Kommentar des Bundesamts für Justiz zur Vollzugsverordnung vom 14. Juni 1993 (Stand am 1. Januar 2008) zum Bundesgesetz über den Datenschutz (VDSG, RS 235.11)

1. Geltungsbereich

Die Verordnung enthält keine besondere Bestimmung zu ihrem Geltungsbereich. Dieser ist in Art. 2 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG) definiert. Zur Präzisierung: Die Verordnung ist nicht direkt auf die Kantone anwendbar, wenn diese gemäss Art. 37 DSG dem Bundesgesetz über den Datenschutz unterstehen. Angesichts ihrer Organisationsautonomie obliegt es den Kantonen, entsprechende Vollzugsbestimmungen zu erlassen. Es steht ihnen jedoch frei, sich an dieser Verordnung zu orientieren und sie gegebenenfalls analog anzuwenden.

2. Gliederung der Verordnung

Die vorliegende Verordnung ist in vier Kapitel unterteilt:

1. Kapitel: Bearbeiten von Personendaten durch private Personen
2. Kapitel: Bearbeiten von Personendaten durch Bundesorgane
3. Kapitel: Register der Datensammlungen, Eidgenössischer Datenschutz- und Öffentlichkeits beauftragter (Beauftragter) und Verfahren vor dem Bundesverwaltungsgericht
4. Kapitel: Schlussbestimmungen

Dieser Aufbau trägt der Tatsache Rechnung, dass das DSG sowohl auf die Bearbeitung von Personendaten durch natürliche oder juristische Personen des Privatrechts als auch auf die Bearbeitung von Personendaten durch die Bundesorgane anwendbar ist. Obwohl die Bestimmungen, welche die beiden Bereiche regeln, nicht von Grund auf verschieden sind, ist es zweckmässig, diese zu unterscheiden, indem man die jeweiligen Bestimmungen in speziellen Kapiteln behandelt. Um jedoch häufige Wiederholungen zu vermeiden, enthält das Kapitel, das die Bundesorgane betrifft, Verweise auf das Kapitel, das den Privatbereich betrifft.

3. Auskunftsrecht (Art. 1 und 2, 13 und 14 VDSG)

3.1 Modalitäten (Art. 1 und 13)

Das Auskunftsrecht ist ein wesentliches Grundelement des Datenschutzrechtes. Betroffene Personen wären ohne dieses Recht nicht in der Lage, ihre Ansprüche in bezug auf den Datenschutz wirksam geltend zu machen und insbesondere herauszufinden, ob über sie Daten bearbeitet werden, von diesen Daten Kenntnis zu erhalten und nötigenfalls ihre Berichtigung oder Löschung zu veranlassen. Das DSG regelt detailliert die Ausübung des Auskunftsrechtes durch die betroffene Person, seinen Umfang und mögliche Einschränkungen.

Das DSG regelt jedoch nicht alle Modalitäten der Ausübung des Auskunftsrechtes. Es erteilt die Kompetenz dazu dem Bundesrat, der auch Ausnahmen vom Grundsatz der Unentgeltlichkeit und der schriftlichen Auskunftserteilung vorsehen kann.

In Art. 1 und 13 der Verordnung sind die Bedingungen für die Ausübung des Auskunftsrechts wie folgt festgelegt:

- Art und Weise der Ausübung des Auskunftsrechts: Die Auskunft muss schriftlich beantragt werden, und die betroffene Person hat sich, z.B. mittels einer Fotokopie der Identitätskarte, über ihre Identität auszuweisen. Sie muss kein Ausweispapier vorlegen, wenn die Identifikation auf eine andere Weise möglich ist. So hat die betroffene Person ihre Identität selbstverständlich nicht zu beweisen, wenn der Inhaber der Datensammlung sie kennt.

- Ebenso ist die Schriftform nicht in jedem Fall erforderlich. In Einzelfällen, wie etwa bei einem Gesuch zur Einsicht in eine Personalakte, kann ein mündliches Gesuch ausreichen. Der Inhaber der Datensammlung hat zu entscheiden, ob er trotzdem auf die Schriftform bestehen will.
- Gewisse Personen haben gewünscht, dass die Verordnung die Ausübung des Auskunftsrechtes in der Weise begrenzt, dass die die Auskunft verlangende Person ihr Gesuch begründen muss und die Datensammlung genau anzugeben hat, aus der sie Informationen erhalten möchte. Eine derartige Beschränkung stünde im Widerspruch zum DSG. Jedoch hat die betroffene Person, soweit sie Kenntnis hat, den Namen der Datensammlung und die Art der Daten anzugeben, um die Nachforschungen des Inhabers der Datensammlung zu erleichtern.
- Die Auskünfte werden grundsätzlich schriftlich, in Form eines Ausdrucks oder einer Fotokopie (Art. 8 Abs. 5, 1. Satz DSG) erteilt. Die angeforderten Auskünfte, inklusive die verfügbaren Angaben zur Herkunft der Daten, sowie die Informationen über Zweck und Rechtsgrundlage der Bearbeitung sowie über die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger (Art. 8 Abs. 2 lit. b DSG) müssen ebenfalls schriftlich erfolgen. Der Inhaber der Datensammlung kann der betroffenen Person auch vorschlagen oder erlauben, die Daten an Ort und Stelle einzusehen (Art. 1 Abs. 3 VDSG). Dieses Vorgehen ist wirtschaftlicher und rationeller, wenn die Daten auf verschiedene Datensammlungen oder Akten verteilt, besonders umfangreich oder in unterschiedlicher Form aufbewahrt sind (z.B. Multimedia-Datenbank mit Text, Bild und Ton). Auch wenn die zu erteilenden Auskünfte Erklärungen erfordern, kann dieses Verfahren gewählt werden. Bei einer Einsicht an Ort und Stelle muss die betroffene Person ebenso die Möglichkeit haben, eine Fotokopie von gewissen Unterlagen aus ihrem Dossier zu verlangen. Ein solches Recht kann insbesondere für die Einsicht in die eigene Personalakte von Bedeutung sein. Die Auskünfte können auch mündlich erteilt werden, z.B. per Telefon. Jedoch kann ein solches Vorgehen nur dann in Betracht gezogen werden, wenn die erteilten Auskünfte keine besonders schützenswerten Daten betreffen und die Auskünfte nicht umfangreich sind. Man kann auf diese Weise nur dann vorgehen, wenn die betroffene Person zugestimmt hat und einwandfrei identifiziert worden ist.
- Art. 1 Abs. 2 sieht vor, dass die Auskunft auch auf elektronischem Weg erfolgen kann, wenn bestimmte Anforderungen erfüllt sind.
- So müssen angemessene Massnahmen getroffen werden, um die Identifizierung der betroffenen Person, die ihr Auskunftsrecht geltend macht, im elektronischen Verkehr sicherzustellen (Abs. 2 lit. a). Der Inhaber der Datensammlung muss überprüfen, ob es sich bei der Person, die das Auskunftsgesuch stellt, um diejenige handelt, deren Daten bearbeitet werden. Dies kann beispielsweise durch die Verwendung elektronischer Signaturen (vgl. dazu das entsprechende Bundesgesetz; SR 943.03) geschehen. In der Terminologie der Informatiksicherheit handelt es sich somit eigentlich nicht um eine Identifizierung, sondern eine Authentifizierung. Um die Einheitlichkeit der Terminologie innerhalb der vorliegenden Bestimmung zu gewährleisten und nicht einen zusätzlichen – und zudem nicht allgemein verständlichen – Begriff einführen zu müssen, wird indessen auch hier von „identifizieren“, und nicht von „authentifizieren“ gesprochen (Art. 1 Abs. 2 lit a).
- Nach Art. 1 Abs. 2 lit. b muss der Inhaber der Datensammlung die persönlichen Daten der betroffenen Person bei der Auskunftserteilung zudem angemessen vor einem Zugriff bzw. einer Einsichtnahme durch Dritte schützen. Dies ist beispielsweise möglich durch Verschlüsselung von E-Mails oder durch Einrichtung einer entsprechend gesicherten Internetverbindung, falls die Daten durch die Betroffenen abgerufen werden können. Diese Anpassungen sind gegenwärtig primär für den privaten Sektor von Bedeutung. Es kann aber nicht ausgeschlossen werden, dass sie künftig auch für den öffentlich-rechtlichen Bereich Bedeutung erlangen werden. Die Angemessenheit der geforderten Massnahmen richtet sich nach den Umständen im konkreten Fall und dem Stand der Technik. Geht es um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, sind die Anforderungen höher, als wenn es um einfache Personendaten geht.
- Die Auskünfte sind innert 30 Tagen seit dem Eingang des Auskunftsbegehrens zu erteilen (Art. 1 Abs. 4). Ist der Inhaber der Datensammlung dazu nicht in der Lage, muss er die betroffene Person benachrichtigen und ihr mitteilen, innert welcher Frist die Auskunft erfolgen wird. Das Auskunftsrecht hat nur dann einen Sinn, wenn die betroffene Person rasch Auskunft erhält, vor allem, wenn die Daten regelmässig aktualisiert werden. Wird die Auskunft verweigert, eingeschränkt oder aufgeschoben, muss der Inhaber der Datensammlung die

interessierte Person ebenfalls innerhalb von 30 Tagen benachrichtigen und ihr die Gründe mitteilen.

- Führen mehrere Inhaber einer Datensammlung eine oder mehrere Datensammlungen gemeinsam, kann das Auskunftsrecht bei jedem von ihnen ausgeübt werden, es sei denn, einer von ihnen ist für die Bearbeitung sämtlicher Auskunftsbegehren für zuständig erklärt worden (Art. 1 Abs. 5). Um das Verfahren zu vereinfachen und um zu vermeiden, dass die betroffene Person mehrere Auskunftsbegehren stellen muss, erteilt der befragte Inhaber der Datensammlung einzig für seinen Aufgabenbereich Auskunft. Ist der Inhaber der Datensammlung zur Auskunftserteilung nicht befugt oder kann er nur teilweise Auskunft geben, so leitet er das Auskunftsbegehren an die anderen zuständigen Inhaber der Datensammlung weiter, die ihrerseits der betroffenen Person Auskunft erteilen.
- Bearbeitet ein Dritter Daten im Auftrag, so muss grundsätzlich der Auftraggeber die verlangten Auskünfte erteilen, sofern er selber Inhaber der Datensammlung ist (Art. 1 Abs. 6). Der Beauftragte ist auskunftspflichtig, wenn er die Identität des Inhabers der Datei nicht preisgibt oder dieser nicht in der Schweiz wohnhaft ist (Art. 8 Abs. 4 DSG). Es kann allerdings vorkommen, dass der Auftraggeber über die verlangten Auskünfte nicht verfügt, weil der Dritte selbst Inhaber der Datensammlung ist. Die betroffene Person kennt jedoch nicht den Dritten und sieht den Auftraggeber als den Inhaber der Datensammlung an. Gemäss dem Grundsatz von Treu und Glauben ist der Auftraggeber in diesem Fall verpflichtet, das Auskunftsbegehren an den wirklichen Inhaber der Datensammlung weiterzuleiten. Solche Situationen ergeben sich häufig im Bereich der adressierten Werbung, wenn Unternehmen auf Rechnung Dritter Werbebotschaften versenden oder für diese sogar Spenden entgegennehmen, ohne dass sie von den betroffenen Personen als Vermittler wahrgenommen werden. Diese Bestimmung betrifft nicht nur den privaten Bereich, sondern auch die Bundesorgane.
- Abs. 7 regelt einen Sonderfall: Auskunftsbegehren, die verstorbene Personen betreffen. Diese Bestimmung ist streng genommen keine Regelung der Anwendung des Art. 8 DSG. Sie setzt unter Wahrung des Persönlichkeitsschutzes der Verwandten die Bedingungen fest, unter denen eine Person Auskunft über Daten von verstorbenen Personen verlangen kann. Diese Bestimmung gibt die von der Rechtsprechung zu Art. 4 der Bundesverfassung (BV) entwickelten Mindestgrundsätze wieder (vgl. insbes. VPB 1991 55/I 3).

3.2 Kostenlosigkeit der Auskunft und Ausnahmen (Art. 2 und 13)

Gemäss Art. 8 Abs. 5 DSG ist die Auskunft grundsätzlich kostenlos. Der Bundesrat kann Ausnahmen vorsehen, die allerdings begrenzt sein sollten, da die Ausübung eines mit der persönlichen Freiheit zusammenhängenden Grundrechts billigerweise nicht von der Entrichtung einer Gebühr abhängig gemacht werden kann. Es gibt zwei Ausnahmen (vgl. Art. 1 und 13), wenn:

- die betroffene Person die Auskunft in den letzten zwölf Monaten bereits erhalten hat. Diese Bestimmung hat den Zweck, missbräuchliche und schikanöse Auskunftsbegehren zu vermeiden. Der Inhaber der Datensammlung darf jedoch keine Gebühr verlangen, wenn die betroffene Person sich auf ein schutzwürdiges Interesse berufen kann, insbesondere wenn die Daten in der Zwischenzeit verändert wurden, ohne dass sie darüber informiert wurde;
- die Auskunftserteilung mit einem besonders grossen Arbeitsaufwand verbunden ist. Dieser Grund kann vor allem dann geltend gemacht werden, wenn die Daten zu statistischen Zwecken bearbeitet und wenn sie teilweise anonymisiert aufbewahrt werden, wenn die Auskunft langwierige Nachforschungen erfordert, was insbesondere der Fall ist, wenn die Datensammlung manuell geführt wird und auf mehrere Dossiers verweist. In gewissem Umfang gilt dasselbe für ein Unternehmen, das Datensammlungen ausschliesslich für interne Zwecke führt und das nicht darauf eingerichtet ist, Daten bekannt zu geben oder Auskünfte zu erteilen. Jedoch müssen die Inhaber der Datensammlung dafür sorgen, dass ihre Datensammlungen so organisiert sind, dass sie der betroffenen Person die Ausübung ihrer Auskunfts- sowie Berichtigungsrechte erlauben (Art. 38 Abs. 2 DSG). Die Berufung auf besonders grossen Arbeitsaufwand ist nicht möglich, wenn dieser auf einer schlechten Organisation und Verwaltung der Datensammlung des angefragten Inhabers der Datensammlung beruht.

Der verlangte Betrag muss jedoch angemessen sein, damit die betroffene Person nicht von der Geltendmachung ihres Auskunftsrechts abgehalten wird. Er soll die teilweise Deckung der entstandenen Unkosten ermöglichen, 300 Franken jedoch keinesfalls überschreiten. Diese Begrenzung ist erforderlich, da bei komplexen Systemen die Kosten der Auskunftserteilung nach dem Grundsatz der Kostendeckung höhere Summen erreichen können. Unter "angemessener Beteiligung" sind die Gebühren zu verstehen, die man von der betroffenen Person verlangt, und nicht die reellen Kosten des Aufwands.

Vor der Erhebung eines solchen Betrages ist die betroffene Person darüber zu informieren. Sie muss die Möglichkeit erhalten, ihr Auskunftsbegehren zurückzuziehen oder den verlangten Betrag anzufechten. Der Inhaber der Datensammlung, der eine Kostenbeteiligung verlangt, hat diese zu begründen. Ist ein Bundesorgan der Ansicht, es sei berechtigt, eine Gebühr gemäss Art. 2 Abs. 1 zu verlangen, kann die betroffene Person eine Verfügung verlangen, die gemäss Art. 25 DSG mit Beschwerde angefochten werden kann.

3.3 Auskunftsrecht gegenüber den diplomatischen Vertretungen der Schweiz im Ausland (Art. 14)

Art. 14 der Verordnung regelt die Modalitäten der Ausübung des Auskunftsrechtes gegenüber den diplomatischen Vertretungen der Schweiz im Ausland und den Missionen bei den internationalen Organisationen. Aus Gründen der diplomatischen Gepflogenheit und der Praktikabilität ist eine direkte Behandlung der Auskunftsbegehren durch unsere Vertretungen im Ausland oder unsere Missionen bei den internationalen Organisationen nicht angebracht. Die verlangten Auskünfte werden daher vom Eidgenössischen Departement der äusseren Angelegenheiten geprüft und allenfalls erteilt.

4. Anmeldung der Datensammlungen (Art. 3, 4, 16 und 18 VDSG)

4.1 Im privaten Bereich (Art. 3 und 4)

4.1.1 Inhalt der Anmeldung (Art. 3)

Datensammlungen nach Art. 11*a* Abs. 3 DSG müssen beim Beauftragten angemeldet werden, bevor sie eröffnet werden. Dies betrifft Datensammlungen von privaten Personen, bei denen regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder regelmässig Personendaten Dritten bekannt gegeben werden.

Die Anmeldung enthält folgende Angaben:

- Name und Adresse des Inhabers der Datensammlung;
- Name und vollständige Bezeichnung der Datensammlung;
- Person, bei welcher das Auskunftsrecht geltend gemacht werden kann;
- Zweck der Datensammlung;
- Kategorien der bearbeiteten Personendaten;
- Kategorien der Datenempfänger;
- Kategorien der an der Datensammlung Beteiligten – d.h. Dritte, die das Recht haben, in der Datensammlung Daten einzufügen oder Mutationen vorzunehmen.

Jeder Inhaber einer Datensammlung muss diese Angaben laufend aktualisieren.

4.1.2 Ausnahmen von der Anmeldepflicht (Art. 4 VDSG)

Art. 11*a* Abs. 5 DSG nennt eine Reihe von Ausnahmen, bei denen die Anmeldepflicht nicht gilt. Sie entfällt namentlich, wenn:

- Daten aufgrund einer gesetzlichen Verpflichtung bearbeitet werden;
- der Bundesrat eine Bearbeitung von der Anmeldepflicht ausgenommen hat, weil sie die Rechte der betroffenen Personen nicht gefährdet;
- 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 Kenntnis der betroffenen Personen;
- die Daten durch Journalisten bearbeitet werden, denen die Datensammlung ausschliesslich als persönliches Arbeitsinstrument dient;
- der Inhaber der Datensammlung einen Datenschutzverantwortlichen bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt;
- der Inhaber der Datensammlung aufgrund eines Zertifizierungsverfahrens nach Art. 11 ein Datenschutz-Qualitätszeichen erworben hat und das Ergebnis der Bewertung dem Beauftragten mitgeteilt wurde.

Art. 4 VDSG konkretisiert Art. *11a* Abs. 5 lit b DSG, gemäss dem der Inhaber der Datensammlung seine Sammlung nicht deklarieren muss, wenn der Bundesrat die Datenbearbeitung als nicht geeignet zur Bedrohung der betroffenen Person erachtet hat.

Art. 4 VDSG hält zuerst fest, dass die in Art. 11*a* Abs. 5 lit. a, c bis f DSG erwähnten Datensammlungen von der Pflicht zur Anmeldung ausgenommen sind, und führt anschliessend die folgenden Ausnahmen auf:

- lit. a sieht eine Ausnahme vor für Datensammlungen von Lieferanten und Kunden, die z.B. im Rahmen der Vertragserfüllung für die Geschäftskorrespondenz verwendet werden. Die Bestimmung entspricht der in Art. 18 Abs. 1 lit. b vorgesehenen Ausnahme für die Bundesorgane: In beiden Fällen gilt die Ausnahme nur für diejenigen Fälle, in denen die Datensammlungen keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten.
- lit. b sieht eine Ausnahme vor für Datensammlungen, deren Daten ausschliesslich zu nicht personenbezogenen Zwecken verwendet werden, namentlich in der Forschung, der Planung und der Statistik. Die Tatsache, dass eine derartige Verwendung ihrem Zweck entsprechend die Personenrechte prinzipiell nicht verletzt, rechtfertigt diese Ausnahme. Das geltende Recht sieht eine solche Ausnahme im Zusammenhang mit der Informationspflicht bei Bekanntgabe ins Ausland bereits vor (Art. 7 Abs. 1 VDSG).
- lit. c nennt als Ausnahme archivierte Datensammlungen, die nur zu historischen oder wissenschaftlichen Zwecken aufbewahrt werden. Diese Ausnahme leitet sich aus Art. 18 Abs. 1 lit. b VDSG her, der besagt, dass Bundesorgane Datensammlungen, die im Bundesarchiv archiviert sind, nicht anmelden müssen.
- lit. d betrifft Datensammlungen, die ausschliesslich Daten enthalten, die veröffentlicht wurden oder welche die betroffene Person selbst allgemein zugänglich gemacht hat, ohne deren Bearbeitung ausdrücklich zu untersagen.
- lit. e verpflichtet den Inhaber der Datensammlung, die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen gemäss Art. 10 VDSG zu protokollieren, wenn präventive Massnahmen den Datenschutz nicht gewährleisten können. Ziel ist es insbesondere, die nachträgliche Überprüfung der Identität von Personen, die Daten in ein System eingeben, zu ermöglichen. Zu diesem Zweck erstellte Datensammlungen müssen dem Beauftragten nicht gemeldet werden. Das Festhalten der Protokolldaten dient in erster Linie dem Schutz der Personen, deren Daten im betreffenden System bearbeitet werden; das Missbrauchsrisiko zulasten derjenigen Personen, die mit dem System arbeiten und deren Zugriffsdaten festgehalten werden, ist vergleichsweise gering.
- lit. f sieht eine Ausnahme für Buchhaltungsunterlagen der Bundesorgane vor, analog Art. 18 Abs. 1 lit. e;
- lit. g schliesst die Hilfsdatensammlungen für die Personalverwaltung des Inhabers der Datensammlung von der Anmeldepflicht aus. Dies allerdings nur dann, wenn sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten. Die Bestimmung entspricht der in Art. 18 Abs. 1 lit. f vorgesehenen Ausnahme.

Art. 4 Abs. 2 VDSG hält ausdrücklich fest, dass der Inhaber der Datensammlung verpflichtet ist, die Massnahmen zu treffen, die erforderlich sind, um die Angaben gemäss Art. 3 Abs. 1 auch dann dem EDÖB und den betroffenen Personen auf Gesuch hin mitteilen zu können, wenn eine Datensammlung nicht der Anmeldepflicht unterliegt. Diese Verpflichtung lässt sich aus den Art. 8 und 29 Abs. 2 DSG ableiten.

4.2 Im öffentlich-rechtlichen Bereich (Art. 16 und 18 VDSG)

4.2.1 Anmeldung

Entsprechend Art. 11*a* DSG müssen die Bundesorgane ihre Datensammlungen anmelden, bevor sie diese eröffnen. Diese Verpflichtung wird in Art. 16 der Verordnung explizit festgehalten. Die Bundesorgane haben bei der Anmeldung die gleichen Informationen zu liefern wie Inhaber von Datensammlungen im privaten Bereich, unter zusätzlicher Angabe der Rechtsgrundlage. Die Bundesorgane sind verpflichtet, diese Angaben laufend zu aktualisieren.

4.2.2 Ausnahmen von der Anmeldepflicht

Die Revision des DSG und der VDSG hebt die Regelung zur vereinfachten Anmeldung bestimmter Kategorien von Datensammlungen auf. Das gilt auch für die Ausnahmen von der Veröffentlichung.

Diese Datensammlungen sind neu von der Anmeldepflicht ausgenommen. Analog zu Art. 4 VDSG nennt Art. 18 diejenigen Datensammlungen mit Personendaten, deren Bearbeitung die Rechte der betroffenen Personen nicht verletzt:

- Art. 18 Abs. 1 lit. a nennt Korrespondenzregistraturen. Das sind einfache Datensammlungen, die Korrespondenz verzeichnen und in erster Linie Namen und Adressen von Absendern, das Eingangsdatum des Begehrens, die für das Begehren verantwortlichen Mitarbeiter, die Antworten und ihre Ausgangsdaten enthalten (Korrespondenzverzeichnis). Zugang zu einer Korrespondenzregistratur hat an sich nur eine stark begrenzte Anzahl von Personen. In erster Linie sind dies die für die Registratur Zuständigen. Eine Datensammlung, die Bürgerbriefe verzeichnet, würde in diese Kategorie fallen. Wenn eine Datensammlung hingegen Verwendungen zulässt, die über das blosse Verzeichnen von Korrespondenz hinausgehen, oder weitere Daten enthält – namentlich besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die aus der Behandlung einer Anfrage stammen und Bearbeitungsweisen einschliessen, bei denen Daten von Dritten, aus Gutachten, Abklärungen, Ermittlungs- oder Einvernahmeprotokollen etc. in die Sammlung aufgenommen werden -, handelt es sich nicht mehr um eine Korrespondenzregistratur, sondern um ein Verwaltungs- und Dokumentationssystem. Die GEVER-Datensammlungen sind dementsprechend grundsätzlich keine blossen Korrespondenzregistraturen und müssen angemeldet werden. Es handelt sich dabei um komplexe Datenverarbeitungssysteme mit vielfältigen Funktionalitäten, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthalten können. Innerhalb eines Departements oder Amts können solche Systeme verschiedenen Diensten oder Sektionen zugänglich sein und viele Zugriffsmöglichkeiten bieten, die nicht einem einzigen Dienst oder Amt vorbehalten sind.
- Art. 18 Abs. 1 lit. b nennt Datensammlungen von Lieferanten oder Kunden, die keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten.
- Art. 18 Abs. 1 lit. c nennt Adressensammlungen, die einzig der Adressierung dienen und keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten (z. B. Verzeichnisse von Expertengremien, selbst wenn diese an Dritte weitergegeben werden).
- Art. 18 Abs. 1 lit. d und e nennt Listen für Entschädigungszahlungen und Buchhaltungsunterlagen.
- Art. 18 Abs. 1 lit. f sieht vor, dass Hilfsdatensammlungen für die Personalverwaltung des Bundes nicht angemeldet werden müssen, wenn sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten.
- Art. 18 Abs. 1 lit. g nennt Bibliothekdatensammlungen (Autorenkataloge, Ausleiher- und Benutzerverzeichnisse).
- Art. 18 Abs. 2 lit. a nimmt Datensammlungen, die beim Bundesarchiv archiviert sind, von der Anmeldepflicht aus.
- Art. 18 Abs. 2 lit. b nennt Datensammlungen, die der Öffentlichkeit in Form von Verzeichnissen zugänglich gemacht werden.
- Art. 18 Abs. 2 lit. c sieht eine Ausnahme von der Anmeldepflicht vor für Datensammlungen, deren Daten ausschliesslich zu nicht personenbezogenen Zwecken verwendet werden, namentlich in der Forschung, der Planung und der Statistik.
- Art. 18 Abs. 3 VDSG hält ausdrücklich fest, dass das zuständige Bundesorgan verpflichtet ist, die Massnahmen zu treffen, die erforderlich sind, um die Angaben gemäss Art. 16 Abs. 1 auch dann dem Beauftragten und den betroffenen Personen auf Gesuch hin mitteilen zu können, wenn eine Datensammlung nicht der Anmeldepflicht unterliegt. Diese Verpflichtung lässt sich aus den Art. 8 und 27 DSG ableiten.

5. Datenbekanntgabe ins Ausland (Art. 5 bis 7 und 19 VDSG)

5.1 Veröffentlichung in elektronischer Form (Art. 5)

Der bisherige Wortlaut von Art. 5 wird nicht beibehalten. Der geänderte Art. 6 DSG bezieht nicht mehr nur auf die Bekanntgabe von ganzen Datensammlungen ins Ausland, sondern allgemein von Personendaten. Daher sind die bisher hier figurierenden Definitionen (und insbesondere lit. b) nicht mehr sinnvoll. Materiell ergibt sich daraus grundsätzlich keine Änderung. Das Zugänglichmachen von

Personendaten durch Abrufverfahren gilt als grenzüberschreitende Bekanntgabe, ebenso die Bekanntgabe an einen Dritten zwecks Bearbeitung im Auftragsverhältnis.

Mit Art. 5 VDSG wird eine neue Bestimmung hinsichtlich der Veröffentlichung von Personendaten zum Zweck der Information der Öffentlichkeit auf Internet oder in anderen Informations- und Kommunikationsdiensten eingeführt. Informationen – seien sie personenbezogen oder nicht – die auf Internet publiziert sind, können auch aus ausländischen Staaten abgerufen werden, in denen kein angemessener Schutz von Personendaten gewährleistet ist. Die betreffenden Daten können auch dort weiterverarbeitet werden. Bei einer Veröffentlichung von Informationen auf Internet ist indessen die (allfällige) Bekanntgabe ins Ausland nicht Zweck, sondern bloss ein Nebeneffekt. Mit der vorliegenden Bestimmung, die sich an Art. 19 Abs. 3bis DSG anlehnt, wird dem Rechnung getragen.[1]

5.2 Informationspflicht (Art. 6 VDSG)

Art. 6 DSG ersetzt die Pflicht, dem Beauftragten die Bekanntgabe von Daten ins Ausland zu melden, durch eine Informationspflicht. Art. 6 Abs. 3 DSG sieht vor, dass der Eidgenössische Datenschutzbeauftragte über die Garantien und die Datenschutzregeln nach Art. 6 Abs. 2 lit. a und g informiert werden muss und dass der Bundesrat die Einzelheiten dieser Informationspflicht regelt. Gemäss der Botschaft (BBl 2003 S. 2130) soll die Verordnung des Bundesrates präzisieren, wann und wie die Information erfolgen muss.

Art. 6 Abs. 1 VDSG verlangt, dass der Inhaber der Datensammlung den Beauftragten soweit möglich vor der Bekanntgabe der Daten ins Ausland informiert. Der Art. setzt keine genaue Frist, sondern räumt dem Inhaber der Datensammlung eine gewisse Flexibilität ein. Falls er nicht in der Lage ist, den Beauftragten vor der Bekanntgabe der Daten zu informieren, holt er dies möglichst bald nach. Die Information besteht darin, dass dem Beauftragten ein Exemplar oder eine Kopie der mit dem Empfänger vereinbarten Garantien oder der in der betroffenen Gesellschaft (bzw. in den betroffenen Gesellschaften) geltenden Datenschutzregeln übermittelt wird. Aus der Botschaft (BBl 2003 2130) geht hervor, dass das Verfahren der Information möglichst einfach ausgestaltet werden soll; zu denken ist beispielsweise an eine Information des Datenschutzbeauftragten per Email.

Wie aus der Botschaft hervorgeht (BBl 2003 2130), bedeutet die in Art. 6 Abs. 3 DSG verankerte Informationspflicht keineswegs, dass der Inhaber der Datensammlung den Datenschutzbeauftragten über jede Einzelübermittlung informieren muss. Art. 6 Abs. 2 lit. a VDSG präzisiert zu diesem Punkt ausdrücklich, dass die Informationspflicht nach einer erstmaligen Information für alle weiteren Bekanntgaben als erfüllt gilt, die unter denselben Garantien erfolgen, soweit die Kategorien der Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben. Der Inhaber der Datensammlung hat damit eine gewisse Flexibilität.

Die Datenschutzregeln innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, gelten für alle Bekanntgaben unter diesen, unabhängig von der Kategorie und vom Zweck der übermittelten Daten. Die Informationspflicht gilt demnach global für alle diese Bekanntgaben, sofern – bzw. solange – die Datenschutzregeln einen angemessenen Schutz gewährleisten (Art. 6 Abs. 2 lit. b VDSG). Änderungen bzw. Anpassungen sind damit in einem gewissen Rahmen möglich, ohne dass eine erneute Information vorgenommen werden muss.

Abs. 3 dieses Artikels sieht eine erleichterte Informationspflicht vor, wenn der Inhaber von Datensammlungen Modellverträge oder Standardvertragsklauseln verwendet, die vom Beauftragten erstellt oder anerkannt wurden, wie beispielsweise die Modellklauseln des Standardvertrags des Europarates. Der Inhaber der Datensammlung muss den Beauftragten lediglich in allgemeiner Art und Weise darüber informieren, dass er für Datenbekanntgaben in ausländische Staaten, die nicht über eine Gesetzgebung verfügen, die einen angemessenen Schutz bietet, generell die vom Beauftragten anerkannten Modellverträge oder Standardvertragsklauseln verwendet (oder gegebenenfalls, dass er mit bestimmten Ausnahmen diese Modellverträge oder Standardklauseln verwendet). Hernach ist eine besondere Meldung einzelner Bekanntgaben bzw. Kategorien von Bekanntgaben (vgl. Abs. 2 der vorliegenden Bestimmung) nicht mehr erforderlich. Sollte der Inhaber der Datensammlung in der Folge in einzelnen Fällen indessen dennoch andere Garantien anwenden, so muss er den Beauftragten darüber ordentlich informieren.

---

[1] vgl. zum Ganzen auch das Urteil des Europäischen Gerichtshofes vom 6. November 2003 in der Rechtssache C-101/01 Lindqvist, RZ 56 ff.

Diese Regelung gilt auch für die Bundesorgane, wenn sie gestützt auf Art. 6 Abs. 2 lit. a DSG Personendaten ins Ausland bekannt geben (Art. 19 VDSG).

Der zweite Satz von Abs. 3 schreibt dem Beauftragten vor, eine Liste der von ihm erstellten und anerkannten Modellverträge oder Standardvertragsklauseln zu veröffentlichen.

Gemäss der Botschaft (BBl 2003 2129) haftet der Inhaber von Datensammlungen, der Personendaten ins Ausland übermittelt, für Nachteile, die sich aus einer Verletzung seiner Sorgfaltspflicht ergeben könnten. Er hat insbesondere nachzuweisen, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten. Die Verordnung konkretisiert diese Sorgfaltspflicht, indem sie vom Inhaber der Datensammlung verlangt, angemessene Massnahmen zu treffen, um sicherzustellen, dass der Empfänger die Datenschutzgarantien oder –regeln beachtet (Abs. 4). Ob die Massnahmen angemessen sind, hängt von den Umständen im konkreten Einzelfall ab. Handelt es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, sind sie höher als für die übrigen Personendaten. Falls der Empfänger die Garantien oder Schutzmassnahmen nicht beachtet, fordert der Inhaber der Datensammlung ihn auf, Abhilfe zu schaffen.

Abs. 5 legt eine Frist von 30 Tagen fest, innert der der Beauftragte prüfen muss, ob die Garantien und Datenschutzregeln, die ihm mitgeteilt werden, ein angemessenes Datenschutzniveau im Sinne des Übereinkommens STE 108 gewährleisten. Ist dies nicht der Fall, so nimmt er mit dem Inhaber der Datensammlung Kontakt auf und erlässt, falls erforderlich, eine Empfehlung nach Art. 29 DSG. Erfolgt innert der gesetzten Frist keine Reaktion des Beauftragten, kann der Inhaber der Datensammlung davon ausgehen, dass der Beauftragte keine Einwände gegen die vorgelegten Garantien und Datenschutzregeln hat.

5.3 Liste der Staaten, die über eine angemessene Datenschutzgesetzgebung verfügen (Art. 7)

Art. 7 VDSG sieht vor, dass der Beauftragte eine Liste der Staaten veröffentlicht, welche über eine Gesetzgebung verfügen, die einen angemessenen Datenschutz gewährleisten. Bei der Erstellung dieser Liste berücksichtigt der Beauftragte die Beschlüsse der Europäischen Kommission in Anwendung von Art. 25 Abs. 6 der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr betreffend die Angemessenheit des Schutzniveaus in Drittländern.

Wenn der Inhaber von Datensammlungen Daten in einen Staat übermittelt, der auf der Liste des Beauftragten aufgeführt wird, gilt er als gutgläubig gemäss Art. 3 Abs. 1 ZGB. Allerdings handelt es sich um eine widerlegbare Vermutung. Der Inhaber der Datensammlung kann sich dann nicht auf seinen guten Glauben berufen, wenn er z.B. aufgrund seiner Erfahrung weiss, dass die Datenschutzvorschriften in einem bestimmten Land nicht beachtet werden.

6. Technische und organisatorische Massnahmen (Art. 8 bis 12, 20 bis 22 VDSG)

6.1 Im privaten Bereich (Art. 8 bis 12)

6.1.1 Inhalt und Grundsätzliches (Art. 8)

Einer der wichtigsten Grundsätze für die Bearbeitung von Personendaten ist derjenige der Datensicherheit. Gemäss Art. 7 DSG müssen diejenigen, welche Personendaten bearbeiten, angemessene technische und organisatorische Massnahmen treffen, um die Daten gegen jedes unbefugte Bearbeiten zu schützen. Es obliegt dem Bundesrat, nähere Bestimmungen zu erlassen und insbesondere Mindestanforderungen für die Datensicherheit festzulegen. Die Datensicherheit ist ein Grundelement des Datenschutzes. Während dieser dem Schutz der Personen gilt, bezieht sich die Datensicherheit auf den Schutz der Informationen. Sie sorgt für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, damit der Datenschutz angemessen gewährleistet werden kann. Die zu treffenden Massnahmen sind organisatorischer und technischer Natur. Eine absolute Datensicherheit gibt es nicht. Ausserdem ist die Frage der Datensicherheit je nach Zweck der Datenbearbeitung, Art der bearbeiteten Daten, Umfang der Datenbearbeitung und Risiken für die betroffenen Personen unterschiedlich zu beurteilen (Verhältnismässigkeitsgrundsatz, Art. 8 Abs. 2). Im Weiteren sind der Stand der Technik sowie in geringerem Masse die Kosten für die Datensicherung und die finanziellen Möglichkeiten der Unternehmung zu berücksichtigen. Die Verordnung definiert den zu erreichenden Mindestrahmen für

die Datensicherheit (Art. 8 bis 12). In Anwendung des Verhältnismässigkeitsprinzips wird eine Abwägung der verschiedenen vorhandenen Interessen vorgenommen. Ausser Art. 10, der eine Protokollierung bei bestimmten Bearbeitungen von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen vorsieht, enthält die Verordnung keine bestimmten Vorgaben für den Einsatz von technischen Vorkehrungen, wie z. B. Passwörter oder andere technische Identifikations- und Authentifikationsmassnahmen, Chiffrierung der Daten usw. Der Inhaber der Datensammlung hat aufgrund der oben aufgeführten Kriterien die zu treffenden Massnahmen selber zu beurteilen. Die Verordnung berücksichtigt, dass die Datensicherheit sich in einem Entwicklungsprozess befindet, der von der jeweiligen technischen Entwicklung abhängt und daher eine regelmässige Überprüfung erfordert (Art. 8 Abs. 3).

In Art. 8 Abs. 1 sind die Risiken aufgeführt, gegen die man Daten in angemessener Weise schützen muss, um den Datenschutz, d.h. den Persönlichkeitsschutz, zu gewährleisten. Es handelt sich vor allem um die folgenden Risiken:

- unbefugte oder zufällige Vernichtung;
- zufälligen Verlust;
- technische Fehler;
- Fälschung, Diebstahl oder unerlaubte Verwendung;
- unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

6.1.2 Automatisierte Bearbeitungen und Datensammlungen (Art. 9)

Die technischen und organisatorischen Massnahmen sollen namentlich bei automatisierten Datensammlungen oder Informationssystemen verhindern, dass die Systeme andere Bearbeitungen erlauben, als sie sollen. Zu diesem Zweck führt Art. 9, Abs. 1 der Verordnung Zielsetzungen auf, die insbesondere für die automatisierte Bearbeitung von Personendaten zu verwirklichen sind. Diese Zielsetzungen beschränken sich absichtlich nicht auf die Existenz einer Datensammlung, weil die aktuelle Tendenz auf eine vermehrte Verteilung von Informationen in umfassenden Informationssystemen hinausläuft, sondern auf die Gesamtheit der bearbeiteten Personendaten in den verschiedenen Organisationseinheiten, welche gleichwohl eine Benutzung nach den betroffenen Personen ermöglicht. Bezugnehmend auf diese neue Tendenz in der Informatik und Telematik ist das Festhalten am Begriff der Datensammlung überholt. Durch diese Wahl folgt die VDSG auch der Entwicklung neuerer europäischer Gesetzgebung, insbesondere auch dem Richtlinienentwurf der Europäischen Gemeinschaft.

In Art. 9 Abs. 1 sind acht Zielsetzungen aufgeführt. Diese sind unter Beachtung des Verhältnismässigkeitsgrundsatzes umzusetzen, wobei, wie bei allen anderen Sicherheitsmassnahmen, die Bearbeitungszwecke, Art und Umfang der Bearbeitungen, die Risikopotentiale für die betroffenen Personen sowie der aktuelle Stand der Technik zu berücksichtigen sind. Ein Informationssystem im Bereich Staatsschutz oder eine Datensammlung im Gesundheitsbereich erfordert andere Sicherheitsmassnahmen als eine Adressdatei.

Es geht um die acht folgenden Zielsetzungen:

- Zugangskontrolle: es sind Vorkehrungen zu treffen, um unbefugten Personen den räumlichen Zugang zu den Einrichtungen zu verwehren, mit denen Personendaten bearbeitet werden; insbesondere der Zugang zu den Räumlichkeiten, in denen sich Computer befinden. Dabei ist nicht nur der Zentralcomputer gemeint, sondern auch periphere Geräte oder Einrichtungen wie Terminals.
- Datenträgerkontrolle: sie soll verhindern, dass unbefugte Personen Datenträger lesen, kopieren, verändern oder entfernen können. Es ist insbesondere zu verhindern, dass Daten unkontrolliert auf Datenträger übertragen werden können. Unter Datenträger versteht man eine physische Trägersubstanz, auf der Daten festgehalten werden können (Papier, Bilder, Lochkarten, magnetische Träger, Festplatten, Disketten, Bänder, Compact-Disks, optische Datenträger, etc.). Ein Datenträger ist nur als solcher zu betrachten, wenn er unabhängig, d. h. nicht in die Datensammlung, in den Computer, ins Informatiksystem oder in die Hauptdatenspeicherinstallation integriert ist.
- Transportkontrolle: diese Zielsetzung soll verhindern, dass Unbefugte bei der Übermittlung oder Weitergabe von Daten diese kopieren, verändern oder löschen können. Der Datenempfänger muss auch die Gewissheit haben, dass er die Daten in ihrer ursprünglichen Form erhält und kein Dritter die Daten unbefugt abfangen kann. Bei erhöhten Risiken der Verletzung der Privatsphäre und der Rechte der betroffenen Personen, insbesondere bei der Bekannt-

gabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, ist mit Chiffrierverfahren oder gleichwertigen Massnahmen die Datensicherheit zu gewährleisten.

- Bekanntgabekontrolle: diese Massnahme soll es ermöglichen, die Datenempfänger zu identifizieren, d. h. es muss feststellbar und überprüfbar sein, an welche Personen oder Organe Daten bekannt gegeben werden. Bei Bedarf muss z. B. anhand von Protokollen feststellbar sein, mit welchen Sachmitteln welche Informationen an wen bekannt gegeben wurden. Eine Protokollierung ist nicht immer notwendig; es muss aber möglich sein, die Abläufe zu überprüfen.
- Speicherkontrolle: diese Zielsetzung soll verhindern, dass nicht autorisierte Personen auf eine Datensammlung oder ein automatisiertes Bearbeitungssystem Zugriff haben können und insbesondere vom Inhalt des Speichers (Funktionseinheit, welche Daten erhalten, speichern und wiedergeben kann) Kenntnis nehmen, ihn verändern oder löschen können. So muss man Massnahmen vorsehen, damit nur die berechtigten Personen die in der Datensammlung oder im automatisierten Bearbeitungssystem registrierten Daten bearbeiten können und auch dies nur im Rahmen ihrer Berechtigung.
- Benutzerkontrolle: durch diese Zielsetzung will man vermeiden, dass unbefugte Personen ein automatisiertes Informationssystem, z. B. mit Hilfe von Datenkommunikationseinrichtungen benutzen können. Es handelt sich insbesondere darum, Dritten ein Eindringen in das System zu verunmöglichen.
- Zugriffskontrolle: diese Zielsetzung soll gewährleisten, dass befugte Personen nur auf diejenigen Daten zugreifen können, welche sie für die Aufgabenerfüllung benötigen. Daher muss der Inhaber der Datensammlung je nach Aufgaben, die der jeweilige Benutzer zu erfüllen hat, unterschiedliche Zugriffsberechtigungen gewähren. Die Zugriffsberechtigung gibt dem Benutzer das Recht, die Daten in einem vorher bestimmten Rahmen und zu einem vordefinierten Zweck zu bearbeiten. Sie muss vor allem Art und Umfang des Zugriffs umschreiben.
- Eingabekontrolle: diese Zielsetzung soll eine nachlaufende Kontrolle der Dateneingabe in die Datensammlung oder das System ermöglichen. Dieser Kontrolle unterliegt nicht nur die Eingabe, sondern auch der Zeitpunkt, in dem sie vorgenommen wurde sowie die Identität des Benutzers. Es geht hier darum, die Nachvollziehbarkeit der Dateneingabe zu gewährleisten. Sie muss nicht zwingend durch eine Protokollierung gewährleistet werden. Die Eingabe muss jedoch anhand der verfügbaren Dokumente kontrolliert werden können.

Art. 9 Abs. 2 hält einen Grundsatz bezüglich der Organisation der Datensammlung fest. Diese muss so gestaltet werden, dass die betroffenen Personen ihr Auskunftsrecht wahrnehmen können. Dies beinhaltet vor allem, dass technische und organisatorische Massnahmen getroffen werden, um den Betroffenen die sie betreffenden Daten zustellen zu können.

6.1.3 Protokollierung (Art. 10)

Art. 10 der Verordnung sieht im übrigen bei der automatisierten Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen eine Protokollierung vor. Diese Protokollierung muss nur dann erfolgen, wenn der Inhaber der Datensammlung nicht andere präventive Massnahmen ergriffen hat, die den Datenschutz gewährleisten und garantieren, dass die Daten nur zu dem Zweck bearbeitet werden, für den sie erhoben oder bekannt gegeben wurden. Als Beispiele für präventive Massnahmen können die Entflechtung der Personendaten von den Programmen, die Differenzierung des Zugriffs gemäss der Aufgabenerfüllung des Benutzers, der Zugriffsschutz, das Vier-Augen-Prinzip, usw., genannt werden. Der Datenschutzbeauftragte kann die Protokollierung auch für andere Bearbeitungen empfehlen, wenn ein erhöhtes Risiko für die Beeinträchtigung des Privatlebens und der Rechte der betroffenen Personen besteht. Dies kann dann der Fall sein, wenn Datensammlungen oder Datenbearbeitungen betrieben werden, welche keine besonders schützenswerten Daten im Sinne von Art. 3 lit. c DSG enthalten, aber beispielsweise durch das Umfeld, in dem die Daten bearbeitet werden (Versicherungen, Auskunftbüros, usw.), und die Konfiguration der Informationssysteme eine gewisse Sensibilität aufweisen, insbesondere im Fall von Abrufverfahren.

Anhand der Protokollierung soll vor allem überprüft werden können, ob die Daten zu demjenigen Zweck bearbeitet wurden, für den sie erhoben oder bekannt gegeben wurden. Es geht insbesondere darum, zu kontrollieren, ob die Daten nicht für unvorhergesehene oder unvereinbare Zwecke verwendet werden. Das Risiko einer Zweckentfremdung steigt, wenn das Informationssystem, in dem die Daten gespeichert sind, einer grossen Anzahl von Benutzern zugänglich gemacht wird oder physisch oder optisch mit anderen Datensammlungen verknüpft ist. Es ist nicht notwendig alles zu protokollieren. In diesem Zusammenhang ist auch der in Art. 8 festgeschriebene Grundsatz zu berücksichti-

gen und das Prinzip der Verhältnismässigkeit anzuwenden (Art. 4 Abs. 2 DSG und Art. 8 Abs. 2 VDSG). Die Protokolle dienen der Überprüfung der Einhaltung der Datenschutzvorschriften. Deshalb dürfen sie nur denjenigen Personen oder Organen zugänglich sein, welche die Umsetzung dieser Vorschriften zu überwachen haben, d. h. insbesondere dem Datenschutzbeauftragten und den internen Kontrollorganen (Verantwortlicher für Datenschutz und -sicherheit innerhalb des Unternehmens oder einer Verwaltungseinheit). Die Protokolle sind während eines Jahres so aufzubewahren, dass eine Kontrolle durchgeführt werden kann, d. h. sie dürfen insbesondere nicht abänderbar sein.

6.1.4 Bearbeitungsreglement (Art. 11)

Unter den technischen und organisatorischen Massnahmen sieht Art. 11 die Erstellung eines Bearbeitungsreglements für die Datensammlungen im privaten Bereich vor, welche gemäss Art. 11 Abs. 3 DSG der Anmeldung unterliegen. Der Inhaber der Datensammlung, der besonders schützenswerte Personendaten oder Persönlichketsprofile bearbeitet oder der regelmässig Personendaten an Dritte bekanntgibt, ist grundsätzlich gehalten, seine Datensammlungen anzumelden und ein Bearbeitungsreglement zu erstellen. Von letzterer Verpflichtung ist er dann entbunden, wenn seine Datensammlung unter eine der erwähnten Ausnahmen gemäss Art. 11*a* Abs. 5 lit. b bis d fällt. Wenn er dagegen einen Datenschutzverantwortlichen bezeichnet oder ein Datenschutzqualitätszeichen erlangt (Art. 11*a* Abs. 5 lit. e DSG), wird er indessen weiterhin ein Bearbeitungsreglement erstellen müssen, auch wenn die Anmeldepflicht für die Datensammlungen in diesen Fällen generell entfällt. Das gleiche gilt für diejenigen Fälle, in denen Daten gestützt auf eine gesetzliche Verpflichtung bearbeitet werden (Art. 11*a* Abs. 5 lit. a DSG).

Das Bearbeitungsreglement ist wie eine Dokumentation oder ein Handbuch aufzubauen, das durch den Inhaber der Datensammlung verwaltet wird. Dieses Reglement beinhaltet Angaben über die interne Organisation des Inhabers der Datensammlung, sowie über die Struktur, in welche die Datensammlung oder das automatisierte Bearbeitungssystem eingebettet ist. Es beschreibt vor allem die Datenbearbeitungs- und Kontrollprozeduren, beinhaltet also die Dokumente betreffend die Planung, Ausarbeitung und den Betrieb der Datensammlung und der eingesetzten Informatikmittel. Das Reglement muss regelmässig angepasst werden und dem Beauftragten oder Datenschutzberater in allgemeinverständlicher Form jederzeit zur Verfügung stehen (Art. 11*a* Abs. 5 lit. e DSG).

6.1.5 Bekanntgabe der Daten (Art. 12)

Der Art. 12 sieht vor, dass der Datenempfänger vor der ersten Datenbekanntgabe über die Aktualität und die Zuverlässigkeit der Daten zu informieren ist. Soweit dies nicht aus den Umständen oder den Daten selbst erkennbar ist, teilt die private Person, welche die Daten bekanntgibt, das Datum der letzten Aktualisierung mit und präzisiert, ob die Daten sicher oder unsicher betreffend ihrer Richtigkeit sind. Diese Forderung ergibt sich direkt aus dem Grundsatz der Richtigkeit der Daten, der in Art. 5 DSG festgehalten ist. Sie liegt auch im Interesse der Person, welche die Daten bekanntgibt, da sie die Verantwortung für die Bekanntgabe von falschen Daten trifft.

6.2 Im öffentlich-rechtlichen Bereich (Art. 20 bis 22)

6.2.1 Technische und organisatorische Massnahmen: Grundsätze (Art. 20)

Art. 20 sieht vor, dass die für eine Bearbeitung oder Datensammlung verantwortlichen Bundesorgane im Sinne von Art. 16 DSG geeignete technische und organisatorische Massnahmen ergreifen, um die Persönlichkeit und die Grundrechte der Personen, über die Daten bearbeitet werden, zu schützen. Diese Massnahmen sind die gleichen wie für den privaten Bereich (Art 8 bis 10, siehe Kommentar unter Punkt 6.1.1, 6.1.2 und 6.1.3). Bei der automatisierten Bearbeitung arbeiten die verantwortlichen Organe mit dem Informatikstrategieorgan Bund (ISB) zusammen. Die Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV, SR 172.010.58) bleibt anwendbar (Art. 20 Abs. 4).

Nicht nur aus finanziellen Gründen und Gründen der Effizienz, sondern auch um die Anforderungen des Datenschutzes überhaupt berücksichtigen zu können, ist es notwendig, diese schon in die ersten Phasen der Entwicklung eines Informatikprojektes mit einzubeziehen. Daher verpflichtet Art. 20 VDSG die Bundesorgane dazu, alle ihre Projekte für eine automatisierte Bearbeitung von Personendaten vom Beginn ihrer Entwicklung an ihrem Datenschutzverantwortlichen nach Art. 11*a* DSG zu unterbreiten (Art. 20 Abs. 2 VDSG). Fehlt ein solcher Verantwortlicher, muss das Projekt dem Beauftragten unterbreitet werden. Wie bisher erfolgt die Anmeldung beim Beauftragten über das BFI gleichzeitig mit der Meldung der Projekte an dieses. Für die übrigen Projekte erfolgt die Anmeldung direkt an den Eidgenössischen Datenschutzbeauftragten.

Um Doppelspurigkeiten und unkoordinierte Handlungen zu vermeiden, sieht Art. 20 Abs. 3 eine Zusammenarbeit zwischen dem Eidgenössischen Datenschutzbeauftragten und dem ISB bei der Überprüfung und Überwachung der technischen Massnahmen, die erforderlich sind, um den Datenschutz zu gewährleisten, vor. Insbesondere holt der Eidgenössische Datenschutzbeauftragte die Stellungnahme des ISB ein, bevor er eine Empfehlung herausgibt.

6.2.2 Bearbeitungsreglement (Art. 21)

Unter den technischen und organisatorischen Massnahmen sieht Art. 21 die Erstellung von Bearbeitungsreglementen für automatisierte Datensammlungen des Bundes vor, die besonders schützenswerte Personendaten enthalten, oder wenn Datensammlungen von mehreren Bundesorganen benutzt werden (wie zum Beispiel das System BV+), oder wenn Datensammlungen den Kantonen (zum Beispiel die Systeme RIPOL oder ZEMIS), ausländischen Behörden, internationalen Organisationen oder Privatpersonen zugänglich gemacht werden. Das Bearbeitungsreglement stellt eine vom verantwortlichen Organ geführte Dokumentation dar und gibt Auskunft über die interne Organisation des verantwortlichen Organs und die Organisation der an der Datensammlung beteiligten Organe oder Personen. Das Reglement gibt Auskunft über die Organisation und die Struktur, in die die Datensammlung oder das automatisierte System eingebunden ist und beschreibt die Erfüllung der Aufgaben durch die Benutzer in zeitlicher und örtlicher Hinsicht. Insbesondere müssen die Datenbearbeitungsverfahren, die Kontrollverfahren und der Ablauf der wichtigsten Funktionen des Systems beschrieben werden. Das Reglement enthält Angaben über die Entwicklung und die Verwaltung der Datensammlung (Darstellung der verschiedenen Funktionen des Systems oder der Datensammlung, Häufigkeit der Bearbeitungen).

Ein solches Reglement liegt sowohl im Hinblick auf den Datenschutz als auch auf eine rationelle Betriebsführung im Interesse jedes Verantwortlichen einer automatisierten Bearbeitung. Es dient auch als Benutzerhandbuch und muss den Kontrollorganen zur Verfügung gehalten werden. Damit das Bearbeitungsreglement zweckdienlich ist, muss es ständig aktualisiert werden. Ein solches Reglement stellt an sich keine zusätzliche Arbeitsbelastung für das verantwortliche Organ dar. Es geht hier darum, Informationen und die Regelungen am gleichen Ort zu vereinen, die ohnehin festgehalten werden müssen. Das Bearbeitungsreglement muss in erster Linie die Informationen enthalten, die gemäss Art. 16 VDSG zur Anmeldung der Datensammlung notwendig sind. Weiter sind Informationen über die Herkunft der Daten (man kann hier ebenfalls die Art der Datenerhebung und die Art der Datenerfassung angeben), über die Zwecke, zu denen die Daten regelmässig übertragen oder ausgetauscht werden, über die Kontrollverfahren und genauer über die technischen und organisatorischen Massnahmen, inklusive Zugriffsregelung für die verschiedenen Benutzer, die Beschreibung der Datenfelder und ihrer Zuordnung zu den verschiedenen Organisations- und Vollzugseinheiten (insbesondere die Zugriffsberechtigungen der Benutzer, die Art und der Umfang dieser Zugriffsberechtigungen in Bezug auf die auszuführenden Aufgaben), ebenfalls im Reglement aufzuführen. Die Datenbearbeitungsverfahren und vor allem das Verfahren, wenn die betroffene Person Gebrauch von ihrem Recht macht, eine Bekanntgabe oder eine Bearbeitung ihrer Daten zu verbieten, die Aufbewahrungsdauer der Personendaten, das Anonymisierungs-, das Archivierungs- oder Vernichtungsverfahren der Daten, sowie Angaben über die Konfiguration der für die Ausführung der Aufgaben benutzten Informatikmittel (technische Angaben über die Installationen, insbesondere Standort der Terminals, Beschreibung der Datenträger und der Art der Datenbekanntgabe, zu den Netzwerken, sowie die verwendete Hard- und Software), sind ebenfalls im Reglement anzugeben. Schliesslich muss das Reglement das Verfahren für die Ausübung des Auskunftsrechtes der betroffenen Personen festlegen und das Organ oder die Person bezeichnen, die für den Datenschutz und die Datensicherheit verantwortlich ist.

6.2.3 Datenbearbeitung im Auftrag (Art. 22)

Art. 10a DSG regelt die Bearbeitung von Daten im Auftrag von Bundesorganen und durch Bundesorgane ausdrücklich. Gemäss Art. 36 Abs. 4 lit. b DSG kann der Bundesrat jedoch die Bedingungen einer solchen Bearbeitung präzisieren. Entsprechend Art. 22 VDSG bleibt das Bundesorgan, das den Auftrag erteilt hat, auch während der Bearbeitung durch Dritte für den Datenschutz verantwortlich. Es ist also verpflichtet, dafür zu sorgen, dass die Bearbeitung auftragsgemäss erfolgt und dass der Beauftragte die Daten nur für die Ausführung des Auftrags bearbeitet. Es hat auch die Ausübung des Auskunftsrechtes zu ermöglichen. Die Erteilung des Auftrages sollte allgemein in einem schriftlichen Vertrag zwischen dem Bundesorgan und dem Beauftragten festgelegt werden, wenn es sich beim Beauftragten nicht ebenfalls um ein Bundesorgan handelt. Ein solcher Vertrag ist auf alle Fälle abzuschliessen, wenn der Beauftragte nicht dem DSG oder Rechtsbestimmungen mit gleichwertiger Schutzwirkung untersteht. Unter Bundesorganen sollte das Auftragsverhältnis in einem schriftlichen Dokument festgehalten werden.

7. Berater für den Datenschutz (Art. 12a, 12b und Art. 23 VDSG)

7.1. Im privaten Bereich (Art. 12a und 12b)

7.1.1. Bezeichnung des Beraters (Art. 12a)

Art. 11*a* Abs. 5 lit. e DSG sieht vor, dass der Inhaber von Datensammlungen seine Sammlung nicht anmelden muss, wenn er einen Datenschutzverantwortlichen bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und Verzeichnisse der Datensammlungen führt. Gemäss der Botschaft (BBl 2003 2138) kann der Bundesrat vorsehen, dass die Befreiung von der Meldepflicht nur erfolgt, wenn die Einsetzung des Datenschutzverantwortlichen dem eidgenössischen Datenschutzbeauftragten mitgeteilt wird.

Die Bezeichnung «Datenschutzverantwortlicher» in der deutschen – sowie «responsabile della protezione dei dati» in der italienischen – Fassung von Art. 11*a* Abs. 5 lit. e DSG bedeutet nicht, dass diese Person die Alleinverantwortung für die Einhaltung des Datenschutzes trägt. Wie nachstehend noch detaillierter dargelegt wird, hat sie lediglich eine beratende – und kontrollierende – Funktion. Die Verantwortung liegt vielmehr in erster Linie bei den Stellen, die als Inhaber einer Datensammlung – und damit als Verantwortliche für die mit den betreffenden Personendaten vorgenommenen Bearbeitungen – gelten müssen. Richtiger ist denn auch die französische Bezeichnung in der erwähnten Bestimmung: «Conseiller à la protection des données».

Zur Umsetzung von Art. 11*a* Abs. 5 lit. e DSG sieht Art. 12a Abs. 1 VDSG vor, dass der Inhaber der Datensammlung, der von seiner Pflicht zur Anmeldung der Datensammlungen befreit werden will, einen Datenschutzverantwortlichen bestimmt, der die Anforderungen erfüllt, die in den vorliegenden Art. 12a Abs. 2 und 12b aufgestellt werden. Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte ist sodann darüber zu informieren.

Der Inhaber der Datensammlungen kann nach Abs. 2 einen Mitarbeiter mit der Funktion des betrieblichen Datenschutzverantwortlichen betrauen. Die Angliederung der Funktion innerhalb der Hierarchie eines Unternehmens ist nicht entscheidend. Zur Gewährleistung der Unabhängigkeit sollte die mit der Funktion betraute Person allerdings direkt der Geschäftsleitung des Inhabers der Datensammlungen unterstellt sein. Datenschutzverantwortlicher kann auch ein Dritter sein. Mit dieser Lösung wird der im DSG geforderte Grundsatz der Unabhängigkeit besser gewährleistet und den kleineren und mittleren Unternehmen erlaubt, einen externen Berater zu beauftragen, ohne eine spezifische Stelle selber schaffen zu müssen.

Der Datenschutzberater muss in der Ausübung seiner Funktionen unabhängig sein (Art. 11*a* Abs. 5 lit. e DSG). Dieser Grundsatz wird in Art. 12a, Abs. 2, 2. Satz, konkretisiert. Der Inhaber der Datensammlung muss nach dieser Bestimmung eine Person bezeichnen, die keine anderen Tätigkeiten ausübt, die mit den Aufgaben, die er für den Inhaber der Datensammlung leistet, in Konflikt geraten könnten. Dies könnte etwa dann der Fall sein, wenn der Datenschutzverantwortliche Direktionsmitglied ist, wenn er Funktionen in Bereichen wie Personalführung, Informationssystemverwaltung oder Informationstechnologien ausübt oder wenn er zu einer Dienststelle gehört, die Bearbeitungen von besonders schützenswerten Daten durchführt. Dagegen ist die Kumulierung des Amtes als Datenschutzverantwortlicher mit dem Amt als Informatiksicherheitsbeauftragter oder als Leiter der Rechtsabteilung grundsätzlich durchaus vereinbar. Der Grundsatz der Unabhängigkeit muss nicht nur vom Inhaber der Datensammlung, sondern auch vom Datenschutzverantwortlichen selbst befolgt werden. Er wird durch die vorliegende Bestimmung dazu verpflichtet, auf jede Tätigkeit zu verzichten, die mit den Aufgaben, die er für den Inhaber der Datensammlung erfüllt, in einen Konflikt geraten könnte.

Der Datenschutzverantwortliche muss weiter über die erforderliche Fachkenntnis verfügen, um seine Aufgaben effizient zu erfüllen (Abs. 2, 2. Satz). Seine Kentnisse müssen die Datenschutzgesetzgebung, technische Standards, die Organisation des Inhabers der Datensammlung sowie die Einzelheiten der durch diesen veranlassten Bearbeitungen von Personendaten umfassen.

Beim betrieblichen Datenschutzverantwortlichen handelt es sich primär um eine Funktion. Somit ist – namentlich im Hinblick auf die Erfüllung der Anforderungen hinsichtlich der Fachkenntnisse – auch denkbar, dass faktisch nicht eine Einzelperson, sondern ein Team diese Funktion ausfüllt, z.B. eine Datenschutzfachperson gemeinsam mit einem Spezialisten oder einer Spezialistin für Informatiksicherheit. Die Gesamtverantwortung für die Aufgabenerfüllung muss indessen klar zugeordnet sein.

Art. 12a überlässt es dem Inhaber von Datensammlungen, sich auf die in Art. 11*a* Abs. 5 lit. e DSG vorgesehene Ausnahme zu berufen. Falls er dies tut, muss er den Beauftragten darüber informieren, dass er einen Datenschutzverantwortlichen eingesetzt hat. Die Verordnung sieht keine Verpflichtung

vor, dem Beauftragten die Identität der Person mitzuteilen, die mit der fraglichen Funktion betraut wurde. Es wäre indessen wünschenswert, wenn er auch diesbezüglich informiert würde. Das Verfahren zur Information des Beauftragten soll so einfach wie möglich ausgestaltet werden; zu denken ist insbesondere an eine Information über Internet. Ist diese Information erfolgt, so ist in der Folge der Inhaber der Datensammlungen von der Anmeldepflicht befreit. Falls dagegen der eingesetzte Datenschutzverantwortliche das Unabhängigkeitserfordernis gemäss DSG nicht erfüllt oder falls der Inhaber der Datensammlung darauf verzichtet, die in Art. 11*a* Abs. 5 Buchst e DSG verankerte Ausnahme geltend zu machen, bleibt er der Anmeldepflicht unterstellt und muss namentlich seine Personaldatensammlung anmelden, wenn sie sensible Personendaten oder Persönlichkeitsprofile enthält.

7.1.2. Aufgaben und Stellung (Art. 12b)

Gemäss Art. 11*a* Abs. 6 DSG, 2. Satz, präzisiert der Bundesrat die Stellung und die Aufgaben der Datenschutzverantwortlichen. Zur Konkretisierung dieser Bestimmung regelt Art. 12*b* Abs. 1 VDSG dessen Aufgaben.

- Nach lit. a muss der Datenschutzverantwortliche die Bearbeitung von Personendaten prüfen und Korrekturmassnahmen empfehlen, wenn er feststellt, dass Vorschriften über den Datenschutz verletzt wurden. Der Inhaber der Datensammlung darf gegen den Datenschutzverantwortlichen keinesfalls Massnahmen mit Sanktionscharakter ergreifen, wenn dieser seine Aufgabe erfüllt. Die Aufgabe nach lit. a zieht keine Haftung des Datenschutzverantwortlichen nach sich, wenn der Inhaber der Datensammlung die Datenschutzgesetzgebung verletzt. Der Inhaber der Datensammlung ist insbesondere gegenüber der betroffenen Person allein verantwortlich.
- Nach lit. b ist der Datenschutzverantwortliche damit beauftragt, eine Liste der Datensammlungen des Inhabers der Datensammlungen zu führen, die vom Beauftragten oder betroffenen Personen, die ein entsprechendes Gesuch stellen, eingesehen werden kann. Diese Liste gewährleistet die Transparenz der nicht mehr meldepflichtigen Datensammlungen gegenüber den betroffenen Personen und gegenüber dem Beauftragten. Nur die Datensammlungen nach Art. 11*a* Abs. 3 DSG müssen auf dieser Liste figurieren.
- Der Datenschutzverantwortliche muss die zur Erfüllung seiner Aufgaben notwendigen Massnahmen ergreifen, selbst wenn die Verordnung diese nicht ausdrücklich erwähnt. Er muss namentlich das Personal des Inhabers der Datensammlung beraten und ausbilden, indem er z.B. Richtlinien oder Weisungen erlässt. Er begutachtet alle Projekte und Massnahmen, welche den Datenschutz betreffen; daraus folgt, dass der Inhaber der Datensammlung ihn jeweils konsultieren muss, bevor eine neue Datenbearbeitung begonnen wird. Er berichtet dem Inhaber der Datensammlung regelmässig über seine Aktivitäten.
- Art. 12b Abs. 2 VDSG verankert den Grundsatz der Unabhängigkeit des Datenschutzverantwortlichen (Art. 11*a* Abs. 5 lit. e DSG). Laut der Botschaft (BBl 2003 2138) darf er gegenüber denjenigen Stellen oder Organisationseinheiten, die selbst unmittelbar für die Bearbeitung von Personendaten verantwortlich sind, nicht weisungsgebunden oder hierarchisch untergeordnet sein.
- Gemäss lit. a unterliegt der Datenschutzverantwortliche bezüglich der fachlichen Ausübung seiner Funktion keinen Weisungen. Gemäss dieser Bestimmung soll der Inhaber der Datensammlung nicht in die Erfüllung der Aufgaben, die dem Datenschutzverantwortlichen übertragen sind, eingreifen. Die Garantie der Unabhängigkeit spielt eine wesentliche Rolle: Es ist nicht auszuschliessen, dass der Datenschutzverantwortliche in Interessenkonflikte gerät, besonders wenn er z.B. die Rechtmässigkeit der Bearbeitungen von Daten über die Mitarbeiter des Inhabers der Datensammlungen zu beurteilen hat und organisatorische oder technische Lösungen empfehlen muss, welche bei der Direktion bzw. den betroffenen Dienststellen nicht unbedingt auf Zustimmung stossen.
- Der Datenschutzverantwortliche ist ausserdem mit den erforderlichen Ressourcen auszustatten, damit er seine Aufgaben unabhängig erfüllen kann. Dazu gehören insbesondere Personal, Infrastruktur und weitere unverzichtbare Ausstattungen (lit. b).
- Der Datenschutzverantwortliche hat im Übrigen Zugang zu allen Datensammlungen und Datenbearbeitungen sowie zu allen Informationen, die er zur Erfüllung seiner Aufgabe benötigt (lit. c). Ausserdem muss er den Inhaber der Datensammlung und seine Mitarbeiter befragen können.

- Es ist schliesslich darauf hinzuweisen, dass weder das Gesetz noch die Verordnung dem Datenschutzverantwortlichen das Recht übertragen, den Beauftragten mit der Angelegenheit zu befassen, wenn seine Empfehlungen nicht befolgt wurden. Hingegen kann er nach Art. 28 DSG in der Ausübung seiner Aufgaben den Beauftragten um Rat fragen.

7.2. Bundesorgane (Art. 23)

Die Wirksamkeit des Datenschutzes erfordert einerseits, dass die Rechte der betroffenen Personen gesetzlich gesichert werden, und andererseits, dass es möglich ist, die Einhaltung der gesetzlichen Regelungen zu kontrollieren. Diese Kontrolle findet auf mehreren Ebenen statt und erfordert insbesondere eine unabhängige Stelle: Dies ist die Funktion des eidgenössischen Datenschutzbeauftragten. Es sollte jedoch auch betont werden, dass in erster Linie das Bundesorgan, welches Personendaten bearbeitet, verantwortlich dafür ist, dass die Datenschutzbestimmungen eingehalten werden (Art. 16 Abs. 1 DSG). Angesichts dessen sollte die Kontrollstruktur verstärkt werden. Die Überwachung muss nahe bei den Organen, welche Personendaten bearbeiten, stattfinden, insbesondere wenn die Bearbeitung automatisiert ist. Dies erhöht die Wirksamkeit (namentlich weil ein Datenschutzberater die Organisation, für die er arbeitet, besser kennt) und erleichtert die Zusammenarbeit mit dem Datenschutzbeauftragten des Bundes. Dadurch soll ausserdem der Datenschutzbeauftragte von Fragen, die leicht innerhalb eines Amtes beantwortet werden können, entlastet werden. Deshalb sieht Art. 23 vor, dass jedes Departement und die Bundeskanzlei einen Berater für den Datenschutz bezeichnen.

Die Hauptaufgabe dieses Beraters ist es, die Anwender über den Datenschutz zu informieren. Im Gegensatz zum unabhängigen Berater nach Art. 11*a* Abs. 5 lit. e DSG gehören Kontrolle und Vertretung nach aussen (z. B. die Behandlung von Zugriffsgesuchen) grundsätzlich nicht zu seinen Aufgaben. Den Verwaltungseinheiten steht es jedoch offen, sein Pflichtenheft zu erweitern und ihm solche Aufgaben zu überantworten. Es steht den Departementen und Ämtern auch offen, mehrere Berater zu bezeichnen. Es ist ausserdem wünschenswert, dass diejenigen Ämter, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder grosse Datenverarbeitungssysteme unterhalten, solche Berater bezeichnen. Mehrere Ämter haben dies bereits getan.

Nach Art. 23 Abs. 1 VDSG umfassen die Aufgabe des Beraters im Wesentlichen die Beratung, die Information und die Ausbildung. Der Berater soll für die Mitarbeiter in seinem Departement oder Amt eine Ansprechperson sein, die über das nötige Wissen im Bereich des Datenschutzes und der Datensicherheit verfügt, die Auskünfte erteilt und dazu beiträgt, dass die Datenschutzbestimmungen intern umgesetzt werden. Er fungiert nicht als Verbindungsperson für den eidgenössischen Datenbeauftragten, aber als Kontaktperson. Abs. 3 bestimmt denn auch, dass die Bundesorgane mit dem Datenschutzbeauftragten über ihren Berater kommunizieren.

Wollen Bundesorgane nach Art. 11*a* Abs. 5 lit. e DSG von der Pflicht zur Anmeldung ihrer Datensammlungen befreit werden, so müssen sie einen unabhängigen Datenschutzverantwortlichen bezeichnen. In diesem Fall sind die Art. 12a und 12b DSG anwendbar (Art. 23 Abs 2 VDSG).

8. Besondere Bestimmungen (Art. 24 bis 27a)

8.1 Beschaffung von Personendaten (Art. 24)

Diese Bestimmung konkretisiert das Postulat einer verbesserten Transparenz bei der Bearbeitung von Personendaten, insbesondere durch die Pflicht zur Orientierung der betroffenen Personen. Sie ergänzt Art. 4, 7a und 18 DSG.). In der Tat kommt es nicht selten vor, dass Daten, vor allem zu statistischen Zwecken, systematisch mittels Fragebogen und fakultativ erhoben werden. Die befragten Personen haben ein Recht zu erfahren, ob sie zur Beantwortung verpflichtet sind und welches die Folgen einer Auskunftsverweigerung oder unrichtiger Angaben sind.

8.2 Persönliche Identifikationsnummer (Art. 25)

Die persönliche Identifikationsnummer dient der Identifizierung einer Person in einer bestimmten öffentlichen Datensammlung. Sie kann auf einen bestimmten Bereich beschränkt oder aber generell oder für mehrere Zwecke verwendet werden. Es kann sich dabei um eine sprechende Nummer handeln, die kodierte Informationen enthält (z.B. Name, Geschlecht, Zivilstand, Nationalität) oder um eine nichtsprechende Nummer, d.h. um zufällig ausgewählte Ziffern. Grundsätzlich sollen die

Bundesorgane mit nichtsprechenden Nummern operieren. Persönliche Identifikationsnummern sind als Personendaten zu betrachten.

Die Verwendung solcher Nummern hat Vor- und Nachteile. Sie ermöglicht vor allem eine grössere Genauigkeit und kann daher zur Effizienz und Wirtschaftlichkeit beitragen (vor allem wenn in der ganzen Verwaltung dieselbe Nummer verwendet wird). Auch werden Verwechslungen gleichnamiger Personen vermieden, und es ist die Möglichkeit gegeben, die Genauigkeit und Zuverlässigkeit einer Datensammlung durch Vergleiche mit anderen Daten zu überprüfen. Andererseits erleichtern Identifikationsnummern die Verknüpfung von Datensammlungen, mit dem entsprechend höheren Risiko, dass umfassende Persönlichkeitsprofile entstehen und der Staat mehr Macht über die Bürger gewinnt. Psychologisch gesehen kann sich die Verwendung einer einzigen Nummer als gefährlich erweisen, indem sich der Bürger auf eine Nummer reduziert und vom Datenbearbeitungsprozess ausgeschlossen fühlt, was zu einer Verletzung der Menschenwürde und des Rechtes auf informationelle Selbstbestimmung führen würde, weil die Staatsorgane zur Datenbeschaffung oder -überprüfung nicht mehr mit den betroffenen Personen in Kontakt zu treten bräuchten. Schliesslich ist mit Identifikationsnummern die Entanonymisierung zu statistischen Zwecken aufbewahrter und verwendeter Daten leichter.

Angesichts solcher Risiken hat der Gesetzgeber den Bundesrat beauftragt, die Verwendung von persönlichen Identifikationsnummern zu regeln (Art. 36 Abs. 4 lit. c) und diejenige herkömmlicher Identifikationsmittel wie z.B. der AHV-Nummer einzuschränken. Daher regelt Art. 25 den Gebrauch von Identifikationsnummern durch die Bundesorgane mit Ausnahme der AHV-Nummer, deren Verwendung in einem Spezialgesetz geregelt wird.

Damit neu geschaffene persönliche Identifikationsnummern nicht sprechend sind und die von den betroffenen Personen nicht erwünschte Preisgabe von Personendaten wie z.B. ihren Zivilstand, ihr Alter, ihr Geschlecht, ihre Staatsangehörigkeit usw. fördert, sind die Bundesorgane gehalten, nichtsprechende Identifikationsnummern zu verwenden. Ihre Verwendung ist ausserdem auf das Tätigkeitsfeld zu beschränken, für welches sie geschaffen werden, um das Risiko unerwünschter Verknüpfungen herabzusetzen (Art. 25 Abs. 1).

Solche Nummern sind nicht nur bei der Eröffnung neuer Datensammlungen zu schaffen, sondern auch wenn die Bedingungen nach Abs. 1 nicht erfüllt sind oder wenn ein Organ bestehende Datensammlungen umorganisiert und dabei die Nummern geändert werden können. Auf diese Weise kann nach und nach ein Identifikationsmittel wie z.B. die AHV-Nummer durch eine bereichsspezifische Nummer ersetzt werden.

Art. 25 Abs. 2 und 3 beugt ebenfalls der Gefahr von Querverbindungen und dadurch möglicher Datenschutzverletzungen vor. Er erlaubt dem Organ, das die Identifikationsnummer geschaffen hat, ihre Verwendung durch andere Organe und Privatpersonen zu kontrollieren. Nach dem Grundsatz der Zweckbindung und der Zielkompatibilität wird die Erlaubnis, die Nummer zu verwenden, durch das zuständige Organ nur erteilt, wenn ein enger Zusammenhang mit dem Bereich besteht, für den die persönliche Identifikationsnummer eingeführt worden ist.

8.3 Bekanntgabe der Daten (Art. 26)

Siehe hierzu den Kommentar oben unter Punkt 6.1.5.

8.4 Pilotversuche

8.4.1 Verfahren

Art. 17a DSG überträgt dem Bundesrat die Befugnis, vor dem Inkrafttreten einer formellgesetzlichen Grundlage die automatisierte Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen im Rahmen von Pilotversuchen zu bewilligen, wenn bestimmte Voraussetzungen erfüllt sind. Die erste Bedingung ist in Art. 17a Abs. 1 DSG verankert, der vorsieht, dass der Beauftragte konsultiert werden muss. Um diese Bestimmung in der Praxis umzusetzen, wird in der Verordnung das Verfahren näher umschrieben.

Wenn ein Bundesorgan beabsichtigt, einen Pilotversuch durchzuführen, muss es nach Art. 27 Abs. 1 dem Beauftragten mitteilen, mit welchen Massnahmen die Einhaltung der sich aus Art. 17a DSG ergebenden Anforderungen sichergestellt werden soll. Der Beauftragte nimmt Stellung, bevor die Ämterkonsultation bei den übrigen interessierten Bundesstellen durchgeführt wird.

Um dem Beauftragten die Stellungnahme zu ermöglichen muss die zuständige Behörde ihm eine Dokumentation im Umfang der Umschreibung in Abs. 2 vorlegen. Sie kann somit nicht bloss in allgemeiner Art und Weise festhalten, dass für eine bestimmte Bearbeitung Art. 17a anwendbar ist,

sondern muss konkret und umfassend darlegen, wie die einzelnen Bedingungen und Voraussetzungen nach Art. 17a DSG eingehalten werden. Die Informationen des zuständigen Bundesorgans müssen es dem Beauftragten ermöglichen, in Kenntnis aller Einzelheiten Stellung zu nehmen. Nach Abs. 3 kann der Beauftragte auch weitere Dokumente anfordern und zusätzliche Abklärungen treffen.

Im Rahmen seiner Stellungnahme untersucht der Beauftragte, ob die Voraussetzungen nach Art. 17a eingehalten werden (Abs. 2). Eine bloss summarische Stellungnahme erfüllt die Anforderungen indessen nicht. Er muss ausdrücklich zu jeder in Art. 17a verankerten Voraussetzung Stellung nehmen und auf die Darlegungen der zuständigen Bundesbehörde Bezug nehmen. Seine Stellungnahme muss es der zuständigen Behörde ermöglichen, falls nötig das Projekt anzupassen, bevor sie es in der Ämterkonsultation den übrigen interessierten Bundesstellen vorlegt.

Wenn das zuständige Bundesorgan – insbesondere im Anschluss an die Ämterkonsultation – an der Konzeption des Pilotversuchs wesentliche Änderungen vornimmt, welche die Einhaltung der Voraussetzungen nach Art. 17a betreffen, so informiert es den Beauftragten darüber. Dieser nimmt, falls erforderlich, erneut Stellung (Abs. 4). Diese Regelung ist erforderlich, weil die Stellungnahme des Beauftragten dem Antrag an den Bundesrat beigefügt wird. Sie muss sich daher auch auf das dem Bundesrat vorgelegte Projekt beziehen und nicht auf eine Fassung, die zwischenzeitlich geändert wurde.

Die zuständige Bundesstelle übermittelt den finalisierten Entwurf mit dem entsprechenden Antrag an den Bundesrat dem jeweiligen Departement, einschliesslich der Stellungnahme des Beauftragten (Abs. 5). Es genügt also nicht, lediglich im Antrag auszuführen, der Beauftragte sei mit dem Projekt einverstanden.

Schliesslich ist darauf hinzuweisen, dass der Bundesrat die Regelung der Modalitäten der automatisierten Bearbeitung in einer Verordnung (Art. 17a Abs. 3 DSG) entweder gleichzeitig mit der Bewilligung des entsprechenden Pilotversuchs oder auch erst in einem zweiten Schritt vornehmen kann. Im Übrigen ist in der Verordnung ausdrücklich die Beschränkung der Geltungsdauer auf 5 Jahre (Art. 17a Abs. 5 DSG) vorzusehen.

8.4.2 Evaluationsbericht bei Pilotversuchen (Art. 27*a*)

Art. 27a trifft eine Verfahrensregelung zu Art. 17a Abs. 4 DSG, der verlangt, dass das zuständige Bundesorgan dem Bundesrat spätestens innert zwei Jahren nach Inbetriebnahme des Pilotsystems einen Evaluationsbericht vorlegt und darin namentlich die Fortführung oder die Einstellung der Bearbeitung vorschlägt. Nachdem bei der Bewilligung des Pilotversuchs durch den Bundesrat die Stellungnahme des Beauftragten zwingend vorliegen muss, ist seine Beurteilung dem Bundesrat konsequenterweise auch bei dieser Etappe des Verfahrens zur Kenntnis zu bringen.

9. Register der Datensammlungen und Anmeldung (Art. 28)

Nach Art. 11*a* DSG führt der Datenschutzbeauftragte ein Register der Datensammlungen, das online zugänglich ist. Das Register verzeichnet alle von den Bundesorganen geführten Datensammlungen sowie von privaten Personen geführte Datensammlungen mit besonders schützenswerten Personendaten, mit Persönlichkeitsprofilen, die regelmässig bearbeitet werden, oder mit Personendaten, die regelmässig Dritten mitgeteilt werden. Solche Datensammlungen müssen angemeldet werden, ausser wenn es sich dabei um Ausnahmen nach Art. 11*a* Abs. 5 DSG und den Artikeln 4 und 18 VDSG handelt. Der Bundesrat regelt die Modalitäten der Anmeldung und der Führung des Registers.

Art. 28 legt den Inhalt des Registers und die Modalitäten seiner Veröffentlichung fest. Das Register der Datensammlungen soll den öffentlichen Zugang zu den Datensammlungen ermöglichen (Prinzip der Transparenz), namentlich um betroffenen Personen die Ausübung des Auskunftsrechts zu erleichtern. Obwohl das Register auch wichtig ist, damit der eidgenössische Datenschutzbeauftragte seine Aufsichts- und Beratungsaufgaben erfüllen kann, darf es nur Daten enthalten, die nötig sind, um den öffentlichen Zugang zu gewährleisten, d. h. um ausreichend über den Inhalt, die Wichtigkeit und den Zweck einer Datensammlung zu informieren. Dementsprechend enthält das Register ausschliesslich die Angaben der Anmeldung nach Art. 11*a* DSG und den Artikeln 3 und 16 VDSG:

- Name und Adresse des Inhabers der Datensammlung;
- Name und vollständige Umschreibung der Datensammlung;
- Person oder Bundesorgan, bei denen das Auskunftsrecht ausgeübt werden kann;

- Rechtsgrundlage und Zweck der Datensammlung (die Rechtsgrundlage informiert über die Rechtmässigkeit der Datensammlung: Sie betrifft nur die Datensammlung der Bundesorgane);
- Kategorie der bearbeiteten Daten (sie gibt Hinweise auf die in der Datensammlung enthaltenen Datenarten, z.B. Name, Adresse, Beruf, Geburtsdatum, usw.);
- Kategorien der Datenempfänger;
- Kategorien der an der Datensammlung Beteiligten.

Die Angaben der letzten beiden Kategorien sind wichtig, damit die betroffene Person sich ein Bild von der Art der Datensammlung machen kann (isoliert, verknüpft oder offen). Über diese Angaben kann sie auch die Entwicklung der sie betreffenden Daten verfolgen und sich gegebenenfalls an die verschiedenen Inhaber einer Datensammlung wenden.

Der Beauftragte kann nach Art. 27 Abs. 3 und Art. 29 Abs. 2 DSG nach der Anmeldung weitere Informationen anfordern. Diese Informationen werden allerdings weder im Register aufgeführt noch veröffentlicht (vgl. auch Art. 34 DSG und Abschnitt 10.3 unten).

Das Register ist öffentlich und online zugänglich. Der Beauftragte erstellt ausserdem auf Gesuch hin kostenlos Auszüge (Art. 28 Abs. 2 VDSG).

Nach der Anmeldung muss eine Datensammlung registriert werden. Art. 28 Abs. 4 VDSG regelt die Registrierung. Nach Art. 11*a* Abs. 4 DSG müssen Datensammlungen angemeldet werden, bevor sie eröffnet werden. Es gibt weder ein Genehmigungsverfahren noch eine materielle Prüfung der Anmeldung. Der Beauftragte prüft summarisch, ob die Anmeldung vollständig ist. Im Anschluss an diese Prüfung registriert er die Datensammlung und veröffentlicht sie im Register der Datensammlungen. Wenn eine Anmeldung unvollständig ist, setzt der Beauftragte dem Inhaber der Datensammlung eine Frist, um seinen Verpflichtungen nachzukommen. Nach Ablauf der Frist kann er gestützt auf die Angaben, die ihm zur Verfügung stehen, von Amtes wegen die Datensammlung registrieren oder die Einstellung der Bearbeitung empfehlen.

Die Registrierung einer Datensammlung bedeutet nicht, dass dem Inhaber damit eine Blankovollmacht erteilt wird. Der Datenschutzbeauftragte kann auch später noch feststellen, dass eine Datenbearbeitung aus der Sicht des Datenschutzes Unzulänglichkeiten aufweist. In diesem Fall und wenn der Inhaber der Datensammlung die Empfehlungen des Datenschutzbeauftragten nicht befolgt, kann dieser gegebenenfalls das zuständige Departement (Art. 27 DSG) oder das Bundesverwaltungsgericht (Art. 29 DSG) ersuchen, die Einstellung der Bearbeitung und die Löschung der Sammlung aus dem Register zu verfügen.

Nach Art. 28 Abs. 3 VDSG führt der Beauftragte ein Verzeichnis der Inhaber von Datensammlungen, die ihrer Pflicht zur Anmeldung der Datensammlungen nach Art. 11*a* Abs. 5 lit. e und f DSG enthoben sind (Erwerb eines Datenschutz-Qualitätszeichens oder Bezeichnung eines Datenschutzverantwortlichen).

10. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (Art. 30 bis 34 VDSG)

10.1 Rechtstellung, Organisation und Dokumentation (Art. 30 bis 32)

Art. 30 bis 32 ergänzen die Bestimmungen des DSG zum Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und regeln insbesondere das Dienstverhältnis der Sekretariatsmitglieder, den Sitz sowie die Beziehungen zu anderen Behörden. Art. 30 Abs. 3 sieht vor, dass das Budget des Beauftragten in einer spezifischen Rubrik des Budgets der Bundeskanzlei figuriert. Dabei handelt es sich um eine erste Konkretisierung von Art. 26 Abs. 3, der festhält, dass der Beauftragte über ein eigenes Budget verfügt. Folglich, gemäss Art. 31, kommuniziert der Beauftragte, der autonom ist, aber administrativ der Bundeskanzlei zugeordnet, mit dem Bundesrat durch eine Mittelsperson, nämlich die Bundeskanzlerin. Sie hat alle Empfehlungen und Berichte des Datenschutzbeauftragten weiterzuleiten, auch wenn sie ihnen nicht zustimmt. Mit den übrigen Behörden und den privaten Personen, die dem Datenschutzgesetz oder dem Öffentlichkeitsprinzip unterstehen, verkehrt der Eidgenössische Datenschutzbeauftragte direkt.

Der Beauftragte verfügt auch über eine eigene Dokumentation (Art. 32). Die Bundesorgane müssen ihm insbesondere alle Gesetzgebungsprojekte vorlegen, welche die Bearbeitung von Personendaten, den Datenschutz und das Transparenzprinzip in der Verwaltung (Zugang zu amtlichen Dokumenten) betreffen. Ebenso müssen die Bundeskanzlei und die Departemente dem Beauftragten ihre

Entscheide anonymisiert sowie ihre Richtlinien in Sachen Datenschutz mitteilen. Diese Information ist notwendig, um dem Datenschutzbeauftragten seine Überwachungsaufgaben und die Beratung der Bundesorgane zu erleichtern.

Um seine Arbeit rationeller und effizienter gestalten zu können, verfügt der Datenschutzbeauftragte für Dokumentationszwecke, für die Registrierung der Akten und die Geschäftskontrolle sowie für das Register der Datensammlungen über ein eigenes automatisiertes Datenbearbeitungssystem. Dieses System erlaubt ihm auch die Indexierung und Kontrolle der Korrespondenz und der Dossiers ebenso wie die Publikation von Informationen allgemeinen Interesses. Die wissenschaftliche Dokumentation wird auch dem Bundesverwaltungsgericht zur Verfügung stehen. Weitere Behörden, insbesondere die Datenschutzberater der Departemente und Bundesämter können später ebenfalls zugelassen werden.

10.2 Gebühren (Art. 33)

Mit Ausnahme der Gutachten werden für die Beratungs- und Überwachungstätigkeiten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten keine Gebühren erhoben; dies aus Rücksicht darauf, dass das Anmeldeverfahren und die Überwachung durch den Beauftragten eine aktive Mitarbeit der Datenbearbeitungsverantwortlichen erfordern. Es wäre nicht sinnvoll, sie durch die Erhebung einer Gebühr zu strafen. Die Registrierung der Datensammlungen, die Meldung von grenzüberschreitenden Datenflüssen und Empfehlungen des EDÖB sind daher gebührenfrei. Auch gegenüber den eidgenössischen oder kantonalen Behörden werden keine Gebühren erhoben.

10.3 Prüfung der Datenbearbeitung von Personendaten (Art. 34)

Dieser Artikel zählt als Beispiele einige Informationen auf, die der Beauftragte vom Inhaber der Datensammlung oder dem verantwortlichen Organ verlangen kann, wenn er die Rechtmässigkeit einer Datenbearbeitung oder der Bekanntgabe von Daten ins Ausland prüft. Ein Teil dieser Informationen kann gegebenenfalls bei der Anmeldung der Datensammlungen oder der Meldung von grenzüberschreitenden Datenflüssen erhoben werden. Diese Informationen werden weder publiziert noch im Register der Datensammlungen festgehalten.