EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT
DEPARTEMENT FEDERAL DE JUSTICE ET POLICE
DIPARTIMENTO FEDERALE DI GIUSTIZIA E POLIZIA
DEPARTAMENT FEDERAL DA GIUSTIA E POLIZIA

ENTWURF ZUR TEILREVISION DES BUNDESGESETZES ÜBER DEN DATENSCHUTZ (DSG) UND

ZUSATZPROTOKOLL ZUM ÜBEREINKOMMEN ZUM SCHUTZ DES MENSCHEN BEI DER AUTOMATISCHEN VERARBEITUNG PERSONENBEZOGENER DATEN BEZÜGLICH AUFSICHTSBEHÖRDEN UND GRENZÜBERSCHREITENDE DATENÜBERMITTLUNG

VERNEHMLASSUNGSENTWURF, TEXT DES ZUSATZPROTOKOLLS UND ERLÄUTERNDER BERICHT

Bern, im August 2001

ERLÄUTERNDER BERICHT

1. Allgemeiner Teil

11 Das geltende Recht

111 Auf eidgenössischer Ebene

Auf eidgenössischer Ebene wird der Datenschutz heute durch das Bundesgesetz vom 19. Juni 1992 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 den in ihren Persönlichkeitsrechten verletzten Personen zustehen, sowie das Verfahren (Art. 15).

Die Art. 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 Art. 19 Abs. 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 Datenschutzkommission 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[1].

112 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[2]. Darüber hinaus gelten gemäss Art. 37 Abs. 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.

Art. 37 Abs. 2 DSG verpflichtet ferner die Kantone zur Bestimmung eines Kontrollorgans, welches für die Einhaltung des Datenschutzes sorgt. Dieser Verpflichtung sind noch nicht alle Kantone nachgekommen. Soweit Kontrollorgane bestimmt sind, können sich deren Rechtsstellung, Befugnisse und Handlungsinstrumente vom einen Kanton zum andern erheblich unterscheiden.

12 Vorbereitungsarbeiten

121 Parlamentarische Vorstösse, die zur Revision geführt haben

121.1 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 Errichtung 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 ausdrückliche Grundlage in einem formellen Gesetz ist sodann erforderlich, wenn in einem Abruf-

---

1 BGE 123 II 542.

2 Vgl. Art. 16 Abs. 2 und 37 Abs. 1 DSG; Art. 16 Abs. 3 BWIS; Art. 16 Abs. 1 und 17 Abs. 1 BStatG.

verfahren 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[3].

121.2 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.

---

[3] Amtl. Bull. 1999 SR 212 und N 2599.

122 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 vollständig mit dem Recht der Europäischen Union in Übereinstimmung zu bringen.

Um die Ansichten von Fachleuten zusammenzutragen, bildete das Bundesamt für Justiz eine informelle Arbeitsgruppe von Datenschutzspezialisten des öffentlichen und privaten Sektors, denen der Vorentwurf unterbreite wurde[4]. 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 europäischen Recht angestrebt werden sowie die Untersuchungs-, Beratungs- und Mediationskompetenzen des Datenschutzbeauftragten verstärkt werden.

Die Teilrevision soll darüber hinaus der Schweiz erlauben, dass Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, zu unterzeichnen. Das Zusatzprotokoll wurde vom Ministerkomitee des Europarates am 23. Mai 2001 verabschiedet und wird ab dem 8. November 2001 zur Unterzeichnung aufliegen (vgl. Ziff. 151.2 unten).

---

[4] 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.

13 Die Grundzüge der Revision

Die Revisionsarbeiten waren vom Bemühen getragen, den Persönlichkeitschutz 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 die Pflicht zur Registrierung von Datensammlungen gemäss Art. 11 DSG praktisch bedeutungslos werden wird. Deshalb wird vorgeschlagen, diese Verpflichtung für die Privatpersonen zu streichen. Ebenso ist die Meldepflicht für die Bekanntgabe von Daten ins Ausland (Art. 6 DSG) aufzuheben 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 behält seine Kompetenz, von sich aus tätig zu werden, indem er Sachverhaltsfeststellungen vornimmt und Empfehlungen erlässt; indessen ist nicht vorgesehen, diese Kompetenzen zu erweitern.

Es wird somit davon ausgegangen, dass die betroffene Person selbst die ihr zustehenden Rechte ausüben kann, wenn sie über die Datenerhebung informiert ist, und dass bezüglich der Kontrollfunktion des Datenschutzbeauftragten keine weitergehenden Massnahmen erforderlich sind. Dieses Konzept hat den Vorteil, dass die Beschränkungen, denen datenerhebende Personen – 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 ungefragt mit Informationen überschwemmt werden. Dies könnte von den Betroffenen nämlich – vor allem bei gängigen Transaktionen – ebenfalls als aufdringlich empfunden werden.

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. Das DSG 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 Datenerhebung erkennbar macht. Er trägt jedoch die Verantwortung für allfällige den durch die Datenerhebung Betroffenen zugefügte Nachteile.

Für die Bearbeitung von Personendaten durch die Bundesorgane wird das Erfordernis der formellgesetzlichen Grundlage minim gelockert. Damit wird den Schwierigkeiten bei der Errichtung von eidgenössischen Datenbanken, zu denen ein Online-

Zugang möglich sein soll, Rechnung getragen. Diese Formen der Datenbearbeitung können während einer begrenzten Pilotphase bereits vor dem Inkrafttreten einer formellgesetzlichen Grundlage erprobt werden, sofern die Aufgaben, deren Erfüllung die Bearbeitung dient, ihrerseits in einem formellen Gesetz geregelt sind.

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. Heute kann der Datenschutzbeauftragte nur zu dem Zeitpunkt eingreifen, in welchem eine Zugriffsberechtigung festgelegt wird. Er hat aber keinerlei Möglichkeit zu kontrollieren, ob der Zugriff in der Folge nicht auf weitere Organe ausgedehnt wird. Soweit Daten des Bundes bearbeitet werden, verfügt die Eidgenossenschaft über eine ausreichende verfassungsmässige Kompetenzgrundlage, um den Kantonen Mindestgarantien aufzuerlegen (vgl. Ziff. 3 nachfolgend).

Als Ergänzung zur Informationspflicht wird vorgeschlagen, die Rechte derjenigen Personen zu stärken, welche die Bearbeitung der sie betreffenden Daten untersagen wollen. Erfahrungsgemäss befinden sich diejenigen, die eine Verletzung erleiden, oft in einer Position, die es ihnen nicht erlaubt, ihre Rechte wirksam auszuüben. Vielfach ist die Verletzung, wenn die Justiz eingreift, bereits erfolgt und kann nicht mehr verhindert werden. In gewissen Fällen erhält die betroffene Person vom Inhaber der Datensammlung nicht die erforderlichen Informationen, um ihren Anspruch geltend machen zu können, namentlich was die Rechtfertigungsgründe der Bearbeitung anbelangt. 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.

Weitere Massnahmen zur Verstärkung der Position der Betroffenen sind ebenfalls denkbar. So wurde angeregt, nach dem Beispiel des Art. 13*a* des Bundesgesetzes gegen den unlauteren Wettbewerb (SR 241) Erleichterungen bei der Beweislast einzuführen, da der Beweis der Unrechtmässigkeit einer Verletzung von Persönlichkeitsrechten oder der Tragweite der erlittenen Beeinträchigung, beispielsweise im Fall einer grenzüberschreitenden Datenübermittlung, regelmässig nicht leicht ist. Die Ausnahmen von den 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 ein Ausgleich von unrechtmässigen Beeinträchtigungen – insbesondere bei grenzüberschreitenden Datenübermittlungen – durch die allgemeinen Haftungsregeln ausreichend sichergestellt ist. 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 ist im schweizerischen Recht sehr ungewöhnlich, besonders in einem Bereich, in welchem nicht durchwegs Beziehungen vertraglicher Natur bestehen. Die Schaffung einer auf Dienstleistungen ausgedehnten Generalklausel betreffend die Verantwortlichkeit von Hilfspersonen, wie dies der Vorentwurf zur Re-

vision und Vereinheitlichung des Haftungsrechts vorsieht, dürfte im Weiteren allfällige Lücken im gegenwärtig geltenden System schliessen.

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 europäische Union zählt daher die Schweiz zu den Ländern, die ein angemessenes Schutzniveau aufweisen, womit der Datentransfer aus den Mitgliedstaaten der Europäischen Union in unser Land erlaubt ist. Obwohl diese Qualifikation seitens der EU jederzeit revidiert werden kann, entspricht das Anliegen einer Angleichung des DSG an das Gemeinschaftsrecht nicht einer unmittelbaren Notwendigkeit; zumal sich der Stand der Rechtsetzung auch in der Europäischen Union in naher Zukunft weiter entwickeln dürfte. Gegenwärtig wird ein Evaluationsbericht zur EU-Datenschutzrichtlinie erwartet. Dennoch verfolgt der Entwurf in mehreren Punkten Ziele, die nahe bei denen der EU-Richtlinie liegen.

Schliesslich ist die im DSG verwendete Terminologie nicht durchwegs zufriedenstellend. Gewisse Begriffe wären neu zu definieren (z.B. „Dritte“ oder „Abrufverfahren“) und der Ausdruck „Inhaber der Datensammlung“ entspricht nicht mehr der international gängigen Begrifflichkeit. 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.

14 Die wesentlichen Neuerungen

141 Die Informationspflicht bei der Erhebung von Personendaten

Eine der hauptsächlichen Neuerungen des Gesetzesentwurfs besteht in 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. Art. 4 Abs. 4 des Entwurfs beschränkt sich für diese Art von Daten auf den Grundsatz, dass die Beschaffung und insbesondere der Zweck der Bearbeitung deutlich 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; ohne dass jedoch die gleich hohen Anforderungen gestellt werden, wie sie Art. 7*a* des Entwurfs für die besonders schützenswerten Daten und die Persönlichkeitsprofile vorsieht.

142 Wegfall 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 aufgegeben. Ebenso entfällt 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). Das vom Eidgenössischen Datenschutzbeauftragten geführte Register der Datensammlungen wird deshalb künftig nur noch die Datensammlungen der Bundesorgane enthalten. Die Meldepflicht betreffend die grenzüberschreitende Bekanntgabe wird durch eine Sorgfaltspflicht ersetzt. Die Aufhebung der Meldepflicht für Datensammlungen der Privatpersonen ist auf Grund des begrenzten Informationswerts dieses Registers gerechtfertigt. Auch hat sich die Durchsetzung der Meldepflicht als schwierig erwiesen. Der praktische Nutzen des Registers würde ohnehin mit der Einführung einer Informationspflicht fast ganz verschwinden. Ein gewisser Ausgleich erfolgt durch die dem Datenschutzbeauftragten zustehende Möglichkeit, im Rahmen von Abklärungen im Privatrechtsbereich eine Liste der Datensammlungen zu verlangen (Art. 29 Abs. 2 des Entwurfs).

143 Das Verfahren der Untersagung der Datenbearbeitung

Das Recht der betroffenen Person, sich der Bearbeitung von sie betreffenden Personendaten zu widersetzen, ist im Fall der Bearbeitung durch private Personen bereits in Art. 12 Abs. 2 Bst. b DSG und im Fall der Bearbeitung durch Bundesorgane in Art. 20 DSG geregelt. Das Verfahren betreffend die Bearbeitung durch private Personen ist in Art. 15 DSG vorgesehen. Der Gesetzesentwurf sieht mit Art. 15*a* eine Neuerung vor. Private werden verpflichtet, die Bearbeitung unverzüglich einzustellen, wenn die betroffene Person die Bearbeitung untersagt. Das Verbot, die Daten zu bearbeiten, gilt solange, als der Inhaber der Datensammlung der betroffenen Person nicht die die Bearbeitung rechtfertigenden Gründe dargelegt hat. Tut er dies, so können die Betroffenen noch innert einer Frist von zehn Tagen vom Richter verlangen, dass er die Bearbeitung gemäss Art. 15 Abs. 1 DSG provisorisch oder definitiv untersagt. Diese Massnahme fliesst indirekt aus der Motion „Erhöhte Transparenz“. Das Recht auf Information hätte keinerlei Nutzen, wenn die betroffene Person sich der Bearbeitung nicht wirksam widersetzen könnte.

144 Bearbeitung von Personendaten durch Bundesorgane vor der Schaffung einer formellgesetzlichen Grundlage

Mit dem Ziel, die Forderungen der Motion „Online-Verbindungen“ zu verwirklichen, wird in einem neuen Art. 17*a* eine Bestimmung vorgeschlagen, die es dem Bundesrat ermöglicht, die automatisierte Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen im Rahmen von Pilotprojekten während einer begrenzten Zeitspanne selbst dann zu gestatten, wenn noch keine formelle gesetzliche Grundlage für eine derartige Bearbeitung vorliegt. Das Erfordernis, dass die die Bearbeitung erfordernden Aufgaben in einem formellen Gesetz umschrieben sein müssen, bleibt indessen bestehen.

145 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). Weiter kann der Datenschutzbeauftragte prüfen, ob bei der Datenbearbeitung in den Kantonen ein angemessenes Datenschutzniveau gewährleistet ist (Art. 27*a* des Entwurfs). Die Möglichkeit, bei den Kantonen oder Dritten Kontrollen durchzuführen, ergibt sich auch aus der Funktion des Inhabers der Datensammlung.

146 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. Art. 37 Abs. 1 des Entwurfs lehnt sich an die beim grenzüberschreitenden Datenfluss anwendbaren Regeln an. Gewährleisten die kantonalen Datenschutzbestimmungen kein angemessenes Schutzniveau, kommen die Bestimmungen des Bundesrechts ergänzend zur Anwendung.

15 Das internationale Umfeld

151 Europarat

151.1 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 (STE 108) vom 28. Januar 1981 beschlossen. Dieses Übereinkommen trat für die Schweiz am 1. Februar 1998[5] 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.

---

[5] Vgl. den Originaltext des Übereinkommens in BBl 1997 I 740 ff.

Die im Übereinkommen STE 108 niedergelegten Grundsätze bilden das Kernstück der Richtlinien der OECD vom 23. September 1980 über den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten. Diese Grundsätze wurden auch in die Richtlinie der Gemeinschaft 95/46/EG (vgl. Ziff. 152 nachstehend) aufgenommen. Das Übereinkommen vervollständigt und konkretisiert im Bereich der automatisierten Bearbeitung von Personendaten die Art. 8 (Recht auf Privatsphäre) und 10 (Meinungsäusserungsfreiheit) der Europäischen Menschenrechtskonvention (durch die Schweiz ratifiziert am 28. November 1974). Das schweizerische Recht genügt bereits heute den Anforderungen des Übereinkommens.

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[6]. 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.

151.2 Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung

Die Delegierten der Minister haben an ihrer Sitzung vom 23. Mai 2001 ein Zusatzprotokoll betreffend die Kontrollbehörden und den grenzüberschreitenden Datenverkehr verabschiedet. Das Zusatzprotokoll soll das Übereinkommen STE 108 in zwei Punkten vervollständigen. Erstens sieht es die Bestellung der 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 die Verletzungen der einschlägigen Bestimmungen des Landesrechts zur Kenntnis bringen können. Zweitens 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

---

[6] 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 beschaffte und bearbeitete Daten; vgl. Ziff. 3.3 der Empfehlung Nr. R (90) 19 über den Schutz personenbezogener, für Zahlungen und andere damit zusammenhängende Operationen verwendete Daten.

Schutzniveau gewährleistet. Die Garantien können insbesondere in entsprechend ausgestaltete Vertragsklauseln gekleidet sein. Das Protokoll wird anlässlich der 109. Sitzung des Ministerkomitees am 8. November 2001 zur Unterzeichnung durch die Signatarstaaten des Übereinkommens STE 108 vorliegen.

Gemäss Art. 27 und 28 DSG verfügt der Eidgenössische Datenschutzbeauftragte bereits über Untersuchungs- und Eingriffsbefugnisse, was die Bearbeitung von Personendaten durch Bundesorgane und private Personen anbelangt. Hinsichtlich der Überwachung der Bundesorgane erlaubt das geltende Recht dem Datenschutzbeauftragten jedoch nicht, vor Gericht Klage zu führen[7]. Die geltende Regelung des grenzüberschreitenden Datenverkehrs genügt den Anforderungen des Zusatzprotokolls nicht; darüber hinaus hat sie sich auch in der Praxis als unbefriedigend erwiesen. Der Revisionsentwurf hat zum Ziel, die eidgenössische Datenschutzgesetzgebung mit den Anforderungen des Protokolls in Übereinstimmung zu bringen. Er sieht dazu insbesondere vor, dem eidgenössischen Datenschutzbeauftragten die Befugnis zur Beschwerde gegen Entscheide der Departemente und der Bundeskanzlei zu erteilen (vgl. Art. 27 des Entwurfs und die diesbezüglichen Erläuterungen).

Der Bundesrat beabsichtigt, das Zusatzprotokoll so schnell wie möglich zu unterzeichnen. Daher führt er die Vernehmlassung zum diesem Protokoll zusammen mit der Vernehmlassung zur Teilrevision des DSG durch. Verzögert sich die Unterzeichnung des Zusatzprotokolls durch die Schweiz zu lange, könnte dies als Anzeichen dafür gewertet werden, dass unser Land das durch den Europarat gewährleistete Schutzniveau, insbesondere im Bereich des grenzüberschreitenden Datenverkehrs, nicht einhalten will. Soweit das durch das Übereinkommen STE 108 und das dazu gehördende Zusatzprotokoll gewährleistete Schutzniveau auch dem für die Europäische Union geltenden Standard entsprechen, könnte die Position der Schweiz im Hinblick auf einen Beitritt zu den Verträgen von Schengen oder zur Übereinkunft von Dublin geschwächt werden. Dem Zusatzprotokoll kommt generell grosse Bedeutung im Rahmen der Schaffung eines harmonisierten Regimes zur Übermittlung von Personendaten aus den Signatarstaaten in Drittländer zu.

Betreffend die Auswirkungen der Ratifikation des Zusatzprotokolls auf das kantonale Recht verweisen wir auf die Ausführungen unter Ziff. 5 nachstehend.

152 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[8] hat die Europäische Union unser Land als Drittstaat mit angemessenem Schutzniveau bezeichnet. Damit attestierte sie,

---

7 BGE 123 II 542.

8 Veröffentlicht im Amtsblatt der Europäischen Gemeinschaften Nr. L 215 vom 25.8.2000, S.1.

dass die schweizerische Gesetzgebung gesamthaft gesehen annähernd das in der Richtlinie geforderte Schutzniveau erreicht. Unsere Gesetzgebung 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 verfolgt, unsere Gesetzgebung vollständig mit dem Gemeinschaftsrecht kompatibel zu gestalten. Dieses könnte sich bereits in naher Zukunft weiter entwickeln (vgl. Ziff. 13 vorstehend). 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 Art. 10 und 11 der Richtlinie. Mit Art. 7*b* schlägt der Gesetzesentwurf ausserdem eine Variante vor, die gewährleistet, 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 europäische Datenschutzrichtlinie 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, das am 23. Mai 2001 durch die Delegierten der Minister verabschiedet wurde, stellt ähnliche Anforderungen auf (vgl. Ziff. 151.2 unten).

Die Bedingungen für die Gültigkeit der Zustimmung der betroffenen Person zu einer Datenbearbeitung definiert Art. 4 Abs. 5 des Entwurfs analog zur EU-Richtlinie.

Der Revisionsentwurf geht vor allem in zwei Punkten nicht so weit wie die Richtlinie. Zunächst wurde darauf verzichtet, die Bearbeitung von sensiblen Personendaten hinsichtlich Rasse, politischen Auffassungen, religiösen oder philosophischen Überzeugungen, Gewerkschaftszugehörigkeit sowie Gesundheit und Sexualleben zu verbieten, wie das die Richtlinie tut. 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 Art. 13 DSG gegeben sein (vgl. Art. 12 Abs. 2 Bst. c DSG). Die für die Beschaffung dieser Kategorie von Daten gemäss Art. 7*a* des Entwurfs vorgesehene Informationspflicht sollte im Übrigen eine dissuasive Wirkung haben, indem die Inhaber der Datensammlungen kein Interesse daran haben, solche Daten zu erheben – und damit den entsprechenden Informationsaufwand leisten zu müssen, wenn dies für 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 ist die Verpflichtung für die Privaten, ihre Datensammlungen beim Datenschutzbeauftragten anzumelden, schon heute stärker begrenzt als es die Richtlinie vorsieht.

Mit der Einführung der Informationspflicht bei der Erhebung im Sinne von Art. 7*a* des Revisionsentwurfs kommt diese Verpflichtung zur Anmeldung nur noch in sehr wenigen Fällen zur Anwendung und verliert somit jede praktische Bedeutung. Darüber hinaus hat sich bereits diese weniger strenge Meldepflicht als unbefriedigend erwiesen. Heute wird der Meldepflicht nicht immer nachgekommen, und der Datenschutzbeauftragte verfügt nicht über die erforderlichen Mittel, um die Einhaltung der gesetzlichen Bestimmungen in diesem Bereich zu gewährleisten. Es wurde dazu der Vorschlag gemacht, die Privaten seien zu verpflichten, selbst eine Liste der von ihnen durchgeführten Bearbeitungen zu führen. Diese Lösung hätte dazu beigetragen, die Aufgabe des Datenschutzbeauftragten zu erleichtern, aber anderseits den Privatpersonen, die bereits die Hauptlast an der Einführung der Informationspflicht bei der Bearbeitung tragen, eine zusätzliche Aufgabe auferlegt. Die Meldepflicht generell einzuführen, wie dies die europäische Richtlinie vorsieht, wäre eine Alternative, doch sind damit erhebliche Kosten verbunden. Als Ausgleich zu den den Privaten auferlegten neuen Aufgaben wird vorgeschlagen, die Meldepflicht für diese Personen zu streichen. Es ist jedoch nicht ausgeschlossen, dass diese Problematik später im Rahmen unserer Beziehungen mit der Europäischen Union neu zu prüfen sein wird.

153 Internationaler Vergleich

153.1 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 überwachen, 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.

153.2 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.

153.3 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.

153.4 Frankreich

Frankreich hat die Richtlinie 95/46/EG noch nicht umgesetzt. Das geltende Gesetz (Gesetz 78/17) datiert vom 6. Januar 1978. Ein Gesetzesentwurf zur Umsetzung der Richtlinie ist in Vorbereitung.

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.

153.5 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. Grundsätzlich 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 Verhaltenkodex erlassen. Weiter kann es von Amtes wegen oder auf Antrag gegenüber jeder Person, die den Grundsätzen des Datenschut-

zes zuwiderhandelt, Weisungen („enforcement notice“) erlassen. Wird eine solche Weisung nicht befolgt, liegt eine Rechtsverletzung vor.

2. Besonderer Teil

Art. 2 Geltungsbereich

Es ist nicht gerechtfertigt, 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, ungleich zu behandeln. 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 Entwurf besser der Rechtswirklichkeit. Das Internationale Komitee vom Roten Kreuz ist einer internationalen Organsiation gleichgestellt[9] und wird daher von dieser Ausnahme erfasst.

Art. 3 Begriffe

Bst. j wird an die neue Bundesverfassung vom 18. April 1999 angepasst, welche in Art. 163 für die Erlasse der Bundesversammlung, die rechtsetzende Bestimmungen enthalten, nicht mehr als zwei Formen vorsieht, nämlich das Bundesgesetz und die Verordnung.

Art. 4 Grundsätze

Die Rechtmässigkeit der Bearbeitung (Abs. 1)

Die geltende Formulierung von Art. 4 Abs. 1 DSG entspricht nicht ganz den Anforderungen von Art. 5 Bst. a der Übereinkunft STE 108. Nicht nur die Beschaffung, sondern jede Bearbeitung muss rechtmässig sein.

Der erkennbare Charakter der Beschaffung (Abs. 4)

Art. 4 Abs. 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. *7a*) vervollständigt.

Die Einführung der Informationspflicht gemäss Art. 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-

---

[9] BBl 1988 II 440; vgl. auch U. Maurer / N.P. Vogt, Kommentar zum Schweizerischen Datenschutzgesetz, ad Art. 2 Abs. 2 Bst. e, § 58 ff.

nössische Datenschutzbeauftragte hätte eine solche Regelung befürwortet. In der Arbeitsgruppe, die an der Ausarbeitung des Entwurfs 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. Art. 4 Abs. 4 des Gesetzesentwurfs bringt somit im Verhältnis zur heutigen Situation eine Verbesserung der Transparenz, ohne aber so weit wie Art. 7*a* zu gehen. Das Erfordernis, dass die Beschaffung erkennbar sein muss, ist in Art. 18 Abs. 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 Art. 7*a* des Entwurfs auf alle Personendaten anzuwenden.

Die Anforderungen, die erfüllt sein müssen, damit von einer „erkennbaren" Beschaffung gesprochen werden kann, beurteilen sich nach den Umständen sowie den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben (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.

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 Elemente der Beschaffung aufmerksam gemacht werden muss, welche Mittel dem Inhaber der Datensammlung zur Verfügung stehen, um diese Elemente 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 Art. 4 Abs. 4 keine neue Verpflichtung mit sich. Daher kann angenommen werden, dass die Anwendung von Art. 4 Abs. 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 mehr mit angemessenen

Mitteln auf die Erhebung und ihre wesentlichen Rahmenbedinungen aufmerksam gemacht werden. Die Mittel, um die Beschaffung erkennbar zu machen, sind von Fall zu Fall unterschiedlich. Bei einer telefonischen Umfrage kann beispielsweise eine mündliche Information über den Zweck der Erhebung, ihre Verwendung 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 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.

Die in Art. 4 Abs. 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. Art. 14 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit, BWIS, SR 120).

Die Voraussetzungen der Zustimmung (Abs. 5)

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 Revisionsentwurf (Art. 6 Abs. 2 Bst. b) wiederholt aufgestellt. Dem Begriff der „Zustimmung“ zur Datenbearbeitung kommt in der Praxis auch grosse Bedeutung zu, denn er wird von den privaten Personen am häufigsten als Rechtfertigungsgrund angerufen. Deshalb sieht Art. 4 Abs. 5 des Entwurfs vor, diesen Begriff gestützt auf die Rechtsprechung zu klären.

Art. 4 Abs. 5 des Entwurfs definiert, unter welchen Voraussetzungen die Zustimmung als gültig gelten kann, sofern in einer bestimmten Situation eine solche Zustimmung vom Gesetz verlangt wird. 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. Es wird lediglich ein Begriff definiert, der in der Praxis grosse Bedeutung hat. Der Begriff der Zustimmung

orientiert sich an demjenigen der „Einwilligung des aufgeklärten Patienten“[10], und zwar in dem Sinne, dass die betroffene Person über alle Informationen verfügt, die erforderlich sind, damit sie eine freie Entscheidung treffen kann. Insbesondere muss sie über mögliche negative Folgen oder Nachteile informiert sein, 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 heute wird gemäss dem Verhältnismässigkeitsgrundsatz davon ausgegangen, dass die Zustimmung umso klarer zu erfolgen hat, je sensibler die fraglichen Personendaten sind[11].

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.

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. Eine schwerwiegende Gefährdung droht namentlich dann, wenn im betreffenden Staat eine Gesetzgebung fehlt, die ein angemessenes Schutzniveau gewährleistet. Art. 6 stellt damit Anforderungen auf, welche denen der Gemeinschaftsrichtlinie 95/46/EG nahe kommen. Das Datenschutzrecht des Bundes wird damitkonform zum Zusatzprotokoll zum europäischen Übereinkommen STE 108 bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung , welches ab dem 8. November 2001 zur Unterzeichnung vorliegt (vgl. Ziff. 151.2 oben).

---

10 Vgl. insbesondere BGE 117 Ib 197, BGE 114 Ia 350 E. 6, BGE 119 II 456.

11 L. Brühwiler-Frésey, Medizinischer Behandlungsvertrag und Datenrecht, Zürich 1996, S. 87.

Art. 6 des Entwurfs untersagt grundsätzlich die Übermittlung von Personendaten ins Ausland, wenn Garantien fehlen, die ein angemessenes Schutzniveau gewährleisten. Diese Garantien können sich aus einer ausländischen Gesetzgebung ergeben, welche ein dem europäischen Übereinkommen STE 108 entsprechendes Schutzniveau gewährleistet, aber auch aus vertraglichen Bestimmungen oder aus einem Verhaltenskodex, 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 mangelnder Sorgfalt 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. Es wurde darauf verzichtet, eine besondere Kausalhaftung vorzusehen, weil aufgrund eines Verstosses gegen Art. 6 verursachter Schaden durch Art. 49*a* des Vorentwurfs des Bundesgesetzes über die Revision und Vereinheitlichung des Haftpflichtrechts grösstenteils gedeckt ist. Dieses Gesetz sieht vor, dass die Person, die sich zum Betrieb einer wirtschaftlichen Unternehmung einer oder mehrerer Hilfspersonen bedient, für den Schaden haftet, der im Rahmen ihrer Tätigkeiten verursacht wird. Sie kann sich der Haftung entschlagen, wenn sie beweist, dass die Organisation der Unternehmung geeignet war, den Schaden zu verhüten[12].

Abs. 2 erlaubt den grenzüberschreitenden Datenverkehr unter bestimmten Voraussetzungen auch dann, wenn die Anforderungen von Abs. 1 nicht erfüllt sind. Die in den Bst. a bis f aufgestellten Bedingungen entsprechen teilweise den Rechtfertigungsgründen von Art. 13 Abs. 1 und 2. Im Gegensatz zur Enumeration der überwiegenden Interessen gemäss Art. 13 Abs. 2 ist die Aufzählung der Bedingungen in Art. 6 Abs. 2 des Entwurfs abschliessend. Der Inhaber der Datensammlung muss den Datenschutzbeauftragten über die Garantien informieren, welche bei Fehlen einer adäquaten Gesetzgebung ein angemessenes Schutzniveau gewährleisten (Art. 6 Abs. 3). Die Verordnung des Bundesrates präzisiert, zu welchem Zeitpunkt und in welcher Art und Weise diese Information zu erfolgen hat. Der Datenschutzbeauftragte kann im Rahmen der ihm zustehenden Untersuchungsbefugnisse wenn nötig prüfen, ob die angegebenen Garantien genügend sind (vgl. Art. 29 Abs. 1 Bst. d des Entwurfs).

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

Art. 7*a* sieht vor, dass wer besonders schützenswerte Daten oder Persönlichkeitsprofile beschafft, verpflichtet ist, die betroffene Person darüber zu informieren. Die Information muss von Amtes wegen erfolgen, was Art. 7*a* vom Auskunftsrecht gemäss Art. 8 unterscheidet. Art 9 des Entwurfs erlaubt die Verweigerung, Einschränkung oder Aufschiebung der Informationspflicht, wenn ein überwiegendes öffentliches oder privates Interesse dies erfordert.

Art. 7*a* geht weiter als Art. 4 Abs. 4 des 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 Persön-

---

[12] Vgl. Revision und Vereinheitlichung des Haftpflichtrechts, erläuternder Bericht, Pierre Widmer und Pierre Wessner, Ziff. 2.4.3.4, S. 130 ff.

lichkeitsprofile insofern, als die Bearbeitung dieser Art von Personendaten zu Diskriminierungen führen kann. Art. 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 Abs. 2 muss der Inhaber der Datensammlung der betroffenen Person 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 der Datenempfänger, wenn die Bekanntgabe an Dritte erwogen wird. 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 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 (Abs.4). Die Information, die bei der erstmaligen Datenbeschaffung erfolgen muss, braucht – soweit die Umstände weiterer Erhebungen denen der erstmaligen Beschaffung entsprechen – somit nicht bei jeder neuerlichen Datenbeschaffung wiederholt zu werden.

Die Information ist keinem Formerfordernis unterworfen und kann mündlich erfolgen. Sie kann den Betroffenen auch 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 im Falle von Art. 4 Abs. 4 muss der Inhaber der Datensammlung der Informationspflicht des Art. 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: Im Bereich der Seuchenbekämpfung beispielsweise kann der Inhaber der Datensammlung, während er über die Datenbeschaffung informiert, gleichzeitig auch die einschlägigen Präventionsregeln darstellen. 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 den Praktikern in jedem Fachbereich liegen, die adäquaten Mittel zur Sicherstellung der Information der Betroffenen zu entwickeln. Art. 7*a* lässt diesbezüglich für die Inhaber der Datensammlungen einen grossen Spielraum offen. Für die Umsetzung der notwendigen Informationsmassnahmen ist eine Übergangsfrist vorgesehen (vgl. Übergangsbestimmungen).

Abs. 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 erhält,

spätestens jedoch bei der ersten Bekanntgabe an Dritte. Es kann allerdings sein, dass die Information der betroffenen Person sich nach den Umständen als unmöglich oder sehr schwierig erweist (z.B. wenn der Inhaber der Datensammlung keine Möglichkeit hat, die betroffene Person zu kontaktieren). Abs. 3 erlaubt in diesem Fall den Verzicht auf die Information. 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 Abs. 3 ist eng auszulegen. Der Inhaber der Datensammlung kann auch dann auf die Information der betroffenen Person verzichten, wenn die Beschaffung oder Bekanntgabe von Daten durch das Gesetz ausdrücklich vorgesehen ist.

Art. 9 sieht Einschränkungen der Informationspflicht vor, wenn das Gesetz es vorsieht 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 Gemeinschaftsrichtlinie 95/46/EG, die Empfehlungen des Europarats und die Datenschutzgesetze der umliegenden Länder sehr ähnliche Informationspflichten vorsehen, deren Tragweite allerdings weiter geht (vgl. Ziff. 15 oben).

Einige Unternehmen haben bereits Massnahmen ergriffen, die ihnen erlauben, die Anforderungen von Art. 7*a* zu 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, und wer nicht wenigstens die in Abs. 2 Bst. a bis c vorgesehenen Angaben liefert, kann strafrechtlich verfolgt werden (Art. 34 des Entwurfs).

Art. 7*b* Informationspflicht bei automatisierten Einzelentscheidungen

Art. 7*b* vervollständigt Art. 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 auf der Grundlage eines automatisierten Entscheids 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 Datenbearbeitungen lediglich eine Informationspflicht vorgesehen wird, geht der Entwurf nicht so weit, wie die Gemeinschaftsrichtlinie 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 Art. 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 selben Zweck.

Art 8 Auskunftsrecht

Art. 8 wird im Abs. 2 Bst. 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 und 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[13]. Diese Änderung trägt zur Erhöhung der Tansparenz 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 beschafft, berücksichtigen muss, dass die betroffene Person über die Herkunft der Daten Informationen verlangen kann.

Art. 9 Einschränkung der Informationspflicht und des Auskunftsrechts

Die Einschränkungen des Auskunftsrechts werden auf die Informationspflicht nach Art. 7*a* ausgedehnt. Liegt ein überwiegendes öffentliches oder privates Interesse vor, kann der Inhaber der Datensammlung die Information gemäss Art. 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 des Entwurfs; vgl. auch Art. 18 Abs. 6 BWIS).

---

[13] Vgl. den nicht veröffentlichten Entscheid vom 18. September 1991, Dr. F gegen Regierungsrat des Kantons St. Gallen, E. 5a; vgl. auch, im Strafrechtsbereich, BGE 118 Ia 457.

Art. 10*a* Datenbearbeitung durch Dritte

Art. 14 DSG wurde in den allgemeinen Teil verschoben und wird zu Art. 10*a*. Art. 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 DSG).

Abs. 1 wurde um einen Bst. c ergänzt: Die Datenbearbeitung kann nur dann einem Dritten übertragen werden, wenn die Datensicherheit gewährleistet ist. Diese Voraussetzung ergibt sich aus den Empfehlungen der Geschäftsprüfungskommission des Ständerats[14]. 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 (vgl. analog den Kommentar zu Art. 6 vorstehend).

Art. 11 Register der Datensammlungen

Heute sind die Privaten verpflichtet, Datensammlungen im Sinne von Art. 11 Abs. 3 DSG anzumelden, wenn die betroffene Person keine Kenntnis von der Bearbeitung gehabt habt (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 (Art. 7*a*) der Meldung der Datensammlungen praktisch keine Bedeutung mehr zu. Sollte das Register der Datensammlungen im Privatsektor noch Sinn machen, müsste die Richtung der Gemeinschaftsrichtlinie 95/46/EG und der Gesetzgebungen der umliegenden Länder eingeschlagen werden, die eine weit über die in Art. 11 DSG hinausgehende Meldepflicht vorsehen. Eine solche Meldepflicht würde für die Inhaber der Datensammlungen eine weitere Belastung bedeuten und überdies erhebliche Mittel, namentlich in personeller Hinsicht, erforderlich machen. Dazu kommt, dass die Pflicht zur Anmeldung der Datensammlungen, wie sie heute besteht, nicht die erwarteten Ergebnisse gebracht hat.

In Berücksichtigung der neuen Art. 4 Abs. 4 und Art. 7*a* sowie der daraus sich ergebenden zusätzlichen Einschränkungen für Privatpersonen, wird im privaten Bereich der Verzicht auf das Instrument der Registrierung von Datensammlungen vorgeschlagen. Die Abschaffung der Meldepflicht für Datensammlungen der Privaten wird teilweise kompensiert durch die grössere Transparenz, zu der die Inhaber der Datensammlungen bei der Beschaffung verpflichtet sind. Hingegen soll für die Bundesorgane die Anmeldepflicht beibehalten werden (vgl. Art. 20*a* des Entwurfs). Es ist indessen eine Änderung der Datenschutzverordnung (DSV, SR 235.11) vorgesehen; im Zuge dieser Änderung soll eine Vereinfachung des Meldeverfahrens geprüft werden. Die Beibehaltung des Registers der Datensammlungen für die Bundesorgane rechtfertigt sich insbesondere dadurch, dass im öffentlichen Sektor weitergehende Einschränkungen der Informationspflicht zulässig sind als im privaten Sektor (vgl. Art. 9 DSG). Die Meldepflicht bleibt ebenfalls bestehen für die kantonalen Organe, die

---

[14] 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.

Daten im Rahmen des Vollzugs von Bundesrecht bearbeiten und die nicht kantonalen Datenschutzbestimmungen unterworfen sind, welche ein angemessenes Schutzniveau gewährleisten (Art. 37 Abs. 1 DSG).

Auch wenn die privaten Personen von der Anmeldepflicht ihrer Datensammlungen befreit werden, müssen sie weiterhin in der Lage sein, jederzeit Informationen über die Daten, die sie bearbeiten, zu liefern. Neben der Auskunftspflicht nach Art. 8 Abs. 2 sieht der Entwurf in Art. 29 Abs. 2 insbesondere auch ausdrücklich vor, dass der Datenschutzbeauftragte im Rahmen seiner Untersuchungsbefugnisse vom Inhaber eine Liste der Datensammlungen verlangen kann. Die Privaten müssen sich folglich entsprechend organisieren. Es liegt im Übrigen auch im Interesse des Inhabers, über eine Liste der von ihm geführten Datensammlungen zu verfügen. Dies ermöglicht eine bessere Kontrolle über die Datenbearbeitungen, die er ausführt oder ausführen lässt; damit wird die Erfüllung seiner datenschutzrechtlichen Pflichten erleichtert.

Art. 12 Persönlichkeitsverletzungen

Aufgrund des mit der Änderung von Art. 6 DSG vorgenommenen Systemwechsels entfällt der Verweis auf Art. 6 Abs. 1, der heute in Art. 12 Abs. 2 Bst. a figuriert.

Art. 14 Datenbearbeitung durch Dritte

Art. 14 wird durch Art. 10*a* ersetzt. Wir verweisen auf den Kommentar zu Art. 10*a* vorstehend.

Art. 15 Rechtsansprüche und Verfahren

Der Text von Abs. 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 Art. 7*a* des Entwurfs vorgeschlagenen Informationspflicht wird aber das Recht, ein Verbot der Bearbeitung zu verlangen, wirksamer (vgl. auch Art. 15*a* nachstehend).

Art. 15*a* Verfahren der Untersagung der Datenbearbeitung

Das Recht, die Datenbearbeitung im privaten Bereich zu untersagen, besteht bereits heute gemäss Art. 12 Abs. 2 Bst. b und 15 DSG. Art. 15*a* des Entwurfs verbessert lediglich die verfahrensmässige Stellung der betroffenen Person. Die Einführung einer Informationspflicht in Art. 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 Art. 15 DSG ausüben zu können.

Die betroffene Person weiss oft nicht, ob der Bearbeitung ein Rechtfertigungsgrund im Sinne von Art. 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 Erklärungen verlangen, doch bleiben solche Gesuche nicht selten unbeantwortet. In diesem Fall müsste die betroffene Person das Risiko auf sich nehmen, eine Klage gemäss Art. 15 DSG einzureichen, ohne einschätzen zu können, wie ihre Erfolgsaussichten sind. Mit Art. 15*a* zwingt eine Untersagung der Datenbearbeitung den Inhaber der Datensammlung, die Bearbeitung unverzüglich einzustellen. Er kann in der Folge von sich aus auf die Bearbeitung verzichten, wenn diese nicht gerechtfertigt ist. Will er die Bearbeitung fortsetzen, muss er dafür Rechtfertigungsgründe im Sinne von Art. 13 angeben. Für die Bekanntgabe der Gründe ist keinerlei Frist festgesetzt. Ist die Bearbeitung eingestellt, liegt es im Interesse des Inhabers der Datensammlung, der betroffenen Personen die Rechtfertigungsgründe so rasch wie möglich bekannt zu geben.

Ab dem Zeitpunkt, in dem die betroffene Person Kenntnis von den die Bearbeitung rechtfertigenden Gründen erhält, steht ihr noch eine Frist von zehn Tagen zur Verfügung, um nach Art. 15 DSG Klage zu erheben und insbesondere vorsorgliche Massnahmen zu verlangen. Tut sie es nicht, wird vermutet, dass die Untersagung zurückgezogen ist und die Bearbeitung weitergeführt werden kann. Ist die Bearbeitung durch einen Rechtfertigungsgrund geschützt, wird sich die betroffene Person in den meisten Fällen mit der Antwort des Inhabers der Datensammlung begnügen und auf eine Klageeinreichung verzichten. Es liegt im Interesse beider Parteien, unnötige Verfahren zu verhindern. Art. 15*a* trägt dazu bei, erlaubt er doch dem Inhaber der Datensammlung, die betroffene Person davon zu überzeugen, dass die Bearbeitung gerechtfertigt ist. Die Bestimmung gibt dem Inhaber der Datensammlung anderseits Gelegenheit, auf die Bearbeitung zu verzichten, wenn sie nicht erforderlich ist. Vor allem erlaubt das vorgeschlagene Verfahren der betroffenen Person, die Aussichten eines gerichtlichen Verfahrens besser abzuschätzen.

Die Frist, während der die Bearbeitung im Vorfeld einer allfälligen richterlichen Intervention einzustellen ist, muss kurz bleiben. Nach Art. 15*a* hängt ihre Dauer einzig vom Inhaber der Datensammlung ab, der ein grosses Interesse hat, der betroffenen Person seine Rechtfertigungsgründe rasch mitzuteilen. In diesem Fall sollte die Einstellung der Bearbeitung nicht länger als 15 Tage dauern. Für periodisch erscheinende Medien, für die Aktualität das höchste Gebot ist, ist diese Frist aber trotz ihrer Kürze offensichtlich nicht praktikabel. Abs. 4 sieht denn auch vor, dass das Verfahren nach Art. 15*a* auf deren Arbeit nicht anwendbar ist. Das bedeutet, dass gegen ein periodisch erscheinendes Medium ausschliesslich Klagen nach Art. 15 DSG erhoben werden können.

Art. 16 Verantwortliches Organ

In Art. 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. Erfolgt die Bearbeitung durch Privatpersonen oder im Ausland, ist die Durchführung von Kontrollen vertraglich zu regeln.

Art. 17 Rechtsgrundlagen

Abs. 2 erfährt einige untergeordnete Änderungen.

In Bst. b wird präzisiert, dass der Bundesrat nur 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. Dennoch empfiehlt es sich, den Unterschied zwischen dieser Art der Bewilligung, die auf einen konkreten Fall begrenzt ist, und der weitergehenden Ermöglichung einer Datenbearbeitung vor der Schaffung einer formellgesetzlichen Grundlage (Art. 17*a* des Entwurfs), deutlicher zu machen.

In Bst. c wird dem Recht der betroffenen Person, die Bearbeitung zu untersagen, Rechnung getragen. In Analogie zum Privatsektor (Art. 12 Abs. 3) und als Folge der Informationspflicht gemäss Art. 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.

Art. 17*a* Automatisierte Datenbearbeitung vor Inkrafttreten einer formellen gesetzlichen Grundlage

Hier geht es um die Umsetzung der Motion „Online-Verbindungen“ (vgl. Ziff. 121.1 oben). Zwei Varianten wurden dazu untersucht. Die in Art. 17*a* vorgeschlagene Lösung besteht in der Möglichkeit einer Bewilligung der automatisierten Bearbeitung von besonders schützenswerten Daten oder von Persönlichkeitsprofilen vor Inkrafttreten eines Gesetzes im formellen Sinne durch den Bundesrat. Die andere Variante wäre enger gefasst gewesen und hätte nur die Bekanntgabe von besonders schützenswerten Daten oder Persönlichkeitsprofilen mittels eines Abrufverfahrens betroffen.

Art. 17*a* enthält eine Delegationsklausel, die es dem Bundesrat für eine auf drei Jahre begrenzte Dauer erlaubt, die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen zu bewilligen. Dies selbst dann, wenn die formellgesetzliche Grundlage, welche die eine Datenbearbeitung erfordernde Aufgabe regelt, dies nicht ausdrücklich vorsieht. Es ist daran zu erinnern, dass besonders schützenswerte Personendaten oder Persönlichkeitsprofile nach dem geltenden Recht nur bearbeitet werden können, wenn ein Gesetz im for-

mellen Sinne dies ausdrücklich vorsieht, oder – ausnahmsweise – wenn eine der Voraussetzungen gemäss Art. 17 Abs. 2 Bst. a bis c DSG erfüllt ist. Ausserdem können besonders schützenswerte Personendaten gemäss Art. 19 Abs. 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.

Die heute vom DSG aufgestellten Anforderungen an die gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen, sind sehr streng. Das ist nicht unproblematisch: Mangels Erprobung vorgesehener Datenbankzugänge unter realistischen Bedingungen wird, um möglichst alle denkbaren Bedürfnisse zu berücksichtigen, der Kreis der Zugangsberechtigten (Bundesbehörden, kantonale Instanzen, in gewissen Fällen auch Privatpersonen) tendenziell zu grosszügig umschrieben. Könnten 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. Diese Massnahme geht in die Richtung der Empfehlungen der Geschäftsprüfungskommission vom 19. November 1998[15], wonach der Bundesrat Online-Verbindungen, bevor sie in einem formellen Gesetz geregelt werden, unter dem Gesichtspunkt von Zweckmässigkeit, Verhältnismässigkeit und Zweckbindung prüfen soll.

Die Transparenz wäre gewährleistet, da die in der Pilotphase vorgesehenen Bearbeitungen – und vor allem die Online-Verbindungen – auf dem Verordnungswege zu regeln wären. Eine Bewilligung der Datenbearbeitung vor Inkrafttreten einer formellgesetzlichen Rechtsgrundlage kann nur erfolgen, wenn die Aufgaben, welche die Bearbeitung erfordern, ihrerseits auf einer gesetzlichen Grundlage im formellen Sinne beruhen. Schliesslich ist die Bewilligung an eine Anzahl weiterer Bedingungen geknüpft. Namentlich müssen angemessene Massnahmen zur Minimierung der Auswirkungen von Persönlichkeitsverletzungen ergriffen werden. Überdies muss die Bewilligung einem erheblichen öffentlichen Interesse dienen, das es nicht erlaubt, die Datenbearbeitung zu verzögern, oder sie muss dadurch gerechtfertigt sein, dass es notwendig ist, eine Testphase zu durchlaufen. In allen Fällen muss der Datenschutzbeauftragte die Bewilligung vorprüfen. Seine Auffassung ist für den Bundesrat nicht bindend. Es ist indessen kaum vorstellbar, dass der Bundesrat - ohne Vorliegen besonderer Umstände - von einer ablehnenden Stellungnahme des Datenschutzbeauftragten abweichen würde.

Abs. 3 präzisiert unmissverständlich, dass die Bearbeitung abgebrochen werden muss, wenn das Parlament innert drei Jahren nicht mit dem Entwurf eines Gesetzes im formellen Sinne befasst ist. Die vorgesehene Frist wurde nicht zufällig gewählt: Damit die Pilotphase sinnvoll ist, muss die Zeit veranschlagt werden, die erforderlich ist, um das System einzurichten, zu evaluieren und um schliesslich einen Gesetzentwurf auszuarbeiten. Eine Pilotphase von weniger als drei Jahren würde ihren Zweck kaum erfüllen.

---

15 Vgl. Empfehlung 261 des Berichts der Geschäftsprüfungskommission, BBl 1999 5869, S. 5895.

Art. 18 Beschaffen von Personendaten

Abs. 2 ist nicht mehr erforderlich, da die Bestimmung, wonach das Beschaffen von Personendaten erkennbar sein muss, nun im allgemeinen Teil in Art. 4 Abs. 4verankert ist und auf jede Beschaffung von Personendaten Anwendung findet.

Art. 19 Bekanntgabe von Personendaten

In Analogie zu Art. 17 Abs. 2 Bst. c trägt Art. 19 Abs. 1 Bst. c des Entwurfs dem Recht der betroffenen Person Rechnung, die Bearbeitung zu untersagen. Der Bst. b wurde an die Definition der gültigen erteilten Zustimmung in Art. 4 Abs. 5 des Entwurfs angepasst. Der Bst. e ist neu und trägt der Tatsache Rechnung, dass der Schutz der Privatsphäre für Personen des öffentlichen Lebens notwendigerweise weniger weit geht als für die übrigen Personen.

Art. 20*a* Register der Datensammlungen von Bundesorganen

Da die Verpflichtung der Privaten zur Anmeldung ihrer Datensammlungen aufgegeben wird (vgl. Art. 11 und die diesbezüglichen Erläuterungen), wird die die Bundesorgane treffende Meldepflicht nun im vierten Abschnitt geregelt. Art. 20*a* bringt für die Bundesorgane gegenüber dem geltenden Recht keine Änderung. Vereinfachungen können jedoch auf dem Verordnungswege ins Auge gefasst werden.

Art. 21 Archivierung der Daten

Art. 21 trägt dem neuen Bundesgesetz vom 26. Juni 1998 über die Archivierung (BGA)[16] Rechnung. Er übernimmt auf Gesetzesstufe fast unverändert die heute geltende Bestimmung des Art. 27 DSV.

Art. 26 Wahl und Stellung des Eidgenössischen Datenschutzbeauftragten

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

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

Art. 27 Aufsicht über Bundesorgane

Aufgrund von Art. 27 und 28 DSG verfügt der Datenschutzbeauftragte bereits heute über Untersuchungs- und Interventionskompetenzen, bezüglich der Datenbearbeitung durch Bundesorgane und Privatpersonen. Im Rahmen der Aufsicht über Bun-

---

16 SR 152.1

desorgane hat der Datenschutzbeauftragte aber keine Beschwerdebefugnis[17]. In seiner Botschaft vom 23. März 1988[18] sah der Bundesrat die Möglichkeit einer Anrufung der Datenschutzkommission durch den Datenschutzbeauftragten vor, wenn dessen Empfehlungen durch die Departemente oder die Bundeskanzlei nicht befolgt werden. 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.

Dem gegenüber ist die Entwicklung des europäischen Rechts in dieser Frage zu berücksichtigen. Sowohl das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung wie auch die EU-Datenschutzrichtlinie 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, schlagen wir vor, den Art. 27 um einen neuen Absatz 6 zu ergänzen, der dem Datenschutzbeauftragten die Kompetenz gibt, gegen Entscheide der Departemente und der Bundeskanzlei Beschwerde zu führen.

Art. 27*a* Aufsicht über kantonale Organe

Art. 27*a* verwirklicht den zweiten Punkt der Motion „Online-Verbindungen“, denn er erlaubt dem Datenschutzbeauftragten, das Niveau des Datenschutzes in den Kantonen zu kontrollieren, wenn die Daten von einem Bundesorgan und von kantonalen Organen gemeinsam bearbeitet werden.

Art. 29 Abklärungen und Empfehlungen im Privatrechtsbereich

Die Änderungen von Abs. 1 Bst. b und c resultieren aus der Aufhebung der Pflicht der Privaten zur Anmeldung der Datensammlungen (Art. 11 DSG) und der Aufhebung der Pflicht zur Meldung der grenzüberschreitenden Bekanntgabe von Daten (Art. 6 DSG). Um das Niveau des Datenschutzes insgesamt nicht herabzusetzen, muss die Untersuchungsbefugnis des Datenschutzbeauftragten in den besonders schutzwürdigen Bereichen aufrechterhalten bleiben. Es sind dies die Bekanntgabe von Personendaten an Dritte, die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen sowie die Bekanntgaben ins Ausland bei Fehlen einer ein angemessenes Schutzniveau gewährleistenden Gesetzgebung im Sinne von Art. 6 Abs. 2 Bst. a des Entwurfs. Abs. 1 Bst. b bezieht sich insbesondere auf Art. 7*a* und erlaubt dem Datenschutzbeauftragten nötigenfalls die Tatsachenfeststellung bei einem Verstoss gegen die bei der Datenbeschaffung bestehende Informationspflicht.

---

17 BGE 123 II 542.

18 BBl 1988 II 413.

Abs. 2 erfährt eine kleinere Änderung, und zwar ebenfalls im Zusammenhang mit der Aufhebung der Pflicht zur Anmeldung der Datensammlungen: Auch wenn die Privatpersonen von der Anmeldung ihrer Datensammlungen entbunden sind, müssen sie dennoch in der Lage sein, eine Liste ihrer Datensammlungen vorzulegen, wenn der Datenschutzbeauftragte dies im Rahmen einer Untersuchung verlangt.

Art. 34 Strafbestimmungen

Die Strafbestimmungen von Art. 34 DSG werden durch Bezugnahme auf Art. 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.

Die Änderung von Abs. 2 ergibt sich aus der Aufhebung der Pflicht der privaten Personen zur Anmeldung der Datensammlungen (Art. 11 DSG) sowie der Aufhebung der Meldepflicht bei der grenzüberschreitenden Bekanntgabe (Art. 6 DSG).

Art. 37 Vollzug durch die Kantone

Art. 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 Informatik-Systemen 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[19].

Der geltende Art. 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. Art. 37 Abs. 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 europäischen Übereinkommens STE 108 entspricht. Das in Art. 37 Abs. 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

---

[19] Vgl. auch den Bericht der Geschäftsprüfungskommission des Ständerats, BBl 1999 5869, S. 5895.

der Kette bestimmt werden. Das Niveau des Datenschutzes kann von einem Kanton zum anderen erheblich variieren.

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 Art. 7*a* zu gewährleisten. Es ist somit nicht vorgesehen, die Informationspflicht von Art. 7*a* rückwirkend auf bereits beschaffte Daten anzuwenden.

3. Rechtliche Grundlagen

Die Bundesverfassung vom 18. April 1999 enthält, wie die alte Bundesverfassung von 1874, keine Bestimmung, die dem Bund ausdrücklich eine Kompetenz im Datenschutzbereich zuweist. Wohl stipuliert die neue Verfassung in Art. 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 Art. 35 Abs. 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 Art. 13 Abs. 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)[20].

Auf dem Gebiet des öffentlichen Rechts hat sich der Bundesgesetzgeber zum Erlass der Datenschutzbestimmungen, die auf Verwaltungsbehörden anwendbar sind, auf die ihm gemäss Art. 82 Ziff. 1 aBV eingeräumte Organisationsgewalt (Art. 173 Abs. 2 in der neuen Verfassung) gestützt. Wie der Bundesrat bereits in seiner Botschaft vom 23. März 1988 betreffend das Bundesgesetz über den Datenschutz[21] 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 – welches seinerseits 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

---

20 BBl 1988 II 424 ff.

21 BBl 1988 II 413 ff., 425.

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 und 27*a* des Entwurfs) wird indessen erweitert.

4. Auswirkungen der Revision

41 Finanzielle und personelle Auswirkungen

411 Auf den Bund

Der Entwurf bewirkt keine bedeutende Ausweitung der Aufgaben oder Kompetenzen des Datenschutzbeauftragten; er wird somit insofern keine zusätzlichen Kosten verursachen.

Es ist schwierig, die finanziellen und personellen Auswirkungen der neuen Anforderungen im Zusammenhang mit der Informationspflicht gemäss Art. 7*a* einigermassen 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 Art. 9 des Entwurfs ein bestimmte Anzahl Ausnahmen von der Informationspflicht vor; diese betreffen insbesondere den öffentlichen Sektor.

412 Auf die Kantone

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 der Übereinkunft STE 108 richtet, dessen Bestimmungen auch für die Kantone gelten.

42 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.

43 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 Konsumentenen 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[22]. 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 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung 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 werden und daher die Möglichkeit haben, ihre Interessen zu verteidigen. Die Untersuchungsbefugnisse des Datenschutzbeauftragten im Privatrechtsbereich bleiben im Wesentlichen die gleichen. Anderseits wird den wirtschaftlichen Akteuren eine grosse Eigen-

---

22 Vgl. BBl 2001 865 und 941.

ständigkeit 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. Die Missachtung von gesetzlichen Bestimmungen wird grundsätzlich auf dem Wege des Zivilprozesses (Art. 28 f. ZGB) und durch Empfehlungen des Datenschutzbeauftragten sanktioniert.

5. Auswirkungen eines Beitritts zum Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung auf die Kantone

Die Auswirkungen eines Beitritts zum Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung wurden bereits dargelegt (vgl. Ziff 151.2 sowie die Erläuterungen zu den Artikeln 6 und 27 des Entwurfs). Der Entwurf strebt eine mit dem Zusatzprotokoll konforme Ausgestaltung des DSG an (vgl. Art. 6 und Art. 27 Abs. 6 des Entwurfs). Aufgrund von Art. 37 Abs. 1 des Entwurfs, wird Art. 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 Art. 27 Abs. 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).

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 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.

Diejenigen Kantone, die noch kein Kontrollorgan bzw. keine Aufsichtsbehörde bezeichnet haben, welches für die Einhaltung des Datenschutzes sorgt, werden diese Lücke füllen müssen. Es sei daran erinnert, dass Art. 37 Abs. 2 DSG die Kantone bereits heute dazu verpflichtet, ein solches Organ zu bezeichnen. Auch diesen kantonalen Aufsichtsbehörden wird 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.

Bundesgesetz über den Datenschutz (DSG)

Änderung vom ...

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
nach Einsicht in die Botschaft des Bundesrates vom ...[1]

beschliesst:

I

Das Bundesgesetz vom 19. Juni 1992[2] über den Datenschutz wird wie folgt geändert:

Art. 2 Abs. 2 Bst. e

[2] Es ist nicht anwendbar auf:

e. Personendaten, die durch internationale Organisationen bearbeitet werden, welche in der Schweiz ansässig sind und mit denen ein Sitzabkommen besteht.

Art. 3 Bst. i (neu), j Ziff. 1 und Bst. k

Die folgenden Ausdrücke bedeuten:

i. (neu; bisher Bst. j)[3] *Inhaber der Datensammlung*: private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden;

j. Gesetz im formellen Sinn:
   1. Bundesgesetze,
   2. *Unverändert*

k. *Aufgehoben*

Art. 4 Abs. 1, 4 und 5 (neu)

[1] Personendaten dürfen nur rechtmässig bearbeitet werden.

---

1 BBl **200...**

2 SR **235.1**

3 In der deutschen Fassung des Gesetzestextes fehlte bisher der Bst. i.

[4] Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.

[5] Macht das Gesetz eine Bearbeitung von Personendaten von der Zustimmung der betroffenen Person abhängig, so ist die Zustimmung für eine Datenbearbeitung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt; bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Zustimmung ausdrücklich erfolgen.

Art. 6 Grenzüberschreitende Bekanntgabe

[1] Personendaten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

[2] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können persönliche Daten ins Ausland bekanntgegeben werden, wenn:

a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
b. die betroffene Person im Einzelfall eingewilligt hat;
c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;
d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
e. die Bekanntgabe im Einzelfall zur Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist;
f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

[3] Der Eidgenössische Datenschutzbeauftragte muss über die Garantien nach Absatz 2 Buchstabe a informiert werden.

Art. 7a (neu) Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen

[1] Werden besonders schützenswerte Personendaten und Persönlichkeitsprofile beschafft, muss der Inhaber der Datensammlung die betroffene Person darüber informieren.

[2] Der betroffenen Person sind mindestens mitzuteilen:

a. der Inhaber der Datensammlung;
b. der Zweck des Bearbeitens;
c. die Kategorien der Datenempfänger, wenn eine Bekanntgabe vorgesehen ist.

[3] Werden die Daten nicht bei der betroffenen Person beschafft, hat deren Information spätestens bei der ersten Bekanntgabe an Dritte zu erfolgen, ausser wenn die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich oder die Beschaffung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist.

[4] Von einer Information der betroffenen Person kann abgesehen werden, wenn diese bereits informiert wurde.

Art. 7b (neu) Informationspflicht betreffend automatisierte Einzelentscheide

[1] Die betroffene Person muss angemessen darüber informiert werden, wenn ein Entscheid, der für sie rechtliche Folgen hat oder sie sonst wesentlich betrifft, ausschliesslich auf einer automatisierten Datenbearbeitung beruht, welche die Bewertung einzelner Aspekte ihrer Persönlichkeit bezweckt.

Art. 8 Abs. 2, Einleitungssatz und Bst. a

[2] Der Inhaber der Datensammlung muss der betroffenen Person mitteilen:
a. alle über sie in der Datensammlung vorhandenen Daten einschliesslich die verfügbaren Angaben über die Herkunft der Daten;

Art. 9 Sachüberschrift und Abs. 1 – 3 sowie Abs. 5
Einschränkung der Informationspflicht und des Auskunftsrecht

[1] Der Inhaber der Datensammlung kann die Information nach Artikel 7a oder die Auskunft nach Artikel 8 verweigern, einschränken oder aufschieben, soweit:
a. ein formelles Gesetz dies vorsieht;
b. es wegen überwiegender Interessen Dritter erforderlich ist.

[2] Ein Bundesorgan kann zudem die Information oder die Auskunft verweigern, einschränken oder aufschieben, soweit:
a. es wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich ist;
b. die Auskunft den Zweck einer Strafuntersuchung oder eines andern Untersuchungsverfahrens in Frage stellt.

[3] Der private Inhaber einer Datensammlung kann zudem die Information oder die Auskunft verweigern, einschränken oder aufschieben, soweit eigene überwiegende Interessen es erfordern und er die Personendaten nicht an Dritte bekanntgibt.

[5] Wurde die Information oder die Auskunft verweigert, eingeschränkt oder aufgeschoben, ist sie bei Wegfall des entsprechenden Grundes unverzüglich nachzuholen, ausser wenn dies nicht oder nur mit unverhältnismässigen Aufwand möglich ist.

Art. 10a (neu) Datenbearbeitung durch Dritte

[1] Das Bearbeiten von Personendaten kann Dritten übertragen werden, wenn:
a. der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte;
b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbieten;
c. die Datensicherheit gewährleistet ist.

[2] Dritte können dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.

Art. 11

Aufgehoben

Art. 12 Abs. 2 Bst. a

[2] Er darf insbesondere nicht ohne Rechtfertigungsgrund:
a. Personendaten entgegen den Grundsätzen von Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten;

Art. 14

Aufgehoben

Art. 15 Abs. 1 und 3

[1] Für Klagen und vorsorgliche Massnahmen zum Schutz der Persönlichkeit gelten die Artikel 28 bis 28l des Zivilgesetzbuches[4]. Der Kläger kann insbesondere verlangen, dass die Datenbearbeitung, namentlich die Bekanntgabe an Dritte, gesperrt oder die Personendaten berichtigt oder vernichtet werden.

[3] Der Kläger kann verlangen, dass die Berichtigung, die Vernichtung, die Sperre, namentlich die Sperre der Bekanntgabe an Dritte, der Vermerk über die Bestreitung oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

Art. 15a (neu) *Verfahren bei Untersagung der Datenbearbeitung*

[1] Wenn die betroffene Person die Datenbearbeitung untersagt, hat der Inhaber der Datensammlung diese unverzüglich einzustellen.

[2] Widersetzt sich der Inhaber der Datensammlung der Untersagung, muss er einen Rechtsfertigungsgrund nach Artikel 13 geltend machen.

---

4 SR **210**

[3] Die betroffene Person kann innert zehn Tagen seit Kenntnis des Rechtfertigungsgrunds vom Richter die Sperre der Datenbearbeitung verlangen (Art. 15). Geschieht dies nicht, gilt die Untersagung als zurückgezogen.

[4] Dieser Artikel ist nicht anwendbar auf Daten, die im redaktionellen Teil eines periodisch erscheinenden Mediums veröffentlicht werden.

Art. 16 Abs. 3 und 4 (neu)

[3] Wer zusammen mit einem Bundesorgan Personendaten bearbeitet, muss diesem erlauben, Kontrollen durchzuführen oder durchführen zu lassen. Wird die Datenbearbeitung an Dritte übertragen, kann das Bundesorgan bei ihnen ebenfalls Kontrollen durchführen oder durchführen lassen.

[4] Erfolgt die Datenbearbeitung durch private Personen oder im Ausland, regelt das zuständige Bundesorgan mittels Vertrag oder Vereinbarung die Ausübung der Kontrolle.

Art. 17 Abs. 2

[2] Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur bearbeitet werden, wenn ein formelles Gesetz es ausdrücklich vorsieht oder wenn:
a. es ausnahmsweise für die Erfüllung einer in einem formellen Gesetz klar umschriebenen Aufgabe unentbehrlich ist;
b. der Bundesrat es im Einzelfall bewilligt, weil die Rechte der betroffenen Person nicht gefährdet sind;
c. die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Art. 17a (neu) Automatisierte Datenbearbeitung vor Inkrafttreten einer formellen gesetzlichen Grundlage

[1] Der Bundesrat kann, nachdem er die Stellungnahme des Eidgenössischen Datenschutzbeauftragten eingeholt hat, vor Inkrafttreten eines formellen Gesetzes die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen bewilligen, wenn:
a. die Aufgaben, die diese Bearbeitung erforderlich machen in einem formellen Gesetz geregelt sind;
b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden;
c. ein wesentliches öffentliches Interesse keine Verzögerung der Datenbearbeitung erlaubt oder eine Testphase vor Inkrafttreten des Gesetzes unentbehrlich ist.

[2] Der Bundesrat regelt in einer Verordnung die Modalitäten der automatisierten Datenbearbeitung unter Gewährleistung eines angemessenen Schutzes der betroffenen Personen.

[3] Die automatisierte Datenbearbeitung muss abgebrochen werden, wenn der Bundesversammlung nicht spätestens drei Jahre nach Inkrafttreten der Verordnung ein Entwurf zu einem entsprechenden formellen Gesetz vorliegt.

Art. 18 Abs. 2

Aufgehoben

Art. 19 Abs. 1 Bst. b, c und e (neu)

[1] Bundesorgane dürfen Personendaten nur bekanntgeben, wenn dafür eine Rechtsgrundlage im Sinne von Artikel 17 besteht oder wenn:
b. die betroffene Person im Einzelfall eingewilligt hat;
c. die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt hat;
e. die bekanntgegebenen Personendaten im Einzelfall eine Person des öffentlichen Lebens betreffen, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Art. 20a (neu) Datensammlungen von Bundesorganen

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

[2] Die Bundesorgane müssen ihre sämtlichen Datensammlungen beim Datenschutzbeauftragten zur Registrierung anmelden.

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

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

Art. 21 Angebot von Unterlagen an das Bundesarchiv

[1]In Übereinstimmung mit dem Bundesgesetz vom 26. Juni 1998 über die Archivierung[5] bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen.

[2]Die Bundesorgane vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese:
a. anonymisiert sind;
b. zu Beweis- oder Sicherheitszwecken aufbewahrt werden müssen.

---

5 SR **152.1**

Art. 26 Abs. 2 und 3

[2] Er erfüllt seine Aufgaben unabhängig und ist der Bundeskanzlei administrativ zugeordnet.

[3] Er verfügt über ein ständiges Sekretariat und über ein eigenes Budget.

Art. 27 Abs. 6 (neu)

[6] Der Datenschutzbeauftragte kann den Entscheid des zuständigen Departements oder der Bundeskanzlei mit Beschwerde bei der Eidgenössischen Datenschutzkommission anfechten.

Art. 27a (neu) Aufsicht über kantonale Organe

Bearbeiten ein Bundesorgan und ein kantonales Organ gemeinsam Personendaten, kann der Datenschutzbeauftragte prüfen, ob ein angemessener Schutz im Sinne dieses Gesetzes bei der Bearbeitung durch das kantonale Organ gewährleistet ist.

Art. 29 Abs. 1 Bst. b, c, d d (neu) sowie Abs. 2

[1] Der Datenschutzbeauftragte klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn:

b. besonders schützenswerte Persondendaten oder Persönlichkeitsprofile bearbeitet werden;
c. Daten regelmässig an Dritte bekanntgegeben werden;
d. Bekanntgaben ins Ausland mitgeteilt werden müssen (Art. 6 Abs. 3).

[2] Er kann dabei Akten, insbesondere eine Liste der Datensammlungen, herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Das Zeugnisverweigerungsrecht nach Artikel 16 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[6] fn1 gilt sinngemäss.

Art. 34 Verletzung der Informationspflicht sowie der Auskunfts- und Mitwirkungspflichten

[1] Private Personen, die ihre Pflichten nach den Artikeln 7a, 8, 9 und 10 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen, werden auf Antrag mit Haft oder mit Busse bestraft.

[2] Private Personen, die bei der Abklärung eines Sachverhalts (Art. 29) dem Datenschutzbeauftragten vorsätzlich falsche Auskünfte erteilen oder die Mitwirkung verweigern, werden mit Haft oder Busse bestraft.

---

6 SR **172.021**

[3] Private Personen, die es vorsätzlich unterlassen, die betroffenen Personen nach Artikel 7a zu informieren oder ihnen nicht mindestens die Informationen nach Art. 7a Absatz 2 Buchstaben a bis c mitteilen, werden auf Antrag mit Haft oder Busse bestraft.

[4] Private Personen, die es vorsätzlich unterlassen, die betroffene Person nach Artikel 7b zu informieren, werden auf Antrag mit Haft oder Busse bestraft.

Art. 36 Abs. 6

Aufgehoben

Art. 37 Abs. 1

[1] Soweit keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten, gelten für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht die Artikel 1-10a, 16-17, 18-22 und 25 Absätze 1-3 dieses Gesetzes.

II

Übergangsbestimmungen

Innert einem Jahr nach Inkrafttreten dieses Gesetzes haben die Inhaber der Datensammlungen die notwendigen Massnahmen zur Information der betroffenen Personen nach Artikel 7a und 7b zu ergreifen.

III

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.