Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz (DSG)

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

Einleitung

Am 24. März 2006 hat die Bundesversammlung eine Änderung des Bundesgesetzes über den Datenschutz sowie einen Bundesbeschluss verabschiedet, der den Bundesrat zur Ratifizierung des Zusatzprotokolls vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung ermächtigt. Die Revision des DSG (BBl *2006* 3547; BBl *2003* 2101) verfolgte zwei Hauptziele: Einerseits sollte der Motion 98.3529 «Erhöhter Schutz für Personendaten bei Online-Verbindungen» der Geschäftsprüfungskommission des Ständerats und der Motion 00.3000 «Erhöhte Transparenz bei der Erhebung von Personendaten» der Kommission für Rechtsfragen des Ständerats Folge geleistet werden. Andererseits musste das DSG im Hinblick auf die Ratifizierung des Zusatzprotokolls zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) an die Anforderungen dieses Zusatzprotokolls angepasst werden.

Das revidierte Gesetz stärkt die Stellung der betroffenen Personen, indem es mehr Transparenz bei der Bearbeitung von Personendaten schafft, insbesondere durch die Einführung einer Informationspflicht gegenüber den betroffenen Personen beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Die grenzüberschreitende Datenbekanntgabe wird neu geregelt; dabei wird namentlich auf die Meldepflicht für die Übermittlung von Datensammlungen ins Ausland verzichtet. Die Bestimmungen über die Anmeldung von Datensammlungen werden an die Verpflichtung zu erhöhter Transparenz angepasst. Eine neue und innovative Bestimmung führt die Möglichkeit ein, dass Datenverarbeitungsprodukte und -systeme zur Bearbeitung von Personendaten zertifiziert werden, und ermutigt die Inhaber von Datensammlungen dazu, Datenschutzverantwortliche zu bezeichnen. Und nicht zuletzt ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) berechtigt, gegen Verfügungen der Bundeskanzlei und der Departemente Beschwerde zu führen, wenn eine von ihm abgegebene Empfehlung abgelehnt wird.

Diese Änderungen werden am 1. Januar 2008 in Kraft treten.

Mit dem Inkrafttreten des Bundesgesetzes vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ, SR 152.3) am 1. Juli 2006 wurde das DSG ebenfalls teilweise geändert. Dabei handelt es sich insbesondere um die Bestimmungen über die Datenbekanntgabe und über die Aufgaben des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten.

Allgemeine Datenschutzbestimmungen

Grundsätze (Artikel 4)

Artikel 4 DSG, der die Grundsätze des Datenschutzes festlegt, wurde dahingehend geändert, dass er einerseits Artikel 5 Buchstabe a des Übereinkommens STE Nr. 108 besser entspricht und dass andererseits die Transparenz bei der Datenbearbeitung verstärkt wird.

So muss nach *Absatz 1* nicht nur die Beschaffung der Daten rechtmässig sein, sondern auch alle anderen Stufen der Datenbearbeitung. Das allein stellt keine materielle Änderung dar, denn nach geltendem Recht muss jede Datenbearbeitung rechtmässig sein: gesetzliche Grundlage für die Datenbe-

arbeitung durch Bundesorgane (Art. 17); keine widerrechtliche Verletzung der Persönlichkeit der betroffenen Personen bei der Datenbearbeitung durch Private (Verletzung nur mit einem Rechtfertigungsgrund) (Art. 12 und 13).

Zur Erhöhung der Transparenz sieht *Artikel 4 Absatz 4* (neu) vor, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein müssen. Diese neue Bestimmung trägt zur Umsetzung der Motion «Erhöhte Transparenz bei der Erhebung von Personendaten» bei. Sie konkretisiert den in Artikel 4 Absatz 2 genannten Grundsatz von Treu und Glauben. Dieses Erfordernis der Erkennbarkeit bestand schon ausdrücklich für Bundesorgane bei der Bearbeitung von besonders schützenswerten Personendaten sowie von Persönlichkeitsprofilen (Art. 18 Abs. 2). Es wird damit auf alle Arten von Daten ausgedehnt und gilt auch für den privaten Bereich. Es handelt sich dabei nicht um eine Informationspflicht. Allerdings wird Artikel 4 Absatz 4 in Artikel 7*a* mit einer Informationspflicht für besonders schützenswerte Personendaten und für Persönlichkeitsprofile ergänzt (vgl. unten).

Artikel 4 Absatz 4 bedeutet, dass es für die betroffene Person unter normalen Umständen erkennbar sein muss, dass Daten, die sie betreffen, beschafft wurden oder möglicherweise beschafft werden (Grundsatz der Voraussehbarkeit). Sie muss den Zweck der Datenbearbeitung kennen oder feststellen können, sei es, dass nach Artikel 4 Absatz 3 der Zweck:

- bei der Beschaffung angegeben wurde; beispielsweise, wenn ein Versicherungsunternehmen im Formular für den Versicherungsantrag anführt, für welche Zwecke die verlangten Angaben verwendet werden;

- aus den Umständen ersichtlich ist; wenn beispielsweise eine Person bei einem Versandhaus Kleider bestellt, so übermittelt sie diesem Informationen, damit es die Bestellung abwickeln und ihr eine Rechnung zustellen kann. Bezahlt die Person die Rechnung nicht, so muss sie damit rechnen, dass ihre Daten für ein Schuldbetreibungsverfahren eingesetzt werden;

- vom Gesetz vorgesehen ist.

Gemäss Botschaft des Bundesrates (BBl 2003 2101 [2124f.]) sind die Anforderungen, die erfüllt sein müssen, damit die Beschaffung als erkennbar gilt, nach den Umständen sowie nach den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben zu beurteilen. Je nach Situation kann der Inhaber der Datensammlung verpflichtet sein, die betroffene Person aktiv zu informieren. Der Umfang der Information wird auch von den Umständen abhängen. Eine aktive Information ist insbesondere dann nötig, wenn die Daten möglicherweise problematisch sind und wenn der Zweck nicht auf Anhieb erkennbar ist. Unter Umständen ist nicht nur über die Beschaffung und über den Bearbeitungszweck zu informieren, sondern auch über andere entscheidende Faktoren wie die Identität des Inhabers der Datensammlung oder die Kategorien der Datenempfänger, falls die Daten zur Weitergabe bestimmt sind. In manchen Fällen müssen die betroffenen Personen auch darauf hingewiesen werden, ob eine Antwort freiwillig oder obligatorisch ist. Hingegen kann in bestimmten Situationen, namentlich bei einfachen Transaktionen, die Information auch knapper ausfallen oder ganz überflüssig sein, wenn die Datenbeschaffung und der Zweck der Datenbearbeitung aus den Umständen ersichtlich sind oder sich aus dem Gesetz ergeben. Wer ein Hotelzimmer reserviert und dem Hotelier Angaben über seine Person macht und die Anzahl gewünschter Übernachtungen angibt, weiss im Allgemeinen, zu welchem Zweck diese Daten bearbeitet werden. Hier ist eine spezielle Information nicht nötig. Gibt der Hotelier die Daten aber an Dritte weiter, so hat die betroffene Person Anspruch, darüber informiert zu werden.

Artikel 4 wird durch einen neuen *Absatz 5* ergänzt, der den Begriff «Einwilligung» klärt und festlegt, unter welchen Bedingungen die Einwilligung gültig ist, falls eine solche für die Bearbeitung von Personendaten erforderlich ist. Die Einwilligung ist – neben dem Gesetz oder einem überwiegenden privaten oder öffentlichen Interesse – einer der Gründe, die die Bearbeitung von Personendaten rechtfertigen können. Das DSG legt keinesfalls fest, dass die Einwilligung – insbesondere im privaten Bereich – eine Voraussetzung für jede Datenbearbeitung ist und dass die Einwilligung der betroffenen Personen namentlich dann einzuholen ist, wenn die Datenbearbeitung auf einem anderen Rechtfertigungsgrund beruht. Die Verwendung des Begriffs der Einwilligung ergibt sich aus der Rechtsprechung des Bundesgerichts und aus dem europäischen Recht, namentlich aus den Empfehlungen des Europarats: Die Einwilligung muss nach angemessener Information und freiwillig erfolgen. Werden besonders schützenswerte Personendaten bearbeitet, so muss die Einwilligung zudem ausdrücklich erfolgen. Die betroffene Person muss über alle Informationen verfügen, die es ihr erlauben, im konkreten Fall eine freie Entscheidung zu treffen. Sie muss insbesondere über die Folgen und Nachteile informiert sein, die sich aus einer Verweigerung ihrer Zustimmung ergeben könnten. Der Bundesrat formuliert diesen Punkt in seiner Botschaft wie folgt: «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.» (BBl *2003* 2127)

Die Änderung von *Artikel 5 Absatz 1* fand sich nicht im Entwurf des Bundesrates. Es handelt sich um eine Präzisierung, mit der die Reichweite von Artikel 5 begrenzt wird. Dieser Artikel verpflichtet die Person, die Daten bearbeitet, sich über deren Richtigkeit zu vergewissern. In der geltenden Fassung ist dieser Grundsatz zu absolut formuliert: «Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.» Diese Formulierung soll nicht bedeuten, dass nur richtige Daten bearbeitet werden dürfen. Hingegen schreibt sie vor, dass man sich über die Richtigkeit der Daten vergewissert. Der Umfang dieser Anforderung hängt von den konkreten Bedingungen der einzelnen Datenbearbeitung ab (namentlich Zweck der Bearbeitung, Grad der Sensibilität der Daten, Bekanntgabe an Dritte). Die Anforderung der Richtigkeit wird weiterhin beibehalten, aber der neue Wortlaut sieht vor, dass die Person, die Daten bearbeitet, «alle angemessenen Massnahmen zu treffen [hat], damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind». Diese Änderung begründet eine Pflicht zur Aktualisierung der Daten, falls dies notwendig ist. Die Notwendigkeit bemisst sich nach dem Grad der Sensibilität der Daten und dem Risiko einer Persönlichkeitsverletzung aufgrund der Unrichtigkeit der Daten. Werden zu Marketingzwecken Daten über Produktpräferenzen bearbeitet, ist es weniger wichtig, dass man sich über die Vollständigkeit und Aktualität der Daten vergewissert, als wenn Daten über die Zahlungsfähigkeit einer Person bearbeitet werden. Eine Aktualisierung ist immer dann nötig, wenn aufgrund der Unrichtigkeit die Persönlichkeit der betroffenen Person verletzt werden könnte, also nicht in jedem Fall. Im Allgemeinen liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person wissentlich akzeptiert, dass unrichtige Daten, die sie betreffen, bearbeitet werden. Diese Relativität des Grundsatzes der Richtigkeit ergibt sich auch aus Artikel 5 Buchstabe d des Übereinkommens STE Nr. 108 und aus Artikel 6 § 1 Buchstabe d der Richtlinie 95/46/EG über den Datenschutz. Der neue Wortlaut lehnt sich enger an den Wortlaut der Richtlinie an. Es geht daraus klar hervor, dass die Unrichtigkeit der Daten auch dadurch entstehen kann, dass sie im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unvollständig sind.

Grenzüberschreitende Bekanntgabe (Art. 6)

Die Regeln für die grenzüberschreitende Datenbekanntgabe wurden revidiert und dem Zusatzprotokoll zum Übereinkommen STE Nr. 108 und in gewissem Mass der Richtlinie 95/46/EG angepasst. Beibehalten wird der Grundsatz, dass Daten nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein dem schweizerischen Datenschutz entsprechender Schutz fehlt. Hingegen wird der Artikel an die Terminologie des Zusatzprotokolls angeglichen. Die Anforderung der «Gleichwertigkeit» wird ersetzt durch «einen angemessenen Schutz» («weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet»). Auf eine Verpflichtung, die Übermittlung von Datensammlungen ins Ausland zu melden, wenn für die Bekanntgabe keine gesetzliche Pflicht besteht und wenn die betroffenen Personen davon keine Kenntnis haben, wurde verzichtet, einerseits, weil die Anzahl Meldungen im Verhältnis zur vermuteten Zahl der grenzüberschreitenden Datenbekanntgaben bescheiden ausgefallen ist, andererseits, weil der Datenschutzbeauftragte nicht die nötigen Ressourcen hat, um alle Meldungen vor der Datenbekanntgabe zu prüfen. Daher wird nur die Sorgfaltspflicht von Privatpersonen oder Bundesorganen bei der grenzüberschreitenden Datenbekanntgabe beibehalten.

Die grenzüberschreitende Datenbekanntgabe ist möglich, wenn verschiedene Voraussetzungen erfüllt sind. Zunächst einmal sind bei der Bekanntgabe die zentralen Datenschutzgrundsätze nach den Artikeln 4, 5 und 7 DSG zu beachten. Die Bekanntgabe muss demnach rechtmässig sein und auf einem Rechtfertigungsgrund beruhen, hat nach Treu und Glauben zu erfolgen, muss verhältnismässig sein und einen klar festgelegten Zweck haben, und die übermittelten Daten müssen richtig sein. Ausserdem ist eine Bekanntgabe in der Regel nur möglich, wenn der Datenempfänger einer Gesetzgebung untersteht, die einen angemessenen Schutz gewährleistet. Die Angemessenheit des Schutzes ist unter Berücksichtigung der gesamten Umstände der Bekanntgabe zu beurteilen. Der Schutz ist also von Fall zu Fall und für jede einzelne Bekanntgabe oder Kategorie von Bekanntgaben zu beurteilen. Dabei sind die Umstände der Bekanntgabe zu prüfen, insbesondere: die Art der Daten; der Zweck und die Dauer der Bearbeitung, für welche die Daten übermittelt werden; das Herkunftsland und das endgültige Zielland; die im betreffenden Staat anwendbaren Rechtsvorschriften allgemeiner und sektorieller Art; die Berufsregeln und die Sicherheitsregelungen, die dort zu beachten sind.

Die Beurteilung der Angemessenheit des Schutzes kann jedoch auch für einen Staat generell erfolgen, so dass alle Datenbekanntgaben in diesen Staat erlaubt sind. Dies setzt insbesondere voraus, dass der Datenempfänger einem Gesetz untersteht, welches ein dem schweizerischen Recht vergleichbaren Datenschutz bietet: Gewährleistung der Rechte der betroffenen Personen (insbesondere Auskunfts- und Informationsrecht), Einhaltung der zentralen Datenschutzgrundsätze, unabhängiges Kontrollorgan. Dies trifft in der Regel dann zu, wenn der Zielstaat Vertragspartei des Übereinkommens STE Nr. 108 und des Zusatzprotokolls ist und die entsprechenden Anforderungen erfüllt. Der EDÖB führt eine Liste der Staaten, die seiner Ansicht nach einen angemessenen Datenschutz gewährleisten. Er berücksichtigt dabei auch die Entscheide, die die Europäische Kommission gestützt auf Artikel 25 § 6 der Richtlinie 95/46/EG trifft.

Fehlt ein angemessener Schutz, so ist die Bekanntgabe in der Regel verboten, weil sie die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet. Wenn die Person, die die Daten bekannt gibt, aber durch angemessene Massnahmen sicherstellt, dass die Datenbekanntgabe die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet, so kann sie die Daten auch dann bekannt geben, wenn eine Gesetzgebung mit angemessenem Schutz fehlt. Artikel 6 Absatz 2 listet sieben alternative Voraussetzungen auf, unter denen eine solche Bekanntgabe möglich ist; die Aufzählung ist abschliessend.

Nach *Artikel 6 Absatz 2 Buchstabe a* ist eine Bekanntgabe zulässig, wenn hinreichende Garantien einen angemessenen Schutz im Ausland gewährleisten. Diese Garantien können in einem Vertrag (Datenschutzklauseln) festgelegt sein (vgl. die verschiedenen vom Europarat und der Europäischen Kommission ausgearbeiteten Musterverträge sowie den Mustervertrag des EDÖB für das Outsourcing, www.derbeauftragte.ch, Rubrik Themen). Sie können sich auch aus einem Verhaltenskodex ergeben, das heisst aus einem Regelwerk, dem sich Private freiwillig unterstellen. Ein solches Regelwerk ist beispielsweise das «Safe Harbor Privacy Framework» (http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm), das von der Europäischen Kommission und den USA ausgehandelt wurde. Gestützt auf die Grundsätze dieses Regelwerks kann sich die amerikanische Empfängerorganisation schriftlich dazu verpflichten, für Daten aus der Schweiz die gleichen Datenschutzregeln anzuwenden wie für Daten aus einem Mitgliedstaat der Europäischen Union. Wer sich auf solche Garantien stützt, bleibt für den Datenschutz aber selber verantwortlich. Der Bundesrat weist in seiner Botschaft darauf hin, es sei «Sache desjenigen, welcher Personendaten ins Ausland übermittelt, nachzuweisen, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten». Zusätzlich muss er den EDÖB nach Absatz 3 über die Garantien informieren (vgl. unten).

Nach *Artikel 6 Absatz 2 Buchstabe b* ist eine Bekanntgabe im Einzelfall auch möglich, wenn die betroffene Person eingewilligt hat. Die Einwilligung muss freiwillig und nach angemessener Information erfolgen (Art. 4 Abs. 5 DSG). Die Einwilligung muss ausdrücklich erfolgen, wenn die Bekanntgabe besonders schützenswerte Personendaten oder Persönlichkeitsprofile betrifft. Die betroffene Person muss wissen, welche sie betreffenden Daten zu welchem Zweck an welchen Empfänger bekannt gegeben werden. Sie ist ebenfalls darüber zu informieren, dass ein angemessener Datenschutz fehlt. Die Bekanntgabe ist auf einen Einzelfall begrenzt, das heisst, sie muss einen konkreten Fall oder eine konkrete Situation betreffen. Die betroffene Person kann nicht pauschal einwilligen und mit einer solchen Einwilligung die regelmässige und systematische Bekanntgabe von Daten ins Ausland zu verschiedenen Zwecken und in verschiedenen Situationen ermöglichen. Hingegen kann die betroffene Person in einem konkreten Fall ihre Einwilligung auch für mehrere Bekanntgaben erteilen, wenn die Umstände, unter denen diese stattfinden, klar feststehen (BBl *1988* II 470). Der Wille der betroffenen Person, in die Bekanntgabe einzuwilligen, muss eindeutig zum Ausdruck kommen.

Eine Bekanntgabe darf auch erfolgen, wenn die Datenbearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt (*Art. 6 Abs. 2 Bst. c*). Diese Voraussetzung ist mit dem Rechtfertigungsgrund nach Artikel 13 Absatz 2 Buchstabe a vergleichbar. Die Datenbekanntgabe muss für den Abschluss oder die Abwicklung des Vertrags unabdingbar sein. Wird beispielsweise mit einem Reisebüro ein Reisevertrag abgeschlossen, der die Reservation eines Hotels im Ausland einschliesst, so darf das Reisebüro die für die Abwicklung des Vertrags nötigen Daten dem betreffenden Hotel bekannt geben.

Artikel 6 Absatz 2 Buchstabe d nennt einen weiteren Grund, der die Datenbekanntgabe trotz Fehlen eines angemessenen Datenschutzes rechtfertigen kann: Wenn die Bekanntgabe im Einzelfall entweder für die Wahrnehmung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist. Diese Bestimmung betrifft ebenfalls Einzelfälle, also konkrete Situationen, und rechtfertigt nicht die systematische und regelmässige Datenbekanntgabe. Die übermittelten Daten können eine Person oder mehrere Personen betreffen und ihre Bekanntgabe muss unerlässlich sein, das heisst, ohne die Daten kann der Zweck der Bekanntgabe nicht erreicht werden. So kann ein überwiegendes öffentliches Interesse daran bestehen, dass ein Fussballclub die Liste der notorischen Hooligans übermittelt, damit verhindert werden kann, dass diese Personen die öffentliche Sicherheit gefährden, wenn der besagte Club im Ausland spielt. Eine Person darf Daten auch bekannt geben, wenn sie ihre Rechte gegenüber einer

Drittperson vor einem Gericht eines Drittstaates geltend machen will (zum Beispiel für eine Schuldbetreibung), auch wenn dieser Staat keinen hinreichenden Datenschutz gewährleistet.

Artikel 6 Absatz 2 Buchstabe e ermöglicht die Datenbekanntgabe ins Ausland bei Fehlen eines angemessenen Schutzes, wenn sie im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. Die Übermittlung ist nur dann zulässig, wenn sie dazu bestimmt ist, lebenswichtige Interessen der betroffenen Person zu schützen. Es geht um Situationen, in denen die betroffene Person nicht in der Lage ist, ihre eigenen Interessen durch eine Einwilligung geltend zu machen, und für die sie vermutlich ihre Einwilligung zur Datenbekanntgabe gegeben hätte. Übermittelt werden dürfen unserer Ansicht nach auch Daten von Personen, die der betroffenen Person nahestehen, wenn diese Personen nicht einwilligen können und das Leben der betroffenen Person sonst in Gefahr wäre.

Die Datenbekanntgabe ist ebenfalls möglich, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (*Art. 6 Abs. 2 Bst. f*).

Schliesslich sieht *Artikel 6 Absatz 2 Buchstabe g* vor, dass die Datenbekanntgabe ins Ausland innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfinden kann, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten. Diese Bestimmung erlaubt die grenzüberschreitende Datenbekanntgabe innerhalb eines Konzerns. Die Tatsache, dass innerhalb derselben juristischen Person oder Gesellschaft oder innerhalb juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, Datenschutzregeln bestehen, befreit diese Gesellschaften nicht von der Pflicht, für die Datenbearbeitungen, die sie in der Schweiz durchführen, die übrigen Bestimmungen des DSG einzuhalten, namentlich betreffend die Information der betroffenen Personen oder das Auskunftsrecht. Diese Regeln sollen im Ausland auch bei Fehlen einer hinreichenden Datenschutzgesetzgebung einen angemessenen Schutz gewährleisten.

Artikel 6 Absatz 3 schreibt zusätzlich vor, dass der EDÖB über die Garantien nach Buchstabe a und die Datenschutzregeln nach Buchstabe g informiert werden muss. Der Bundesrat regelt die Einzelheiten dieser Informationspflicht. Die Informationspflicht bedeutet nicht, dass der EDÖB sein Einverständnis zu den Garantien oder den Datenschutzregeln geben muss. Sie gibt ihm aber die Möglichkeit, gegebenenfalls zu prüfen, ob die Garantien und Regeln hinreichend sind, um trotz Fehlen einer vergleichbaren Gesetzgebung einen angemessenen Datenschutz zu gewährleisten (Art. 31 Abs. 1 Bst. e DSG). Stellt er Mängel fest, kann er deren Behebung verlangen und gegebenenfalls eine Empfehlung abgeben (Art. 27 und 29 DSG). Stützen sich die Datenschutzklauseln auf Musterverträge oder -reglemente, die der EDÖB erstellt oder anerkannt hat, führt er keine Prüfung durch. Der Inhaber der Datensammlung muss ihn aber darüber informieren, dass er sich auf solche Garantien stützt (Art. 5 Abs. 3 der revidierten VDSG). Es muss auch nicht bei jeder Einzelbekanntgabe über die Garantien oder Datenschutzregeln informiert werden. Keine neue Information ist nötig, solange nach der Information des EDÖB bei der Datenübermittlung die gleichen Garantien gelten, sofern die Empfängerkategorien, der Zweck der Bearbeitung und die Datenkategorien nicht ändern. Dasselbe gilt für Bekanntgaben nach Buchstabe g, solange sie innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfinden und solange die Datenschutzregeln unverändert bleiben. Der EDÖB wird eine Liste der Musterverträge veröffentlichen, die verwendet werden können.

Information der betroffenen Personen (Artikel 7a)

Artikel 7a verpflichtet die Inhaber von Datensammlungen, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschaffen, die betroffene Person darüber zu informieren. Diese Pflicht besteht nicht nur dann, wenn die Daten direkt bei der betroffenen Person beschafft werden, sondern auch bei der Beschaffung bei Dritten. Mit dieser Informationspflicht wird die Motion 00.3000 «Erhöhte Transparenz bei der Erhebung von Personendaten» der Kommission für Rechtsfragen des Ständerats umgesetzt, ausserdem erreicht man dadurch eine Angleichung an die europäische Gesetzgebung, insbesondere an die Richtlinie 95/46/EG und an die Empfehlungen des Europarats. Der neue Artikel 7*a* unterscheidet sich aber insofern von den europäischen Erlassen, als er die Informationspflicht auf besonders schützenswerte Personendaten und Persönlichkeitsprofile beschränkt. Die europäischen Regelungen gelten für jegliche Beschaffung von Personendaten, unabhängig von der Art dieser Daten. Die Informationspflicht stärkt aber auch in ihrer eingeschränkten Form die Stellung der betroffenen Personen, die so einfacher und schneller ihre Rechte geltend machen und sich einer Bearbeitung, die ihnen nicht gerechtfertigt scheint, widersetzen können. Die Informationspflicht zwingt auch die Inhaber von Datensammlungen, wachsamer zu sein und keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile zu beschaffen und zu bearbeiten, wenn diese zur Erfüllung der Aufgaben nicht unbedingt erforderlich sind.

Artikel 7a Absatz 2 legt den Umfang der Informationspflicht fest. Mitzuteilen sind alle wesentlichen Informationen, mit deren Hilfe sich die betroffene Person eine Vorstellung von der Datenbearbeitung machen und gegebenenfalls ihre Rechte geltend machen kann. So muss laut Botschaft des Bundesrats «der Inhaber der Datensammlung der betroffenen Person – in der Regel ausdrücklich – alle Informationen zukommen lassen, die für eine Bearbeitung nach dem Grundsatz von Treu und Glauben und der Verhältnismässigkeit erforderlich sind» (BBl *2003* 2131). Die betroffene Person muss mindestens die Identität des Inhabers der Datensammlung, den Zweck der Bearbeitung sowie, wenn eine Datenbekanntgabe vorgesehen ist, die Kategorien der Datenempfänger kennen (Abs. 2 Bst. a-c). Sind zusätzliche Informationen erforderlich, damit sich die betroffene Person ein Bild machen kann, muss der Inhaber der Datensammlung gemäss dem Grundsatz von Treu und Glauben der betroffenen Person auch diese Zusatzinformationen liefern. So ist gegebenenfalls darüber zu informieren, ob die Datenbeschaffung obligatorisch oder freiwillig ist und welche Folgen die Weigerung hat, bestimmte Fragen zu beantworten.

Die betroffene Person muss auch informiert werden, wenn die Daten nicht bei ihr beschafft werden. Die Information hat spätestens bei der Speicherung der Daten zu erfolgen oder, wenn die Daten nicht gespeichert werden, bei der ersten Bekanntgabe an Dritte (*Art. 7a Abs. 3*). In letzterem Fall wäre es wünschenswert, dass die betroffene Person vor der Datenbekanntgabe informiert würde, damit sie Zeit zum Reagieren hat; dies namentlich dann, wenn die Datenübermittlung nicht vorgeschrieben ist.

Der Inhaber der Datensammlung muss die betroffenen Personen nur insoweit informieren, als sie nicht bereits informiert wurden (*Art. 7a Abs. 4*). Die betroffene Person kann früher vom Inhaber der Datensammlung oder von einem Dritten informiert worden sein. Hat der Inhaber der Datensammlung die betroffene Person also bereits bei einer ersten Datenbeschaffung informiert, so muss er diese Information nicht bei jeder neuen Datenbeschaffung wiederholen, ausser wenn die Umstände der Bearbeitung sich ändern, insbesondere wenn die Daten für einen anderen Zweck als dem früher mitgeteilten beschafft werden.

Der Inhaber der Datensammlung hat ebenfalls keine Informationspflicht, wenn die Speicherung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist (*Art. 7a Abs. 4 Bst. a*) oder wenn die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist (*Art. 7a Abs. 4 Bst.*

b), etwa wenn der Inhaber der Datensammlung keine Möglichkeit hat, die betroffene Person zu kontaktieren. Der Inhaber der Datensammlung muss trotzdem alles unternehmen, was von ihm nach den Umständen vernünftigerweise verlangt werden kann. «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» (BBl *2003* 2132).

Der Inhaber der Datensammlung kann die Information auch verweigern, einschränken oder aufschieben, wenn eine der Bedingungen nach Artikel 9 erfüllt ist, nämlich:

- soweit ein Gesetz im formellen Sinn dies vorsieht (Art. 1 Bst. a);
- soweit es wegen überwiegender Interessen Dritter erforderlich ist (Abs. 1 Bst. b);
- wenn es sich um ein Bundesorgan handelt: soweit es wegen überwiegender öffentlicher Interessen erforderlich ist (Abs. 2 Bst. a) oder die Information den Zweck einer Strafuntersuchung oder eines andern Untersuchungsverfahrens in Frage stellt (Abs. 2 Bst. b);
- wenn es sich um einen privaten Inhaber einer Datensammlung handelt: soweit eigene überwiegende Interessen es erfordern und er die Personendaten nicht Dritten bekannt gibt (Abs. 3).

Im Gegensatz zur Auskunftsverweigerung im Fall, in dem die betroffene Person ihr Auskunftsrecht ausübt (Art. 8 und 9 Abs. 4 DSG), muss der Inhaber der Datensammlung nicht begründen, warum er die Information verweigert, einschränkt oder aufschiebt. Anders als noch im Entwurf des Bundesrates vorgesehen, wollte das Parlament keine Informationspflicht vorschreiben für den Fall, dass der Einschränkungsgrund wegfällt. Es ist allerdings zu empfehlen, dass die betroffene Person informiert wird, sobald die Gründe für die Verweigerung oder die Einschränkung weggefallen sind, sofern dies möglich und nicht unverhältnismässig ist.

Das DSG schreibt die Form der Information nicht vor. Die betroffene Person muss nicht schriftlich informiert werden, möglich ist auch eine mündliche Information. Aus Beweisgründen wird dennoch die schriftliche Form empfohlen. Denn wer vorsätzlich seine Informationspflicht missachtet, kann auf Antrag mit Haft oder Busse bestraft werden (Art. 34 Abs. 1 Bst. b Ziff. 1). Die Form der Information muss auch den Umständen angemessen sein. Denkbar sind insbesondere eine Veröffentlichung, ein Aushang, ein Prospekt, eine Aufnahme in die Allgemeinen Bedingungen, ein Schreiben an die betroffenen Personen oder ein Anhang zu einem Vertrag oder einer Rechnung. Die Information kann auch auf der Einstiegsseite eines Internet-Angebots stehen. Wichtig ist, dass die Information gut sichtbar und dass sie verständlich und lesbar ist. Der Inhaber der Datensammlung kann die Information mit weiteren Zielen verbinden. Wird beispielsweise «die Bekanntgabe von Daten an Dritte beabsichtigt und ist diese weder gesetzlich vorgeschrieben noch zur Erfüllung eines Vertrages notwendig, so 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» (BBl *2003* 2132).

Die Inhaber von Datensammlungen haben eine Frist von einem Jahr ab Inkrafttreten des Gesetzes, um die notwendigen Massnahmen zur Information der betroffenen Personen zu ergreifen (Übergangsbestimmung). Die Informationspflicht gilt nicht im Fall von Daten, die vor Inkrafttreten des revidierten DSG erhoben wurden, ausser wenn in Zusammenhang mit einer bestehenden Datensamm-

lung neue Daten gesammelt werden oder wenn eine Person von dieser Sammlung noch nicht betroffen war.

Datenbearbeitung durch Dritte (Art. 10a)

Artikel 10a regelt die Bearbeitung von Personendaten im Auftragsverhältnis. Diese Bestimmung nimmt den Inhalt des geltenden Artikels 14 auf und dehnt dessen Geltungsbereich auf die Bundesorgane aus. Die Datenbearbeitung im Auftrag eines Bundesorgans war bisher nicht ausdrücklich im DSG, sondern in Artikel 22 VDSG geregelt. Im Vergleich zum geltenden Recht präzisiert Artikel 10*a* einerseits, dass die Übertragung durch Vereinbarung oder Gesetz erfolgen muss. Ausserdem muss der Auftragnehmer die Datensicherheit gewährleisten, das heisst die technisch und organisatorisch erforderlichen Massnahmen treffen, um die Personendaten vor jeder unbefugten Bearbeitung zu schützen. Ist die Datenbearbeitung durch Dritte nicht in einem Gesetz vorgesehen, so muss sie in einer Vereinbarung (Vertrag) zwischen dem für die Bearbeitung Verantwortlichen (Auftraggeber) und dem mit der Bearbeitung beauftragten Dritten (Auftragnehmer) geregelt werden. In dieser Vereinbarung sind die Pflichten des Auftragnehmers zu regeln, insbesondere der Umfang der Bearbeitung und die Sicherheitsanforderungen. Der Auftraggeber bleibt für den Datenschutz verantwortlich und haftet auch für den Schaden, der durch Übertragung der Datenbearbeitung an Dritte verursacht wurde, namentlich wenn er die Datensicherheit nicht sichergestellt hat (vgl. auch 9. Tätigkeitsbericht 2000/2001 des EDÖB, S. 36ff.).

Zertifizierungsverfahren (Art. 11)

Artikel 11 (neu) ist ein erster Schritt Richtung Selbstregulierung, mit der die gesetzlichen Anforderungen ergänzt und konkretisiert werden sollen. Gemäss dieser Bestimmung können die Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen und Bundesorgane, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen. Dadurch sollen der Datenschutz und die Datensicherheit verbessert werden. Zertifiziert werden können Produkte (Hard- und Software) und Verfahren. Die Zertifizierung ermöglicht eine praktische Umsetzung der gesetzlichen Bestimmungen dadurch, dass Produkte und Systeme entwickelt werden, die den Anforderungen des Datenschutzes entsprechen. Dank der Zertifizierung kann auch den technologischen Entwicklungen Rechnung getragen werden. Kommt die Zertifizierungsstelle nach Abschluss des Zertifizierungsverfahrens zum Schluss, dass die gesetzlichen Bestimmungen und die technischen Normen eingehalten sind, verleiht sie ein Datenschutz-Qualitätszeichen (Datenschutzlabel). Private Personen und Bundesorgane, die eine Zertifizierung erhalten haben, sind von der Pflicht befreit, die zertifizierten Datensammlungen anzumelden (*Art. 11a Abs. 5 Bst. f*). Das Akkreditierungsverfahren für Zertifizierungsstellen, die Voraussetzungen für das Zertifizierungsverfahren und die Bedingungen für die Erteilung des Qualitätszeichens werden in einer eigenen Verordnung geregelt. Der EDÖB ist zwar weder Akkreditierungs- noch Zertifizierungsstelle, er spielt aber trotzdem eine wichtige Rolle bei der Einführung der Zertifizierung. So prüft er insbesondere die Zertifizierungsverfahren und gibt dazu gegebenenfalls Empfehlungen ab (*Art. 31 Abs. 1 Bst. f*). Die Schweizerische Akkreditierungsstelle zieht ihn zudem für das Akkreditierungsverfahren und die Nachkontrolle bei (Art. 2 des Entwurfs der Verordnung über die Datenschutzzertifizierungen, VDSZ). Der EDÖB ist ebenfalls zuständig für die Anerkennung der ausländischen Zertifizierungsstellen, die in der Schweiz tätig sein wollen (Art. 3 Entwurf VDSZ).

Register der Datensammlungen (Art. 11a)

Die Revision behält das Register der Datensammlungen bei. Dieses trägt zur Transparenz der Datenbearbeitungen bei und soll es den betroffenen Personen ermöglichen, die ihnen gesetzlich zustehenden Rechte geltend zu machen. Heute wird das Register zu wenig wahrgenommen, namentlich weil die Ressourcen für seine regelmässige Veröffentlichung fehlen. Mit der Revision soll diese Situation verbessert werden: Das Register wird online zugänglich gemacht (Veröffentlichung im Internet). Zudem wird das Meldeverfahren vereinfacht: Die Inhaber von Datensammlungen werden ihre Datensammlungen künftig online anmelden können. Dieses System wird zunächst der Bundesverwaltung zur Verfügung stehen, sollte aber rasch auch von privaten Personen genutzt werden können.

Die Forderung nach mehr Transparenz bei der Datenbearbeitung (Art. 4 Abs. 4, Art. 7*a*) wirkt sich auch auf Pflicht zur Anmeldung der Datensammlungen aus. Bundesorgane müssen wie bisher sämtliche Datensammlungen anmelden. Im privaten Bereich wird die Meldepflicht ausgedehnt: Künftig muss der Inhaber einer Datensammlung die Datensammlung anmelden, wenn er regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder wenn er regelmässig Personendaten an Dritte bekannt gibt, selbst wenn die betroffene Person über die Datenbearbeitung informiert ist. Daraus ergibt sich, dass Datensammlungen, die vor Inkrafttreten des revidierten DSG nicht angemeldet werden mussten, nun anzumelden sind. Obwohl es die Revision nicht explizit vorsieht, wird der EDÖB den Inhabern von Datensammlungen eine Frist von einem Jahr gewähren, um ihre Praktiken mit den neuen Bestimmungen in Einklang zu bringen (in Analogie zu Art. 38 DSG). Die Datensammlungen müssen angemeldet werden, bevor sie eröffnet werden (Art. 11*a* Abs. 4).

Das Gesetz sieht allerdings einige Ausnahmen von der Anmeldepflicht vor (Art. 11*a* Abs. 5). Diese Ausnahmen gelten sowohl für Bundesorgane als auch für private Personen. So muss eine Datensammlung nicht angemeldet werden, wenn:

- private Personen Daten aufgrund einer gesetzlichen Verpflichtung bearbeiten;
- der Bundesrat eine Bearbeitung von der Anmeldepflicht ausgenommen hat, weil sie die Rechte der betroffenen Personen nicht gefährdet; diese Datensammlungen und Bearbeitungen sind in den Artikeln 4 und 18 der revidierten VDSG aufgeführt;
- der Inhaber der Datensammlung die Daten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet und keine Daten an Dritte weitergibt, ohne dass die betroffenen Personen davon Kenntnis haben; diese Ausnahme ist nicht neu, sondern war bereits in Artikel 4 VDSG enthalten;
- die Daten durch Journalisten bearbeitet werden, denen die Datensammlung ausschliesslich als persönliches Arbeitsinstrument dient; diese Ausnahme fand sich ebenfalls schon in Artikel 4 VDSG;
- der Inhaber der Datensammlung einen Datenschutzverantwortlichen bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt. Diese Ausnahme soll ebenfalls die Selbstregulierung fördern. Die Institution des Datenschutzverantwortlichen innerhalb eines Unternehmens oder einer öffentlichen Verwaltung ist auch in der Richtlinie 95/46/EG vorgesehen. Sie existiert bereits in verschiedenen Ländern, so namentlich in Deutschland, Frankreich, den Niederlanden und Schweden, und wird nicht nur von den Datenschutzbehörden, sondern auch von den Unternehmen und den Verwaltungen, die sie eingeführt haben, positiv bewertet. Damit die Aus-

nahme von der Anmeldepflicht geltend gemacht werden kann, muss der Datenschutzverantwortliche seine Tätigkeit unabhängig ausüben können und genügend Ressourcen für die Erfüllung seiner Aufgaben – Beratung, Ausbildung, Sensibilisierung und Kontrolle – haben. Seine Stellung im Unternehmen muss es ihm erlauben, seine Aufgaben wahrzunehmen, ohne dass Druck auf ihn ausgeübt wird und ohne dass er in einen Interessenkonflikt mit anderen Aufgaben gerät. Der Datenschutzverantwortliche kann also beispielsweise nicht gleichzeitig Personalverantwortlicher sein. Der Datenschutzverantwortliche muss weiter die für die Ausübung seiner Aufgaben nötigen Fachkenntnisse haben. Er darf von seinem Arbeitgeber nicht unter Druck gesetzt werden, was die Art und Weise seiner Aufgabenerfüllung betrifft, und er darf nicht diskriminiert werden, weil er seine Aufgaben wahrnimmt;

- der Inhaber der Datensammlung aufgrund eines Zertifizierungsverfahrens nach Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben hat und das Ergebnis der Bewertung dem Beauftragen mitgeteilt wurde.

Das Verzeichnis der Inhaber der Datensammlungen, welche der Meldepflicht enthoben sind, wird veröffentlicht.

Bearbeiten von Personendaten durch private Personen

Im privaten Bereich ist die Bearbeitung von Personendaten möglich, solange die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt wird. Für die Datenbearbeitung gelten namentlich die allgemeinen Grundsätze, die in Artikel 4 und den folgenden Artikeln festgelegt sind. Wird die Persönlichkeit verletzt, so muss diese Verletzung auf einem Rechtfertigungsgrund beruhen (Gesetz, Einwilligung der betroffenen Person, überwiegendes privates oder öffentliches Interesse, Art. 13 DSG).

Mit der Revision erfolgt eine Klärung von Artikel 12 Absatz 2. In seinem geltenden Wortlaut legt dieser Artikel fest, dass niemand ohne Rechtfertigungsgrund Personendaten entgegen den Grundsätzen von Artikel 4 und den folgenden Artikeln bearbeiten (Bst. a), Daten einer Person gegen deren ausdrücklichen Willen bearbeiten (Bst. b) und besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben darf (Bst. c). Wörtlich genommen lässt sich diese Bestimmung so verstehen, dass es bei Vorliegen eines Rechtfertigungsgrundes möglich ist, Daten unter Missachtung des Grundsatzes von Treu und Glauben oder unrechtmässig und unverhältnismässig zu bearbeiten, dass falsche Daten bearbeitet werden dürfen oder dass auf organisatorische und technische Massnahmen, mit denen die Daten gegen unbefugten Zugriff durch Dritte geschützt werden sollen, verzichtet werden kann. Sogar die Abweichung von Artikel 4 Absatz 3 (Zweckbindung) scheint zulässig. Eine solche Auslegung ist schockierend und entspricht weder der Praxis noch dem Geist des Gesetzes. Der neue Artikel 12 Absatz 2 legt jetzt ausdrücklich fest, dass die Bearbeitung von Daten unter Missachtung der Grundsätze von Artikel 4 und der folgenden Artikel, einschliesslich des Grundsatzes der Zweckbindung, nicht möglich ist. Was den Grundsatz der Zweckbindung betrifft, so rechtfertigt sich dies durch die Verstärkung der Transparenz bei Datenbearbeitungen (Art. 4 Abs. 5 und Art. 7*a*).

Zu Unrecht wird teilweise befürchtet, dass durch diese Präzisierung künftig bestimmte Datenbearbeitungen verhindert würden. So kann etwa ein Versicherungsunternehmen einer versicherten Person anbieten, dass sie neben ihrer Krankenzusatzversicherung eine Lebensversicherung abschliesst, und dafür die bereits zu dieser Person gespeicherten Daten verwenden, wenn die betroffene Person ihre Einwilligung gibt oder die Bearbeitung gestützt auf einen anderen Rechtfertigungsgrund erfolgt. In diesem Fall handelt es sich um eine neue Bearbeitung und um einen neuen Zweck. Die Beschaffung der Daten und namentlich der Bearbeitungszweck müssen für die betroffene Person erkennbar sein.

Eine Pflicht zur aktiven Information besteht dann, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden, was im Bereich der Lebensversicherungen der Fall ist (vgl. auch die Auslegungshilfe des Bundesamtes für Justiz, Januar 2007, http://www.bj.admin.ch/etc/medialib/data/staat_buerger/gesetzgebung/datenschutz.Par.0019.File.tmp/20070111-Auslegungshilfe-d.pdf).

Bearbeiten von Daten durch Bundesorgane

Verantwortliches Organ und Kontrolle (Art. 16 Abs. 2)

Artikel 16 Absatz 2 präzisiert die Kompetenzen des Bundesrates bei der gemeinsamen Bearbeitung von Personendaten. Der Bundesrat kann nicht nur die Verantwortung der verschiedenen beteiligten Organe für den Datenschutz regeln, sondern auch die Art der Kontrolle, mit der die Einhaltung der Datenschutzbestimmungen gewährleistet werden soll. Er kann insbesondere verlangen, dass ein Bundesorgan, das die Datenbearbeitung einem Dritten überträgt oder das Daten zusammen mit Privaten oder mit kantonalen Organen bearbeitet, die Sicherheitsbedingungen prüft, bevor es Zugriff auf schützenswerte Informationen gewährt.

Rechtsgrundlagen

Artikel 17 Absatz 2 erfährt einige kleinere Änderungen. In Buchstabe b wird präzisiert, dass der Bundesrat die Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen bei fehlender Rechtsgrundlage nur im Einzelfall bewilligen kann. Die Bewilligung darf also nicht für eine unbestimmte Anzahl von Fällen erfolgen. Diese Präzisierung entspricht der bisherigen Auslegung dieser Bestimmung.

Buchstabe c wird, analog zu Artikel 12 Absatz 3, um das Recht der betroffenen Personen ergänzt, eine Datenbearbeitung zu untersagen, selbst wenn sie ihre Daten allgemein zugänglich gemacht haben. Demnach kann das Bundesorgan auch bei fehlender formeller Gesetzesgrundlage besonders schützenswerte Personendaten oder Persönlichkeitsprofile ausnahmsweise bearbeiten, wenn die betroffene Person sie allgemein zugänglich gemacht hat, sofern sie die Bearbeitung nicht ausdrücklich untersagt hat. Die Untersagung muss klar ausgedrückt werden, so dass kein Zweifel über den Willen der betroffenen Person besteht.

Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen (Art. 17a)

Artikel 17a führt eine weitere Ausnahme vom Erfordernis eines Gesetzes im formellen Sinn für die Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen ein. Es ist eine Art «Übergangsbestimmung»; sie erlaubt es dem Bundesrat, eine solche Bearbeitung zu bewilligen, bevor die erforderlichen gesetzlichen Grundlagen verabschiedet sind, wenn für die technische Umsetzung einer bestimmten Bearbeitung oder eines Informatiksystems eine Testphase zwingend erforderlich ist. Damit lassen sich die mit der Bearbeitung verbundenen Bedürfnisse abschätzen, der Kreis der Zugriffsberechtigten kann präziser gefasst werden und es wird vermieden, dass eine ungenaue oder rasch überholte gesetzliche Grundlage geschaffen wird, die nicht der Realität entspricht.

Diese Ausnahmebestimmung ist aber nur anwendbar, wenn gleichzeitig drei Bedingungen erfüllt sind:

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

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

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

Absatz 2 listet die Kriterien auf, nach welchen zu beurteilen ist, ob eine Testphase zwingend erforderlich ist:

- Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zuerst evaluiert werden müssen. «Dies ist insbesondere dann der Fall, wenn etwa eine bestimmte Software bisher noch nicht mit realen Daten benutzt bzw. getestet wurde oder wenn neue Technologien für die Informationserfassung und -übermittlung eingeführt werden sollen (z.B. Systeme zur automatisierten Erkennung der Nummernschilder von Fahrzeugen)» (BBl *2003* 2143).

- Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone. Ein Beispiel wäre die Umsetzung einer Datenbank für DNA-Profile, in der die Informationsflüsse und die Rollen der verschiedenen Beteiligten präzis definiert werden müssen, damit der Schutz der betroffenen Personen optimal gewährleistet werden kann.

- Die Bearbeitung erfordert die Übermittlung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen an kantonale Behörden mittels eines Abrufverfahrens. So lässt sich abklären, ob ein solcher Zugriff wirklich erforderlich ist, namentlich was die die Zugriffsfrequenz betrifft.

Bevor der Bundesrat eine solche Testphase bewilligt, muss er die Stellungnahme des EDÖB einholen. Die Pflicht zur Einholung der Stellungnahme obliegt dem für die Datenbearbeitung verantwortlichen Organ. Es muss den EDÖB insbesondere darüber informieren, wie es sicherstellen will, dass die Anforderungen von Artikel 17*a* DSG eingehalten werden. Gemäss Artikel 26*a* der revidierten VDSG muss es dem EDÖB alle notwendigen Unterlagen zur Verfügung stellen, insbesondere eine allgemeine Beschreibung des Pilotversuchs, einen Bericht, der die Notwendigkeit der Testphase und der Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen nachweist, den Verordnungsentwurf, Informationen über technische und organisatorische Massnahmen sowie Informationen über die Planung des Pilotversuchs. Gestützt darauf gibt der EDÖB eine Stellungnahme ab, die für den Bundesrat aber nicht bindend ist. Dieser sollte trotzdem nicht von der Stellungnahme abweichen, wenn nicht besondere Umstände es rechtfertigen (BBl *2003* 2143).

Die Testphase ist zeitlich beschränkt. Das zuständige Bundesorgan muss dem Bundesrat innert zwei Jahren nach Inbetriebnahme des Pilotsystems einen Evaluationsbericht vorlegen. Darin muss es namentlich die Fortführung oder die Einstellung der Bearbeitung vorschlagen (*Abs. 4*). Im Bericht ist insbesondere eine vollständige Bilanz über die Testphase zu ziehen und es sind nicht nur die Vorteile der Lösung, sondern auch ihre Nachteile darzulegen. Die Datenbearbeitung muss in jedem Fall abgebrochen werden, wenn innert fünf Jahren nach der Inbetriebnahme des Pilotsystems kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage enthält (*Abs. 5*).

Beschaffen von Personendaten (Art. 18)

Die Aufnahme des neuen Artikels 4 Absatz 4 (Erkennbarkeit der Beschaffung) hat die Aufhebung von Artikel 18 Absatz 2 zur Folge. Die Anforderung der Erkennbarkeit gilt für alle Personendaten, unabhängig von ihrer Art.

Bekanntgabe der Daten (Art. 19)

Mit der Änderung von Artikel 19 soll einerseits die Definition der Einwilligung nach Artikel 4 Absatz 5 berücksichtigt werden: Zukünftig darf die Einwilligung nicht mehr vorausgesetzt werden (Art. 19 Abs. 1 Bst. b). Andererseits soll analog zu Artikel 17 Absatz 2 Buchstabe c die Bekanntgabe von Daten, die die betroffene Person allgemein zugänglich gemacht hat, nur soweit möglich sein, als die betroffene Person die Bekanntgabe nicht ausdrücklich untersagt hat.

Mit der Verabschiedung des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) wurde Artikel 19 DSG ebenfalls geändert. Artikel 7 BGÖ sieht nämlich vor, dass amtliche Dokumente ausnahmsweise auch dann zugänglich gemacht werden können, wenn dadurch die Privatsphäre Dritter beeinträchtigt wird, sofern das öffentliche Interesse an Transparenz das Interesse am Schutz der Privatsphäre überwiegt. Artikel 9 Absatz 2 BGÖ legt fest, dass sich der Zugang zu Personendaten nach dem DSG richtet. In diesem Fall kommt Artikel 19 DSG zur Anwendung, insbesondere Artikel 19 Absatz 1^{bis} (neu). Diese Bestimmung will ein Gleichgewicht schaffen zwischen den Anforderungen des Datenschutzes einerseits und dem Grundsatz der Öffentlichkeit der Verwaltung andererseits. So dürfen nach der neuen Bestimmung Bundesorgane Personendaten im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz bekannt geben, wenn die Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an ihrer Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Es ist von Fall zu Fall durch eine Interessenabwägung zu beurteilen, welche Daten bekannt gegeben werden dürfen. So darf laut Botschaft des Bundesrates (BBl *2003* 2033) die Veröffentlichung «nicht unvereinbar sein mit dem Zweck, für den die Daten ursprünglich beschafft wurden (vgl. Art. 4 Abs. 3 DSG): Die Information durch die Behörden kann zumindest unter gewissen Voraussetzungen als vereinbar mit dem datenschutzrechtlichen Gebot der Zweckbindung gelten, da sie sich auf Verpflichtungen stützt, die formellgesetzlich verankert sind. Dabei ist insbesondere zu berücksichtigen, ob die Angabe der Daten freiwillig erfolgt ist oder ob dazu eine Verpflichtung bestand, um welche Art von Daten es sich handelt und welche Auswirkungen die Veröffentlichung auf die betroffene Person hat. […] Insbesondere wird auf die Zweckbindung verwiesen, indem festgehalten wird, dass die bekanntzugebenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen müssen.» Nach Artikel 19 Absatz 3^{bis} DSG darf ein Bundesorgan Personendaten auch mittels automatisierter Informations- und Kommunikationsdienste, also etwa über Internet, allgemein zugänglich machen (aktive Information), wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn das Bundesorgan der Öffentlichkeit die Informationen gestützt auf Artikel 19 Absatz 1^{bis} zugänglich macht. Diese Möglichkeit ist allerdings zeitlich begrenzt. Sobald das öffentliche Interesse an der Zugänglichmachung nicht mehr besteht, müssen die Daten wieder entfernt oder gelöscht werden. Dadurch soll insbesondere verhindert werden, dass veraltete Daten eingesehen und bearbeitet werden können. Beim Zugänglichmachen der Daten muss der Grundsatz der Verhältnismässigkeit beachtet werden; so ist beispielsweise in bestimmten Fällen der Zugang auf einen bestimmten Personenkreis zu beschränken. Um zu verhindern, dass die Daten leicht in andere Datenbanken übernommen werden können, sollten die Informatiksysteme zudem so ausgestaltet sein, dass Suchmaschinen nicht auf sie zugreifen können.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Mit dem Inkrafttreten des BGÖ erhielt der EDÖB neue Aufgaben. Er ist insbesondere zuständig für die Schlichtung zwischen einem Bundesorgan, das den Zugang zu amtlichen Dokumenten verweigert, und der Person, die den Zugang wünscht, oder zwischen einem Bundesorgan und einer betroffenen Person, deren Daten einem Dritten bekannt gegeben werden sollen (Art. 13 und 18 BGÖ). Im Rahmen des BGÖ ist er ebenfalls Beratungsorgan und informiert Behörden und Privatpersonen über die Modalitäten des Zugangs zu amtlichen Dokumenten. Auch soll er sich zu Erlassentwürfen und Massnahmen des Bundes äussern, welche das Öffentlichkeitsprinzip wesentlich betreffen (Art. 18). Schliesslich hat er dem Bundesrat regelmässig Bericht zu erstatten und insbesondere den Vollzug, die Wirksamkeit, und die durch die Umsetzung des BGÖ verursachten Kosten zu überprüfen.

Die Revision des DSG bringt ebenfalls ein paar Änderungen für die Zuständigkeiten des EDÖB mit sich (vgl. Art. 29 Abs. 2 Bst. c, Art. 31 Abs. 1 Bst. d-g). So kann er künftig beim Bundesverwaltungsgericht gegen die Verfügungen der Bundeskanzlei und der Departemente Beschwerde führen, wenn diese eine Empfehlung an ein Bundesorgan nicht berücksichtigen (Art. 27 Abs. 6 DSG).

Schlussbestimmungen

Bearbeitung von Personendaten durch Kantone (Art. 37)

Das DSG gilt nicht für die Datenbearbeitung durch kantonale Organe, ausser wenn in einem Kanton keine kantonalen Datenschutzvorschriften bestehen und die Bearbeitung beim Vollzug von Bundesrecht erfolgt. Im Vergleich zum geltenden Recht erhöht die Revision die Anforderungen an die Kantone. Es reicht nicht mehr aus, dass für die Bearbeitung von Personendaten beim Vollzug von Bundesrecht kantonale Datenschutzvorschriften gelten müssen, damit nicht das Bundesrecht zur Anwendung kommt; diese kantonalen Bestimmungen müssen auch einen angemessenen Schutz gewährleisten. Der Schutz ist dann angemessen, wenn er den Anforderungen des Übereinkommens STE Nr. 108 und des Zusatzprotokolls entspricht (BBl *2003* 2147).