gegenüber der automatischen Verarbeitung der ihn betreffenden personenbezogenen Daten zu verstärken. In allen Mitgliedstaaten soll ein Minimum an Persönlichkeitsschutz bei der Verarbeitung von Personendaten und eine gewisse Harmonisierung des Schutzsystems sichergestellt werden; anderseits gewährleistet das Übereinkommen den internationalen Datenverkehr dadurch, dass keine Vertragspartei den Transfer von Informationen an eine andere Vertragspartei, welche den vom Übereinkommen vorgesehen Mindestschutz gewährleistet, untersagen darf.

Die im Übereinkommen STE 108[10] niedergelegten Grundsätze des Datenschutzes finden sich auch in den Richtlinien der OECD vom 23. September 1980 über den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten. Diese Grundsätze wurden auf Ebene der EU auch in die Richtlinie 95/46/EG (vgl. Ziff. 1.2.3.2) aufgenommen. Das Übereinkommen vervollständigt und konkretisiert im Bereich der automatisierten Bearbeitung von Personendaten die Artikel 8 (Recht auf Privatsphäre) und 10 (Meinungsäusserungsfreiheit) der Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten[11] (EMRK; durch die Schweiz ratifiziert am 28. November 1974). Das schweizerische Recht genügt bereits heute den Anforderungen des Übereinkommens.

8 SR **0.235.1**
9 Vgl. den Originaltext des Übereinkommens in BBl **1997** I 740 ff.
10 SR **0.235.1**
11 SR **0.101**

Das Ministerkomitee hat mehrere Empfehlungen im Datenschutzbereich angenommen. Diese sehen generell vor, dass wer Personendaten erhebt, die Betroffenen angemessen zu informieren hat. Diese Informationen betreffen vor allem die rechtliche Grundlage für die Beschaffung bzw. Bearbeitung, die Kategorie der erhobenen oder bearbeiteten Daten, die Identität des für die Bearbeitung Verantwortlichen sowie Angaben über die Personen und Organismen, bei denen Daten erhoben wurden oder denen die Daten bekannt gegeben werden können. Ferner ist darüber zu informieren, ob es sich um eine freiwillige oder obligatorische Erhebung handelt, sowie über die Möglichkeit, die Angabe der Daten zu verweigern, und die Folgen einer Verweigerung[12]. Mit der Umsetzung der Motion «Erhöhte Transparenz» durch Einführung einer detaillierten Informationspflicht für die Erhebung von besonders schützenswerten Daten und von Persönlichkeitsprofilen und einer weniger weitgehenden Informationspflicht für die übrigen Datenkategorien schlägt der vorliegende Entwurf die Richtung dieser Empfehlungen ein.

1.2.3.1.2 Zusatzprotokoll zum Übereinkommen STE 108

Die Delegierten der Minister haben an ihrer Sitzung vom 23. Mai 2001 ein Zusatzprotokoll betreffend die Kontrollbehörden und den grenzüberschreitenden Datenverkehr verabschiedet. Das Zusatzprotokoll ergänzt das Übereinkommen STE 108[13], das von der Schweiz bereits ratifiziert worden ist. Es soll die Umsetzung der im Übereinkommen STE 108 enthaltenen Grundsätze verbessern. Die Verbesserung der Umsetzung ist heute aufgrund der steigenden Zahl von grenzüberschreitenden Datentransaktionen aus einem Vertragsstaat in einen Drittstaat oder in eine Drittorganisation nötig geworden. Sie umfasst zwei Aspekte: Einerseits geht es um eine Harmonisierung der Zuständigkeiten der Kontrollbehörden; andrerseits soll vermieden werden, dass Datentransfers in Drittstaaten oder an Drittorganisationen zu einer Umgehung der Gesetzgebung eines Herkunftsstaates führen, der das Übereinkommen STE 108 unterzeichnet hat.

Das Zusatzprotokoll sieht insbesondere die Einsetzung von Kontrollbehörden vor, denen es obliegt, über die Einhaltung der Massnahmen zu wachen, welche im jeweiligen Landesrecht die im Übereinkommen und im Protokoll stipulierten Grundsätze durchsetzen sollen. Diese Behörden sollten über Untersuchungsbefugnisse verfügen sowie Klagen führen bzw. der zuständigen Gerichtsbehörde Verletzungen der einschlägigen Bestimmungen des Landesrechts zur Kenntnis bringen können. Weiter sieht das Protokoll vor, dass der Transfer von personenbezogenen Daten an einen Datenempfänger, der vom Übereinkommen nicht erfasst ist, nur erfolgen kann, wenn der Empfängerstaat oder die Empfängerorganisation ein angemessenes

12 Vgl. Ziff. 3.2 der Empfehlung Nr. R (95) über den Schutz personenbezogener Daten im Telekommunikationsbereich, namentlich im Hinblick auf telefonische Dienstleistungen; vgl. Ziff. 5 der Empfehlung Nr. R (97) 5 bezüglich des Schutzes medizinischer Daten; vgl. Ziff. 5 der Empfehlung Nr. R (97) 18 betreffend den Schutz personenbezogener, für statistische Zwecke beschaffter und bearbeiteter Daten; vgl. Ziff. 3.3 der Empfehlung Nr. R (90) 19 über den Schutz personenbezogener, für Zahlungen und andere damit zusammenhängende Operationen verwendeter Daten; vgl. Ziff. 5 der Empfehlung Nr. R (2002) 9 betreffend den Schutz personenbezogener, für Versicherungszwecke beschaffter und bearbeiteter Daten.

13 SR **0.235.1**

Schutzniveau gewährleistet. Die Garantien können insbesondere aus entsprechend ausgestalteten Vertragsklauseln hervorgehen. Die vom Zusatzprotokoll vorgesehenen Anforderungen bezüglich der Aufsichtsbehörden und den grenzüberschreitenden Datenverkehr sind jenen der Richtlinie 95/46/EG sehr ähnlich.

Das Zusatzprotokoll kann nur von denjenigen Staaten unterzeichnet werden, die auch das Übereinkommen STE 108 unterzeichnet haben. Für das Inkrafttreten sind fünf Ratifikationen nötig. Jeder Vertragsstaat kann das Protokoll jederzeit mit einer Notifikation an das Generalskretariat des Euroaparates kündigen.

Der Bundesrat hat das Zusatzprotokoll am 17. Oktober 2002 unterzeichnet und beantragt die Genehmigung durch das Parlament. Bisher haben zwei Staaten das Zusatzprotokoll ratifiziert. Mit der Ratifikation des Protokolls nähert sich die Schweiz dem Datenschutzsystem der EU an und gibt darüber hinaus ihrem klaren Willen Ausdruck, das vom Europarat festgelegte Datenschutzniveau, insbesondere bei grenzüberschreitenden Datenübermittlungen, einzuhalten.

Betreffend die Auswirkungen der Ratifikation des Zusatzprotokolls auf das kantonale Recht kann auf die untenstehenden Ausführungen unter Ziffer 3.2.2 verwiesen werden.

1.2.3.1.2.1 Aufsichtsbehörden

Das Protokoll verpflichtet jeden Vertragsstaat, eine oder mehrere unabhängige Aufsichtsbehörden vorzusehen (Art. 1 Ziff. 1 und Ziff. 3). Diese Behörden müssen Ermittlungen durchführen und einschreiten können sowie die Befugnis haben, Klagen anzustrengen bzw. den zuständigen Justizbehörden Verstösse gegen die innerstaatlichen Rechtsvorschriften zur Umsetzung der Grundsätze des Übereinkommens STE 108[14] oder des Zusatzprotokolls zur Kenntnis zu bringen (Art. 1 Ziff. 2). Jede Aufsichtsbehörde kann von jeder Person angerufen werden, die in deren Zuständigkeitsbereich den Schutz ihrer Rechte und grundlegenden Freiheiten beim Verarbeiten personenbezogener Daten verlangt (Art. 1 Ziff. 2). Die Entscheide der Aufsichtsbehörden können vor Gericht angefochten werden (Art. 1 Ziff. 4). Die Aufsichtsbehörden pflegen die Zusammenarbeit und insbesondere den Informationsaustausch (Art. 1 Ziff. 5):

Das DSG sieht bereits zwei unabhängige Aufsichtsbehörden vor, nämlich den Eidgenössischen Datenschutzbeauftragten, der seine Aufgaben unabhängig erfüllt (Art. 26 Abs. 2 DSG) und die Eidgenössische Datenschutzkommission, welche eine Schieds- und Rekurskommission im Sinne des Bundesgesetzes vom 20. Dezember 1968[15] über das Verwaltungsverfahren ist (Art. 33 DSG). Der Datenschutzbeauftragte hat Untersuchungskomptenzen (Art. 27 Abs. 1–3 sowie Art. 29 Abs. 1 und 2 DSG) und bestimmte Eingriffsmöglichkeiten; insbesondere kann er Empfehlungen abgeben (Art. 27 Abs. 4 und 5 und Art. 29 Abs. 3 und 4 DSG). Er kann von Amtes wegen oder auf Gesuch Dritter hin tätig werden. Das geltende Recht entspricht demnach bereits in weiten Teilen den Anforderungen des Protokolls, mit einer Ausnahme: Der Datenschutzbeauftragte hat heute im Rahmen der Aufsicht über

14 SR **0.235.1**
15 SR **172.021**

Bundesorgane nicht die Kompetenz, Beschwerde zu führen[16]. Artikel 27 Absatz 6 des Gesetzesentwurfs bringt das schweizerische Recht in diesem Punkt in Übereinstimmung mit dem Protokoll.

1.2.3.1.2.2 Grenzüberschreitender Datenverkehr

Das Protokoll verpflichtet die Vertragsstaaten dazu, sicherzustellen, dass personenbezogene Daten nur dann an Empfänger übermittelt werden, die der Rechtshoheit eines Staates oder einer Organisation unterliegen, welche nicht Vertragspartei des Übereinkommens sind, wenn dieser Staat bzw. diese Organisation einen adäquaten Schutz für die beabsichtigte Datenübermittlung gewährleistet (Art. 2 Ziff. 1). Die Vertragsstaaten können im innerstaatlichen Recht Abweichungen von diesem Grundsatz vorsehen um bestimmten Interessen der Betroffenen oder legitimen überwiegenden Interessen, insbesondere wichtigen öffentlichen Interessen, Rechnung zu tragen (Art. 2 Ziff. 2 Bst. a). Desgleichen können sie die Übermittlung zulassen, sofern von der für die Übermittlung verantwortlichen Person Sicherheitsvorkehrungen getroffen werden (die sich insbesondere aus vertraglichen Klauseln ergeben können) und diese nach Auffassung der zuständigen Behörde ausreichend sind (Art. 2 Ziff. 2 Bst. b).

Ob das Schutzniveau im Empfängerstaat oder bei der Empfängerorganisation angemessen ist, ist mit Blick auf die gesamten Umstände der Datenübermittlung zu prüfen. Diese Prüfung umfasst auch die Berücksichtigung der im Übereinkommen STE 108[17] und im Zusatzprotokoll aufgestellten Grundsätze in der Gesetzgebung sowie der Rechtspraxis des Empfängerstaates. Ebenfalls ist zu berücksichtigen, wie die betroffene Person bei Nichteinhaltung dieser Grundsätze ihre Interessen wahren kann. Die zuständige Behörde eines Vertragsstaates kann die Angemessenheit des Schutzniveaus für bestimmte Staaten oder Organisationen als Ganzes evaluieren.

Bei der Bestimmung der Abweichungen vom Grundsatz des angemessenen Schutzniveaus verfügen die Vertragsstaaten über einen Ermessensspielraum. Solche Abweichungen können vorgesehen werden um ein wichtiges öffentliches Interesse im Sinne von Artikel 8 Ziffer 2 der EMRK[18] oder Artikel 9 Ziffer 2 des Übereinkommens STE 108[19] zu schützen. Ausnahmen sind ebenfalls möglich, um bestimmten Interessen der betroffenen Person Rechnung zu tragen (z.B. die Erfüllung eines Vertrags, der Schutz lebenswichtiger Interessen der betroffenen Person oder das Vorliegen der Zustimmung der betroffenen Person).

Das DSG regelt heute schon die Übermittlung von personenbezogenen Daten ins Ausland; die Regelung weicht indessen vom Protokoll ab. Artikel 6 DSG untersagt die Bekanntgabe von Personendaten ins Ausland, wenn die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein Datenschutz fehlt, der dem schweizerischen gleichwertig ist. Andererseits muss, wer Datensammlungen ins Ausland übermitteln will, dies dem Datenschutzbeauftragten vorher melden, wenn für die Bekanntgabe keine gesetzliche Pflicht besteht und die

16 BGE **123** II 542
17 SR **0.235.1**
18 SR **0.101**
19 SR **0.235.1**

betroffenen Personen davon keine Kenntnis haben (Art. 6 Abs. 2 DSG): Der Gesetzesentwurf sieht vor, diese Meldepflicht durch ein System im Sinne des Protokolls zu ersetzen, das auch dem der Richtlinie 95/46/EG weitgehend entspricht.

1.2.3.2 Das Gemeinschaftsrecht

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachstehend: Richtlinie 95/46/EG) ist einerseits auf die Gewährleistung des Schutzes der Grundrechte – insbesondere der Privatsphäre – der natürlichen Personen gerichtet. Anderseits strebt sie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten an.

Mit Kommissionsbeschluss vom 26. Juli 2000[20] hat die Europäische Union die Schweiz als Drittstaat mit angemessenem Schutzniveau bezeichnet (vgl. Art. 25 Abs. 2 der Richtlinie 95/46/EG). Damit attestierte sie, dass die schweizerische Gesetzgebung gesamthaft gesehen annähernd das in der Richtlinie geforderte Schutzniveau erreicht. Das DSG stimmt jedoch nicht in allen Punkten mit dieser Richtlinie überein.

Es wäre zum heutigen Zeitpunkt verfrüht, eine Totalrevision des DSG ins Auge zu fassen, die das Ziel einer vollständigen Kompatibilität mit dem Gemeinschaftsrecht verfolgt (vgl. Ziff. 1.2.1). Der Gesetzesentwurf nähert indessen das schweizerische Recht dem EU-Recht in verschiedenen Punkten an. Durch die Einführung einer Informationspflicht bei der Erhebung von besonders schützenswerten Daten oder Persönlichkeitsprofilen (Art. 7*a*), und – bezüglich der übrigen Fälle – mit der Forderung, dass die Erhebung für die betroffene Person erkennbar sein müsse (Art. 4 Abs. 4), erfüllt der Entwurf teilweise die Anforderungen von Artikel 10 und 11 der Richtlinie. Die Bedingungen für die Gültigkeit der Zustimmung der betroffenen Person zu einer Datenbearbeitung definiert Artikel 4 Absatz 5 des Entwurfs analog zur Richtlinie 95/46/EG.

Mit Artikel 7*b* gewährleistet der Gesetzesentwurf ausserdem, dass die von einer automatisierten Einzelentscheidung betroffene Person gebührend über die Art und Weise des Zustandekommens der Entscheidung informiert wird. Damit geht er allerdings nicht so weit wie die Richtlinie, welche den betroffenen Personen das Recht zuerkennt, überhaupt keinen Entscheidungen unterworfen zu werden, die allein gestützt auf eine automatisierte Verarbeitung erlassen wurden. Schliesslich sieht der Revisionsentwurf vor, dem Datenschutzbeauftragten eine Befugnis zur Beschwerde gegen Entscheide der Departemente und der Bundeskanzlei zu übertragen (Art. 27, Abs. 6). Die Richtlinie sieht ebenfalls vor, dass die Kontrollbehörde die Kompetenz haben muss, Klagen zu führen oder der zuständigen Gerichtsbehörde die Verletzungen der einschlägigen Bestimmungen des Landesrechts zur Kenntnis bringen zu können. Das Zusatzprotokoll zum Übereinkommen STE 108[21] stellt ähnliche Anforderungen auf (vgl. Ziff. 1.2.3.1.2).

20 Veröffentlicht im ABl L 215 vom 25.8.2000, S.1.
21 SR **0.235.1**

Der Revisionsentwurf geht auch noch in anderen Punkten nicht so weit wie die Richtlinie. Diese verbietet beispielsweise die Bearbeitung von sensiblen Personendaten hinsichtlich Rasse, politischen Auffassungen, religiösen oder philosophischen Überzeugungen, Gewerkschaftszugehörigkeit sowie Gesundheit und Sexualleben (wobei dieses Verbot nicht absolut ist und durch eine Reihe von Ausnahmen gemildert wird). Solche Daten fallen nach schweizerischen Recht weitgehend in die Kategorie der besonders schützenswerten Personendaten. Ihre Bearbeitung ist strengen Anforderungen unterworfen. So muss für die Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen an Dritte ein Rechtfertigungsgrund nach Artikel 13 DSG gegeben sein (vgl. Art. 12 Abs. 2 Bst. c DSG). Die für die Beschaffung dieser Kategorie von Daten gemäss Artikel 7*a* des Entwurfs vorgesehene Informationspflicht sollte im Übrigen eine dissuasive Wirkung haben. Die Inhaber der Datensammlungen werden kein Interesse daran haben, solche Daten zu erheben – und damit den entsprechenden Informationsaufwand leisten zu müssen –, wenn dies für ihre Tätigkeit oder die Erfüllung ihrer Aufgaben nicht unbedingt erforderlich ist. Weiter sieht die Richtlinie vor, dass der für die Bearbeitung Verantwortliche zu verpflichten ist, vor der Durchführung einer ganz oder teilweise automatisierten Bearbeitung eine Meldung an die Kontrollbehörde zu erstatten. Im schweizerischen Recht geht die Verpflichtung für die Privaten, ihre Datensammlungen beim Datenschutzbeauftragten anzumelden, heute weniger weit, als die Richtlinie es vorsieht. Der vorliegende Entwurf bringt zwar einige Anpassungen; diese gehen indessen nicht so weit wie die von der Richtlinie vorgesehene Meldepflicht. Im Gegensatz zum schweizerischen Recht sieht die Richtlinie auch vor, dass die betroffene Person eine Datenbearbeitung zum Zwecke der Direktwerbung untersagen kann.

1.2.3.3 Internationaler Vergleich

1.2.3.3.1 Italien

Gemäss dem Gesetz Nr. 675 vom 31. Dezember 1996 müssen die betroffenen Personen vor jeder Bearbeitung mündlich oder schriftlich über den Zweck der Bearbeitung, für welche die Daten bestimmt sind, den obligatorischen oder freiwilligen Charakter der Bearbeitung, die Folgen einer allfälligen Verweigerung der geforderten Angaben, die Datenempfänger oder Kategorien von Datenempfängern, denen die Daten bekannt gegeben werden können, die Rechte bezüglich Information und Auskunft, sowie den Namen und Firmennamen des Dateninhabers oder des für die Bearbeitung Verantwortlichen informiert werden.

Das italienische Gesetz unterstellt die Datenbearbeitung durch Privatpersonen oder öffentliche Organe grundsätzlich der ausdrücklichen Einwilligung der betroffenen Person, sieht aber eine Anzahl Ausnahmen vor. Die betroffene Person hat das Recht, sich aus gesetzlich anerkannten Gründen der Bearbeitung sie betreffender Daten zu widersetzen. Die Datenbearbeitung zu kommerziellen Zwecken oder für Kundenwerbung können Betroffene auch ohne Angabe von Gründen verbieten.

Das Kontrollorgan («il garante») ist ein aus vier Mitgliedern zusammengesetztes Gremium, gewählt von der Abgeordnetenkammer und dem Senat. Es verfügt über ein Autonomiestatut. Ihm obliegt namentlich die Aufgabe, ein Register der Datensammlungen zu führen, die Anwendung der gesetzlichen Bestimmungen zu überwa-

chen, die Dateninhaber und für die Bearbeitung Verantwortlichen auf die Massnahmen aufmerksam zu machen, die zur Einhaltung der Datenschutzgesetzgebung erforderlich sind, über die von den betroffenen Personen eingereichten Beschwerden zu befinden, die von Amtes wegen verfolgten Verstösse anzuzeigen, und diejenigen Bearbeitungen zu untersagen, welche ein konkretes Risiko bergen, einer oder mehreren Personen Schaden zuzufügen. Das Kontrollorgan kann auch Sanktionen verhängen.

1.2.3.3.2 Deutschland

Der Bundestag hat das deutsche Datenschutzgesetz am 7. April 2001 revidiert, um die europäische Richtlinie 95/46/EG umzusetzen. Die Revision zielte vor allem darauf ab, die Transparenz für die betroffenen Personen zu erhöhen. Werden Daten beschafft, ohne dass die Betroffenen davon Kenntnis haben, muss der für die Bearbeitung Verantwortliche der betroffenen Person seine Identität, den Zweck der Datenerhebung oder der Bearbeitung sowie – im privaten Bereich – die Kategorie der gesammelten Daten mitteilen. Muss die betroffene Person nach den Umständen im konkreten Fall nicht damit rechnen, dass eine Bekanntgabe der Daten an Dritte erfolgt, ist sie auch über die Kategorien der Empfänger zu informieren, denen die Daten bekanntgegeben werden sollen. Ausserdem dürfen Entscheidungen, die für den Einzelnen rechtliche Folgen nach sich ziehen oder ihn auf andere Weise wesentlich betreffen, nicht ausschliesslich auf eine automatisierte Bearbeitung personenbezogener Daten gestützt werden, die der Bewertung bestimmter Persönlichkeitsmerkmale dient.

1.2.3.3.3 Österreich

Das Bundesgesetz über den Schutz personenbezogener Daten 2000 auferlegt dem für die Bearbeitung Verantwortlichen bei der Datenerhebung eine Informationspflicht gegenüber der betroffenen Person. Diese Informationspflicht ist, je nach Umständen, mehr oder weniger streng. Der für die Bearbeitung Verantwortliche muss mindestens Informationen über den Zweck der Bearbeitung und seine Identität liefern. Wenn es der Grundsatz von Treu und Glauben verlangt, müssen auch noch weitere Informationen erfolgen. Niemand darf ferner einer Entscheidung unterworfen werden, die ausschliesslich auf Grund einer automatisierten Datenbearbeitung ergeht, mittels der gewisse Aspekte seiner Person bewertet werden, wie beispielsweise die beruflichen Leistungsfähigkeit, die Kreditfähigkeit, die Zuverlässigkeit oder andere Verhaltensmerkmale der betroffenen Person.

Das Gesetz setzt zur Wahrung des Datenschutzes eine Datenschutzkommission und einen Datenschutzrat ein. Die Kommission besteht aus sechs Mitgliedern, die in der Ausübung ihrer Funktionen vollständig unabhängig sind. Jede Bearbeitung muss ihr vorgängig zwecks Eintrag in ein Register gemeldet werden. An die Kommission kann sich auch wenden, wer sich über eine Verletzung seiner Rechte beschweren will. Sie hat das Recht, Untersuchungen vorzunehmen, wenn Anzeichen vorliegen, die einen Verstoss gegen das Gesetz vermuten lassen. Die Kommission kann Empfehlungen herausgeben. Werden sie nicht befolgt, kann sie – je nach der Art des

Verstosses – Strafklage einreichen, vor den Zivilgerichten auftreten oder sich an die vorgesetzte Instanz der handelnden Behörde wenden. Die Kommission kann ferner von Personen angerufen werden, die von einer Verletzung der Informationspflicht bei der Datenerhebung betroffen sind.

1.2.3.3.4 Frankreich

Frankreich hat die Richtlinie 95/46/EG noch nicht umgesetzt. Das geltende Datenschutzgesetz (Gesetz 78/17) datiert vom 6. Januar 1978. Ein Revisionsentwurf zur Umsetzung der Richtlinie wird derzeit vom französischen Parlament beraten.

Das Gesetz 78/17 setzte eine «Commission nationale de l'informatique et des libertés (CNIL)» ein, welche mit der Überwachung der Einhaltung der gesetzlichen Vorschriften beauftragt ist. Die CNIL ist eine unabhängige Verwaltungsbehörde, welche über Verordnungskompetenz verfügt. Sie besteht aus siebzehn Mitgliedern. Zu ihren Aufgaben gehört die Überprüfung der Datensammlungen, die Durchführung von Kontrollen vor Ort, die Gewährleistung des Auskunftsrechts, die Instruktion der Klagen – wobei Lösungen im gegenseitigen Einvernehmen angestrebt werden –, sowie Information und Beratung. Sie erlässt auch vereinfachte Bestimmungen für diejenigen Bearbeitungen, die am gängigsten sind und bei denen nur eine geringe Gefahr von Persönlichkeitsverletzungen besteht.

Jede natürliche Person hat das Recht, sich aus schützenswerten Gründen einer Bearbeitung von sie betreffenden personenbezogenen Informationen zu widersetzen. Ausnahmen können mittels Rechtsverordnung vorgesehen werden.

Die Personen, bei denen personenbezogene Informationen erhoben werden, müssen darüber informiert werden, ob sie verpflichtet sind, die verlangten Angaben zu machen, oder ob dies freiwillig ist. Weiter ist ihnen mitzuteilen, welche Folgen eine Verweigerung der Antwort hat, für welche natürlichen oder juristischen Personen die Informationen bestimmt sind sowie dass ihnen ein Recht auf Zugang zu ihren Personendaten und zu deren Berichtigung zusteht. Werden die Informationen mittels Fragebogen erhoben, ist auf diese Vorschriften hinzuweisen. Weiter kann sich keine gerichtliche Entscheidung, die eine Bewertung menschlichen Verhaltens beinhaltet, auf eine automatisierte Datenbearbeitung stützen, die der Definition eines Persönlichkeitsprofils der betroffenen Person dient.

1.2.3.3.5 Vereinigtes Königreich

Die betroffene Person kann sich einer Bearbeitung personenbezogener Daten zu kommerziellen Zwecken mittels einfacher schriftlicher Erklärung beim für die Bearbeitung Verantwortlichen widersetzen. Das gleiche Recht steht ihr zu, wenn ein sie belastender Entscheid lediglich gestützt auf eine automatisierte Datenbearbeitung ergeht, welche der Beurteilung gewisser Persönlichkeitsaspekte (z.B. Kreditwürdigkeit, Zuverlässigkeit, andere Verhaltensmerkmale, berufliche Leistungsfähigkeit) dient. Die betroffene Person kann ferner mittels einfacher schriftlicher Erklärung und unter Geltendmachung ihrer schützenswerten Interessen jeder Bearbeitung entgegentreten, die geeignet ist, ihr einen erheblichen Nachteil zuzufügen. Die Datenbearbeitung hängt von der Zustimmung der betroffenen Person ab. Grundsätz-

lich darf keine Bearbeitung stattfinden, die nicht vorgängig dem Kontrollorgan gemeldet und von diesem in das Register der Datensammlungen eingetragen wurde. Bei der Beschaffung muss die betroffene Person – soweit dies möglich ist – über die Identität des für die Bearbeitung Verantwortlichen und seines Stellvertreters, den Zweck der Bearbeitung und alle anderen Informationen, die erforderlich sind, damit eine Datenbearbeitung nach Treu und Glauben gewährleistet ist («to enable processing to be fair»), ins Bild gesetzt werden.

Das Kontrollorgan («Information Commissioner») hat Informations- und Beratungsaufgaben. Es kann einen Verhaltenskodex erlassen. Weiter kann es von Amtes wegen oder auf Antrag gegenüber jeder Person, die den Grundsätzen des Datenschutzes zuwiderhandelt, Weisungen («enforcement notice») erlassen. Wird eine solche Weisung nicht befolgt, liegt eine Rechtsverletzung vor.

1.2.4 Zusammenhang mit anderen Rechtsetzungsvorhaben

Zum gegenwärtigen Zeitpunkt befindet sich ein Bundesgesetz über die Öffentlichkeit der Verwaltung (Öffentlichkeitsgesetz) in Ausarbeitung[22]. Dieses Gesetz wird ein allgemeines Recht auf Zugang zu amtlichen Dokumenten schaffen. Durch diesen neuen Erlass werden punktuell einige Bestimmungen des DSG anzupassen sein, um die Koordination zwischen Datenschutz und Informationszugang zu gewährleisten. Es handelt sich dabei namentlich um eine Ergänzung des Artikels 19 DSG, mit der den Behörden erlaubt wird, unter bestimmten Voraussetzungen ausnahmsweise Zugang zu amtlichen Dokumenten zu gewähren, die Personendaten enthalten. Darüber hinaus soll im gleichen Zug auch eine gesetzliche Grundlage geschaffen werden, die den Behörden erlaubt, Dokumente, die nebst anderen Informationen auch Personendaten umfassen (z.B. Berichte, die einzelne Namen oder Adressen beinhalten), im Rahmen ihrer Informationstätigkeiten auf Internet zu veröffentlichen.

Weitere Bestimmungen werden anzupassen sein, um die Koordination der im Öffentlichkeitsgesetz vorgesehenen Verfahrensbestimmungen mit dem Verfahren nach DSG zu gewährleisten.

Die Änderungen des Datenschutzgesetzes, die mit dem Öffentlichkeitsgesetz notwendig werden, wurden im Zuge des Vorverfahrens der Gesetzgebung mit dem vorliegenden Entwurf abgestimmt. Sie werden dem Parlament aber nicht mit der vorliegenden Teilrevision, sondern mit dem Entwurf zum Öffentlichkeitsgesetz unterbreitet, um die materielle Kohärenz sicherzustellen.

1.2.5 Vernehmlassungsverfahren

Zwischen September 2001 und Januar 2002 wurde die Vernehmlassung zum Entwurf zur Teilrevision des Bundesgesetzes über den Datenschutz und das Zusatzprotokoll zum Übereinkommen STE 108[23] durchgeführt.

22 Vgl. die Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung vom 12. Februar 2003.
23 SR **0.235.1**

Die grundsätzlichen Ziele der Reform, insbesondere soweit sie der Motion «Erhöhte Transparenz» entsprechen, wurden weitgehend unterstützt. 16 Kantone, 5 politische Parteien (FDP, Jungfreisinnige, Liberale, SP und SVP) und 14 Organisationen unterstützen grundsätzlich die vorgeschlagene Revision des Datenschutzgesetzes. Wirtschaftskreise lehnen die Revisionsvorschläge hingegen überwiegend oder teilweise ab. Sie befürchten einen unverhältnismässigen Aufwand und praktische Schwierigkeiten. Uneinigkeit herrschte bezüglich der Frage, ob darüber hinaus ein Reformbedarf bestehe. Verschiedene Vernehmlasser – darunter namentlich einige Kantone – hielten die vorgeschlagene Teilrevision für eine Minimallösung, während ein anderer Teil der Vernehmlasser die Revision auf den sich unmittelbar aus den beiden Motionen ergebenden Anpassungsbedarf beschränken wollte.

Mehrheitlich gut aufgenommen worden sind die Einführung des Beschwerderechts des Eidg. Datenschutzbeauftragten, die Verbesserung der Position der Person, die sich einer Bearbeitung sie betreffender Daten widersetzen will sowie die Festlegung von Mindeststandards für die Datenschutzvorschriften der Kantone.

Umstritten war hingegen die Lockerung der Vorschrift, wonach bei der Bearbeitung von Personendaten durch Bundesorgane eine formellgesetzliche Grundlage bestehen muss. Kontrovers aufgenommen wurden ferner die Aufhebung der Meldepflicht für Datensammlungen von Privatpersonen sowie die Kompetenz des Datenschutzbeauftragten, bei den Kantonen Kontrollen durchzuführen, wenn Bundesorgane und kantonale Behörden gemeinsam Daten bearbeiten.

Nahezu unbestritten war schliesslich die Unterzeichnung des Zusatzprotokolls zum Europäischen Übereinkommen STE 108[24].

1.2.6 Wichtigste Änderungen gegenüber dem Vernehmlassungsentwurf

Der vorliegende Entwurf wurde aufgrund der Ergebnisse der Vernehmlassung in den folgenden Punkten angepasst:

- Der Datentransfer an eine ausländische Gesellschaft, die demselben Konzern angehört und sich in einem Land befindet, das nicht über eine Datenschutzgesetzgebung verfügt, die einen angemessenen Schutz gewährleistet, wird unter bestimmten Voraussetzungen vereinfacht (Art. 6 Abs. 2 Bst. g);
- es wird die Einführung einer Bestimmung betreffend Zertifizierungsverfahren (Datenschutzlabel) vorgeschlagen (Art. 11);
- die Meldepflicht für Datensammlungen wird in angepasster Form beibehalten (Art. 11*a*);
- die Voraussetzungen für die Bewilligung von automatisierten Bearbeitungen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen im Rahmen von Pilotversuchen wurden strenger formuliert (Art. 17*a*);
- die Kompetenz des Datenschutzbeauftragten, bei kantonalen Organen Kontrollen durchzuführen, wenn diese mit Bundesorganen zusammen Daten bearbeiten, wurde gestrichen.

24 SR **0.235.1**

1.3 Vorgesehene Umsetzung der Teilrevision

Im öffentlichrechtlichen Bereich sind – zumindest für die Bundesbehörden – keine bedeutenden Umsetzungsmassnahmen notwendig. Auch zur Umsetzung der Teilrevision im privatrechtlichen Bereich sind seitens des Bundes keine besonderen Massnahmen notwendig. Es obliegt den privaten Inhabern von Datensammlungen, die für sie jeweils erforderlichen Schritte – namentlich zur Erfüllung der neu eingeführten Informationspflichten – zu unternehmen. Die Umsetzung im privatrechtlichen Bereich wird durch den Eidgenössischen Datenschutzbeauftragten im Rahmen seiner Kompetenzen nach Artikel 29 DSG überwacht.

Die mit dem Entwurf angestrebte Förderung von Selbstregulierungsansätzen, insbesondere der Zertifizierung, wird ihrerseits für die privaten Inhaber von Datensammlungen einen Anreiz zur Umsetzung der Teilrevision – wie auch der Datenschutzgesetzgebung überhaupt – schaffen. Im Übrigen sollte die Vereinfachung der Wahrnehmung der Rechte der betroffenen Personen dazu beitragen, dass die privaten Inhaber der Datensammlungen ein Interesse haben, die mit der Teilrevision aufgestellten zusätzlichen Anforderungen einzuhalten.

Die kantonalen Gesetzgebungen müssen angepasst werden, soweit sie noch kein angemessenes Schutzniveau erreichen.

1.4 Erledigung parlamentarischer Vorstösse

Mit dem vorliegenden Gesetzesentwurf können die Motion 00.3000 vom 28. Januar 2000 («Erhöhte Transparenz bei der Erhebung von Personendaten») der Kommission für Rechtsfragen des Ständerats und die Motion 98.3529 vom 17. November 1998 («Online-Verbindungen. Erhöhter Schutz für Personendaten») der Geschäftsprüfungskommission des Ständerats als erfüllt abgeschrieben werden (vgl. Ziff. 1.1.2).

2 Erläuterungen zu einzelnen Artikeln

2.1 Art. 2 Geltungsbereich

Nach geltendem Recht wird das Internationale Komitee vom Roten Kreuz gegenüber den anderen internationalen Organisationen mit Sitz auf dem Hoheitsgebiet der Schweizerischen Eidgenossenschaft, mit denen ein Sitzabkommen geschlossen wurde, unterschiedlich behandelt. Eine solche Ungleichbehandlung ist indessen nicht gerechtfertigt. Internationale Organisationen können, soweit ihnen der Status von Völkerrechtssubjekten zukommt, nicht ohne Weiteres dem schweizerischen Recht unterworfen werden. Indem alle internationalen Organisationen ausdrücklich vom Geltungsbereich des Gesetzes ausgenommen werden, entspricht der vorliegende Änderungsvorschlag besser der Rechtswirklichkeit als die geltende Regelung.

Das Internationale Komitee vom Roten Kreuz ist einer internationalen Organisation gleichgestellt[25] und wird daher von dieser Ausnahme erfasst.

Artikel 3 Absatz 2 Buchstabe a des Übereinkommens STE 108[26] sieht vor, dass die Signatarstaaten bestimmte Datensammlungen vom Geltungsbereich des Übereinkommens ausnehmen können, wenn diese Datensammlungen nach innerstaatlichem Recht keinen Datenschutzvorschriften unterliegen. Die Schweiz hat von dieser Ausnahme Gebrauch gemacht und anlässlich der Hinterlegung der Ratifikationsurkunde am 2. Oktober 1997 eine entsprechende Erklärung abgegeben. Die Änderung von Artikel 2 Absatz 2 Buchstabe e wird eine neue Erklärung erfordern, mit welcher dem Generalsekretär des Europarats die von der vorliegenden Bestimmung erfassten Datensammlungen, für die das Übereinkommen STE 108 nicht anwendbar ist, bekanntgegeben werden.

2.2 Art. 3 Begriffe

Buchstabe j wird neu zum bisher im deutschen Text fehlenden Buchstaben i; der bisherige Buchstabe k wird zum Buchstaben j. Ziffer 1 wird an die neue Bundesverfassung vom 18. April 1999[27] angepasst, welche in Artikel 163 Absatz 1 und Artikel 164 für die Erlasse der Bundesversammlung, die rechtsetzende Bestimmungen enthalten, nur noch zwei Formen vorsehen, nämlich das Bundesgesetz und die Verordnung. Ziffer 2 bleibt unverändert.

2.3 Art. 4 Grundsätze

Die Rechtmässigkeit der Bearbeitung (Abs. 1)

Die geltende Formulierung von Artikel 4 Absatz 1 DSG entspricht nicht ganz den Anforderungen von Artikel 5 Buchstabe a des Übereinkommens STE 108[28]. Nicht nur die Beschaffung, sondern jede Bearbeitung muss rechtmässig sein.

Der erkennbare Charakter der Beschaffung (Abs. 4)

Artikel 4 Absatz 4 des Entwurfs trägt zur Verwirklichung der Motion «Erhöhte Transparenz» bei. Er verankert den Grundsatz, dass die Beschaffung für die betroffene Person erkennbar sein muss, namentlich was den Zweck anbelangt. Dieser allgemeine Grundsatz wird für die besonders schützenswerten Personendaten und die Persönlichkeitsprofile durch eine detailliertere Informationspflicht (Art. 7*a*) vervollständigt.

Die Einführung der Informationspflicht gemäss Artikel 7*a* für die Beschaffung *aller* Personendaten wird nicht vorgesehen, obwohl dies dem europäischen Recht – insbesondere den Empfehlungen des Europarats – besser entsprechen würde; der Eidge-

25 BBl **1988** II 440; vgl. auch U. Maurer / N.P. Vogt, Kommentar zum Schweizerischen Datenschutzgesetz, ad Art. 2 Abs. 2 Bst. e, § 58 ff.
26 SR **0.235.1**
27 SR **101**
28 SR **0.235.1**

nössische Datenschutzbeauftragte hätte eine solche Regelung befürwortet. In der Arbeitsgruppe, die an der Ausarbeitung des Vorentwurfs beteiligt war, wurde indessen die Ansicht vertreten, dass damit den Inhabern der Datensammlungen eine unverhältnismässig weit gehende Verpflichtung aufgebürdet würde. Deshalb soll die Informationspflicht, wie die Motion dies vorsieht, auf die Beschaffung von besonders schützenswerten Daten und von Persönlichkeitsprofilen beschränkt und ansonsten nur verlangt werden, dass die Beschaffung erkennbar ist. Artikel 4 Absatz 4 des vorliegenden Entwurfs bringt somit im Verhältnis zur heutigen Situation eine Verbesserung der Transparenz, ohne aber so weit wie Artikel 7*a* zu gehen. Das Erfordernis, dass die Beschaffung erkennbar sein muss, ist in Artikel 18 Absatz 2 DSG bereits für die Bundesorgane verankert; sie wird lediglich auf die privaten Personen ausgedehnt. Dazu ist auch zu bemerken, dass gewisse Unternehmen bereits Massnahmen ergriffen haben, die ihnen erlauben, den gestiegenen Ansprüchen bezüglich der Transparenz der Datenbearbeitung Rechnung zu tragen. Es ist auch im Interesse dieser Unternehmen, bei der Erhebung von Personendaten so transparent wie möglich vorzugehen, wollen sie das Vertrauen der Konsumentinnen und Konsumenten gewinnen. Die Anforderungen des Entwurfs stellen indessen nur einen Minimalstandard dar; die Unternehmen sind frei, weitergehende Massnahmen zu treffen und die Informationspflicht nach Artikel 7*a* des Entwurfs auf alle Personendaten anzuwenden.

Die Anforderungen, die erfüllt sein müssen, damit von einer «erkennbaren» Beschaffung gesprochen werden kann, sind nach den Umständen sowie den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben zu beurteilen (Art. 4 Abs. 2 DSG). Die Praxis wird die dem Einzelfall angepassten Kriterien zu entwickeln haben. Dies betrifft insbesondere die Frage, welche Informationen der Inhaber der Datensammlung nach Treu und Glauben in einer konkreten Situation der betroffenen Person erteilen muss. Es geht dabei nicht nur um die Beschaffung an sich, sondern auch um deren Rahmenbedingungen, wie beispielsweise den ihr zugrunde liegenden Zweck, die Identität des Inhabers der Datensammlung oder die Kategorien von möglichen Datenempfängern, falls eine Bekanntgabe erwogen wird. In gewissen Fällen kann es auch erforderlich sein, die betroffenen Personen darüber aufzuklären, ob die Beantwortung der gestellten Fragen freiwillig oder obligatorisch ist, sowie sie über die Folgen im Fall einer Verweigerung der Antwort zu informieren.

Allerdings ist darauf hinzuweisen, dass – je nach Situation – auch eine weniger umfassende und ausdrückliche Information genügen kann.

Beispiele:

- Wird eine *Kundenkarte eines Geschäfts* beantragt, und sind dazu Personalien anzugeben, ist grundsätzlich klar, dass das Geschäft die Angaben für die Zustellung von eigener Werbung nutzen kann. Wenn aber beim Gebrauch der Kundenkarten Daten über die Konsumgewohnheiten beschafft und für die Erstellung von Konsumentenprofilen benutzt oder gar an Dritte verkauft werden, so sind die Kundinnen und Kunden in geeigneter Art und Weise (z.B. einem Hinweis auf dem Antragsformular der Kundenkarte) darauf aufmerksam zu machen.
- Wenn dagegen ein *Hotelzimmer* reserviert wird und dazu Daten angegeben werden müssen, die im Zusammenhang mit dieser Reservation stehen (Adresse, Anzahl der Übernachtungen, Kreditkartennummer etc.), so muss (sofern das Hotel diese Daten nicht an Dritte weitergibt) keine besondere Information erfolgen, denn die Datenbeschaffung und ihr Zweck sind aus den Umständen erkennbar.

Je komplexer eine Transaktion ist und je länger die Zeitspanne, während der die Daten infolge dieser Transaktion einer Bearbeitung unterliegen können, desto höher sind die Anforderungen an die Erkennbarkeit der Beschaffung. Unter dem Gesichtspunkt der Verhältnismässigkeit muss geprüft werden, in welchem Mass die betroffene Person auf die wesentlichen Rahmenbedingungen der Beschaffung aufmerksam gemacht werden muss, welche Mittel dem Inhaber der Datensammlung zur Verfügung stehen, um diese Rahmenbedingungen erkennbar zu machen, und in welchem Umfang von ihm erwartet werden kann, dass er diese Mittel auch einsetzt, namentlich unter Berücksichtigung ihrer Kosten und ihrer Wirksamkeit. Zu berücksichtigen sind ferner die in der Branche oder für die betreffende Art von Transaktionen geltenden Usanzen. Für die einfachen Transaktionen des täglichen Lebens, die so geartet sind, dass die Beschaffung und ihr Zweck sowie die Identität des Inhabers der Datensammlung für die betroffene Person auf Anhieb leicht und deutlich erkennbar sind, bringt Artikel 4 Absatz 4 keine neue Verpflichtung mit sich. Daher kann angenommen werden, dass die Anwendung von Artikel 4 Absatz 4 für die meisten der geläufigen Transaktionen keine besonderen Probleme mit sich bringt. Ist eine Beschaffung auf Grund der Umstände hingegen weniger deutlich erkennbar, muss die betroffene Person umso eher mit angemessenen Mitteln auf die Erhebung und ihre wesentlichen Rahmenbedingungen aufmerksam gemacht werden. Bei einer telefonischen Umfrage kann beispielsweise eine mündliche Information über den Zweck der Erhebung, die Verwendung der Daten und die Identität des Inhabers der Datensammlung genügen. Im Internet ist in den meisten Fällen ein Hinweis auf dem Eingangsportal in einer genügend sichtbaren Rubrik, der auf weitere Angaben zur Beschaffung und Verwendung der Daten verweist, in den meisten Fällen ein einfaches und angemessenes Informationsmittel. Auch andere Mittel, wie beispielsweise eine Warnung auf einem vorgedruckten Formular, mit der die betroffene Person darüber informiert wird, dass die Daten – sofern sie sich dem nicht widersetzt – für Kundenwerbung oder zu anderen Zwecken an Dritte weitergegeben werden, können die Anforderungen ohne Weiteres erfüllen, ohne dass damit ein unverhältnismässiger Aufwand für den Inhaber der Datensammlung verbunden wäre. Ist die Angabe der betreffenden Daten freiwillig, sollte allenfalls der betroffenen Person selbst dann die Möglichkeit gegeben werden, ihr Einverständnis mit der Erhebung bzw. Bearbeitung deutlich zu machen, wenn dies vom Gesetz an sich nicht verlangt wird. In vielen Fällen würde dies dazu beitragen, Probleme zu vermeiden, und der Inhaber der Datensammlung hätte die Gewähr, dass die Beschaffung hinreichend erkennbar war und dass die Zustimmung der betroffenen Person vorliegt.

Auch die Beschaffung von Personendaten bei einer Drittperson muss für die Betroffene oder den Betroffenen grundsätzlich erkennbar sein.

Die in Artikel 4 Absatz 4 verlangte Transparenz, ergänzt um die strengere Informationspflicht hinsichtlich der Beschaffung besonders schützenswerter Personendaten und Persönlichkeitsprofile (Art. 7*a* des Entwurfs), verleiht dem Recht, die Bearbeitung zu untersagen (Art. 12 Abs. 2 Bst. b DSG), ebenfalls eine neue Dimension. Das Recht, sich der Bearbeitung zu widersetzen, muss so lange blosse Theorie bleiben, als die betroffenen Personen sich über eine Datenbeschaffung und ihre wesentlichen Rahmenbedingungen gar nicht im Klaren sind. Die Transparenz der Beschaffung und die Information der betroffenen Person bilden somit den eigentlichen Eckpfeiler des ganzen Datenschutzsystems.

Es versteht sich von selbst, dass der Grundsatz der Erkennbarkeit der Datenerhebung dann nicht anwendbar ist, wenn eine gesetzliche Grundlage besteht, die es den Behörden erlaubt, Daten ohne Wissen der betroffenen Personen zu sammeln (vgl. z.B. Artikel 14 des Bundesgesetzes vom 21. März 1997[29] über Massnahmen zur Wahrung der inneren Sicherheit, BWIS).

Die Voraussetzungen der Zustimmung (Abs. 5)

Vorweg ist darauf hinzuweisen, dass Artikel 4 Absatz 5 des Gesetzesentwurfs das geltende Recht nicht ändert, sondern lediglich den Begriff «Zustimmung» klärt.

Das Erfordernis der Zustimmung als Bedingung für die Datenbearbeitung wird vom geltenden DSG (Art. 13 Abs. 1, Art. 17 Abs. 2 Bst. c) und vom vorliegenden Revisionsentwurf (Art. 6 Abs. 2 Bst. b) wiederholt aufgestellt. Dem Begriff der «Zustimmung» zur Datenbearbeitung kommt in der Praxis auch grosse Bedeutung zu; die Zustimmung wird von den privaten Personen am häufigsten als Rechtfertigungsgrund geltend gemacht. Deshalb sieht Artikel 4 Absatz 5 des Entwurfs vor, diesen Begriff gestützt auf die Rechtsprechung zu klären.

Absatz 5 definiert, unter welchen Voraussetzungen die Zustimmung als gültig gelten kann. Es geht somit nicht darum, die Zustimmung zur Bedingung für *jede* Datenbearbeitung zu erheben, noch geht es darum, gegenüber dem geltenden Recht weitergehende Anforderungen aufzustellen. Der Begriff der Zustimmung orientiert sich an demjenigen der «Einwilligung des aufgeklärten Patienten»[30], und zwar in dem Sinne, dass die betroffene Person über alle Informationen im konkreten Fall verfügen muss, die erforderlich sind, damit sie eine freie Entscheidung treffen kann. Der Begriff «freiwillig» entspricht im Übrigen auch der im Gemeinschaftsrecht verwendeten Terminologie. Das bedeute insbesondere, dass die betroffen Person über mögliche negative Folgen oder Nachteile informiert sein muss, die sich aus der Verweigerung ihrer Zustimmung ergeben können. Die alleinige Tatsache, dass eine Verweigerung einen Nachteil für die betroffene Person nach sich zieht, kann dagegen die Gültigkeit der Zustimmung nicht beeinträchtigen. Dies ist nur dann der Fall, wenn dieser Nachteil keinen Bezug zum Zweck der Bearbeitung hat oder diesem gegenüber unverhältnismässig ist. So gibt eine Person, die einem Kreditinstitut das Einverständnis zur Überprüfung ihrer Kreditwürdigkeit erteilt, um eine Kreditkarte zu erhalten, ihre Zustimmung freiwillig. Dies, obwohl sie weiss, dass sie ohne Zustimmung keine solche Karte erhalten wird. In einer solchen Situation ist der aus der Nichtzustimmung resultierende Nachteil gegenüber dem Zweck der Bearbeitung verhältnismässig. Dagegen kann der Arbeitnehmer, der gezwungen ist, in eine nicht im Arbeitsvertrag vorgesehene Datenbearbeitung einzuwilligen, weil ihm die Entlassung angedroht wird, diese Zustimmung nicht freiwillig erteilen. Der Nachteil, der aus einer Verweigerung der Zustimmung resultieren würde, wäre eindeutig unverhältnismässig.

Die Einwilligung ist nicht an eine bestimmte Form gebunden und kann stillschweigend bzw. durch konkludentes Handeln erfolgen, sofern es nicht um die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen geht. Bereits

29 SR **120**
30 Vgl. insbesondere BGE **117** Ib 197; BGE **114** Ia 350 E. 6; BGE **119** II 456.

heute wird gemäss dem Verhältnismässigkeitsgrundsatz davon ausgegangen, dass die Zustimmung umso klarer zu erfolgen hat, je sensibler die fraglichen Personendaten sind[31].

2.4 Art. 6 Bekanntgabe von Personendaten ins Ausland

Die Verpflichtung, dem Datenschutzbeauftragten die Bekanntgabe von Personendaten ins Ausland zu melden, hat sich in der Praxis nicht bewährt. Nur wenige Unternehmen erstatten diese Meldung, und der Datenschutzbeauftragte verfügt – vor allem in personeller Hinsicht – nicht über die erforderlichen Mittel, um Kontrollen durchzuführen. Dies ist einer der Gründe, warum der Revisionsentwurf diese Meldepflicht zu Gunsten einer Sorgfaltspflicht aufgibt, die private Personen und Bundesorgane trifft, welche Personendaten ins Ausland übermitteln. Die Sorgfaltspflicht ist verbunden mit einer Informationspflicht, die im Gegensatz zur bisherigen Meldepflicht allerdings nur noch punktuell besteht und in der praktischen Umsetzung vereinfacht werden soll.

Absätze 1 und 2

Artikel 6 Absatz 1 verlangt neu als grundsätzliche Voraussetzung für eine gesetzeskonforme Datenübermittlung ins Ausland, dass die *Gesetzgebung* im Bestimmungsland einen angemessenen Schutz gewährleistet. Dies bedeutet aber im Ergebnis nicht, dass gegenüber dem geltenden Recht – wo ein der Schweiz gleichwertiger *Datenschutz* verlangt wird – eine Verschärfung der Anforderungen für eine grenzüberschreitende Bekanntgabe vorgenommen wird. Absatz 2 der Bestimmung enthält – anders als das geltende Recht – eine Liste der alternativen Bedingungen, unter welchen die Bekanntgabe von persönlichen Daten ins Ausland erlaubt ist. Dadurch verdeutlicht der Revisionsentwurf die verschiedenen Möglichkeiten der Sicherstellung einer gesetzeskonformen Übermittlung und lässt die Inhaber der Datensammlungen in der Wahl ihrer Mittel frei. Auch mit der Verwendung des Begriffes «bekanntgeben» statt wie im geltenden Recht «übermitteln» wird keine materielle Änderung angestrebt, sondern lediglich durch die Verwendung des in Artikel 3 definierten Begriffes die Terminologie vereinheitlicht.

Die Gesetzgebung im Empfängerstaat gewährleistet dann ein «angemessenes Schutzniveau», wenn sie den Anforderungen des Übereinkommens STE 108[32] entspricht. Darüber hinaus ist aber insbesondere zu berücksichtigen, wie diese Gesetzgebung in der Praxis umgesetzt wird. Der Datenschutzbeauftragte führt eine Liste jener Staaten, welche die entsprechenden Anforderungen erfüllen.

Privatpersonen und Bundesorgane, welche Personendaten ins Ausland übermitteln, müssen mit angemessenen Mitteln gewährleisten, dass die Übermittlung der Daten die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet. Artikel 6 stellt damit Anforderungen auf, welche denen der Richtlinie 95/46/EG nahe

31 L. Brühwiler-Frésey, Medizinischer Behandlungsvertrag und Datenrecht, Zürich 1996, S. 87.
32 SR **0.235.1**

kommen. Das Datenschutzrecht des Bundes wird damit konform zum Zusatzprotokoll zum Übereinkommen STE 108[33] (vgl. Ziff. 1.2.3.1.2).

Nach *Artikel 6 Absatz 2 Buchstabe a* ist eine Bekanntgabe ins Ausland beim Fehlen einer Gesetzgebung mit angemessenem Schutz zulässig, wenn andere hinreichende Garantien vorliegen. Solche können sich beispielsweise aus einem Verhaltenskodex ergeben, d.h. aus einem Regelwerk, dem sich Private freiwillig unterstellen können, wie etwa dem «Safe Harbor Privacy Framework», das zwischen der EU-Kommission und den USA ausgehandelt wurde[34], dem die Empfängerorganisation oder der ausländische Staat verpflichtet ist. Wer Personendaten ins Ausland übermittelt, verfügt also über einen grossen Handlungsspielraum, doch haftet er für Nachteile, die sich aus einer Verletzung der Sorgfaltspflicht ergeben können. Es ist grundsätzlich Sache desjenigen, welcher Personendaten ins Ausland übermittelt, nachzuweisen, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.

Absatz 2 erlaubt den grenzüberschreitenden Datenverkehr unter bestimmten Voraussetzungen auch dann, wenn die Anforderungen von Absatz 1 nicht erfüllt sind. Die in den Buchstaben a–g aufgestellten Bedingungen entsprechen teilweise den Rechtfertigungsgründen von Artikel 13 Absatz 1 und 2 DSG. Im Gegensatz zur Enumeration der überwiegenden Interessen gemäss Artikel 13 Absatz 2 DSG ist die Aufzählung der Bedingungen in Artikel 6 Absatz 2 des vorliegenden Entwurfs aber *abschliessend*. Es ist darauf hinzuweisen, dass es sich ausschliesslich um alternative Bedingungen handelt.

Absatz 2 Buchstabe b betrifft eine konkrete ausservertragliche Situation. Der Ausdruck «im Einzelfall» ist in dem Sinne weit zu interpretieren als nicht jede einzelne grenzüberschreitende Datenübermittlung, sondern auch eine Gesamtheit von Übermittlungen erfasst werden kann. So ist zum Beispiel die Übermittlung von mehreren Protokollen einer Arbeitsgruppe, der Personen aus verschiedenen Ländern angehören, zulässig, ohne dass die Zustimmung jeder betroffenen Person für die Übermittlung jedes Dokuments eingeholt werden muss.

Absatz 2 Buchstabe c sieht vor, dass im Rahmen einer vertraglichen Beziehung Personendaten ins Ausland bekanntgegeben werden können, wenn die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht und es sich um Personendaten des Vertragspartners handelt. Es ist darauf hinzuweisen, dass diese Bestimmung nur Anwendung findet, wenn die Bekanntgabe von Personendaten ins Ausland für den Abschluss oder den Vollzug eines Vertrages unabdingbar ist.

Absatz 2 Buchstabe e lässt die grenzüberschreitende Bekanntgabe von Personendaten zu, wenn sie im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. Eine Übermittlung ist gestützt auf diese Bestimmung also einzig dann zulässig, wenn es darum geht, lebenswichtige Interessen der betroffenen Person zu schützen. Buchstabe e will jene Situation regeln, wo die betroffene Person nicht in der Lage ist, ihre eigenen Interessen geltend zu machen und vermutet werden kann, dass sie ihre Zustimmung zu einer solchen Datenübermittlung gegeben hätte. Der Ausdruck «Schutz des Lebens oder

33 SR **0.235.1**
34 http://www.export.gov/safeharbor/sh_documents.html

der körperlichen Integrität» entspricht dem Begriff «Schutz lebenswichtiger Interessen» der im Gemeinschaftsrecht verwendet wird (Art. 26 Abs. 1 Bst. e und Abs. 7 Bst. d der Richtlinie 95/46/EG)

Absatz 2 Buchstabe g sieht vor, dass Personendaten ins Ausland bekanntgegeben werden dürfen, wenn die Bekanntgabe zwischen juristischen Personen unter einheitlicher Leitung erfolgt oder unter juristischen Personen, die einheitlichen Datenschutzregeln unterstehen, die einen angemessenen Schutz gewährleisten. Der Konzernbegriff entspricht jenem von Artikel 663*e* Absatz 1 des Obligationenrechts[35]. Mit dieser Bestimmung wird der in der Vernehmlassung erhobenen Forderung nach einer speziellen Regelung für den Datentransfer innerhalb von Konzernen ein Stück weit entgegengekommen.

Absatz 3

Auf europäischer Ebene ergibt sich aus Artikel 2 Absatz 2 Buchstabe b des Zusatzprotokolls, dass die zuständige Behörde überprüfen können muss, ob die Schutzmassnahmen angemessen sind, wenn die Gesetzgebung des Empfängerstaates keinen genügenden Schutz bietet. Aus diesem Grund sieht die Revisionsvorlage eine Informationspflicht vor.

Nach Artikel 6 Absatz 3 des vorliegenden Entwurfs muss der Inhaber der Datensammlung den Datenschutzbeauftragten über die Garantien im Sinne von Artikel 6 Absatz 2 Buchstabe a informieren. Keinesfalls besteht automatisch eine Informationspflicht für jede Einzelübermittlung (z.B. Briefe, E-Mails), wie dies einzelne Vernehmlasser befürchteten. Ebenso ist der Datenschutzbeauftragte über die zur Anwendung gelangenden Datenschutzregeln zu informieren, wenn gestützt auf Artikel 6 Absatz 2 Buchstabe g grenzüberschreitende Datenbekanntgaben an eine Konzerngesellschaft erfolgen, die sich in einem Land befindet, in dem eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

Die Verordnung des Bundesrats wird – soweit erforderlich – präzisieren, wann und wie die Information erfolgen muss. Auch die Tragweite der Informationspflicht wird in der Verordnung noch zu präzisieren sein. So könnte z.B. vorgesehen werden, dass eine einmalige Information genügt, wenn eine Firma allgemeine und verbindliche Regeln für die Übermittlung aufgestellt hat oder wenn regelmässig bestimmte Standardvertragsklauseln[36] verwendet werden. Beim Datentransfer zwischen Konzerngesellschaften wird eine einmalige Information über die für die beteiligten Firmen verbindlichen Datenschutzregeln genügen. Es wird darauf zu achten sein, dass das Verfahren der Information möglichst einfach ausgestaltet wird; zu denken ist insbesondere an eine Information des Datenschutzbeauftragten über Internet.

Der Datenschutzbeauftragte kann im Rahmen seiner Untersuchungsbefugnisse abklären, ob die Garantien angemessen sind (vgl. Art. 29 Abs. 1 Bst. d des vorliegenden Entwurfs).

35 SR **220**

36 Vgl. z.B. die von der EU-Kommission genehmigten Standardvertragsklauseln; Entscheidung 2001/497/EG vom 15. Juni 2001, ABl L 181 vom 4. Juli 2001, S. 19 ff., und Entscheidung 2002/16/EG vom 27. Dezember 2001, ABl L 6 vom 10. Januar 2002, S. 52 ff.

2.5 Art. 7*a* Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen

Artikel 7*a* sieht vor, dass wer besonders schützenswerte Daten oder Persönlichkeitsprofile beschafft, verpflichtet ist, die betroffene Person darüber zu informieren. Dieser Informationspflicht muss der Inhaber der Datensammlung von sich aus nachkommen, was Artikel 7*a* vom Auskunftsrecht nach Artikel 8 unterscheidet. Artikel 9 des Entwurfs erlaubt die Verweigerung, Einschränkung oder Aufschiebung der Information, wenn ein überwiegendes öffentliches oder privates Interesse dies erfordert.

Artikel 7*a* geht bezüglich des Grundsatzes der Erkennbarkeit der Datenbeschaffung weiter als Artikel 4 Absatz 4 des vorliegenden Entwurfs, denn er sieht eine Pflicht zur aktiven Information vor. Er entspricht der Motion «Erhöhte Transparenz». Ein verstärkter Schutz rechtfertigt sich für die besonders schützenswerten Daten und die Persönlichkeitsprofile insofern, als die Bearbeitung dieser Art von Personendaten zu Diskriminierungen führen kann. Artikel 7*a* sollte indirekt auch eine präventive Wirkung haben: Muss der Inhaber der Datensammlung die betroffene Person aktiv und ausführlich informieren, wird er bestrebt sein, keine besonders schützenswerten Daten oder Persönlichkeitsprofile zu beschaffen, die er für seine Tätigkeit nicht unbedingt benötigt.

Gemäss Absatz 2 muss der Inhaber der Datensammlung der betroffenen Person – in der Regel ausdrücklich – alle Informationen zukommen lassen, die für eine Bearbeitung nach dem Grundsatz von Treu und Glauben und der Verhältnismässigkeit erforderlich sind. Es sind dies mindestens die Informationen gemäss den Buchstaben a bis c, das heisst die Identität des Inhabers der Datensammlung, den Zweck des Bearbeitens und die Kategorien allfälliger Datenempfänger (nicht aber die Identität jedes einzelnen Datenempfängers). Erfordert es der Grundsatz von Treu und Glauben, muss der Inhaber der Datensammlung indessen noch weitere Informationen liefern, beispielsweise darüber, ob die Beantwortung der gestellten Fragen freiwillig oder obligatorisch ist und über die Folgen einer Verweigerung der verlangten Angaben (vgl. dazu den Kommentar zu Art. 4 Abs. 4).

Ist eine Person bereits informiert (unabhängig davon, ob sie vom Inhaber der Datensammlung selbst oder von einem Dritten informiert wurde), braucht der Inhaber der Datensammlung sie nicht erneut zu informieren. Die Information, die bei der erstmaligen Datenbeschaffung erfolgen muss, braucht – soweit die Umstände weiterer Erhebungen (namentlich der Zweck der Bearbeitung) denen der erstmaligen Beschaffung entsprechen – somit nicht bei jeder neuerlichen Datenbeschaffung wiederholt zu werden.

Die Information ist keinem Formerfordernis unterworfen; sie kann also mündlich erfolgen. Dennoch wird die schriftliche Form aus Beweisgründen empfohlen. Die Information kann den Betroffenen schriftlich abgegeben oder in schriftlicher Form an einem genügend sichtbaren Ort angebracht werden (z.B. Aushang, einem Vertrag oder einer Rechnung beigelegter Text, gut sichtbar platzierte Rubrik auf einer Internetseite etc.). Wie im Falle von Artikel 4 Absatz 4 muss der Inhaber der Datensammlung der Informationspflicht des Artikels 7*a* gemäss den Grundsätzen von

Verhältnismässigkeit sowie Treu und Glauben nachkommen (Art. 4 Abs. 2 DSG). Die Information muss demnach genügend sichtbar, lesbar und verständlich sein. Der Inhaber der Datensammlung kann die Information auch mit weiteren Angaben verbinden. Wird die Bekanntgabe von Daten an Dritte beabsichtigt und ist diese weder gesetzlich vorgeschrieben noch zur Erfüllung eines Vertrages notwendig, kann die betroffene Person mittels einer Klausel eingeladen werden, ihre Zustimmung zu dieser Bekanntgabe zu geben, oder diese zu verweigern. So können sich die Inhaber der Datensammlungen darüber vergewissern, dass die Betroffenen die Information erhalten haben und sich später, sofern sie der Bekanntgabe zugestimmt haben, dieser nicht widersetzen werden (Art. 12 Abs. 2 DSG). Es wird an der Praxis liegen, die jeweils situationsgerechten Instrumente zur Sicherstellung der Information der Betroffenen zu entwickeln. Artikel 7*a* lässt diesbezüglich für die Inhaber der Datensammlungen einen grossen Spielraum. Für die Umsetzung der notwendigen Informationsmassnahmen ist eine Übergangsfrist vorgesehen (vgl. Übergangsbestimmungen).

Beispiele:

- Eine Krankenkasse muss ausdrücklich – z.B. in einem Schreiben oder im mit den Versicherten abzuschliessenden Vertrag – darauf hinweisen, wie die ihr zugänglichen Gesundheitsdaten des Versicherten verwendet werden.
- Ein Arzt muss einen Patienten, der einen HIV-Test macht, darüber informieren, dass nach Epidemiengesetz[37] ein allfälliger positiver Befund dem Bundesamt für Gesundheit gemeldet wird (eine neuerliche Information durch das Amt ist nicht mehr erforderlich). Diese Information kann beispielsweise mündlich erfolgen, aber es ist auch denkbar, dass sie – in der notwendigen Deutlichkeit, d.h. nicht im «Kleingedruckten» – etwa in einer AIDS-Aufklärungsbroschüre enthalten ist.

Absatz 3 regelt den Fall, dass die Daten nicht bei der betroffenen Person beschafft werden, sondern bei Dritten: In diesem Fall muss die betroffene Person möglichst dann informiert werden, wenn der Inhaber der Datensammlung die Daten beschafft, spätestens jedoch bei deren Speicherung oder bei der ersten Bekanntgabe an Dritte. Der Begriff der Speicherung umfasst dabei nicht nur den technischen Vorgang, mittels desselben die beschafften Daten beispielsweise in einem Informatiksystem aufgezeichnet werden. Er umfasst jede sich an die Beschaffung anschliessende Tätigkeit, die eine weitere Verwertung der Daten vorbereitet.

Der Inhaber der Datensammlung kann nur dann darauf verzichten, die betroffene Person zu informieren, wenn er sich auf eine Beschaffung von Personendaten beschränkt oder wenn sich die Information der betroffenen Person nach den Umständen als unmöglich oder sehr schwierig erweist (z.B. wenn der Inhaber der Datensammlung keine Möglichkeit hat, die betroffene Person zu kontaktieren). Der Inhaber der Datensammlung muss dennoch alles unternehmen, was von ihm nach den Umständen vernünftigerweise verlangt werden kann, um seiner Informationspflicht nachzukommen. Er darf sich nicht mit der blossen Vermutung begnügen, dass die Information unmöglich oder unverhältnismässig ist. Das Verhalten des Inhabers der Datensammlung ist unter dem Gesichtspunkt von Treu und Glauben zu prüfen; die Ausnahmebestimmung von Absatz 3 ist eng auszulegen. Der Inhaber der Datensammlung kann auch dann auf die Information der betroffenen Person ver-

37 SR **810.101**

zichten, wenn die Beschaffung oder Bekanntgabe von Daten durch das Gesetz ausdrücklich vorgesehen ist.

Leiten Kantone von ihnen beschaffte besonders schützenswerte Personendaten und Persönlichkeitsprofile im Rahmen des Vollzuges von Bundesrecht an Bundesbehörden weiter (Beispiel: Übermittlung von Angaben über Führerausweisentzüge an das Bundesamt für Strassen zwecks Registrierung im Administrativmassnahmen-Register nach Artikel 104*b* Strassenverkehrsgesetz[38]), so obliegt ihnen die Information der betroffenen Personen. Die Bundesbehörden sind nicht zu einer neuerlichen Information verpflichtet (Art. 7*a* Abs. 3).

In der Vernehmlassung wurde verschiedentlich vorgeschlagen, für die Weitergabe von Personendaten innerhalb eines Konzerns ausdrücklich – und insbesondere in Bezug auf Artikel 7*a* Absatz 3 – eine Ausnahme von den Regeln betreffend die Bekanntgabe an Dritte vorzusehen. Eine gewisse Erleichterung wird nun in Artikel 6 Absatz 2 Buchstabe g für grenzüberschreitende Übermittlungen vorgesehen (vgl. Erläuterungen zu dieser Bestimmung). Bezüglich der hier verankerten Informationspflicht dagegen würde eine generelle Ausnahme von Bekanntgaben unter Konzerngesellschaften dem Zweck der Schaffung von mehr Transparenz für die Betroffenen zuwiderlaufen.

Artikel 9 sieht Einschränkungen der Informationspflicht vor, wenn das Gesetz es vorschreibt und wenn überwiegende Interessen Dritter dies verlangen. Die Bundesorgane können ferner die Information verweigern, wenn ein überwiegendes öffentliches Interesse dies erfordert, ebenso wenn die Bekanntgabe das Risiko in sich birgt, den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage zu stellen.

Es ist darauf hinzuweisen, dass die Richtlinie 95/46/EG, die Empfehlungen des Europarats und die Datenschutzgesetze der umliegenden Länder sehr ähnliche Informationspflichten vorsehen, deren Tragweite allerdings weiter geht (vgl. Ziff. 1.2.3).

Bereits heute gibt es Unternehmen, welche die Informationspflichten nach Artikel 7*a* erfüllen. Es ist noch einmal darauf hinzuweisen, dass es auch im Interesse der Unternehmen ist, bei der Beschaffung von Personendaten so transparent wie möglich vorzugehen. Nur so können sie das Vertrauen der Konsumentinnen und Konsumenten gewinnen. Dies trifft insbesondere für die Entwicklung im Bereich des elektronischen Handels zu.

Wer die Pflicht zur Information der von der Bearbeitung betroffenen Person vorsätzlich verletzt oder nicht die in Absatz 2 Buchstabe a bis c vorgesehenen Angaben macht oder wer vorsätzlich falsch informiert, kann strafrechtlich verfolgt werden (Art. 34 Abs. 1).

38 SR **741.01**

2.6 Art. 7*b* Informationspflicht bei automatisierten Einzelentscheidungen

Artikel 7*b* vervollständigt Artikel 7*a* des Entwurfs durch eine besondere Informationspflicht. Diese besteht dann, wenn ein Entscheid, der für die betroffene Person rechtliche Folgen hat oder sie sonst wesentlich betrifft, ausschliesslich auf einer automatisierten Datenbearbeitung beruht, welche die Bewertung einzelner Aspekte ihrer Persönlichkeit bezweckt. Damit soll verhindert werden, dass die Bewertung von Persönlichkeitsaspekten der betroffenen Person ausschliesslich in automatisierter Form erfolgt, ohne dass eine Beurteilung durch Menschen vorgenommen und ohne dass die betroffene Person darüber informiert wird, wie dieser Entscheid getroffen wurde. Solche Entscheidungen dienen der Bewertung von Merkmalen wie z.B. der Kreditwürdigkeit, der Zuverlässigkeit, des Verhaltens oder von spezifischen Risiken und stützen sich auf allgemeine statistische Daten (dies wäre z.B. dann der Fall, wenn bei einer Privathaftpflichtversicherung eine Lenkerin, die ein wenig sportliches Fahrzeug fährt, automatisch in eine bessere Risikoklasse eingestuft würde als der Lenker eines Sportwagens).

Indem für die automatisierten Einzelentscheidungen lediglich eine Informationspflicht vorgesehen wird, geht der Entwurf nicht so weit, wie die Richtlinie 95/46/EG und die Gesetzgebungen unserer Nachbarländer. Diese sehen vor, dass jede Person das Recht hat, keinem Entscheid unterworfen zu werden, der ausschliesslich auf der Basis einer automatisierten Datenbearbeitung zustande gekommen ist. Damit wird für die betroffene Person ein Stück weit das rechtliche Gehör gewährleistet. Die Informationspflicht gemäss Artikel 7*b* erschwert die Tätigkeit des Inhabers der Datensammlung in keiner Art und Weise. Sie kann sehr einfach umgesetzt werden, indem auf dem automatisierten Entscheid ein knapper Hinweis in Form eines Standardsatzes erfolgt. Obwohl in der Motion «Erhöhte Transparenz» nicht angesprochen, verfolgt die hier festgelegte Informationspflicht den gleichen Zweck.

Wer es vorsätzlich unterlässt die betroffene Person nach Artikel 7*b* zu informieren, kann strafrechtlich verfolgt werden (Art. 34 Abs. 1).

2.7 Art. 8 Auskunftsrecht

Artikel 8 wird in Absatz 2 Buchstabe a um die Verpflichtung ergänzt, der betroffenen Person Informationen über die Herkunft der Daten bekannt zu geben, sofern und soweit diese verfügbar sind. Die betroffene Person kann nämlich durchaus ein legitimes Interesse daran haben, die Herkunft der Daten zu kennen, beispielsweise um auf die Datenquellen zurückgreifen zu können oder die Korrektur allfälliger Fehler zu veranlassen. Das Interesse der betroffenen Person, die Herkunft der Daten zu kennen, wird denn auch in der Rechtsprechung bereits anerkannt[39]. Diese Änderung trägt zur Erhöhung der Transparenz im Sinne der von den Eidgenössischen Räten angenommenen Motion bei und klärt die Tragweite des Auskunftsrechts. Die Präzisierung kann auch eine präventive Wirkung haben, indem derjenige, der Daten

[39] Vgl. das nicht veröffentlichte Urteil des Bundesgerichts vom 18. September 1991, Dr. F gegen Regierungsrat des Kantons St. Gallen, E. 5a; vgl. auch, im Strafrechtsbereich, BGE **118** Ia 457.

beschafft, berücksichtigen muss, dass die betroffene Person über die Herkunft der Daten Informationen verlangen kann.

2.8 Art. 9 Einschränkung der Informationspflicht und des Auskunftsrechts

Die Gründe, die eine Einschränkung des Auskunftsrechts erlauben, werden auf die Informationspflicht nach Artikel 7*a* ausgedehnt. Liegt ein überwiegendes öffentliches oder privates Interesse vor, kann der Inhaber der Datensammlung die Information gemäss Artikel 7*a* verweigern, einschränken oder aufschieben. Da die Gründe für die Beschränkung der Informationspflicht dieselben sind wie für die Beschränkung des Auskunftsrechts, sollte die Anwendung dieser Bestimmung keine besonderen Probleme aufgeben. Wenn der Inhaber der Datensammlung die Information verweigert, einschränkt oder aufschiebt, muss er die betroffene Person informieren, sobald der Grund für die Einschränkung wegfällt, sofern dies nicht einen unverhältnismässigen Aufwand erfordert (Art. 9 Abs. 5; vgl. auch Art. 18 Abs. 6 BWIS[40]).

2.9 Art. 10*a* Datenbearbeitung durch Dritte

Artikel 14 DSG wurde in den allgemeinen Teil verschoben und wird neu zu Artikel 10*a*. Artikel 14 DSG findet zur Zeit nur auf die Datenbearbeitung durch private Personen Anwendung. Mit der Verschiebung in den allgemeinen Teil findet diese Bestimmung neu auch auf Bundesorgane Anwendung sowie ergänzend auf die kantonalen Organe, welche Daten im Rahmen des Vollzugs von Bundesrecht bearbeiten (Art. 37 Abs. 1).

Die Bearbeitung von Daten kann einem Dritten nur übertragen werden, wenn die Datensicherheit gewährleistet ist (Abs. 2). Diese Voraussetzung ergibt sich unter anderem aus den Empfehlungen der Geschäftsprüfungskommission des Ständerats[41]. In der Vernehmlassung wurde von verschiedener Seite gefordert, die diesbezüglichen Anforderungen zu konkretisieren und im Gesetz zu verankern. Soweit zusätzliche technisch-organisatorische Regelungen notwendig sind, werden diese in die Verordnung Eingang finden. Im Übrigen ist darauf hinzuweisen, dass der Auftragnehmer bezüglich der Datensicherheit zur Einhaltung derselben Anforderungen verpflichtet ist, wie der Auftraggeber (vgl. insbesondere Art. 8 und 9 der Verordnung vom 14. Juni 1993[42] zum Bundesgesetz über den Datenschutz; Datenschutzverordnung).

Absatz 2 weicht bezüglich der Tragweite der Sorgfaltspflicht des Auftraggebers nicht vom geltenden Recht ab. Er stellt aber die Verpflichtung, die den Auftraggeber trifft, deutlicher in den Vordergrund, indem er sie ausformuliert: Der Auftraggeber muss sich vergewissern, dass der Auftragnehmer die notwendigen Sicherheitsstan-

40 SR **120**
41 Vgl. Empfehlung 267, Bericht der Geschäftsprüfungskommission des Ständerates vom 19. November 1998, «Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens», BBl **1999** 5869, S 5895.
42 SR **235.11**

dards einhält. Der Auftraggeber kann sich dabei auch auf ein dem Auftragnehmer verliehenes Datenschutz-Qualitätszeichen oder eine ähnliche Zertifizierung durch unabhängige Sachverständige (vgl. Erläuterungen zu Art. 11) stützen. Der Auftraggeber muss sich insbesondere vergewissern, dass die Sicherheitsstandards beim Auftragnehmer tatsächlich angewendet werden. Weitere Einzelheiten, insbesondere bezüglich des Weisungsrechts des Auftraggebers sowie das Sicherheitskonzept und technisch-organisatorischer Massnahmen beim Auftragnehmer sind auf Verordnungsstufe zu regeln, soweit dies über die bereits bestehenden Regelungen hinaus erforderlich ist.

Unter den Rechtfertigungsgründen, auf die Absatz 3 Bezug nimmt, sind einerseits die Rechtfertigungsgründe nach Artikel 13 DSG zu verstehen, aber – bedingt durch die jetzt allgemeine Geltung der Bestimmung – auch Rechtsgrundlagen im Sinne von Artikel 17 DSG.

Der Inhaber der Datensammlung haftet für den verursachten Schaden, wenn er die Bearbeitung an einen Dritten übertragen hat, ohne sich zu vergewissern, dass die Datensicherheit gewährleistet ist.

2.10 Art. 11 Zertifizierungsverfahren

Mit der hier gegenüber dem Vernehmlassungsentwurf neu vorgeschlagenen Bestimmung wird ein Element der Selbstregulierung ins Datenschutzgesetz eingeführt. Damit soll die Selbstverantwortung der Inhaber der Datensammlungen gestärkt und der Wettbewerb stimuliert werden. Dies trägt zu einer kontinuierlichen Verbesserung von Datenschutz und Datensicherheit bei; bestehende Defizite beim Vollzug der einschlägigen Gesetzgebung können so abgebaut werden. Darüber hinaus führt das Konzept der Selbstkontrolle zu einem gewissen Grad zu einer Berücksichtigung der technologischen Entwicklung. Das Fehlen entsprechender Bestimmungen im Vernehmlassungsentwurf wurde von verschiedenen Vernehmlassern kritisiert. Die vorliegende Bestimmung orientiert sich an Artikel 43*a* Umweltschutzgesetz[43], mit dem positive Erfahrungen gemacht werden.

Absatz 1 hält das Grundprinzip fest. Gefördert werden sollen sowohl Zertifizierungsverfahren von datenschutzrelevanten betrieblichen Abläufen bzw. Organisationsstrukturen (Datenschutz-Audits) als auch die Evaluation informatiktechnischer Systeme oder Programme – also von Produkten – hinsichtlich der Einhaltung von Datenschutzstandards. Das Zertifizierungsverfahren soll, wenn festgestellt wird, dass die einschlägigen gesetzlichen und technischen Normen und Standards eingehalten werden, zur Vergabe eines Datenschutz-Qualitätszeichens (Datenschutz-Label) führen. Diese Auszeichnung kann durch zertifizierte Firmen insbesondere zu Werbezwecken verwendet und dazu der Öffentlichkeit zur Kenntnis gebracht werden. Zertifizierte Behörden und Firmen sind von der Pflicht zur Meldung ihrer Datensammlungen nach Artikel 11*a* Absatz 2 bzw. 3 ausgenommen, wenn sie das Ergebnis des Zertifizierungsverfahrens dem Datenschutzbeauftragten mitgeteilt haben (Art. 11*a* Abs. 5 Bst. f). Dieser Erleicherung soll eine Anreizfunktion zukommen.

43 SR **814.01**

Die Stellen, die solche Zertifizierungsverfahren durchführen, müssen gegenüber den zu bewertenden Privaten oder Behörden vor allem organisatorisch, aber auch faktisch, unabhängig sein. Die Anerkennung der Zertifizierungsstellen wird durch den Bundesrat in der Verordnung zu regeln sein (Abs. 2). Denkbar ist etwa, dort vorzusehen, dass die Zertifizierungsstellen über eine Akkreditierung verfügen müssen[44]. Darüber hinaus hat der Datenschutzbeauftragte zu überprüfen, ob Bewertungsverfahren und Vergabe der Gütesiegel mit dem geltenden Recht vereinbar sind (vgl. Art. 31 Abs. 1 Bst. f). Er kann mit den vom DSG vorgesehenen Instrumenten eingreifen (insb. Abgabe von Empfehlungen; vgl. Art. 29 DSG). Der Datenschutzbeauftragte wird aber nicht selbst als zertifizierende Instanz auftreten.

In der Schweiz wird heute schon ein solches Datenschutz-Qualitätszeichen angeboten; einige Unternehmen haben sich bereits einer Zertifizierung unterzogen. Auch in Deutschland wurde ein Qualifizierungsinstrument entwickelt, das gegenwärtig in der Praxis getestet wird.

2.11 Art. 11*a* Register der Datensammlungen

Heute sind die Privaten verpflichtet, Datensammlungen im Sinne von Artikel 11 Absatz 3 DSG anzumelden, wenn die betroffene Person keine Kenntnis von der Bearbeitung hat (Art. 11 Abs. 3 Bst. b DSG). Nun kommt angesichts der Verpflichtung, die Beschaffung erkennbar zu machen (Art. 4 Abs. 4), sowie der Informationspflicht bei der Beschaffung von besonders schützenswerten Daten und von Persönlichkeitsprofilen (Art. 7*a*) der Meldung der Datensammlungen eine weniger grosse Bedeutung zu.

Im Vernehmlassungsentwurf wurde zunächst eine Streichung der Registrierpflicht vorgeschlagen. Damit sollte einerseits ein Ausgleich zu den zusätzlichen Informationspflichten geschaffen werden, welche für die Privaten mit der vorliegenden Revision geschaffen werden. Andererseits erschien es zum Zeitpunkt der Ausarbeitung des Vernehmlassungsentwurfs möglich, dass die EU ihr Recht in diesem Punkt ändern könnte. Dies ist indessen nicht der Fall; darüber hinaus stiess die Abschaffung der Registrierpflicht in der Vernehmlassung nicht auf ungeteilte Zustimmung. Deshalb wird nun die Registrierpflicht grundsätzlich beibehalten, allerdings ohne die Ausnahme, die heute in Absatz 3 Buchstabe b vorgesehen ist. Indessen wird die Registrierpflicht durch zusätzliche neue Ausnahmebestimmungen gemildert, die auch eine gewisse Annäherung an die EU-Richtlinie bringen.

Die Meldung selbst soll künftig administrativ vereinfacht werden, z.B. indem entsprechende Formulare im Internet bereitgestellt werden.

In *Absatz 1* wird neu ausdrücklich festgehalten, dass das Register der Datensammlungen auf Internet zugänglich sein muss. Entsprechende Vorbereitungen sind zur Zeit bereits im Gange. Mit dieser Massnahme wird die Transparenz weiter verbessert.

Dem Grundsatz nach ist in *Absatz 3* neu vorgesehen, dass Datensammlungen anzumelden sind, wenn regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder Daten an Dritte bekanntgegeben werden.

44 Vgl. Art. 2 Akkreditierungs- und Bezeichnungsverordnung (AkkBV, SR **946.512**).

Entgegen dem heute geltenden Recht gilt dies auch dann, wenn die betroffenen Personen darüber informiert sind.

Absatz 4 hält fest, dass Datensammlungen vor ihrer Eröffnung angemeldet werden müssen.

Absatz 5 sieht eine Reihe von Ausnahmen vor. Neu ist namentlich, dass die Bundesbehörden gleich behandelt werden, wie die Privaten. Auch die Richtlinie 95/46/EG sieht keine Trennung zwischen Behörden und Privaten vor; damit erfolgt in diesem Punkt eine gewisse Annäherung. Bereits heute besteht die Meldepflicht nicht, wenn Daten aufgrund einer gesetzlichen Pflicht bearbeitet werden; ebenso kann der Bundesrat heute schon Ausnahmen vorsehen (Bst. a und b). Die Bestimmungen der Buchstaben c und d, welche Ausnahmen für Medienschaffende vorsehen, werden der Vollständigkeit halber in die vorliegende Aufzählung aufgenommen worden; sie sind heute in Artikel 4 der Datenschutzverordnung[45] verankert.

Buchstabe e sieht eine Neuerung vor, mit der die Registrierpflicht sich an das System der Meldung nach der Richtlinie 95/46/EG anpassen lässt. Die Bestimmung entspricht dem Selbstregulierungsansatz, der bereits mit der Förderung von Zertifizierungen verfolgt wird. Die Inhaber der Datensammlungen können eigene Datenschutzverantwortliche einsetzen, die betriebsintern für die Einhaltung der datenschutzrechtlichen Rahmenbedingungen wachen und eine Liste der Datensammlungen führen. Der oder die Datenschutzverantwortliche muss organisatorisch unabhängig (das heisst, nicht weisungsgebunden oder hierarchisch untergeordnet) sein. Der Bundesrat regelt Stellung und Aufgaben der Datenschutzverantwortlichen im Detail (Abs. 6). Er kann insbesondere vorsehen, dass deren Einsetzung nur gültig erfolgen kann, wenn sie dem eidgenössischen Datenschutzbeauftragten mitgeteilt wird.

Die unter *Buchstabe f* vorgesehene Ausnahme stellt die Konsequenz der Förderung von Zertifizierungen dar. Wenn der Inhaber der Datensammlung ein Qualitätszeichen erlangen konnte, so ist grundsätzlich gewährleistet, dass er die gesetzlichen Anforderungen einhält. Das Ergebnis des Zertifizierungsverfahrens ist dem Datenschutzbeauftragten mitzuteilen. Damit ist sichergestellt, dass eine Kontrolle stattfinden kann, wenn dazu Anlass bestehen sollte und dass die betroffenen Personen sich beim Datenschutzbeauftragten erkundigen können, ob eine Firma zertifiziert ist. Der Bundesrat kann vorsehen, dass der Datenschutzbeauftragte eine Liste der zertifizierten Unternehmen und Behörden veröffentlicht.

2.12 Art. 12 Persönlichkeitsverletzungen

Aufgrund des mit der Änderung von Artikel 6 DSG vorgenommenen Systemwechsels entfällt der Verweis auf Artikel 6 Absatz 1, der heute in Artikel 12 Absatz 2 Buchstabe a figuriert.

Aus Artikel 12 Absatz 2 Buchstabe a DSG ist abzuleiten, dass eine Bekanntgabe von Personendaten ins Ausland auch dann zulässig ist, wenn das Risiko einer Persönlichkeitsverletzung besteht, sofern der Inhaber der Datensammlung einen Rechtfertigungsgrund nach Artikel 13 DSG geltend machen kann. Im mit dem vorliegen-

45 SR **235.11**

den Revisionsentwurf vorgesehenen neuen Artikel 6 werden nun aber die Gründe, die eine Abweichung vom Grundsatz des Artikel 6 Absatz 1 rechtfertigen können, in Absatz 2 bereits *abschliessend* aufgezählt.

2.13 Art. 14 Datenbearbeitung durch Dritte

Artikel 14 wird durch Artikel 10*a* ersetzt. Es wird dazu auf den Kommentar zu dieser Bestimmung verwiesen.

2.14 Art. 15 Rechtsansprüche und Verfahren

Der Text von Absatz 1 und 3 erfährt eine redaktionelle Änderung. Damit wird stärker betont, dass der Kläger nicht nur die Sperrung der Bekanntgabe von Daten an Dritte fordern kann, sondern auch die Möglichkeit hat, die Sperrung der Bearbeitung als solche zu verlangen. Dieses Recht besteht zwar bereits heute (vgl. Art. 12 Abs. 2 Bst. b in Verbindung mit Art. 15 Abs. 1 DSG). Mit der Einführung der in Artikel 7*a* des vorliegenden Entwurfs vorgeschlagenen Informationspflicht wird aber das Recht, ein Verbot der Bearbeitung zu verlangen, wirksamer (vgl. auch den Kommentar zu Art. 15*a* nachstehend).

2.15 Art. 15*a* Verfahren der Untersagung der Datenbearbeitung

Das Recht, die Datenbearbeitung auf zivilrechtlichem Weg zu untersagen, besteht bereits heute gemäss Artikel 12 Absatz 2 Buchstabe b und Artikel 15 DSG. Artikel 15*a* des Entwurfs verbessert lediglich in bescheidenem Ausmass die verfahrensmässige Stellung der betroffenen Person. Die Einführung einer Informationspflicht in Artikel 7*a* birgt das Risiko eines geringen praktischen Nutzens in sich, wenn die Person, die über die Datenbeschaffung informiert ist, sich der Bearbeitung nicht wirksam widersetzen kann. Anderseits ist das Recht auf Untersagung der Datenbearbeitung nur dann wirklich sinnvoll, wenn die Bearbeitung eingestellt werden kann, bevor ein für die betroffene Person nur noch schwer zu behebender Nachteil entsteht. Schliesslich soll die betroffene Person Kenntnis von den Gründen erhalten, welche die Bearbeitung rechtfertigen, um ihre Rechte im Sinne von Artikel 15 DSG ausüben zu können.

Die betroffene Person weiss oft nicht, ob der Bearbeitung ein Rechtfertigungsgrund im Sinne von Artikel 13 DSG zugrunde liegt oder nicht, und der Inhaber der Datensammlung ist nach heutigem Recht nicht verpflichtet, die Bearbeitung zu begründen. Wohl kann die betroffene Person vom Inhaber der Datensammlung Auskünfte verlangen, doch bleiben diesbezügliche Gesuche nicht selten unbeantwortet. In diesem Fall müsste die betroffene Person das Risiko auf sich nehmen, eine Klage gemäss Artikel 15 DSG einzureichen, ohne einschätzen zu können, wie ihre Erfolgsaussichten sind.

Gestützt auf Artikel 15*a* kann die betroffene Person die Bearbeitung von Daten, die sie betreffen, untersagen, indem sie vom Inhaber der Datensammlung die sofortige

Einstellung der Bearbeitung verlangt. Um Missbräuche seitens der betroffenen Person zu verhindern, sieht die erwähnte Bestimmung vor, dass eine Bearbeitung, die aufgrund einer gesetzlichen Pflicht erfolgt, nicht eingestellt werden muss; diesfalls ist die betroffene Person *sofort* darüber zu informieren (Abs. 3, 2. Satz). Um mit der Bearbeitung fortfahren zu können, wird der Inhaber der Datensammlung die Rechtfertigungsgründe, auf die er die Bearbeitung stützt, der betroffenen Person schnellstmöglich bekanntgeben; er hat dafür 10 Tage Zeit. Ist die Bearbeitung nicht gerechtfertigt, kann er von sich aus darauf verzichten.

Gestützt auf die vom Inhaber der Datensammlung nach *Absatz 3* angegebenen Rechtfertigungsgründe kann die betroffene Person die Zulässigkeit der Bearbeitung beurteilen. In den meisten Fällen wird sie sich mit der Antwort des Inhabers der Datensammlung begnügen und auf eine Klageeinreichung verzichten. Es liegt im Interesse beider Parteien, unnötige Verfahren zu verhindern. Artikel 15*a* trägt dazu bei, erlaubt er doch dem Inhaber der Datensammlung, die betroffene Person davon zu überzeugen, dass die Bearbeitung gerechtfertigt ist. Der betroffenen Person ermöglicht er, die Aussichten eines gerichtlichen Verfahrens besser abzuschätzen.

Wenn die betroffene Person von den vom Inhaber der Datensammlung vorgebrachten Rechtfertigungsgründen nicht überzeugt ist, hat sie zehn Tage Zeit, um die in Artikel 15 DSG vorgesehen Klagen zu erheben und vorsorgliche Massnahmen zu beantragen. Insbesondere kann sie die Berichtigung der Daten oder deren Vernichtung verlangen oder sie kann verlangen, dass die Bekanntgabe an Dritte gesperrt wird.

Absatz 4 klärt die Auswirkungen der Untersagung der Datenbearbeitung. Der Inhaber der Datensammlung ist zur Einstellung der Bearbeitung im engen Sinn des Wortes verpflichtet, darf aber die fraglichen Daten aufbewahren, archivieren oder speichern, bis die Rechtslage geklärt ist, d.h. solange für die betroffene Person die Frist zur Klageeinreichung läuft und bis gegebenenfalls der Richter über die Zulässigkeit der besagten Bearbeitung entschieden hat und der Entscheid definitiv geworden ist. Ruft die betroffene Person nicht innert Frist den Richter an, kann der Inhaber der Datensammlung die Bearbeitung in jedem Fall fortführen. Die hier vorgenommene Präzisierung ist nötig, weil der Begriff «bearbeiten» nach Artikel 3 Buchstabe e DSG auch die in der vorliegenden Bestimmung erwähnten Tätigkeiten umfasst.

Wenn die betroffene Person innert der gesetzlichen Frist keine Klage erhebt, gilt die Untersagung als zurückgezogen. Der Inhaber der Datensammlung ist dann berechtigt, die Datenbearbeitung und alle damit verbundenen Tätigkeiten fortzusetzen. Die in *Absatz 5* vorgesehene Frist beschränkt also einzig die Dauer der Untersagung der Datenbearbeitung im Sinne der vorliegenden Bestimmung und nicht das Recht der betroffenen Person, ihre Ansprüche nach Artikel 15 DSG vor dem Richter geltend zu machen. Die Bearbeitung kann nur dann erneut untersagt werden, wenn sich die sachlichen oder rechtlichen Voraussetzungen wesentlich geändert haben. Ist dies nicht der Fall, dürfte eine wiederholte Untersagung rechtsmissbräuchlichen Charakter haben.

Absatz 6 sieht ausdrücklich vor, dass das Verfahren nach Artikel 15*a* für periodisch erscheinenden Medien, für die Aktualität das höchste Gebot ist, nicht anwendbar ist. Das bedeutet, dass gegen ein periodisch erscheinendes Medium ausschliesslich Klagen nach Artikel 15 DSG erhoben werden können.

2.16 Art. 16 Verantwortliches Organ

In Artikel 16 werden zwei neue Absätze eingeführt. Sie erlauben dem für die Bearbeitung verantwortlichen Bundesorgan die Durchführung von Kontrollen, wenn es gemeinsam mit kantonalen Organen oder privaten Personen Daten bearbeitet. Es kann vorkommen, dass kantonale Organe und private Personen Daten gemeinsam mit einem Bundesorgan bearbeiten, ohne dass diese Bearbeitung notwendigerweise mit dem Vollzug von Bundesrecht zusammenhängt. Soweit Datenbanken des Bundes betroffen sind, muss das Bundesorgan dafür sorgen, dass die Bearbeitung der Daten mit dem DSG vereinbar ist; insbesondere muss es sicherstellen, dass die Informatiksicherheit gewährleistet ist. Erfolgt die Bearbeitung durch Privatpersonen oder im Ausland, ist die Durchführung von Kontrollen vertraglich zu regeln. Das Bundesorgan arbeitet bei der Durchführung von Kontrollen mit dem kantonalen Kontrollorgan zusammen.

2.17 Art. 17 Rechtsgrundlagen

Absatz 2 erfährt einige untergeordnete Änderungen.

In *Buchstabe b* wird präzisiert, dass der Bundesrat nur ausnahmsweise im Einzelfall Bewilligungen zur Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen erteilen kann. Gestützt auf die vorliegende Delegationsklausel kann somit nicht eine unbestimmte Anzahl von Fällen bewilligt werden. Dies entspricht der bisherigen Auslegung.

In *Buchstabe c* wird dem Recht der betroffenen Person, die Bearbeitung zu untersagen, Rechnung getragen. In Analogie zur für den Privatsektor geltenden Regelung (Art. 12 Abs. 3 DSG) und als Folge der Informationspflicht gemäss Artikel 7*a* ist es gerechtfertigt, dass das Recht der betroffenen Person, sich der Bearbeitung zu widersetzen, selbst dann stärker gewichtet wird, wenn sie ihre Daten allgemein zugänglich gemacht hat. Mit der Entwicklung des Internet nimmt die Bearbeitung von besonders schützenswerten Personendaten eine Dimension an, die der Kontrolle der betroffenen Personen entgleiten kann. Dies rechtfertigt, dass eine Bearbeitung auch untersagt werden kann, obwohl die fraglichen Daten allgemein zugänglich gemacht wurden.

2.18 Art. 17*a* Automatisierte Bearbeitung von Personendaten im Rahmen von Pilotversuchen

Die vorliegende Bestimmung steht im Zusammenhang mit der Umsetzung der Motion «Online-Verbindungen» (vgl. Ziff. 1.2.1.1).

Im Vernehmlassungsentwurf wurde vorgeschlagen, dem Bundesrat sei es zu ermöglichen, die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen vor Inkrafttreten eines Gesetzes im formellen Sinne zu bewilligen. Aufgrund der mehrheitlich skeptischen Aufnahme dieses Vorschlages wurde eine enger gefasste Variante eingehend geprüft, die nur Erleichte-

rungen für die Einrichtung neuer Online-Verbindungen vorgesehen hätte. Es zeigte sich indessen, dass diese Minimalvariante es nicht erlauben würde, die sich in der Praxis stellenden Probleme zu lösen. Daher wurde ein Ansatz gewählt, der dem ursprünglichen Vorschlag grundsätzlich entspricht, der aber die Erleichterung bei der Erfordernis der formellgesetzlichen Grundlage ausdrücklich auf Fälle beschränkt, in denen Pilotversuche unbedingt erforderlich sind. Die vorgeschlagenen Neuerung nimmt die Empfehlungen der Geschäftsprüfungskommission des Ständerates vom 19. November 1998[46] auf, wonach der Bundesrat Online-Verbindungen, bevor sie in einem formellen Gesetz geregelt werden, unter dem Gesichtspunkt von Zweckmässigkeit, Verhältnismässigkeit und Zweckbindung prüfen soll. Bereits heute stellt indessen die Einrichtung *neuer* Online-Verbindungen *nicht* mehr das eigentliche Problem dar. Die Struktur eines Informatiksystems muss vielmehr von Beginn an auf solche Verbindungen ausgerichtet sein, wenn es nicht von Vornherein als rein internes System angelegt ist. Das bedeutet indessen letztlich, dass es nicht genügt, wenn nur neue Verbindungen in Pilotversuchen getestet werden können, sondern dass es sinnvollerweise möglich sein muss, ein System als Ganzes in einem Versuchsbetrieb zu evaluieren.

Es sei daran erinnert, dass besonders schützenswerte Personendaten oder Persönlichkeitsprofile nach dem geltenden Recht nur bearbeitet werden können, wenn ein Gesetz im formellen Sinne dies ausdrücklich vorsieht, oder – ausnahmsweise – wenn eine der Voraussetzungen gemäss Artikel 17 Absatz 2 Buchstaben a bis c DSG erfüllt ist. Ausserdem können besonders schützenswerte Personendaten gemäss Artikel 19 Absatz 3 DSG nur mittels eines Abrufverfahrens zugänglich gemacht werden, wenn ein formelles Gesetz es ausdrücklich vorsieht. Anerkanntermassen genügt eine formellgesetzliche Grundlage nicht, welche einzig die die Bearbeitung erforderlich machenden Aufgaben regelt. Die gesetzliche Grundlage muss das Organ bezeichnen, welches Zugang zu den Daten hat. Weiter muss sie den Zweck nennen, dem der Zugang dienen soll sowie den Umfang der Zugangsberechtigung umreissen.

Diese heute vom DSG aufgestellten Anforderungen an die gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen, sind sehr streng. Das kann problematische Auswirkungen haben: Oft wird mangels Erprobung von Datenbankzugängen unter realistischen Bedingungen, um möglichst alle denkbaren Bedürfnisse zu berücksichtigen, der Kreis der Zugangsberechtigten (Bundesbehörden, kantonale Instanzen, in gewissen Fällen auch Privatpersonen) tendenziell zu grosszügig umschrieben. Könnten beispielsweise Datenbankzugänge, vor allem mittels Online-Verbindungen, während einer Pilotphase erprobt werden, würde dies bei der Erarbeitung eines Gesetzes im formellen Sinne eine bessere Abgrenzung der Zugriffsbedürfnisse erlauben. Es genügt aber nicht, lediglich neue Online-Verbindungen unter erleichterten Bedingungen einrichten und testen zu können, sondern es ist auch notwendig, in bestimmten Fällen die Konzeption – und insbesondere die Vernetzung – neuer Systeme in ihrer Gesamtheit im Rahmen von Pilotversuchen zu evaluieren. Aufgrund der verhältnismässig langen Dauer des Gesetzgebungsprozesses muss heute mit der Ausarbeitung der gesetzlichen Grundlage begonnen werden, bevor die Details des betreffenden Informatiksystems bekannt sind. Bei diesem Vorgehen ist das Risiko gross, dass die gesetzliche Grundlage nur ungenügend auf die Zweckbestimmung des Systems ausgerichtet ist.

46 Vgl. Empfehlung 261 des Berichts der Geschäftsprüfungskommission des Ständerates, BBl **1999** 5869, S. 5895.

Artikel 17*a* enthält eine Delegationsklausel, die es dem Bundesrat für eine auf höchstens fünf Jahre begrenzte Dauer erlaubt, die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen zu bewilligen, wenn die technische Umsetzung einer bestimmten Bearbeitung eine Versuchsphase zwingend erforderlich macht. Mit dem neuen Artikel 17*a* DSG wird das Erfordernis der gesetzlichen Grundlage für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen nicht generell gelockert. Die neue Bestimmung beschränkt sich darauf, dort, wo eine entsprechende Notwendigkeit wirklich besteht, eine «experimentelle Gesetzgebung» zuzulassen. Diese ermöglicht, die Auswirkungen einer geplanten Regelung zunächst während einer Pilotphase zu überprüfen und genau zu evaluieren.

Absatz 1 verpflichtet den Bundesrat, den Datenschutzbeauftragten vorgängig zu konsultieren. Dessen Stellungnahme ist zwar nicht bindend, es ist indessen kaum vorstellbar, dass der Bundesrat ohne Vorliegen besonderer Umstände von einer ablehnenden Stellungnahme abweichen würde. Weiter legt Absatz 1 die Kriterien fest, die kumulativ erfüllt sein müssen, wenn der Bundesrat die Bewilligung eines Pilotversuches erwägt. Die Aufgaben, welche die fragliche Bearbeitung erfordern, müssen ihrerseits auf einer gesetzlichen Grundlage im formellen Sinne beruhen (Bst. a). Zudem müssen Massnahmen getroffen werden, die geeignet sind, Persönlichkeitsverletzungen zu minimieren (Bst. b). Buchstabe c hält fest, dass eine Pilotphase aufgrund der praktischen Umsetzung – d.h. der technischen oder organisatorischen Implementation – einer bestimmten Bearbeitung erforderlich sein muss, bevor eine entsprechende formellgesetzliche Grundlage geschaffen wird. Ist diese Notwendigkeit einer Versuchsphase nicht gegeben, kann der Bundesrat keine Bewilligung erteilen.

Absatz 2 stellt die Kriterien auf, nach denen zu beurteilen ist, ob im konkreten Fall tatsächlich die Notwendigkeit der Durchführung einer Pilotphase gegeben ist. Entweder sind für die praktische Umsetzung einer bestimmten Bearbeitung technische Neuerungen notwendig, deren Auswirkungen im Einzelnen von vornherein noch nicht absehbar sind (Bst. a). Dies ist insbesondere dann der Fall, wenn etwa eine bestimmte Software bisher noch nicht mit realen Daten benutzt bzw. getestet wurde oder wenn neue Technologien für die Informationserfassung und –übermittlung eingeführt werden sollen (z.B. Systeme zur automatisierten Erkennung der Nummernschilder von Fahrzeugen).

Weiter ist es möglich, dass die Erfüllung einer bestimmten Aufgabe, die eine Datenbearbeitung notwendig macht, komplexe organisatorische Vorkehrungen erfordert. Dies ist etwa dann häufig der Fall, wenn Bundesorgane mit kantonalen Organen zusammenarbeiten müssen (Bst. b). So mussten etwa für die Einrichtung einer DNA-Datenbank[47] die Aufgaben einer Vielzahl von verschiedenen Beteiligten sowie die Informationsflüsse präzise definiert werden; dies nicht zuletzt, um den bestmöglichen Schutz der betroffenen Personen zu gewährleisten.

Bei der Einrichtung von Abrufverfahren schliesslich kann sich – wie oben bereits erläutert – häufig eine Pilotphase als notwendig erweisen, damit der Kreis derjenigen Stellen, die zur Erfüllung ihrer jeweiligen Aufgabe über eine Zugangsberechti-

47 Vgl. dazu die Botschaft zum Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten und vermissten Personen vom 8. November 2000, BBl **2001** 29.

gung verfügen müssen, genau ermittelt werden kann (Bst. c). Insbesondere können so auch Zugangsberechtigungen optimiert werden. Im Rahmen von Pilotphasen kann darüber hinaus abgeklärt werden, ob die Einrichtung von Abrufverfahren in einem bestimmten Fall gegenüber bisher praktizierten Informationsabläufen vorzuziehen wäre.

Nach *Absatz 3* hat der Bundesrat die Modalitäten der Bearbeitung in einer Verordnung zu regeln. Damit wird die Transparenz dieser Pilotversuche sichergestellt; zudem kann der Bundesrat in seiner Verordnung Massnahmen zum Schutz der betroffenen Personen festlegen.

Absatz 4 verpflichtet das verantwortliche Bundesorgan dazu, dem Bundesrat innert zwei Jahren nach dem Beginn des Versuchsbetriebes einen Evaluationsbericht vorzulegen. Gestützt auf diesen Bericht hat es die Einstellung oder die Fortsetzung der Bearbeitung zu beantragen. Der Bericht wird auch die Grundlage für die Ausarbeitung der formellgesetzlichen Grundlage liefern können, falls die Fortsetzung der Bearbeitung vorgeschlagen wird. Mit dieser Bestimmung wird der experimentelle Charakter der mit der vorliegenden Regelung ermöglichten Pilotversuche betont; darüber hinaus wird bezüglich dieser Versuchsbetriebe zusätzliche Transparenz geschaffen.

Absatz 5 präzisiert unmissverständlich, dass die Bearbeitung abgebrochen werden muss, wenn die formellgesetzliche Grundlage nicht innerhalb von fünf Jahren nach der Einrichtung des Pilotsystems in Kraft getreten ist; das blosse Vorliegen eines Entwurfes genügt nicht. Diese Frist ist nicht verlängerbar.

2.19 Art. 18 Beschaffen von Personendaten

Artikel 18 Absatz 2 kann gestrichen werden, da die Bestimmung, wonach das Beschaffen von Personendaten erkennbar sein muss, nun im allgemeinen Teil in Artikel 4 Absatz 4 verankert ist und auf jede Beschaffung von Personendaten Anwendung findet.

2.20 Art. 19 Bekanntgabe von Personendaten

In Analogie zu Artikel 17 Absatz 2 Buchstabe c trägt Artikel 19 Absatz 1 Buchstabe c des Entwurfs dem Recht der betroffenen Person Rechnung, die Bearbeitung zu untersagen. Der Buchstabe b wurde an die Definition der gültigen erteilten Zustimmung in Artikel 4 Absatz 5 des Entwurfs angepasst.

2.21 Art. 21 Archivierung der Daten

Artikel 21 trägt dem neuen Bundesgesetz vom 26. Juni 1998 über die Archivierung (BGA)[48] Rechnung. Er übernimmt auf Gesetzesstufe fast unverändert die heute geltende Bestimmung des Artikel 27 der Datenschutzverordnung[49].

48 SR **152.1**
49 SR **235.11**

2.22 Art. 26 Wahl und Stellung des Eidgenössischen Datenschutzbeauftragten

Absatz 2 wird den heutigen Verhältnissen angepasst, da der Datenschutzbeauftragte bereits gegenwärtig der Bundeskanzlei zugeordnet ist.

Absatz 3 gesteht dem Datenschutzbeauftragten, analog zu anderen Behörden mit einem unabhängigen Status (z.B. Eidgenössische Finanzkontrolle), ein eigenes Budget zu.

2.23 Art. 27 Aufsicht über Bundesorgane

Aufgrund von Artikel 27 und 29 DSG verfügt der Datenschutzbeauftragte bereits heute über Untersuchungs- und Interventionskompetenzen, bezüglich der Datenbearbeitung durch Bundesorgane und Privatpersonen. Im Rahmen der Aufsicht über Bundesorgane hat der Datenschutzbeauftragte aber keine Beschwerdebefugnis[50]. In seiner Botschaft vom 23. März 1988[51] sah der Bundesrat die Möglichkeit einer Anrufung der Datenschutzkommission durch den Datenschutzbeauftragten vor, wenn dessen Empfehlungen durch die Departemente oder die Bundeskanzlei nicht befolgt wurden. Die Bundesversammlung jedoch wollte den Departementsvorsteherinnen und Departementsvorstehern bzw. der Bundeskanzlerin oder dem Bundeskanzler den Entscheid über Befolgung oder Nichtbefolgung der Empfehlungen überlassen. Der Nationalrat bestätigte diese Haltung am 3. März 1999, indem er die Motion von Felten 98.3030 (Beschwerderecht für den Datenschutzbeauftragten) ablehnte[52].

Dem gegenüber ist die Entwicklung des europäischen Rechts in dieser Frage zu berücksichtigen. Sowohl das Zusatzprotokoll zum Übereinkommen STE 108[53] wie auch die Richtlinie 95/46/EG fordern die Befugnis der Aufsichtsbehörden, Klagen führen oder einer gerichtlichen Instanz Verletzungen des nationalen Rechts zur Kenntnis bringen zu können. Um das Bundesrecht mit dem europäischen Recht in Übereinstimmung zu bringen und damit die Unterzeichnung des Zusatzprotokolls zu ermöglichen, sieht der vorliegende Entwurf vor, den Artikel 27 DSG um einen neuen Absatz 6 zu ergänzen, der dem Datenschutzbeauftragten die Kompetenz gibt, gegen Entscheide der Departemente und der Bundeskanzlei Beschwerde zu führen. Es ist darauf hinzuweisen, dass der Datenschutzbeauftragte gestützt auf Artikel 100 Absatz 2 Buchstabe a und Artikel 103 Buchstabe c OG[54] ans Bundesgericht gelangen kann. Die Kompetenzen des Datenschutzbeauftragten im Rahmen seiner Aufsicht über die Bundesorgane werden somit analog zu seinen bestehenden Kompetenzen im privatrechtlichen Bereich (Art. 29 DSG) ausgestaltet.

50 BGE **123** II 542
51 BBl **1988** II 413
52 AB N **1999** 115.
53 SR **0.235.1**
54 SR **173.10**

2.24 Art. 29 Abklärungen und Empfehlungen im Privatrechtsbereich

Die Untersuchungsbefugnis des Datenschutzbeauftragten ist an die im Rahmen der vorliegenden Teilrevision vorgenommenen Änderungen anzupassen. Absatz 1 Buchstabe b bezieht sich vor allem auf die mit Artikel 7*a* neu eingeführte Informationspflicht und erlaubt dem Datenschutzbeauftragten nötigenfalls die Tatsachenfeststellung wenn Verdacht auf einen Verstoss gegen die bei der Datenbeschaffung bestehende Informationspflicht besteht.

Mit den Änderungen von Absatz 1 Buchstabe c und d wird die vorliegende Bestimmung an die Änderungen betreffend die Pflicht der Privaten zur Anmeldung der Datensammlungen (Art. 11*a*) und die Informationspflicht bei bestimmten Fällen der grenzüberschreitenden Bekanntgabe von Daten (Art. 6 Abs. 3) angepasst.

2.25 Art. 31 Weitere Aufgaben

Die Liste der weiteren Aufgaben des Datenschutzbeauftragten nach Artikel 31 wird in im Hinblick auf Artikel 6 Absatz 1 und Absatz 3 sowie Artikel 11 ergänzt bzw. präzisiert.

2.26 Art. 34 Strafbestimmungen

Die Strafbestimmungen von Artikel 34 DSG werden durch Bezugnahme auf Artikel 7*a* und 7*b* des Entwurfs vervollständigt. Sie erlauben die strafrechtliche Sanktionierung der Personen, welche im Rahmen ihrer Informationspflicht vorsätzlich ungenaue oder unvollständige Auskünfte erteilen, oder die es unterlassen, die betroffene Person bei der Datenbeschaffung oder bei automatisierten Einzelentscheidungen zu informieren.

Absatz 2 Buchstabe a wird an die Neuregelung von Artikel 6 angepasst.

2.27 Art. 37 Vollzug durch die Kantone

Artikel 37 setzt die zweite Forderung der Motion «Online-Verbindungen» um und zielt auf die Erhöhung des Schutzes der von den kantonalen Organen beim Vollzug von Bundesrecht bearbeiteten Personendaten ab. Die Motion verlangt, dass für die Errichtung von Online-Verbindungen zu Informatiksystemen des Bundes Mindeststandards geschaffen werden, welche die Verbesserung der Zusammenarbeit zwischen Bund und Kantonen erlauben. Sie beauftragt ferner den Bund, den Zugriff zu seinen Datenbanken, sowie deren Nutzung, Schutz und Kontrolle zu regeln[55].

Der geltende Artikel 37 DSG enthält eine ergänzende Bestimmung, wonach das Bundesrecht nur Anwendung findet, wenn die Bearbeitung nicht kantonalen Datenschutzbestimmungen unterliegt. Dies ist in einigen Kantonen heute noch der Fall.

55 Vgl. auch den Bericht der Geschäftsprüfungskommission des Ständerats, BBl **1999** 5869, S. 5895.

Artikel 37 Absatz 1 des Entwurfs geht weiter und legt einen Mindestschutzstandard fest. Diese Bestimmung hat aber weiterhin ergänzenden Charakter. Das Bundesrecht findet somit künftig nicht nur dann Anwendung, wenn kantonale Datenschutzvorschriften fehlen, sondern auch, wenn diese kantonalen Bestimmungen kein angemessenes Schutzniveau gewährleisten. Unter einem «angemessenen Schutzniveau», wird ein solches verstanden, das dem des Übereinkommens STE 108[56] entspricht. Das in Artikel 37 Absatz 1 vorgesehene System funktioniert somit analog zu demjenigen, welches beim Datenverkehr ins Ausland Anwendung findet. Es liegt also in der Verantwortung des Bundes, dafür zu sorgen, dass die Privatpersonen und die Behörden, an die er von ihm bearbeitete Personendaten bekannt gibt, die gleichen Schutzstandards einhalten, wie er selbst. So weist der Bundesrat in seiner Antwort auf die Motion «Online-Verbindungen» darauf hin, dass die Sicherheit eines Informatiksystems und der Schutz der darin enthaltenen Daten durch das schwächste Glied der Kette bestimmt werden. Das Niveau des Datenschutzes kann von einem Kanton zum anderen erheblich variieren.

In der Vernehmlassung wurde teilweise die Kompetenz des Bundes zum Erlass der hier vorgesehenen Regelung in Frage gestellt. Diesbezüglich ist festzuhalten, dass es dem Bund grundsätzlich zusteht, im Bundesrecht den Kantonen im Rahmen der Regelung des Vollzugs auch Vorgaben bezüglich des Datenschutzes zu machen, soweit seine Gesetzgebungskompetenz nicht auf Rahmenregelungen beschränkt ist. Darüber hinaus werden die Kantone durch vom Bund abgeschlossene Staatsverträge – im vorliegenden Fall das Übereinkommen STE 108[57] – auch in ihren eigenen Kompetenzbereichen verpflichtet.

Der Bund ist verpflichtet, die kantonale Autonomie (namentlich die Organisationsautonomie) möglichst zu schonen (Art. 46 Abs. 2 und Art. 47 BV). Vorliegend ist diese Anforderung erfüllt, da die Regeln des DSG nur dann anwendbar sind, wenn die kantonalen Datenschutzvorschriften kein angemessenes Schutzniveau gewährleisten, d.h. wenn sie nicht einmal dem Standard des Übereinkommens STE 108[58] entsprechen.

2.28 Übergangsbestimmungen

Die Inhaber der Datensammlungen erhalten eine einjährige Frist ab Inkrafttreten des Gesetzes, damit sie die erforderlichen Massnahmen ergreifen können, um die Information der betroffenen Personen im Sinne von Artikel 4 Absatz 4, Artikel 7*a* und Artikel 7*b* zu gewährleisten. Es ist somit nicht vorgesehen, die Informationspflicht von Artikel 7*a* rückwirkend auf bereits beschaffte Daten anzuwenden.

56 SR **0.235.1**
57 SR **0.235.1**
58 SR **0.235.1**

3 Auswirkungen der Revision

3.1 Bund: Finanzielle und personelle Auswirkungen

Es ist schwierig, die finanziellen und personellen Auswirkungen der neuen Anforderungen im Zusammenhang mit der Informationspflicht gemäss Artikel 7*a* präzise abzuschätzen. Aller Voraussicht nach sollten sie geringfügig sein. Erfolgt die Datenbeschaffung nämlich direkt bei der betroffenen Person, kann die Information ohne grossen Aufwand erfolgen (beispielsweise mittels eines Standardsatzes auf dem Dokument, das der Beschaffung dient). Werden Daten bei Dritten beschafft, ist es sehr wahrscheinlich, dass Beschaffung oder Bekanntgabe der Daten in den meisten Fällen ausdrücklich vom Gesetz vorgesehen sind (vgl. Art. 17 Abs. 2 DSG); in einem solchen Fall kann auf die Information der betroffenen Person verzichtet werden (Art. 7*a* Abs. 3, in fine). Schliesslich sieht Artikel 9 des Entwurfs ein bestimmte Anzahl Ausnahmen von der Informationspflicht vor; diese betreffen insbesondere den öffentlichen Sektor.

Dem Datenschutzbeauftragten werden aufgrund des vorliegenden Entwurfes nur in geringfügigem Ausmass neue Kompetenzen übertragen; daher ergibt sich aufgrund der Revision keine Notwendigkeit einer Aufstockung seines Sekretariates.

3.2 Auswirkungen auf die Kantone

3.2.1 Finanzielle und personelle Auswirkungen

Die Revision tangiert die Kantone nur am Rande. Sie könnte indirekt bewirken, dass diejenigen Kantone, die noch kein angemessenes Schutzniveau gewährleisten, ihre Gesetzgebung im Datenschutzbereich verbessern, um weiterhin vom Bund Personendaten erhalten zu können. Weiter ist daran zu erinnern, dass das erforderliche Schutzniveau sich nach dem Übereinkommen STE 108[59] richtet, dessen Bestimmungen auch für die Kantone gelten.

3.2.2 Auswirkungen eines Beitritts zum Zusatzprotokoll auf die Kantone

Die Auswirkungen eines Beitritts zum Zusatzprotokoll zum Übereinkommen STE 108[60] wurden bereits dargelegt (vgl. Ziff 1.2.3.1.2 sowie die Erläuterungen zu den Artikeln 6 und 27). Der Entwurf strebt eine mit dem Zusatzprotokoll konforme Ausgestaltung des DSG an (vgl. Art. 6 und Art. 27 Abs. 6 des Entwurfs). Aufgrund von Artikel 37 Absatz 1 des Entwurfs wird Artikel 6 auch dann anwendbar sein, wenn kantonale Organe im Rahmen des Vollzugs von Bundesrecht Personendaten bearbeiten und das kantonale Datenschutzrecht kein ausreichendes Schutzniveau sicherstellt. Was Artikel 27 Absatz 6 des Entwurfs betrifft, wird er analog für die von den Kantonen bezeichneten Kontrollorgane gelten, wenn kantonalen Behörden Personendaten im Rahmen des Vollzugs von Bundesrecht bearbeiten (Art. 37 Abs. 2 DSG).

59 SR **0.235.1**
60 SR **0.235.1**

Soweit die Kantone nicht im Rahmen des Vollzugs von Bundesrecht tätig werden und daher das DSG nicht anwendbar ist, werden die Kantone ihre Gesetzgebung an die Anforderungen des Zusatzprotokolls anpassen müssen. Dies bedeutet, dass sie die Übermittlung von Personendaten in einen anderen Staat oder an eine Organisation nur dann erlauben dürfen, wenn beim Empfänger ein adäquates Schutzniveau sichergestellt ist. Das kantonale Recht kann Ausnahmen vorsehen für Fälle, in denen bestimmte Interessen der betroffenen Person überwiegen. Ausnahmen können ebenfalls vorgesehen werden, wenn weitere legitime Interessen – insbesondere wichtige öffentliche Interessen – dies rechtfertigen oder wenn genügende vertragliche Garantien bestehen. Der eidgenössische Datenschutzbeauftragte publiziert bereits heute eine Liste derjenigen Staaten, die über eine Datenschutzgesetzgebung verfügen, die ein Schutzniveau sicherstellt, welches dem schweizerischen vergleichbar ist. Diesbezüglich sollte die Anwendung des Zusatzprotokolls für Behörden und Private keine grösseren praktischen Schwierigkeiten verursachen.

Kantone, in welchen Stellung und Befugnisse des Kontrollorgans bzw. der Aufsichtsbehörde die Anforderungen des Zusatzprotokolls nicht erfüllen, werden entsprechende Anpassungen vornehmen müssen. Namentlich wird auch kantonalen Aufsichtsbehörden die Befugnis übertragen werden müssen, Untersuchungen durchzuführen oder in anderer Form zu intervenieren sowie Klage zu führen bzw. Verletzungen von Datenschutzvorschriften einem Gericht zur Kenntnis zu bringen. Gegen Entscheide der Aufsichtsbehörden muss eine Beschwerde offen stehen. Jede Person muss im Übrigen die Möglichkeit haben, die Aufsichtsbehörden anzurufen, soweit es um Fragen des Schutzes ihrer Rechte bezüglich der Bearbeitung ihrer Personendaten geht. Die Aufsichtsbehörden müssen ihre Funktion unabhängig ausüben.

Jeder Kanton wird prüfen müssen, ob seine Gesetzgebung mit den erwähnten Neuerungen vereinbar ist.

3.3 Auswirkungen im Informatikbereich

Eines der Ziele des Revisionsentwurfs besteht darin, für grössere Transparenz zu sorgen, dies vor allem bei der automatisierten Datenbearbeitung und im Internet. Die Inhaber der Datensammlungen sollen insbesondere auf der informatiktechnischen Ebene die erforderlichen Massnahmen ergreifen, um eine mit dem Datenschutzgesetz zu vereinbarende Datenbearbeitung zu gewährleisten. Sie müssen, vor allem im Internet, für eine Darstellung sorgen, welche die Beschaffung von Personendaten erkennbar macht und die Information der betroffenen Person bei der Beschaffung von besonders schützenswerten Daten und Persönlichkeitsprofilen gewährleistet. Ferner müssen sie über die Datensicherheit wachen, wenn sie die (informatiktechnische) Bearbeitung solcher Daten an Dritte übertragen. Diese aufgrund des vorliegenden Revisionsentwurfs notwendig werdenden Massnahmen haben auch den Vorteil, dass sie Transaktionen im Bereich des elektronischen Handels erleichtern. Sie können daher ganz allgemein einer effektiveren Nutzung der heute verfügbaren Informatikmittel dienen.

Für die Bundesbehörden ergibt sich aufgrund der vorliegenden Teilrevision kaum die Notwendigkeit von Anpassungen bei Informatiksystemen. Schon heute müssen die Bundesorgane das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen erkennbar machen (Art. 18 Abs. 2 DSG). Sie werden

prüfen müssen, ob die Pflicht zur aktiven Information über die Beschaffung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen gewisse Anpassungen verlangt. Die Zugänglichkeit des Registers der Datensammlungen, welches der Datenschutzbeauftragte führt, per Internet (vgl. Erläuterungen zu Art. 11*a*), wird zur Zeit unabhängig von der vorliegenden Teilrevision vorbereitet.

Für die Kantone und Gemeinden ergeben sich aus der Teilrevision voraussichtlich analoge Auswirkungen auf die Informatik.

3.4 Auswirkungen auf die Wirtschaft

Der Revisionsentwurf zielt auf die Erhöhung der Transparenz im Datenschutzbereich ab, indem er vor allem ein Recht der betroffenen Person vorsieht, über Datenbearbeitungen informiert zu werden. Es wird für die Betroffenen mit der Entwicklung der automatisierten Datenbearbeitung und des Internets immer schwieriger zu wissen, wer über sie Daten beschafft, zu welchem Zweck dies geschieht und welches die Datenempfänger sind. Der Gesetzesentwurf will weiter den Datenverkehr ins Ausland erleichtern, indem er gewährleistet, dass Daten grenzüberschreitend ausgetauscht werden können. Indirekt wird der Entwurf auch eine Stärkung des Vertrauens der Konsumentinnen und Konsumenten hinsichtlich der Bearbeitung ihrer personenbezogenen Daten bewirken, insbesondere bei den auf elektronischem Wege erfolgenden Transaktionen. Aus dieser Sicht wird der Revisionsentwurf positive Auswirkungen haben, und zwar nicht nur für die Konsumentinnen und Konsumenten. Auch die Unternehmen können so, namentlich im Bereich des elektronischen Handels, die Attraktivität ihrer Angebote verbessern. Dies wiederum stärkt ihre Wettbewerbsfähigkeit. Die Bedeutung des Datenschutzes für den elektronischen Handel wird auch von der OECD anerkannt. Sie hat Richtlinien zum Schutz der Konsumentinnen und Konsumenten im elektronischen Geschäftsverkehr verabschiedet und ein Instrument zur Zertifizierung von Web-Sites geschaffen[61]. Die Kosten für organisatorische Massnahmen zur Sicherstellung der Information werden durch diese positiven Auswirkungen mehr als kompensiert; die Markteffizienz wird insgesamt verbessert. Die neue Regelung trägt ebenfalls zur Erhöhung der Attraktivität der Schweiz als Wirtschaftsstandort bei. Sie fördert den Handel, weil eine Gesetzgebung, die ein den internationalen Anforderungen entsprechendes Niveau des Datenschutzes gewährleistet, den freien grenzüberschreitenden Datenverkehr erleichtert. Die Unterzeichnung des Zusatzprotokolls Übereinkommen STE 108[62] verfolgt dasselbe Ziel.

In erster Linie werden die Konsumentinnen und Konsumenten von den im Gesetzesentwurf vorgesehenen Massnahmen, namentlich im Informationsbereich, profitieren. Sie werden ihre Rechte besser verteidigen und sich gegen allfällige Verletzungen ihrer Persönlichkeitssphäre wehren können. Die Privaten werden insofern Vorteile erhalten, als die neuen Informationsverpflichtungen durch Erleichterungen bei der Meldepflicht kompensiert werden. Überdies ist der staatliche Eingriff auf das absolute Minimum beschränkt. Ob das Gesetz eingehalten wird, hängt inskünftig noch stärker von der Initiative der betroffenen Personen ab, die besser informiert sein

61 Vgl. BBl **2001** 865 und 941
62 SR **0.253.1**

werden und daher die Möglichkeit haben, ihre Interessen zu verteidigen. Die Untersuchungsbefugnisse des Datenschutzbeauftragten im Privatrechtsbereich bleiben im Wesentlichen die gleichen. Den wirtschaftlichen Akteuren wird eine grosse Eigenständigkeit belassen; sie können mittels freiwilliger Massnahmen, wie z.B. durch Abschluss von Vereinbarungen oder durch Annahme eines Verhaltenskodexes, für ein angemessenes Datenschutzniveau sorgen, namentlich beim Datenverkehr ins Ausland. Auch Unternehmen, die Selbstkontrollmechanismen einrichten (interner Beauftragter oder Beauftragte, Zertifikate) werden Erleichterungen gewährt. Die Missachtung von gesetzlichen Bestimmungen wird grundsätzlich auf dem Wege des Zivilprozesses (Art. 28 f. ZGB) und durch Empfehlungen des Datenschutzbeauftragten sanktioniert.

4 Verhältnis zur Legislaturplanung

Die Vorlage ist in der Legislaturplanung 1999–2003 als weiteres Geschäft angekündigt[63].

5 Rechtliche Grundlagen

5.1 Verfassungsrecht

Die neue Bundesverfassung enthält, wie die alte Bundesverfassung von 1874, keine Bestimmung, die dem Bund ausdrücklich eine Kompetenz im Datenschutzbereich zuweist. Wohl stipuliert die neue Verfassung in Artikel 13 den Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten. Es handelt sich hier aber um ein Grundrecht, das dem Bund keine Zuständigkeiten überträgt. Gemäss Artikel 35 Absatz 2 und 3 BV sind Personen, die staatliche Aufgaben wahrnehmen, an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen, und die Behörden sorgen dafür, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. In diesem Sinn trägt der Gesetzesentwurf an die Verwirklichung von Artikel 13 Absatz 2 BV bei, und zwar sowohl hinsichtlich der Beziehungen zwischen Staat und Privaten als auch zwischen Individuen.

Der Teilrevisionsentwurf basiert auf den Zuständigkeiten, über die der Bund schon bei der Annahme des Gesetzes verfügte. Im Privatrechtsbereich kann der Gesetzgeber sich auf seine Gesetzgebungskompetenz auf dem Gebiet des Zivilrechts abstützen (Art. 122 BV), desgleichen auf seine Gesetzgebungskompetenz bezüglich der Ausübung privatwirtschaftlicher Erwerbstätigkeit (Art. 95 BV) und des Schutzes der Konsumentinnen und Konsumenten (Art. 97 BV). Andere Verfassungsnormen ergänzen diese Bestimmungen, wie zum Beispiel die Gesetzgebungskompetenz auf dem Gebiet des Privatversicherungswesens (Art. 98 Abs. 3 BV)[64].

Auf dem Gebiet des öffentlichen Rechts hat sich der Bundesgesetzgeber zum Erlass der Datenschutzbestimmungen, die auf Verwaltungsbehörden anwendbar sind, auf die ihm gemäss Artikel 82 Ziff. 1 aBV eingeräumte Organisationsgewalt (Art. 173 Abs. 2 in der neuen Verfassung) gestützt. Wie der Bundesrat bereits in seiner Bot-

63 BBl **2000** 2276
64 BBl **1988** II 424 ff.

schaft vom 23. März 1988 betreffend das Bundesgesetz über den Datenschutz[65] betonte, kommt den Kantonen eine volle Organisationsautonomie zu; es ist an ihnen, in ihrem Bereich den Datenschutz zu regeln. Der Bund kann daher für die kantonalen und kommunalen Verwaltungen grundsätzlich keine Datenschutzbestimmungen erlassen. Eine Ausnahme bilden die Bereiche, in denen den Kantonen die Umsetzung des Bundesrechts – welche ihrerseits selbstverständlich über eine Grundlage in der Bundesverfassung verfügen muss – übertragen ist; selbst in diesem Fall muss der Bund aber möglichst vermeiden, in die kantonale Organisationshoheit einzugreifen. Für diese Bereiche hat der Bund Datenschutzbestimmungen erlassen, die auch für die Kantone gelten (vgl. namentlich Art. 37 DSG); der vorliegende Entwurf hält sich weiterhin an die diesbezügliche Grenze. Der Datenschutz bei der Datenbearbeitung durch kantonale Organe beim Vollzug von Bundesrecht (Art. 37 des Entwurfs) und bei der Datenbearbeitung durch ein Bundesorgan gemeinsam mit kantonalen Organen (Art. 16 Abs. 3) wird indessen erweitert.

5.2 Verhältnis zum internationalen Recht

Der Entwurf entspricht dem Übereinkommen STE 108[66] und ermöglicht die Ratifikation des Zusatzprotokolls vom 8. November 2001. Er ermöglicht zugleich eine teilweise Annäherung an die Richtlinie 95/46/EG. Weiter Ausführungen finden sich unter Ziffer 1.2.3 oben.

5.3 Übertragung von Rechtsetzungsbefugnissen

Der Bundesrat regelt die Einzelheiten der bei Datenbekanntgaben ins Ausland in bestimmten Fällen neu vorgesehenen Pflicht zur Information des Datenschutzbeauftragten (Art. 6 Abs. 3).

Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens (Art. 11 Abs. 2).

Weiter regelt der Bundesrat die Modalitäten der Anmeldung der Datensammlungen, der Führung und Veröffentlichung des Registers der Datensammlungen durch den Datenschutzbeauftragten sowie weitere Einzelheiten im Zusammenhang mit der Meldepflicht (Art. 11*a* Abs. 6).

Der Bundesrat kann unter bestimmten Voraussetzungen in einer Verordnung die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen im Rahmen von Pilotversuchen bewilligen (Art. 17*a*).

65 BBl **1988** II 413 ff., 425.
66 SR **0.235.1**

Inhaltsverzeichnis