Informationen zum revidierten Datenschutzgesetz

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni

Herausgeber
Schweizerischer Versicherungsverband SVV
C.F. Meyer-Strasse 14
Postfach 4288, CH-8022 Zürich
Tel. +41 44 208 28 28
Fax +41 44 208 28 00
info@svv.ch
www.svv.ch

Zuständiges Gremium
Arbeitsgruppe Datenschutz der Kommission Recht & Compliance:
Marcel Süsskind (Vorsitz), AXA Winterthur
Ursula Holliger, Swiss Life
Michèle Karlen, Zürich Schweiz
Frank Kilchenmann, Helvetia
Nadine Probst, Die Mobiliar
Alex Schweizer, Helsana
Barbara Widmer, Allianz Suisse
Niggi Zittel, Basler Versicherungen

Redaktion und Kontaktperson
Franziska Streich, Rechtsanwältin
C.F. Meyer-Strasse 14
Postfach 4288, CH-8022 Zürich
Tel. +41 44 208 28 63
Fax +41 44 208 28 07
franziska.streich@svv.ch

Bestelladresse
print@svv.ch

Download
www.extranet.svv.ch
(Issue Management / 3000 Wirtschaft & Recht / 3250 Datenschutz)

Stand 1. Juli 2007

Das Bundesgesetz über den Datenschutz (DSG) und die dazugehörige Verordnung (VDSG) sind seit 1. Juli 1993 in Kraft. Am 24. März 2006 hat das Parlament eine Teilrevision des DSG verabschiedet. Mit einer Inkraftsetzung des revidierten Datenschutzrechts (DSG, VDSG und Verordnung über Datenschutzzertifizierungen) ist vermutlich nicht vor Herbst 2007 zu rechnen.

Auf den folgenden Seiten werden die wesentlichen Änderungen, die das revidierte Recht vorsieht, erläutert. Ausgangspunkt bilden der Wortlaut der revidierten Bestimmungen und die Materialien der Revision, insbesondere die Botschaft des Bundesrates, die im Bundesblatt vom 18. März 2003 unter *www.admin.ch* abrufbar ist. Die Erläuterungen haben naturgemäss keinen abschliessenden Charakter, solange Präjudizien zu den revidierten Bestimmungen fehlen. Massgebend werden primär Entscheide der Zivilgerichte sein. Der Datenschutz- und Öffentlichkeitsbeauftragte kann gegenüber privaten Datenbearbeitern nur im beschränkten Umfang von Art. 29 DSG sog. Empfehlungen abgeben.

Die Erläuterungen sind in Zusammenarbeit mit der Arbeitsgruppe Datenschutz der Kommission Recht & Compliance verfasst worden. Sie ersetzen – was Ziffer III betrifft – die Empfehlung des SVV vom 11. März 2002 über die Verwendung von Einwilligungsklauseln zur Datenbearbeitung (Rundschreiben SVV Nr. 8/2002).

Ihr Schweizerischer Versicherungsverband

I. Checkliste zum revidierten Datenschutzgesetz

Die verbindlichen Massnahmen, die aufgrund des revidierten Datenschutzgesetzes (DSG) zu ergreifen sind, lassen sich im Wesentlichen wie folgt zusammenfassen:

Information der betroffenen Personen

Die betroffenen Personen – d.h. die Antragsteller, Versicherungsnehmer, geschädigte Dritte etc. – sind gemäss den neuen Informationspflichten über die Datenbearbeitung zu informieren. Eine Information nach DSG (Art. 7a bzw. 4 Abs. 4 DSG) erübrigt sich, sofern die betroffene Person bereits nach VVG (Art. 3 Abs. 1 lit. g bzw. Abs. 3 VVG) informiert wurde.

Einwilligung der betroffenen Person

Für Datenbearbeitungen, die eine Einwilligung der betroffenen Person erfordern, hat die Einwilligung künftig folgende Vorgaben zu erfüllen: angemessene vorgängige Information, ausdrückliche Einwilligung bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen sowie Freiwilligkeit der Einwilligung.

Pflichten gegenüber EDÖB

Es ist zu prüfen, ob die Datensammlungen der geänderten Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) unterliegen. Das Formular zur Anmeldung der Datensammlungen ist auf der Website des EDÖB unter *www.edoeb.admin.ch* abrufbar (Rubrik «Dienstleistungen»).

Bei grenzüberschreitenden Datenbekanntgaben besteht gegenüber dem EDÖB eine Informationspflicht, wenn die ausländische Gesetzgebung keinen angemessenen Schutz gewährleistet und dieser Mangel durch andere Garantien (z.B. eine vertragliche Regelung mit dem ausländischen Datenempfänger) oder bei konzerninternen Datentransfers durch konzerninterne Datenschutzregeln ausgeglichen wird.

Auskunftsrecht der betroffenen Person

Die um Auskunft angefragten Stellen sind künftig auch zur Mitteilung der verfügbaren Angaben über die Herkunft der Daten verpflichtet.

Beizug Dritter für Datenbearbeitungen (Outsourcing)

Im Hinblick auf Haftungsfragen empfiehlt es sich, im Outsourcing-Vertrag die datenschutzrechtlichen Pflichten der Vertragsparteien klar zu regeln. Das gilt gemäss revidiertem DSG insbesondere bezüglich Datensicherheit.

Folgende Massnahmen sind freiwillig und befreien die privaten Datenbearbeiter von der Meldepflicht für Datensammlungen, wenn sie ergriffen werden: **Bezeichnung eines Datenschutzverantwortlichen oder Teilnahme an Zertifizierungsverfahren.**

II. Änderungen im Einzelnen

1. Verstärkung des Transparenzprinzips

1.1 Allgemeines

Im Zentrum der Revision steht die Verstärkung des Transparenzprinzips. Es handelt sich dabei nicht um ein neues Prinzip. Bereits aus dem im geltenden DSG enthaltenen Grundsatz von Treu und Glauben wird abgeleitet, dass die Datenbearbeitung für die betroffene Person transparent erfolgen muss. Ziel der Revision ist es, dieses Prinzip durch die Aufnahme von expliziten Transparenzvorschriften zu verstärken. Das revidierte Recht unterscheidet zwischen:

- Informationspflicht beim Beschaffen von besonders schützenswerten Daten und Persönlichkeitsprofilen (Art. 7a DSG),
- Erkennbarkeit der Datenbeschaffung bei «gewöhnlichen» Daten (Art. 4 Abs. 4 DSG) sowie
- Information der betroffenen Person vor ihrer Einwilligung (Art. 4 Abs. 5 DSG, siehe Ziffer III. der Erläuterungen).

Im Zusammenhang mit diesen neuen Transparenzvorschriften gilt es zu beachten, dass das revidierte VVG neu ebenfalls eine einschlägige Informationspflicht enthält. Es stellt sich daher die Frage nach dem Verhältnis dieser neuen Vorschriften (siehe Ziffer II. 1.4 der Erläuterungen).

1.2 Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen

Neu trifft den Inhaber von Datensammlungen eine Informationspflicht, wenn er besonders schützenswerte Personendaten (z.B. Daten über die Gesundheit oder Vorstrafen) oder Persönlichkeitsprofile natürlicher Personen (z.B. Interessenprofile) beschafft (Art. 7a DSG). In diesen Fällen muss der Inhaber der Datensammlung der betroffenen Person künftig mindestens folgende Angaben machen:

- **Inhaber der Datensammlung;** die Angaben sollten so präzise sein, dass die betroffene Person bei Bedarf weiss, gegenüber wem sie ihre Rechte nach DSG – z.B. das Auskunftsrecht (Art. 8 DSG) – wahrnehmen kann.
- **Zweck des Bearbeitens;** es sollten die beabsichtigten Bearbeitungszwecke angegeben werden.
- **Kategorien der Datenempfänger;** es genügt, die Kategorien möglicher Datenempfänger anzugeben (z.B. Vorversicherer, Ärzte, UVG-Versicherer etc.). Es müssen nicht die einzelnen Datenempfänger erwähnt werden.

Die Informationspflicht gilt, wenn die Daten bei der betroffenen Person oder bei Dritten erhoben werden. Der wesentliche Unterschied bei der Erhebung bei Dritten ist der Zeitpunkt der Information: Sie hat spätestens mit der Speicherung der Daten oder der ersten Bekanntgabe an Dritte zu erfolgen.

Der neue Art. 7a DSG äussert sich nicht zur Form der Information. Sie kann daher schriftlich oder mündlich erfolgen. Zu Beweiszwecken empfiehlt sich jedoch eine schriftliche Information. Die Information muss bei der erstmaligen Beschaffung der Daten bzw. Profile erfolgen. Bei weiteren Erhebungen muss sie nicht wiederholt werden, wenn der Inhaber der Datensammlung, der Zweck der Datenbearbeitung und die Kategorien der Datenempfänger denen der erstmaligen Beschaffung entsprechen.

Das revidierte Recht sieht eine Reihe von Ausnahmen vor, bei denen die Informationspflicht entfällt (siehe Art. 7a und 9 DSG):

- Die betroffene Person ist über die von Art. 7a DSG geforderten Angaben **bereits informiert,** z.B. aufgrund einer Information gemäss VVG (Art. 3 Abs. 1 lit. g bzw. Abs. 3 VVG) oder diese Angaben ergeben sich klar aus den konkreten Umständen.
- Die Information ist **nicht möglich** oder würde einen **unverhältnismässigen Aufwand** erfordern.
- Es liegt eine entsprechende **gesetzliche Vorschrift** vor.
- Die Einschränkung der Informationspflicht ist wegen **überwiegender Interessen Dritter** nötig oder **eigene überwiegende Interessen** erfordern es und die Personendaten werden nicht Dritten bekannt gegeben.

Zur Umsetzung der neuen Informationspflicht ist eine Übergangsfrist von einem Jahr nach Inkrafttreten des revidierten Rechts vorgesehen (Art. 38 DSG). Nach Ablauf dieser einjährigen Übergangsfrist wird die vorsätzliche Nichteinhaltung der Informationspflicht auf Antrag der betroffenen Person mit Haft oder Busse bestraft (Art. 34 DSG).

1.3 Erkennbarkeit der Beschaffung bei «gewöhnlichen» Personendaten

Die neue Informationspflicht gemäss Art. 7a DSG ist auf die Beschaffung von besonders schützenswerten Daten und Persönlichkeitsprofilen beschränkt. Bei der Bearbeitung von gewöhnlichen Daten genügt es gemäss neuem Recht, wenn deren Beschaffung und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sind.

Die Anforderungen, die erfüllt sein müssen, damit eine «erkennbare» Beschaffung vorliegt, sind gemäss Botschaft nach den Umständen sowie nach den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben zu beurteilen. Die betroffene Person muss mit angemessenen Mitteln auf die Datenerhebung und den Zweck der Bearbeitung aufmerksam gemacht werden, falls die Beschaffung nicht erkennbar ist (S. 2125 f. Botschaft).

Ist die nötige Erkennbarkeit nicht gegeben, wird dies – im Gegensatz zur Verletzung der Informationspflicht – nicht strafrechtlich geahndet. Es kann aber eine widerrechtliche Persönlichkeitsverletzung und damit zivilrechtliche Forderungen der betroffenen Person zur Folge haben (Art. 12 Abs. 2 lit. a DSG in Verbindung mit Art. 15 DSG).

Im Unterschied zur Informationspflicht hat es der Gesetzgeber unterlassen, Ausnahmen von der Erkennbarkeit vorzusehen. Im Sinne einer systematischen Auslegung des DSG sollten jedoch die Ausnahmen, die beim Beschaffen von besonders schützenswerten Daten gelten, auch bei gewöhnlichen Daten, die über weniger Gefährdungspotenzial verfügen, analog zur Anwendung kommen.

1.4 Informationspflicht des revidierten VVG

Die Versicherer müssen die Versicherungsnehmer seit 1. Januar 2007 darüber informieren, wie mit ihren Daten umgegangen wird (Art. 3 Abs. 1 lit. g VVG). Dazu gehören Angaben zur Bearbeitung der Personendaten einschliesslich Zweck und Art der Datensammlung sowie Empfänger und Aufbewahrung der Daten. Eine analoge Pflicht statuiert das VAG für die Vermittler (Art. 45 Abs. 1 lit. e VAG).

Es stellt sich daher die Frage nach dem Verhältnis der Informationspflicht nach VVG zu den neuen Transparenzbestimmungen des DSG. Das VVG und das DSG sowie die Materialien zu diesen Revisionen äussern sich nicht zu dieser Frage. Ein Vergleich zeigt, dass der Zweck dieser neuen Bestimmungen identisch ist. Es geht um die Verstärkung des Transparenzprinzips. Im Übrigen unterscheiden sich die Bestimmungen aber in folgender Hinsicht:

- **Anwendungsbereich:** Die Informationspflicht nach VVG ist eine branchenspezifische Norm, die ihre Grundlage im Verhältnis zwischen dem Versicherer und dem Antragsteller (künftigen Versicherungsnehmer) hat. Sie gilt für die Bearbeitung jeglicher Daten, richtet sich aber nur an die Versicherungsnehmer und gestützt auf Art. 3 Abs. 3 VVG an die versicherten Personen bei kollektiven Personenversicherungen, nicht aber an die übrigen versicherten und begünstigten Personen und auch nicht an die Geschädigten in der Haftpflichtversicherung. Demgegenüber ist die Informationspflicht nach DSG branchenunabhängig und gilt für private und staatliche Stellen, zu denen auch die Sozialversicherer gehören. Sie kommt nur bei der Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen zur Anwendung, gilt dann aber gegenüber allen versicherten, begünstigen und geschädigten Personen.
- **Umfang:** Die Informationspflicht nach VVG verpflichtet zu mehr Angaben als die Informationspflicht des DSG. Weiter sieht das VVG im Gegensatz zum DSG keine Ausnahmen vor, bei denen die Informationspflicht entfällt.

- **Sanktion:** Bei Nichteinhaltung der Informationspflicht gemäss VVG verfügt der Versicherungsnehmer über ein Kündigungsrecht (Art. 3a VVG). Dabei handelt es sich um eine privatrechtliche Sanktion. Demgegenüber ist die Sanktion bei Art. 7a DSG öffentlich-rechtlicher Natur (Haft oder Busse).

Diese Unterschiede legen den Schluss nahe, dass die branchenunabhängige Informationspflicht des DSG in der Informationspflicht des VVG aufgeht und Art. 7a sowie Art. 4 Abs. 4 DSG für die Versicherer subsidiären Charakter haben. Dafür spricht auch, dass die Informationspflicht nach DSG entfällt, wenn die betroffene Person bereits informiert wurde (Art. 7a Abs. 4 DSG).

1.5 Beispiele zur Informationspflicht gemäss DSG und VVG

Vertragsabschluss

Der Versicherer informiert den Versicherungsnehmer vor Vertragsabschluss gemäss VVG. Diese Information umfasst auch die von Art. 7a DSG geforderten Angaben (Inhaber der Datensammlung, Zweck des Bearbeitens, Kategorien der Datenempfänger). Das gilt – mit Ausnahme der Transportversicherung – für alle Erstversicherungsverträge und für die Kollektivversicherungen (Art. 3 Abs. 1 lit. g bzw. Abs. 3 VVG). ⇢ Eine Information nach Art. 7a DSG ist nicht erforderlich. Das VVG geht als lex specialis dem DSG vor.

Schadenfall

Schadenfall eines Versicherungsnehmers: Es gilt der Grundsatz der lex specialis, soweit der Versicherer in der vorvertraglichen Information nach VVG ausreichend über die Datenbearbeitung im Schadenfall orientiert hat. ⇢ Eine zusätzliche Information nach DSG erscheint nicht notwendig.

Kollektive Krankentaggeldversicherung: Ein Arbeitnehmer erkrankt und der Arbeitgeber meldet dem Versicherer den Schadenfall. Es gilt der Grundatz der lex specialis, soweit der Arbeitgeber den Arbeitnehmer aufgrund entsprechender Unterlagen des Versicherers nach Art. 3 Abs. 3 VVG ausreichend über die Datenbearbeitung im Schadenfall (Krankheit) informiert hat. ⇢ Eine zusätzliche Information nach DSG erscheint nicht notwendig.

Haftpflichtfall: Der Geschädigte meldet seine Ansprüche bei der Haftpflichtversicherung des Schädigers an. Diese benötigt zur Schadenprüfung Gesundheitsdaten des Geschädigten. Für die Einholung von Auskünften bei Ärzten muss der Geschädigte diese vom Arztgeheimnis entbinden. ⇢ Es liegt ein Anwendungsfall von Art. 7a DSG vor. Die von dieser Bestimmung geforderten Angaben dürften sich in der Regel aus den konkreten Umständen ergeben, wenn die Korrespondenz über den Schadenfall direkt zwischen dem Geschädigten und dem Versicherer stattfindet, denn dieser wird dann kennen müssen, für welche Zwecke seine Daten bearbeitet werden (Beurteilung der Haftung und Höhe des Schadenersatzes). Eine gesonderte Information ist aber unter Umständen nötig, wenn der Versicherer Gesundheitsdaten des Geschädigten an Dritte (z.B. den UVG-Versicherer) weiterleitet bzw. von Dritten beschafft, da der Geschädigte dies meist nicht schon aus den Umständen herauslesen kann.

Obligatorische Unfallversicherung: Ein Arbeitnehmer verunfallt und der Arbeitgeber meldet den Fall der Unfallversicherung. Diese holt beim Spital einen ärztlichen Zwischenbericht ein. Im Rahmen von Art. 54a UVG bedarf es keiner Entbindung vom Arztgeheimnis. ⇢ Unter Vorbehalt der Ausnahmen gemäss Ziffer II. 1.2 der Erläuterungen muss der Unfallversicherer den betroffenen Arbeitnehmer nach Art. 7a DSG informieren.

2. Änderung von Art. 12 Abs. 2 lit. a DSG

Private und staatliche Stellen müssen bei Datenbearbeitungen die Grundsätze des DSG beachten (Rechtmässigkeit, Treu und Glauben / Transparenz, Verhältnismässigkeit, Zweckbindung, Richtigkeit der Daten und Datensicherheit). Aufgrund des neuen Wortlauts von Art. 12 Abs. 2 lit. a DSG stellt sich die Frage, ob Private eine nicht rechtfertigungsfähige Persönlichkeitsverletzung begehen, wenn sie gegen diese Grundsätze verstossen. Wie die nachfolgenden Überlegungen zeigen, behalten die Rechtfertigungsgründe auch nach der Revision von Art. 12 Abs. 2 lit. a DSG ihre Bedeutung:

- Es gilt der Grundsatz der lex specialis, d.h. die Datenschutzvorschriften in anderen Bundesgesetzen (z.B. im Geldwäschereigesetz) wirken weiterhin rechtfertigend.
- Im Sinne des Rechts auf informationelle Selbstbestimmung sollte auch unter revidiertem Recht eine Einwilligung der betroffenen Person (z.B. in eine Zweckänderung) zulässig sein, sofern die Einwilligung die Vorgaben des neuen Art. 4 Abs. 5 DSG erfüllt.
- Dass überwiegende Interessen der Datenbearbeiter weiterhin rechtfertigend sind, ergibt sich bereits aus dem Grundsatz der Verhältnismässigkeit der Datenbearbeitung. Dieser verlangt – auch bei Datenbearbeitungen von privaten Stellen – die Prüfung der Geeignetheit und der Erforderlichkeit sowie eine Abwägung der entgegenstehenden Interessen des Datenbearbeiters und der betroffenen Person.

Diese Beurteilung der Änderung von Art. 12 Abs. 2 lit. a DSG wird durch die Auslegungshilfe des Bundesamtes für Justiz, die im Anhang der Broschüre aufgeführt wird, gestützt.

3. Meldepflicht für Datensammlungen

Das Register der Datensammlungen des EDÖB wird im revidierten DSG beibehalten. Datensammlungen sind somit vor ihrer Eröffnung weiterhin beim EDÖB anzumelden, sofern sie unter die geänderte Meldepflicht fallen: Neu müssen grundsätzlich alle Datensammlungen angemeldet werden, in welchen regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder aus denen regelmässig Personendaten an Dritte bekannt gegeben werden. Die Kenntnis der betroffenen Personen von den Datensammlungen befreit nicht mehr von der Meldepflicht. Dieser Grundsatz wird durch eine Reihe von Ausnahmen durchbrochen. Keine Meldepflicht besteht in folgenden Fällen:

- Die Datenbearbeitung erfolgt aufgrund einer **gesetzlichen Verpflichtung** (wie bisher).
- Der Inhaber der Datensammlung verfügt über einen **Datenschutzverantwortlichen,** der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und Verzeichnisse der Datensammlungen führt (neue Ausnahme). Die Stellung und die Aufgaben des Datenschutzverantwortlichen werden in der VDSG geregelt (siehe Art. 12a und 12b Vernehmlassungsentwurf VDSG vom 18. Januar 2006, abrufbar unter *www.admin.ch,* Rubrik «Dokumentation»).
- Aufgrund eines Zertifizierungsverfahrens hat der Inhaber der Datensammlung ein **Datenschutz-Qualitätszeichen** erworben und das Ergebnis der Bewertung dem EDÖB mitgeteilt (neue Ausnahme). Die konkrete Ausgestaltung des Zertifizierungsverfahrens erfolgt in einer neuen Verordnung des Bundesrates (siehe Vernehmlassungsentwurf VDSZ vom 1. Februar 2007, abrufbar unter *www.admin.ch,* Rubrik «Dokumentation»).
- Der Bundesrat kann **weitere Ausnahmen in der VDSG** vorsehen, wenn die Rechte der Betroffenen nicht gefährdet sind (wie bisher, siehe Art. 4 Vernehmlassungsentwurf VDSG vom 18. Januar 2006).

4. Grenzüberschreitende Datenbekanntgabe

4.1 Angemessener ausländischer Datenschutz

In materieller Hinsicht hält das revidierte Recht am Grundsatz fest, dass ein Datentransfer ins Ausland nur zulässig ist, wenn die dortige Gesetzgebung einen angemessenen (aber nicht mehr zwingend gleichwertigen) Schutz gewährleistet. Es wird auf die Liste der Staaten mit angemessener Datenschutzgesetzgebung verwiesen, die der EDÖB erstellen wird (Art. 7 Vernehmlassungsentwurf VDSG vom 18. Januar 2006).

Dieser Grundsatz wird im revidierten Recht durch eine Reihe von Ausnahmen durchbrochen, bei denen der Datentransfer zulässig ist, obwohl im Ausland ein angemessener Schutz fehlt (siehe abschliessende Liste der Ausnahmen in Art. 6 Abs. 2 DSG). In der Praxis sind insbesondere folgende Ausnahmen von Relevanz:

- vertragliche Regelung mit dem ausländischen Empfänger der Daten,
- Abschluss oder Abwicklung eines Vertrages oder
- Prozess im Ausland.

4.2 Informationspflicht gegenüber EDÖB

In formeller Hinsicht entfällt künftig die Meldepflicht gegenüber dem EDÖB für die Übermittlung von Datensammlungen ins Ausland. Sie wird ersetzt durch eine Informationspflicht.

Diese besteht aber nur, wenn die ausländische Gesetzgebung mangelhaft ist und dieser Mangel durch hinreichende andere Garantien (z.B. eine vertragliche Regelung mit dem ausländischen Empfänger der Daten) oder bei konzerninternen Datentransfers durch konzerninterne Datenschutzregeln ausgeglichen wird. In diesen Fällen ist der EDÖB über die Garantien bzw. die konzerninternen Datenschutzregeln zu informieren (Art. 6 Abs. 3 DSG).

5. Auskunftsrecht

Das DSG gewährt den Personen, die von Datenbearbeitungen betroffen sind, ein Auskunftsrecht. Das Auskunftsrecht verpflichtet den Inhaber der Datensammlung auf Ersuchen der betroffenen Person zu bestimmten, vom DSG vorgeschriebenen Angaben, wie u.a. Mitteilung der zur betroffenen Person vorhandenen Daten.

Dieser Katalog der Angaben wurde mit der Revision erweitert, indem neu die Mitteilung der «verfügbaren Angaben über die Herkunft der Daten» zum Katalog der Auskünfte gehört (Art. 8 Abs. 2 lit. a DSG).

6. Beizug Dritter für Datenbearbeitungen (Outsourcing)

Es ist die Outsourcing-Bestimmung des DSG zu beachten, wenn die Datenbearbeitung einem Dritten übertragen wird (z.B. einem Treuhandunternehmen). Bezüglich dieser Bestimmung sieht das revidierte Recht folgende Änderungen vor:

- Neu gilt die Bestimmung von Art. 10a DSG auch für staatliche Stellen, zu denen auch die Sozialversicherer gehören. Bislang kam sie nur in der Privatwirtschaft zur Anwendung.
- Die Grundsätze des DSG sind gemäss bisherigem und revidiertem Recht auch bei der Auslagerung der Datenbearbeitung zu beachten (Rechtmässigkeit, Treu und Glauben / Transparenz, Verhältnismässigkeit, Zweckbindung, Richtigkeit der Daten und Datensicherheit). Für den Grundsatz der Datensicherheit hält dies das revidierte Recht explizit fest, indem es den Auftraggeber verpflichtet, sich insbesondere zu vergewissern, dass der Dritte die Datensicherheit gewährleistet. Im Hinblick auf Haftungsfragen empfiehlt es sich daher, im Outsourcing-Vertrag die datenschutzrechtlichen Pflichten der Vertragsparteien – insbesondere bezüglich der Datensicherheit (siehe dazu Art. 7 DSG in Verbindung mit Art. 8 ff. VDSG) – klar zu regeln.

III. Einwilligung der betroffenen Person

1. Einleitung

1.1 Anwendungsbereich des neuen Art. 4 Abs. 5 DSG

Der neue Art. 4 Abs. 5 DSG ist zu beachten, wenn für die Datenbearbeitung die Einwilligung der betroffenen Person erforderlich ist:

- Private Stellen müssen eine Einwilligung einholen, wenn die Datenbearbeitung eine Persönlichkeitsverletzung zur Folge haben kann und dafür kein anderer Rechtfertigungsgrund gegeben ist (Art. 12 und 13 DSG). Diesbezüglich ist voraussichtlich die **Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofile an Dritte** der wichtigste Anwendungsfall für eine Einwilligung. Eine Einwilligung kann auch für die Abweichung von den Datenbearbeitungsgrundsätzen abgegeben werden (siehe Ziffer II. 2 der Erläuterungen). Die diesbezüglichen Anwendungsfälle sind wohl aber begrenzt, da es kaum denkbar ist, dass die betroffene Person eine gültige, d.h. informierte und freiwillige Einwilligung, z.B. in eine unrechtmässige Datenbearbeitung oder eine Bearbeitung mit unrichtigen Daten, geben wird.
- Eine Einwilligung steht weiter bei **grenzüberschreitenden Datenbekanntgaben** zur Diskussion (Art. 6 Abs. 2 lit. b DSG).

1.2 Bedeutung dieser Bestimmung

In den oben genannten Fällen hat die Einwilligung künftig folgende Vorgaben zu erfüllen: angemessene vorgängige Information, ausdrückliche Einwilligung bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen sowie Freiwilligkeit der Einwilligung.

Die Einwilligung ist ungültig, wenn diese Vorgaben nicht eingehalten werden. Eine ungültige Einwilligung kann nicht als Rechtfertigungsgrund angerufen werden.

2. Voraussetzungen einer gültigen Einwilligung nach Art. 4 Abs. 5 DSG

2.1 Angemessene vorgängige Information

Die vorgängige Information muss angemessen sein. Der Begriff der Angemessenheit wird im revidierten Recht nicht definiert. Gemäss Botschaft soll die vorgängige Information der betroffenen Person eine freie Entscheidung bezüglich der Bearbeitung ihrer persönlichen Daten ermöglichen (S. 2127 Botschaft).

Folgende Informationen sollten vorgängig mitgeteilt werden:

- Massgebend ist der Anwendungsbereich der Einwilligung (siehe Ziffer III. 1.1 der Erläuterungen), d.h., die Einwilligungsklausel ist passend zum Anwendungsbereich der Einwilligung zu formulieren. Für gleichartige Anwendungsfälle können standardisierte Texte verwendet werden. Beim voraussichtlich wichtigsten Anwendungsfall der Bekanntgabe von besonders schützenswerten Personendaten an Dritte sollte über den Zweck der Weitergabe dieser Daten und die Kategorien der Datenempfänger informiert werden.
- Gemäss Botschaft soll über die Nachteile orientiert werden, die sich aus der Verweigerung der Einwilligung ergeben können (S. 2127 Botschaft).

2.2 Form der Einwilligung

Es kommt darauf an, welche Daten von der Einwilligung betroffen sind:

- Falls für die Bearbeitung von besonders schützenswerten Personendaten (z.B. Gesundheitsdaten oder Vorstrafen) oder Persönlichkeitsprofilen eine Einwilligung erforderlich ist, ist eine ausdrückliche Zustimmung der betroffenen Person einzuholen. Eine aus den Umständen abgeleitete, konkludente Erklärung genügt nicht. Die Einwilligung hat gemäss Botschaft umso klarer zu erfolgen, je sensibler die fraglichen Personendaten sind (S. 2127 f. Botschaft). Aus Beweiszwecken empfiehlt es sich, die Einwilligung in Schriftform einzuholen.
- In den übrigen Fällen kann die Einwilligung formfrei und stillschweigend erfolgen.

2.3 Freiwilligkeit der Einwilligung

Die Einwilligung muss freiwillig, d.h. frei von Zwang, erfolgen. Bei dieser Voraussetzung kommt es darauf an, welche Nachteile die Verweigerung der Einwilligung zur Folge haben kann. Gemäss Botschaft liegt eine freiwillige Einwilligung vor, wenn der Nachteil einen Bezug zum Zweck der Bearbeitung hat bzw. diesem Zweck gegenüber verhältnismässig ist (S. 2127 Botschaft).

In diesem Sinne und da der Nachweis des Versicherungsanspruchs dem Versicherungsnehmer / Anspruchsberechtigten obliegt, sollte es z.B. unproblematisch sein, wenn der Versicherer im Schadenfall darauf hinweist, dass er bei Nichterteilung der Einwilligung die erforderlichen Abklärungen nicht vornehmen kann, was zu einer ungenügenden Substantiierung des Schadens und damit zur Ablehnung der Versicherungsleistung führen kann.

Es versteht sich von selbst, dass eine freiwillige Einwilligung jederzeit widerrufen werden kann. Im Rahmen eines anderen Rechtfertigungsgrundes, d.h. eines überwiegenden Interesses des Datenbearbeiters oder einer entsprechenden gesetzlichen Bestimmung, kann die fragliche Datenbearbeitung aber trotz Widerruf zulässig sein.

Gesetzestext mit Änderung vom 24. März 2006

Änderungen sind blau markiert

Bundesgesetz über den Datenschutz (DSG)

vom 19. Juni 1992

Die Bundesversammlung der Schweizerischen Eidgenossenschaft, gestützt auf die Artikel 31bis Absatz 2, 64, 64bis und 85 Ziffer 1 der Bundesverfassung nach Einsicht in die Botschaft des Bundesrates vom 23. März 1988 / **19. Februar 2003,** beschliesst:

1. Abschnitt: Zweck, Geltungsbereich und Begriffe

Art. 1 Zweck

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

Art. 2 Geltungsbereich

1 Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch:

a. private Personen;
b. Bundesorgane.

2 Es ist nicht anwendbar auf:

a. Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt;
b. Beratungen in den Eidgenössischen Räten und in den parlamentarischen Kommissionen;
c. hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren;
d. öffentliche Register des Privatrechtsverkehrs;
e. Personendaten, die das Internationale Komitee vom Roten Kreuz bearbeitet.

Art. 3 Begriffe

Die folgenden Ausdrücke bedeuten:

a. Personendaten (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;
b. betroffene Personen: natürliche oder juristische Personen, über die Daten bearbeitet werden;
c. besonders schützenswerte Personendaten: Daten über:
   1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
   2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
   3. Massnahmen der sozialen Hilfe,
   4. administrative oder strafrechtliche Verfolgungen und Sanktionen;
d. Persönlichkeitsprofil: eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;
e. Bearbeiten: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekannt geben, Archivieren oder Vernichten von Daten;
f. Bekannt geben: das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen;
g. Datensammlung: jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind;
h. Bundesorgane: Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind;
~~j.~~ **i.** Inhaber der Datensammlung: private Personen oder Bundesorgane, die über den Zweck und den Inhalt ~~einer~~**der** Datensammlung entscheiden;
~~k.~~ **j.** ~~formelles~~ Gesetz **im formellen Sinn:**
   1. Bundesgesetze ~~und referendumspflichtige allgemeinverbindlicheBundesbeschlüsse,~~
   2. für die Schweiz verbindliche Beschlüsse internationaler Organisationen und von der Bundesversammlung genehmigte völkerrechtliche Verträge mit Recht setzendem Inhalt.

2. Abschnitt: Allgemeine Datenschutzbestimmungen

Art. 4 Grundsätze

1 Personendaten dürfen nur rechtmässig ~~beschafft~~ **bearbeitet** werden.

2 Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

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

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

5 Ist für die Bearbeitung von Personendaten die Zustimmung der betroffenen Person erforderlich, so ist diese Zustimmung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Zustimmung zudem ausdrücklich erfolgen.

Art. 5 Richtigkeit der Daten

1 Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. **Es sind alle angemessenen Massnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie beschafft oder bearbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden.**

2 Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden.

Art. 6 ~~Bekanntgabe ins Ausland~~ Grenzüberschreitende Bekanntgabe

1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ~~ein Datenschutz~~ **eine Gesetzgebung** fehlt, ~~der dem schweizerischen gleichwertig ist~~ **die einen angemessenen Schutz gewährleistet**.

~~2 Wer Datensammlungen ins Ausland übermitteln will, muss dies dem Eidgenössischen Datenschutzbeauftragten vorher melden, wenn:~~
~~a. für die Bekanntgabe keine gesetzliche Pflicht besteht und~~
~~b. die betroffenen Personen davon keine Kenntnis haben.~~

Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können persönliche Daten ins Ausland nur bekannt gegeben werden, wenn:

a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
b. die betroffene Person im Einzelfall zugestimmt hat;
c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;
d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;
f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;
g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

~~3 Der Bundesrat regelt die Meldungen im Einzelnen. Er kann vereinfachte Meldungen oder Ausnahmen von der Meldepflicht vorsehen, wenn das Bearbeiten die Persönlichkeit der betroffenen Personen nicht gefährdet.~~ **Der Beauftragte muss über die Garantien nach Absatz 2 Buchstabe a und die einheitlichen Datenschutzregeln nach Absatz 2 Buchstabe g informiert werden. Der Bundesrat regelt die Einzelheiten dieser Informationspflicht.**

Art. 7 Datensicherheit

1 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

2 Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit.

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

1 Der Inhaber der Datensammlung ist verpflichtet, die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen zu informieren; diese Informationspflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden.

2 Der betroffenen Person sind mindestens mitzuteilen:

a. der Inhaber der Datensammlung;

b. der Zweck des Bearbeitens;

c. die Kategorien der Datenempfänger, wenn eine Datenbekanntgabe vorgesehen ist.

3 Wenn Daten nicht bei der betroffenen Person beschafft werden, hat deren Information spätestens bei Beginn der Speicherung der Daten, oder, wenn auf die Speicherung verzichtet wird, mit der ersten Bekanntgabe an Dritte zu erfolgen.

4 Die Informationspflicht des Inhabers der Datensammlung entfällt, wenn die betroffene Person bereits informiert wurde, oder, in Fällen nach Absatz 3, wenn:

a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist; oder

b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

Art. 8 Auskunftsrecht

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

2 Der Inhaber der Datensammlung muss ~~ihr~~ **der betroffenen Person** mitteilen:

a. alle über sie in der Datensammlung vorhandenen Daten **einschliesslich der verfügbaren Angaben über die Herkunft der Daten;**

b. den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.

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

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

5 Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen. Der Bundesrat regelt die Ausnahmen.

6 Niemand kann im Voraus auf das Auskunftsrecht verzichten.

Art. 9 Einschränkungen der Informationspflicht und des Auskunftsrechts; im Allgemeinen

1 Der Inhaber der Datensammlung kann **die Information nach Artikel 7a oder** die Auskunft **nach Artikel 8** verweigern, einschränken oder aufschieben, soweit:

a. ein ~~formelles~~ Gesetz **im formellen Sinn** dies vorsieht;

b. es wegen überwiegender Interessen ~~eines~~ Dritter~~n~~ erforderlich ist.

2 Ein Bundesorgan kann zudem **die Information oder** die Auskunft verweigern, einschränken oder aufschieben, soweit:

a. es wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich ist;

b. **die Information oder** die Auskunft den Zweck einer Strafuntersuchung oder eines andern Untersuchungsverfahrens in Frage stellt.

3 ~~Private als~~ **Der private** Inhaber einer Datensammlung ~~können~~ **kann** zudem **die Information oder** die Auskunft verweigern, einschränken oder aufschieben, soweit eigene überwiegende Interessen es erfordern und ~~sie~~ **er** die Personendaten nicht ~~an~~ Dritte**n** bekannt ~~geben~~ **gibt.**

4 Der Inhaber der Datensammlung muss angeben, aus welchem Grund er die Auskunft verweigert, einschränkt oder aufschiebt.

Art. 10 Einschränkungen des Auskunftsrechts für Medienschaffende

1 Der Inhaber einer Datensammlung, die ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet wird, kann die Auskunft verweigern, einschränken oder aufschieben, soweit:

a. die Personendaten Aufschluss über die Informationsquellen geben;
b. Einblick in Entwürfe für Publikationen gegeben werden müsste;
c. die freie Meinungsbildung des Publikums gefährdet würde.

2 Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen eine Datensammlung ausschliesslich als persönliches Arbeitsinstrument dient.

Art. ~~14~~ 10a Datenbearbeitung durch Dritte

1 Das Bearbeiten von Personendaten kann **durch Vereinbarung oder Gesetz** ~~einem~~ Dritten übertragen werden, wenn:

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

2 Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.

~~2~~**3** ~~Der~~ Dritte ~~kann~~ **können** dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.

Art. 11 Zertifizierungsverfahren

1 Um den Datenschutz und die Datensicherheit zu verbessern, können die Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Bundesbehörden, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

2 Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.

Art. 11a Register der Datensammlungen

1 Der Eidgenössische Datenschutzbeauftragte führt ein Register der Datensammlungen**, das über Internet zugänglich ist**. Jede Person kann das Register einsehen.

2 Bundesorgane müssen sämtliche Datensammlungen beim Datenschutzbeauftragten zur Registrierung anmelden.

3 Private Personen~~, die regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder Personendaten an Dritte bekannt geben,~~ müssen **Datens**Sammlungen anmelden, wenn:

a. ~~für das Bearbeiten keine gesetzliche Pflicht besteht und~~ **regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden; oder**
b. ~~die betroffenen Personen davon keine Kenntnis haben.~~ **regelmässig Personendaten an Dritte bekannt gegeben werden.**

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

5 Entgegen den Bestimmungen der Absätze 2 und 3 muss der Inhaber von Datensammlungen seine Sammlungen nicht anmelden, wenn:

a. private Personen Daten aufgrund einer gesetzlichen Verpflichtung bearbeiten;
b. der Bundesrat eine Bearbeitung von der Anmeldepflicht ausgenommen hat, weil sie die Rechte der betroffenen Personen nicht gefährdet;

c. er 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;
d. die Daten durch einen Journalisten oder eine Journalistin bearbeitet werden, dem oder der die Datensammlung ausschliesslich als persönliches Arbeitsinstrument dient;
e. er einen Datenschutzverantwortlichen bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und Verzeichnisse der Datensammlungen führt;
f. er aufgrund eines Zertifizierungsverfahrens nach Artikel 11 ein Datenschutz-Qualitätszeichen erworben hat und das Ergebnis der Bewertung dem Datenschutzbeauftragten mitgeteilt wurde.

56 Der Bundesrat regelt **die Modalitäten der** ~~die~~ Anmeldung der Datensammlungen, ~~sowie die~~ **der** Führung und ~~die~~ **der** Veröffentlichung des Registers **sowie die Stellung und die Aufgaben der Datenschutzverantwortlichen nach Absatz 5 Buchstabe e und die Veröffentlichung eines Verzeichnisses der Inhaber der Datensammlungen, welche nach Absatz 5 Buchstaben e und f der Meldepflicht enthoben sind.** ~~Er kann für bestimmte Arten von Datensammlungen Ausnahmen von der Meldepflicht oder der Registrierung vorsehen, wenn das Bearbeiten die Persönlichkeit der betroffenen Personen nicht gefährdet.~~

3. Abschnitt: Bearbeiten von Personendaten durch private Personen

Art. 12 Persönlichkeitsverletzungen

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

2 Er darf insbesondere nicht ~~ohne Rechtfertigungsgrund~~:
a. Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 ~~6 Absatz 1~~ und 7 Absatz 1 bearbeiten;
b. **ohne Rechtfertigungsgrund** Daten einer Person gegen deren ausdrücklichen Willen bearbeiten;
c. **ohne Rechtfertigungsgrund** besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben.

3 In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Art. 13 Rechtfertigungsgründe

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

2 Ein überwiegendes Interesse der bearbeitenden Person fällt insbesondere in Betracht, wenn diese:
a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;
b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben;
c. zur Prüfung der Kreditwürdigkeit einer anderen Person weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile bearbeitet und Dritten nur Daten bekannt gibt, die sie für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen;
d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet;
e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind;
f. Daten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Art. 15 Rechtsansprüche und Verfahren

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

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

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

4 Über Klagen zur Durchsetzung des Auskunftsrechts entscheidet der Richter in einem einfachen und raschen Verfahren.

4. Abschnitt: Bearbeiten von Personendaten durch Bundesorgane

Art. 16 Verantwortliches Organ und Kontrolle

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

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

Art. 17 Rechtsgrundlagen

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

2 Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen sie nur bearbeiten, wenn ein ~~formelles~~ Gesetz **im formellen Sinn** es ausdrücklich vorsieht oder wenn ausnahmsweise:

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

Art. 17a Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen

1 Der Bundesrat kann, nachdem er die Stellungnahme des Datenschutzbeauftragten eingeholt hat, vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen bewilligen, wenn:

a. die Aufgaben, die diese Bearbeitung erforderlich machen, in einem Gesetz im formellen Sinn geregelt sind;
b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden; und
c. die praktische Umsetzung einer Datenbearbeitung eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn zwingend erfordert.

2 Die praktische Umsetzung einer Datenbearbeitung kann eine Testphase dann zwingend erfordern, wenn:

a. die Erfüllung einer Aufgabe technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen,
b. die Erfüllung einer Aufgabe bedeutende organisatorische oder technische Massnahmen erfordert, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone; oder wenn
c. sie die Übermittlung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen an kantonale Behörden mittels eines Abrufverfahrens erfordert.

3 Der Bundesrat regelt die Modalitäten der automatisierten Datenbearbeitung in einer Verordnung.

4 Das zuständige Bundesorgan legt dem Bundesrat spätestens innert zwei Jahren nach Inbetriebnahme des Pilotsystems einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor.

5 Die automatisierte 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, welches die erforderliche Rechtsgrundlage umfasst.

Art. 18 Beschaffen von Personendaten

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

~~2 Das Beschaffen von besonders schützenswerten Personendaten sowie von Persönlichkeitsprofilen muss für die betroffenen Personen erkennbar sein.~~

Art. 19 Bekanntgabe von Personendaten

1 Bundesorgane dürfen Personendaten bekannt geben, wenn dafür **eine** Rechtsgrundlage~~n~~ im Sinne von Artikel 17 bestehe~~nt~~ oder wenn:

a. die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind;
b. die betroffene Person im Einzelfall eingewilligt hat ~~oder die Einwilligung nach den Umständen vorausgesetzt werden darf~~;
c. die betroffene Person ihre Daten allgemein zugänglich gemacht **und eine Bekanntgabe nicht ausdrücklich untersagt** hat; oder
d. der Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder die Bekanntgabe sperrt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher wenn möglich Gelegenheit zur Stellungnahme zu geben.

1bis Bundesorgane dürfen im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn:

a. die betreffenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen; und
b. an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

2 Bundesorgane dürfen auf Anfrage Name, Vorname, Adresse und Geburtsdatum einer Person auch bekannt geben, wenn die Voraussetzungen von Absatz 1 nicht erfüllt sind.

3 Bundesorgane dürfen Personendaten durch ein Abrufverfahren zugänglich machen, wenn dies ausdrücklich vorgesehen ist. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein formelles Gesetz es ausdrücklich vorsieht.

3bis Bundesorgane dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste jedermann zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie gestützt auf Absatz 1bis Informationen der Öffentlichkeit zugänglich machen. Besteht das öffentliche Interesse an der Zugänglichmachung nicht mehr, so sind die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst zu entfernen.

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

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

Art. 20 Sperrung der Bekanntgabe

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

2 Das Bundesorgan verweigert die Sperrung oder hebt sie auf, wenn:

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

3 Die Sperrung steht unter dem Vorbehalt von Artikel 19 Absatz 1bis.

Art. 21 ~~Anonymisieren und Vernichten von Personendaten~~ Angebot von Unterlagen an das Bundesarchiv

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

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

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

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

Art. 22 Bearbeiten für Forschung, Planung und Statistik

1 Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn:
a. die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt;
b. der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt und
c. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

2 Die Anforderungen der folgenden Bestimmungen müssen nicht erfüllt sein:
a. Artikel 4 Absatz 3 über den Zweck des Bearbeitens
b. Artikel 17 Absatz 2 über die Rechtsgrundlagen für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen;
c. Artikel 19 Absatz 1 über die Bekanntgabe von Personendaten.

Art. 23 Privatrechtliche Tätigkeit von Bundesorganen

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

2 Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.

Art. 24 (Aufgehoben)

Art. 25 Ansprüche und Verfahren

1 Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es:
a. das widerrechtliche Bearbeiten von Personendaten unterlässt;
b. die Folgen eines widerrechtlichen Bearbeitens beseitigt;
c. die Widerrechtlichkeit des Bearbeitens feststellt.

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

3 Der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan:
a. Personendaten berichtigt, vernichtet oder die Bekanntgabe an Dritte sperrt;
b. seinen Entscheid, namentlich die Berichtigung, Vernichtung, Sperre oder den Vermerk über die Bestreitung Dritten mitteilt oder veröffentlicht.

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

5 (Aufgehoben)

Art. 25bis Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten

Solange ein Verfahren betreffend den Zugang zu amtlichen Dokumenten im Sinne des Öffentlichkeitsgesetzes vom 17. Dezember 2004, welche Personendaten enthalten, im Gange ist, kann die betroffene Person im Rahmen dieses Verfahrens die Rechte geltend machen, die ihr aufgrund von Artikel 25 des vorliegenden Gesetzes bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.

5. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Art. 26 Wahl und Stellung

1 Der Beauftragte wird vom Bundesrat gewählt.

2 Er erfüllt seine Aufgaben unabhängig und ist ~~dem Eidgenössischen Justiz- und Polizeidepartement~~ **der Bundeskanzlei** administrativ zugeordnet.

3 Er verfügt über ein ständiges Sekretariat **und ein eigenes Budget**.

Art. 27 Aufsicht über Bundesorgane

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

2 Der Beauftragte klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab.

3 Bei der Abklärung kann er Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Die Bundesorgane müssen an der Feststellung des Sachverhaltes mitwirken. Das Zeugnisverweigerungsrecht nach Artikel 16 des Verwaltungsverfahrensgesetzes gilt sinngemäss.

4 Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, so empfiehlt der Beauftragte dem verantwortlichen Bundesorgan, das Bearbeiten zu ändern oder zu unterlassen. Er orientiert das zuständige Departement oder die Bundeskanzlei über seine Empfehlung.

5 Wird eine Empfehlung nicht befolgt oder abgelehnt, so kann er die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen. Der Entscheid wird den betroffenen Personen mitgeteilt.

6 Der Beauftragte ist berechtigt, gegen die Verfügung nach Absatz 5 und gegen den Entscheid der Beschwerdebehörde Beschwerde zu führen.

Art. 28 Beratung Privater

Der Beauftragte berät private Personen in Fragen des Datenschutzes.

Art. 29 Abklärungen und Empfehlungen im Privatrechtsbereich

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

a. Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler);

b. Datensammlungen registriert werden müssen (Art. 11**a**);

c. ~~Bekanntgaben ins Ausland gemeldet werden müssen (Art. 6)~~ **wenn eine Informationspflicht nach Artikel 6 Absatz 3 besteht.**

2 Er kann dabei Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Das Zeugnisverweigerungsrecht nach Artikel 16 des Verwaltungsverfahrensgesetzes gilt sinngemäss.

3 Der Beauftragte kann aufgrund seiner Abklärungen empfehlen, das Bearbeiten zu ändern oder zu unterlassen.

4 Wird eine solche Empfehlung des Beauftragten nicht befolgt oder abgelehnt, so kann er die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen. **Er ist berechtigt, gegen diesen Entscheid Beschwerde zu führen.**

Art. 30 Information

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

2 In Fällen von allgemeinem Interesse kann er die Öffentlichkeit über seine Feststellungen und Empfehlungen informieren. Personendaten, die dem Amtsgeheimnis unterstehen, darf er nur mit Zustimmung der zuständigen Behörde veröffentlichen. Verweigert diese die Zustimmung, so entscheidet der Präsident der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts endgültig.

Art. 31 Weitere Aufgaben

1 Der Beauftragte hat insbesondere folgende weitere Aufgaben:

a. Er unterstützt Organe des Bundes und der Kantone in Fragen des Datenschutzes.

b. Er nimmt Stellung zu Vorlagen über Erlasse und Massnahmen des Bundes, die für den Datenschutz erheblich sind.

c. Er arbeitet mit in- und ausländischen Datenschutzbehörden zusammen.

d. Er begutachtet, inwieweit ~~der~~ **die** Datenschutz**gesetzgebung** im Ausland ~~dem schweizerischen gleichwertig ist~~ **einen angemessenen Schutz gewährleist.**

e. Er prüft die ihm nach Artikel 6 Absatz 3 gemeldeten Garantien und Datenschutzregeln.

f. Er prüft die Zertifizierungsverfahren nach Artikel 11 und kann dazu Empfehlungen nach Artikel 27 Absatz 4 oder 29 Absatz 3 abgeben.

g. Er nimmt die ihm durch das Öffentlichkeitsgesetz vom 17. Dezember 2004 übertragenen Aufgaben wahr.

2 Er kann Organe der Bundesverwaltung auch dann beraten, wenn dieses Gesetz nach Artikel 2 Absatz 2 Buchstaben c und d nicht anwendbar ist. Die Organe der Bundesverwaltung können ihm Einblick in ihre Geschäfte gewähren.

Art. 32 Aufgaben im Bereich der medizinischen Forschung

1 Der Beauftragte berät die Sachverständigenkommission für das Berufsgeheimnis in der medizinischen Forschung (Art. 321bis StGB).

2 Hat die Kommission die Offenbarung des Berufsgeheimnisses bewilligt, so überwacht er die Einhaltung der damit verbundenen Auflagen. Er kann dazu Abklärungen nach Artikel 27 Absatz 3 vornehmen.

3 Der Beauftragte kann Kommissionsentscheide mit Beschwerde beim Bundesverwaltungsgericht anfechten.

4 Er wirkt darauf hin, dass die Patienten über ihre Rechte informiert werden.

6. Abschnitt: Rechtsschutz

Art. 33

1 Der Rechtsschutz richtet sich nach den allgemeinen Bestimmungen über die Bundesrechtspflege.

2 Stellt der Beauftragte bei einer Sachverhaltsabklärung nach Artikel 27 Absatz 2 oder nach Artikel 29 Absatz 1 fest, dass den betroffenen Personen ein nicht leicht wieder gutzumachender Nachteil droht, so kann er dem Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Das Verfahren richtet sich sinngemäss nach den Artikeln 79–84 des Bundesgesetzes vom 4. Dezember 1947 über den Bundeszivilprozess.

7. Abschnitt: Strafbestimmungen

Art. 34 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten

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

a. die ihre Pflichten nach den Artikeln 7a und 8–10 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;

b. die es vorsätzlich unterlassen:

1. die betroffene Person nach Artikel 7a Absatz 1 zu informieren; oder

2. ihr die Angaben nach Artikel 7a Absatz 2 Buchstaben a–c zu liefern.

2 Mit Haft oder Busse werden private Personen bestraft, die vorsätzlich:

a. ~~Datensammlungen nach Artikel 11 oder Datenbekanntgaben ins Ausland nach Artikel 6 nicht melden oder bei der Meldung falsche Angaben machen~~ **die Information nach Artikel 6 Absatz 3 oder die Meldung nach Artikel 11a unterlassen oder dabei vorsätzlich falsche Angaben machen;**

b. dem Beauftragten bei der Abklärung eines Sachverhaltes (Art. 29) falsche Auskünfte erteilen oder die Mitwirkung verweigern.

Art. 35 Verletzung der beruflichen Schweigepflicht

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

2 Gleich wird bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Tätigkeit für den Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.

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

8. Abschnitt: Schlussbestimmungen

Art. 36 Vollzug

1 Der Bundesrat erlässt die Ausführungsbestimmungen.

2 (Aufgehoben)

3 Er kann für die Auskunftserteilung durch diplomatische und konsularische Vertretungen der Schweiz im Ausland Abweichungen von den Artikeln 8 und 9 vorsehen.

4 Er kann ferner bestimmen:
a. welche Datensammlungen ein Bearbeitungsreglement benötigen;
b. unter welchen Voraussetzungen ein Bundesorgan Personendaten durch einen Dritten bearbeiten lassen oder für Dritte bearbeiten darf;
c. wie die Mittel zur Identifikation von Personen verwendet werden dürfen.

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

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

Art. 37 Vollzug durch die Kantone

1 Soweit keine kantonalen Datenschutzvorschriften bestehen**, die einen angemessenen Schutz gewährleisten**, gelten für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht die Artikel 1–11**a,** ~~16–23,~~ **16, 17, 18–22** und 25 Absätze 1–3 dieses Gesetzes.

2 Die Kantone bestimmen ein Kontrollorgan, welches für die Einhaltung des Datenschutzes sorgt. Die Artikel 27, 30 und 31 sind sinngemäss anwendbar.

Art. 38 Übergangsbestimmungen

1 Die Inhaber von Datensammlungen müssen bestehende Datensammlungen, die nach Artikel 11 zu registrieren sind, spätestens ein Jahr nach Inkrafttreten dieses Gesetzes anmelden.

2 Sie müssen innert einem Jahr nach Inkrafttreten dieses Gesetzes die notwendigen Vorkehren treffen, damit sie die Auskünfte nach Artikel 8 erteilen können.

3 Bundesorgane dürfen eine bestehende Datensammlung mit besonders schützenswerten Personendaten oder mit Persönlichkeitsprofilen noch bis am 31. Dezember 2000 benützen, ohne dass die Voraussetzungen von Artikel 17 Absatz 2 erfüllt sind.

4 Im Asyl- und Ausländerbereich wird die Frist nach Absatz 3 bis zum Inkrafttreten des totalrevidierten Asylgesetzes sowie der Änderung des Bundesgesetzes vom 26. März 1931 über Aufenthalt und Niederlassung der Ausländer verlängert.

Innert einem Jahr nach Inkrafttreten dieses Gesetzes haben die Inhaber der Datensammlungen die notwendigen Massnahmen zur Information der betroffenen Personen nach Artikel 4 Absatz 4 und 7a zu ergreifen.

Art. 39 Referendum und Inkrafttreten

1 Dieses Gesetz untersteht dem fakultativen Referendum.

2 Der Bundesrat bestimmt das Inkrafttreten (Datum des Inkrafttretens: 1. Juli 1993) / **Inkraftsetzungsbeschluss des Bundesrates für Änderung vom 24. März 2006 – unter Vorbehalt der vorzeitigen Inkraftsetzung des neuen Art. 17a DSG – noch ausstehend.**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ
Hauptabteilung Staats- und Verwaltungsrecht
Abteilung Rechtsetzungsprojekte und -methodik

10. Oktober 2006 / BRU

Änderung von Art. 12 Abs. 2 Bst. a DSG: Auslegungshilfe

1. Ausgangslage

Die Artikel 12 und 13 Datenschutzgesetz umschreiben die Voraussetzungen, unter denen eine Datenbearbeitung durch Private rechtmässig ist. Artikel 12 Datenschutzgesetz hält in Absatz 1 die Grundregel fest, dass wer Personendaten bearbeitet, die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen darf. Absatz 2 umschreibt verschiedene Verletzungstatbestände. So liegt eine Persönlichkeitsverletzung namentlich dann vor, wenn Personendaten entgegen den allgemeinen Datenschutzgrundsätzen (Artikel 4 [Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbindung], 5 Absatz 1 [Richtigkeit], 6 Absatz 1 [Datenübermittlung ins Ausland] und 7 Absatz 1 [Datensicherheit]) bearbeitet werden und dafür kein Rechtfertigungsgrund geltend gemacht werden kann. Rechtfertigungsgründe sind die Einwilligung des Verletzten (bzw. der betroffenen Person), überwiegendes privates oder öffentliches Interesse oder gesetzliche Vorschriften (Art. 13 Abs. 1). Artikel 13 Absatz 2 konkretisiert anhand einer Aufzählung von Beispielen, wann ein überwiegendes Interesse des Datenbearbeiters in Betracht fällt.

Im Zuge der Revision des Datenschutzgesetzes vom 24. März 2006 wurde bei Artikel 12 Absatz 2 Buchstabe a der Vorbehalt des Rechtfertigungsgrundes gestrichen[1]. Zudem wurde bei den Datenschutzgrundsätzen mit einem neuen Artikel 4 Absatz 4 explizit der Grundsatz der Erkennbarkeit von Beschaffung und Zweck der Bearbeitung verankert. Diese Änderung hat unter Praktikern die Befürchtung hervorgerufen, dass viele bisher zulässige Datenbearbeitungen (z.B. Zweckänderungen gestützt auf die Einwilligung der Betroffenen, gesetzlich vorgeschriebene Bearbeitungen oder Bekanntgaben) künftig nicht mehr rechtmässig seien. Die nachstehenden Ausführungen sollen daher klären, wie die Änderung zu verstehen ist.

2. Parlamentarisches Verfahren

Der Antrag, der schliesslich zur beschriebenen Änderung geführt hat, war nicht im bundesrätlichen Entwurf vorgesehen, sondern wurde erst im parlamentarischen Verfahren eingebracht. Er wurde damit begründet, dass die Formulierung im geltenden Recht missverständlich sei. Mit der Änderung solle klargestellt werden, dass namentlich die in Artikel 4 DSG genannten Grundsätze der Datenbearbeitung generell gelten. Es sei insb. nicht denkbar, dass Datenbearbeitungen, die nicht rechtmässig sind, wider Treu und Glauben verstossen oder den Grundsatz der Verhältnismässigkeit verletzen, als zulässig betrachtet werden können.

[1] Bei Art. 6 DSG wurde mit der Revision gestützt auf das Zusatzprotokoll zum Europäischen Datenschutzübereinkommen eine Änderung vorgenommen, die ein Abweichen per se ausschliesst. Die Bestimmung wurde daher schon im bundesrätlichen Entwurf aus der Aufzählung in Art. 12 Abs. 2 Bst. a gestrichen.

Im Nationalrat wurde die Änderung diskussionslos genehmigt (AB 2005 N 1450). Im Ständerat erläuterte der Berichterstatter der Kommission die Änderung ausführlich. Er betonte, dass es sich um eine Klarstellung dessen handle, was bereits bisher gelte. Der Vorsteher des EJPD bestätigte diese Darstellung und wies ausdrücklich darauf hin, dass Fälle, in denen eine gesetzliche Verpflichtung zur Datenbekanntgabe besteht, nicht betroffen seien (AB 2005 S 1159). Ein Antrag auf Festhalten an der Fassung des Bundesrates (und damit auf Verzicht auf die Änderung) wurde daraufhin zurückgezogen.

Im Zuge des Differenzbereinigungsverfahrens kam die nationalrätliche Kommission auf die Änderung zurück. Ein Vorschlag, zwischen den verschiedenen Grundsätzen zu differenzieren und bezüglich der Grundsätze der Zweckbindung und der Erkennbarkeit Abweichungen bei Vorliegen eines Rechtfertigungsgrundes zuzulassen, wurde nicht aufgenommen. Ein modifizierter Antrag, gerechtfertigte Abweichungen nur bezüglich des Erkennbarkeitsgrundsatzes zu ermöglichen, wurde nach längerer Diskussion ganz knapp abgelehnt. Ein Rückkommen auf die bereits durch beide Räte beschlossene Änderung wurde damit verworfen. Es wurde im Zuge der Beratungen wiederum betont, dass die Änderung lediglich eine Präzisierung, und keine Änderung der bisherigen Praxis bedeute.

3. Beurteilung der Tragweite der Änderung

3.1 Allgemeines

Der Mechanismus, wie er in den Artikeln 12 und 13 DSG nach geltendem Recht formuliert ist, ist nicht in jeder Hinsicht überzeugend. Nach dem Wortlaut werden Rechtfertigungsgründe auch bezüglich solcher Grundsätze vorgesehen, die gar nicht relativiert werden können (insb. Rechtmässigkeit sowie Treu und Glauben). Mit der Änderung sollte diesbezüglich Klarheit geschaffen werden.

Aus den vorangegangenen Darlegungen werden zwei Grundanliegen der Änderung deutlich:

- der Gesetzgeber wollte nicht grundsätzlich vom heutigen System abweichen;
- er wollte die Rechtfertigungsgründe bei Abweichungen von den allgemeinen Datenschutzgrundsätzen nicht generell ausschliessen, wohl aber:
  - durch die textliche Änderung verdeutlichen, dass eine Rechtfertigung nicht vorschnell angenommen werden darf;
  - Missverständnisse vermeiden bei Grundsätzen, bei denen kaum denkbar ist, dass ihre Verletzung zu rechtfertigen ist.

Daraus ist zu schliessen, dass Datenbearbeitungen, die gemäss geltendem DSG rechtmässig sind, dies auch in Zukunft sein sollen. Die Änderung hat lediglich zur Folge, dass künftig rechtfertigende Umstände primär bei der Auslegung der allgemeinen Grundsätze zu berücksichtigen sein werden.

3.2 Hinweise zur Beurteilung der Rechtmässigkeit von Datenbearbeitungen

- Vorliegen einer Einwilligung: Ist die Bearbeitung für die Betroffenen erkennbar (Art. 4 Abs. 4 revDSG) oder wurden sie hinreichend darüber informiert (Art. 7*a* revDSG) und entspricht die Einwilligung den Voraussetzungen nach Art. 4 Abs. 5 revDSG, so ist die darauf gestützte Datenbearbeitung zulässig.

- Überwiegende Interessen der Datenbearbeiter: Dass überwiegende Interessen der Datenbearbeiter bei der Beurteilung der Rechtmässigkeit zu berücksichtigen sind, ergibt sich bereits aus dem Verhältnismässigkeitsgrundsatz. Dieser verlangt – auch bei Datenbearbeitungen durch Private – die Prüfung von Geeignetheit, Erforderlichkeit

sowie (im Rahmen der Prüfung des Verhältnisses von Bearbeitungszweck und –mitteln) die Abwägung der entgegenstehenden Interessen.

- Spezialgesetzlich geregelte Bearbeitung: Wenn eine spezialgesetzliche Rechtsgrundlage eine Bearbeitung von Personendaten vorsieht, so ist die Rechtmässigkeit der Bearbeitung weiterhin grundsätzlich gegeben. Das bringt schon der geltende Art. 4 Abs. 3 DSG zum Ausdruck, der bezüglich von Abweichungen vom Zweckbindungsgrundsatz spezialgesetzliche Bestimmungen vorbehält. Beispiele für solche spezialgesetzlichen Rechtsgrundlagen sind etwa die an Private gerichteten Mitteilungspflichten nach dem Konsumkreditgesetz[2], dem Epidemiengesetz[3] oder dem Geldwäschereigesetz[4].

[2] Art. 25 ff. Bundesgesetz über den Konsumkredit, SR 221.214.1
[3] Art. 27 Epidemiengesetz, SR 818.101
[4] Art. 9 Geldwäschereigesetz, SR 955.0

Struktur einer Einwilligungsklausel

(siehe Ziffer III. der Erläuterungen)

Nachfolgend wird für den künftig wohl wichtigsten Anwendungsfall der Einwilligung – die Bekanntgabe von besonders schützenswerten Personendaten an Dritte (siehe markierte Passage) – eine mögliche Grundstruktur einer Einwilligungsklausel aufgeführt. Diese soll es der einzelnen Versicherungsgesellschaft erleichtern – abgestimmt auf Branche und Anwendungsbereich der Einwilligung – ihre individuelle Klausel zu formulieren:

Bei Vertragsabschluss

Es geht um die Einwilligung des potentiellen Versicherungsnehmers:

«Der /die Unterzeichnete ist damit einverstanden, dass seine persönlichen Daten [Datenarten aufzählen, z.B. «Name, Adresse, Geburtsdatum, …»] zum Zweck der [Zwecke anführen, z.B. «zur Antrags- / Risikoprüfung, Vertragsabwicklung, …»] bearbeitet werden **und allenfalls an [Kategorien der Datenempfänger anführen, z.B. «andere Konzerngesellschaften, Mit-, Vor-, Rückversicherer, …»] zum Zweck der [Übermittlungszwecke angeben] übermittelt werden.** Die Antrags- / Risikoprüfung kann auch das Einholen von Auskünften bei [mögliche Kategorien der Auskunftserteilenden aufzählen, z.B. «anderen Konzerngesellschaften, Vorversicherern, …»] beinhalten.

[Hinweis auf Nachteil, der sich aus der Nichterteilung der Einwilligung ergeben kann.]»

Im Schadenfall

Im Schadenfall kommen – neben dem Versicherungsnehmer – auch andere Einwilligende in Frage, z.B. geschädigte Dritte in Haftpflichtfällen:

«Der /die Unterzeichnete ist damit einverstanden, dass seine persönlichen Daten [Datenarten aufzählen, z.B. «Name, Adresse, Geburtsdatum, …»] zum Zweck der [Zwecke anführen, z.B. «Schadenprüfung …»] bearbeitet werden **und allenfalls an [Kategorien der Datenempfänger anführen, z.B. «involvierte Versicherer, …»] zum Zweck der [Übermittlungszwecke angeben, z.B. «Missbrauchsbekämpfung, …»] übermittelt werden.** Die Schadenprüfung kann auch das Einholen von Auskünften bei [mögliche Kategorien der Auskunftserteilenden aufzählen] beinhalten.

[Hinweis auf Nachteil, der sich aus der Nichterteilung der Einwilligung ergeben kann.]»

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni

Schweizerischer Versicherungsverband (SVV)
C. F. Meyer-Strasse 14
Postfach 4288
CH-8022 Zürich
Tel. +41 44 208 28 28
Fax +41 44 208 28 00
info@svv.ch
www.svv.ch