UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Schleswig-Holsteins
Servicezentrum für Datenschutz
und Informationszugang

1. Auflage

Verbraucher-
zentrale
Schleswig-
Holstein e.V.

Verbraucherzentrale
Bundesverband e.V.

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Datenschutz für Verbraucher

99+1 Beispiele und viele Tipps zum Bundesdatenschutzgesetz

99+1 Beispiele und viele Tipps zum Bundesdatenschutzgesetz

Vorwort

der Verbraucherzentrale Bundesverband e.V.
von Edda Müller

Sie haben sich im Internet für Kurreisen wegen Rückenproblemen umgesehen – sollte ihr künftiger Arbeitgeber davon erfahren?
Sie haben im Apotheken-Versandhandel Medikamente bestellt – Infos, die für ihre Krankenversicherung bestimmt sind?
Sie sind in den vergangenen zwei Jahren zweimal in die Vereinigten Arabischen Emirate geflogen und essen kein Schweinefleisch – kann das Ärger bei der nächsten USA-Reise geben?
All dies sind fiktive Beispiele – sind es auch fiktive Probleme?

Datenschutz ist seit den Anfängen der Verbraucherarbeit und verstärkt mit den zunehmenden Digitalisierung unser Gesellschaft ein wesentliches Verbraucherthema. So hat uns etwa der Handel mit Kundenadressen beschäftigt, dem zum Beispiel durch Eintrag in Sperrlisten begegnet werden konnte. Heute werden solche Gegenmaßnahmen und damit schließlich der Selbstschutz des Verbrauchers immer schwieriger, denn es wird selbst für Experten zunehmend undurchschaubarer, wo durch wen welche Daten erhoben, verarbeitet und weitergegeben werden. Im Gegensatz zur Offline-Welt wird in der Online-Welt jede Lebensregung Datenspuren erzeugen. Mit den damit verbundenen unkontrollierbaren Datenströmen nimmt potentiell die Einflussmöglichkeit der Verbraucher ab. Bei steigendem Wert personenbezogener Daten und deren wachsender Bedeutung für die Informationswirtschaft als weitere Einnahmequelle müssen hier Verbraucherpolitik und Verbraucherschutz ansetzen, um die dadurch entstehenden nachteiligen Entwicklungen zu begrenzen. Es geht um nicht und nicht weniger als Chancen- und Waffengleichheit zwischen Verbrauchern als „Datenträger“ und Anbietern als „Datenjäger und -sammler“ herzustellen.

Gleichzeitig geht es um eigenverantwortliches Handelns der Verbraucher: Sie sollten die Brisanz ihrer eigenen Daten begreifen, die Risiken im Umgang mit ihren Daten erkennen und entsprechend handeln können. Nur so kann der Schutz der Daten zu einem wirksamen Schutz der Verbraucher führen. Datenschutz in der digitalen Welt – ein Reizbegriff, bei dem es vor allem um Aufklärung und nüchterne Information geht. Auf der einen Seite gibt es eine große Anzahl von Verbrauchern, die besondere Sicherheitsbedenken haben und aus diesem Grunde vor allem am elektronischen Geschäftsverkehr nur sehr zögerlich teilnehmen. Gründe dafür gibt es viele: dazu zählen Unkenntnis aufgrund mangelnder Transparenz der neuen Informations- und Kommunikationstechniken sowie wiederholte Pressemeldungen über Sicherheitsmängel von zuvor als „absolut sicher“ angepriesenen neuen Technologien.

Auf der anderen Seite gibt es aber auch die große Gruppe der Verbraucher, die keine oder nur sehr gering ausgeprägte Sicherheitsbedenken haben. Hier beobachten wir einen teilweise sorglosen Umgang mit den eigenen Daten. Auch hier sind die Gründe zu suchen im fehlenden Bewusstsein für die Brisanz der eigenen Daten sowie in der Unkenntnis der technischen Möglichkeiten zur Erhebung, Verarbeitung und Übermittlung von Daten. Wer Kundenkarten, Mailinglisten oder Newsletter bedenkenlos nutzt, unterschätzt die Möglichkeiten von Unternehmen, das eigene Konsumverhalten nicht nur zu bewerten, sondern zu steuern und zu beeinflussen.

So unterschiedlich Verbraucher bisher also mit dem Datenschutz umgehen – die vorliegende Broschüre soll einen umfassenden Überblick über die Risiken eines allzu sorglosen Umgangs mit den eigenen Daten und über Möglichkeiten des Selbstschutzes geben. Letztlich geht es darum, dass Verbraucherinnen und Verbraucher von ihren Rechten selbstbewusster Gebrauch machen und beim Einkaufen in der Fußgängerzone oder in der digitalen Welt höchste Datenschutzstandards einfordern.

Prof. Dr. Edda Müller ist Vorstand
des Verbraucherzentrale Bundesverbands e.V.
www.vzbv.de

Vorwort

Der Datenschutz ist für die Menschen da – also für SIE. Der Schutz IHRER Privatsphäre ist auch das zentrale Anliegen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holsteins. Diese vorliegende Broschüre dient deshalb in erster Linie dazu, Sie als Bürgerin oder Bürger über Ihr Datenschutzrecht zu informieren. Dabei werden typische Fälle vorgestellt, in denen es datenschutzrechtliche Probleme geben kann. Praktische Verbrauchertipps geben Ihnen die Möglichkeit, selbst zu reagieren.

In zweiter Linie wendet sich die Broschüre an die Unternehmen, die Datenschutz zunehmend als eine vertrauensbildende Geschäftsbedingung begreifen. Um diesen Ansatz zu unterstützen, werden neben der Darstellung gesetzlicher Vorgaben vor allem im letzten Textabschnitt Empfehlungen gegeben, wie mit vertretbarem Aufwand eine datenschutzfreundliche Geschäftspraxis gepflegt werden kann. Für Sie als Bürger geben diese Hinweise zugleich Anhaltspunkte, wie sorgfältig ein Unternehmen mit Ihren Daten umgeht.

Wenn Sie in dieser Broschüre nach Informationen suchen, sind drei Wege möglich:

- Sie orientieren sich an Themen (Datenverarbeitung – Transparenz – Betroffenenrechte und Rechtsbehelfe – Hinweise für Kleine und Mittlere Unternehmen zur Datenschutzorganisation).
- Falls Sie juristische Vorkenntnisse besitzen oder Themen zu einem bestimmten Paragrafen suchen, benutzen Sie die Inhaltsübersicht.
- Schließlich können Sie im Stichwortverzeichnis nachschlagen, welche Themen/Branchen Sie interessieren.

Diese Broschüre erhebt nicht den Anspruch auf Vollständigkeit. Sie will Sie vor allem auf Ihre Datenschutzrechte hinweisen, die Ihnen praktische Einflussmöglichkeiten geben. Viele weiterführende Informationen finden Sie auf der Homepage des Unabhängigen Landeszentrums für Datenschutz (www.datenschutzzentrum.de) und dem gemeinsamen Internetportal der Datenschutzbehörden (www.datenschutz.de).

Der Verfasser dieser Broschüre, Dr. Thomas Petri, wird gerne etwaige Ergänzungsvorschläge und Anregungen entgegennehmen und Rückfragen beantworten (Tel.: 0431-988 1394; E-Mail: LD8@datenschutzzentrum.de).
Die letzten Seiten des vierten Teils sind überwiegend der Broschüre „Neuregelungen im Bundesdatenschutzgesetz“ entlehnt, die das Unabhängige Landeszentrum für Datenschutz und der Berliner Beauftragte für Datenschutz und Informationsfreiheit gemeinsam herausgegeben haben. Werden in den folgenden Texten Paragrafen zitiert, so sind dies Paragrafen des Bundesdatenschutzgesetzes (BDSG). Andere Gesetzesparagrafen werden mit dem Namen des jeweiligen Gesetzes gekennzeichnet.

Eine abschließende Bemerkung: Die Broschüre richtet sich gleichermaßen an alle Bürgerinnen und Bürger. Sollte im Folgenden überwiegend die männliche Form gewählt sein, geschieht dies nur aus Gründen der sprachlichen Verständlichkeit.

Dr. Helmut Bäumler
Landesbeauftragter für Datenschutz Schleswig-Holstein

Inhalt

Einführung

Wen schützt das BDSG? (§ 3 Abs. 1)

Nach § 3 Absatz 1 sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlicher Person (Betroffener).“ Vom BDSG geschützt wird also jeder lebende Mensch. Datenschutz betrifft nicht Informationen über Verstorbene.

Beispiel 1 | Eine Frau unterhält bei einem Kreditinstitut (Bank, Sparkasse) ein Konto. Als sie verstirbt, informiert das Kreditinstitut einen Verwandten der Verstorbenen über den Kontostand.[1] Die Datenübermittlung ist in Bezug auf die Verstorbene nicht mehr vom BDSG erfasst.

Beispiel 2 | GmbH´s und Aktiengesellschaften (AG) sind Unternehmen, die eine eigene Rechtspersönlichkeit besitzen. Sie können mit anderen Worten Träger von Rechten und Pflichten sein. Solche Unternehmen nennt man „juristische Personen“. Diese sind in der Regel nicht vom BDSG geschützt (unter Umständen aber ihre Eigentümer! siehe Beispiel 5).

Die Person muss „bestimmt“ oder „bestimmbar“ sein. Bestimmbar ist eine Person, wenn man mithilfe der zur Verfügung stehenden Angaben eine bestimmte Person ermitteln kann. So kann der Kontostand in Beispiel 1 ein personenbezogenes Datum des oder der Erben sein, weil der Erbe der Verstorbenen relativ leicht zu ermitteln ist. Bestimmt ist eine Angabe, wenn sie sich nur auf eine einzige Person bezieht.

Beispiel 3 | In der Regel ist der Name einer Person ein bestimmtes Datum. Dem Verfasser dieser Broschüre ist es allerdings bei seiner Musterung zum Wehrdienst passiert, dass neben ihm ein Namensvetter sogar mit dem gleichen Geburtsdatum saß! In einem solchen Fall ist die betroffene Person anhand des Namens „nur“ bestimmbar. Bei sehr geläufigen Namen wie etwa Müller, Schmidt usw. kommen Fälle der Namensgleichheit öfters vor.

Beispiel 4 | Beim Surfen im Internet sind viele Verbraucher auf „Access-Provider“ angewiesen, die den Zugriff auf das Internet ermöglichen. Dabei wird dem Computer des Verbrauchers (zumindest) für die Dauer des Zugriffs auf das Internet eine so genannte IP-Nummer zugewiesen. Die IP-Nummer ist ein Zahlencode, der zwischen vernetzten Rechnern wie eine postalische Adresse wirkt. Auf diese Art und Weise können Computer im Internet miteinander kommunizieren. Gleichzeitig kann eine IP-Nummer auch ein personenbezogenes Datum des Verbrauchers sein, wenn man die Zuweisung der IP-Nummer zu bestimmten Rechnern kennt oder ermitteln kann.[2]

Der Begriff „Einzelangaben über persönliche oder sachliche Verhältnisse“ ist sehr weit zu verstehen. Persönliche Verhältnisse können Eigenschaften des Betroffenen sein, sachliche Verhältnisse Dinge, die dem Betroffenen zuzuordnen sind.

Beispiel 5 | Kontostände geben Auskunft über einen Teil des Vermögens einer Person. Sie sind deshalb Einzelangaben über sachliche Verhältnisse eines Kontoinhabers.

Beispiel 6 | Eine so genannte Einmann-GmbH ist eine juristische Person, die im alleinigen Eigentum eines Gesellschafters ist. Das Betriebsvermögen dieser „Einmann-GmbH“ enthält auch Informationen über das Vermögen des Gesellschaftseigners.

„Einzelangaben“ liegen nicht mehr vor, wenn die Informationen nicht mehr auf eine Person zurückzuführen sind.

Beispiel 7 | Markt- und Meinungsforschungsinstitute sind häufig kommerziell ausgerichtete Unternehmen, die Verbraucherdaten sammeln und auswerten, um sie anderen Unternehmen oder auch Behörden zu verkaufen. Wenn die Angaben über Verbraucher anonym, also ohne Zuordnung zu einer bestimmten Person erhoben werden, liegen zwar statistische Angaben einer Gruppe vor, meistens aber keine personenbezogenen Daten.

TIPP
Für Verbraucher

Markt- und Meinungsumfragen

Spricht Sie ein Markt- oder Meinungsforschungsinstitut an, prüfen Sie sorgfältig, ob Sie Informationen über sich preisgeben wollen! Bei seriösen, Ihnen bekannten Instituten, die beispielsweise im Auftrag von Behörden nur statistische Angaben erheben und speichern, bestehen keine grundsätzlichen datenschutzrechtliche Bedenken. Nachfragen nach der weiteren Verwendung der Daten kann allerdings auch da nicht schaden!
Andere Institute erfragen von Ihnen Informationen zumeist nur, um sie als personenbezogene Daten weiterzuverkaufen. Diese Daten werden regelmäßig in vielfältiger Weise ausgewertet. Sie müssen damit rechnen, dass Sie künftig von Vertragspartnern der Institute zu Werbezwecken angesprochen werden oder dass Ihre Angaben dazu benutzt werden, Ihre Kreditwürdigkeit zu überprüfen

Welche Datenverarbeitungen fallen unter das BDSG?

Das BDSG setzt in vielfacher Hinsicht die Vorgaben einer Europäischen Richtlinie um. Diese so genannte „EU-Datenschutzrichtlinie“ (EU-DSRL)[3] gibt den Mitgliedstaaten Datenschutzziele vor, die in innerstaatliches Recht umgesetzt werden müssen. Wie diese Ziele umgesetzt werden, wird den Mitgliedstaaten überlassen.[4] Dem entsprechend weicht das BDSG in der Wortwahl zulässig von der der EU-DSRL ab. Relevante Verarbeitungsformen sind nach dem BDSG die Datenerhebung[5], die Verarbeitung (= Speicherung, Veränderung, Übermittlung, Sperrung, Löschung)[6] und Nutzung[7] personenbezogener Daten. Unter Datenerhebung wird das Beschaffen von personenbezogenen Daten verstanden. Sie ist regelmäßig gegeben, wenn sich die Stelle Informationen aktiv beschafft.

Beispiel 8 | Ein Bürger interessiert sich für ein bestimmtes Buch. Da er weiß, in welchem Verlag das Buch erschienen ist, schreibt er den Verlag an und bestellt das Buch. Der Verlag hat nichts dazu getan, um seine Daten zu erhalten, deshalb liegt keine Datenerhebung durch den Verlag vor.

Beispiel 9 | Die SCHUFA ist ein Unternehmen, das kreditrelevante Verbraucherinformationen sammelt und Vertragspartnern zur Verfügung stellt. Viele Unternehmen, die Ihnen gegenüber in Vorleistung treten, nehmen eine SCHUFA-Abfrage vor, bevor sie Ihnen gegenüber eine Leistung erbringen. Diese Abfrage ist eine Datenerhebung, weil sich das Unternehmen Informationen über Sie verschafft.

TIPP
Für Verbraucher

SCHUFA-Abfragen

Die Zulässigkeit einer SCHUFA-Abfrage ist nur für Unternehmen unstreitig, die in Waren- oder Geldform Kredite geben. Nicht jedes wirtschaftliches Interesse rechtfertigt eine SCHUFA-Abfrage! Insbesondere bei Unternehmen der Wohnungswirtschaft, bei Versicherungen oder Inkassounternehmen ist die Rechtmäßigkeit einer SCHUFA-Abfrage zumindest zweifelhaft. Falls solche Unternehmen mit Sitz in Schleswig-Holstein eine SCHUFA-Abfrage vornehmen, können Sie sich an das Unabhängige Landeszentrum für Datenschutz wenden; es überprüft für Sie gerne im Einzelfall die Rechtmäßigkeit der Datenabfrage.
Es hängt natürlich von Ihnen ab, ob Sie trotz einer solchen SCHUFA-Abfrage z. B. eine Wohnung mieten wollen. Wenn Sie für Ihr Vertragsverhältnis Störungen befürchten, können Sie auch die SCHUFA-Abfrage kommentarlos dulden und dann das Unabhängige Landeszentrum (ULD) infomieren.
Eine Überprüfung durch das ULD kann auch diskret (ohne Hinweis auf Sie) erfolgen.

Der datenschutzrechtliche Begriff Speichern entspricht dem allgemeinen Wortgebrauch. Er ist allerdings nicht auf ein Speichermedium beschränkt. Deshalb spricht das BDSG von „Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger.“

Beispiel 10 | Digitale Ton- oder Bildaufnahmen sind ebenso ein Speichern wie das Abspeichern von Daten auf einem Computer.

Beispiel 11 | Auch nichtelektronische Aufbewahrungsformen können Speicherungen sein. Immer noch gängig ist die Speicherung von Daten in Karteien oder strukturierten Akten.

Es ist dabei nicht erforderlich, dass die Speicherung dauerhaft erfolgt.[8] Verändern ist das „inhaltliche Umgestalten gespeicherter personenbezogener Daten".

Beispiel 12 | Wenn umgangssprachlich davon die Rede ist, dass Ihr Vertragspartner Ihre neue Wohnadresse „speichert", ist datenschutzrechtlich eine Veränderung gemeint.

Beispiel 13 | Wenn Sie feststellen, dass eine Stelle über Sie falsche personenbezogene Daten speichert, können Sie eine Berichtigung der Daten verlangen. Diese Berichtigung (dazu später mehr!) stellt begrifflich auch eine Veränderung dar.

Das Übermitteln ist das Weitergeben von personenbezogenen Informationen an einen Dritten. Diese Form der Datenverarbeitung ist bedeutsam, weil die Information den ursprünglichen Verwenderkreis verlässt. Damit findet also eine Erweiterung des Kreises der Datenverarbeiter statt.

Beispiel 14 | Ein Konzernunternehmen gibt Ihre Daten an das Konzernmutterunternehmen ab. Datenschutzrechtlich ist dieser Datentransfer als Datenübermittlung zu werten, der den allgemeinen Regeln zu folgen hat. Das Datenschutzrecht kennt kein Konzernprivileg.

Beispiel 15 | Die Abteilung „Lebensversicherungen" einer Versicherung gibt Ihre Daten hausintern an eine andere Abteilung (z. B. Sachversicherungen) weiter. Diese Datenweitergabe ist keine Datenübermittlung, weil eine rechtlich unselbständige Abteilung als Bestandteil des Unternehmens gewertet wird. Selbstverständlich kann auch eine solche Datenweitergabe datenschutzrechtlich relevant sein! Eine Datenübermittlung liegt hingegen vor, wenn eine Versicherungsgruppe für jede Versicherungssparte eine eigenständige juristische Person gegründet hat und der Datentransfer zwischen diesen Unternehmen erfolgt.

TIPP

Für Verbraucher

Werbung, Markt- und Meinungsforschung

Wenn Sie die Zusendung von Werbezuschriften nicht wünschen, achten Sie bitte bei Vertragsabschlüssen auf so genannte „Datenschutzhinweise", „Datenschutzklauseln" oder „Datenverarbeitungsklauseln". Häufig weisen sie darauf hin, dass die Unternehmen Ihre Daten an Dritte weitergeben wollen.

Soll diese Datenübermittlung zu Zwecken der Werbung, der Markt- oder Meinungsforschung erfolgen, können Sie bereits beim Vertragsabschluss der Datenübermittlung widersprechen (für einen solchen Widerspruch genügt ein einfacher Vermerk auf dem Vertragsformular: „Bitte keine Datenweitergabe zu Zwecken der Werbung, Markt- oder Meinungsforschung!"

Löschen ist das Unkenntlichmachen (das Tilgen) von gespeicherten personenbezogenen Daten. Ein Löschen liegt nur vor, wenn die Daten unwiederbringlich getilgt sind.

Beispiel 16 | Das Schwärzen mit einem Filzstift erschwert vielleicht das Lesen eines Textes, dieser ist aber nicht endgültig getilgt, wenn er mit bestimmten Methoden erkennbar gemacht werden kann (Papier gegen das Licht halten usw.).

Beispiel 17 | Wenn Sie die „Löschfunktion" in einem Textprogramm Ihres Rechners betätigen (delete – entf oder Ähnliches), beseitigt der Rechner lediglich den Datenzugriff (Zugriffspfad) und ermöglicht damit auch das Überschreiben des ursprünglich gespeicherten Textes. Mit bestimmten Programmen sind die „gelöschten" Texte aber wieder herstellbar. Unternehmen, die sensible Daten über Sie speichern, dürfen sich daher nicht damit begnügen, die Löschfunktionen zu verwenden.

TIPP

Für Verbraucher

Löschprogramme

Auch für Verbraucher gibt es bereits kostengünstige oder gar kostenlose Programme, die eine zuverlässige Löschung ermöglichen. Nähere Informationen dazu finden Sie auf der Website des ULD Schleswig-Holstein (www.datenschutzzentrum.de) unter Systemdatenschutz/Systemmeldungen.

Gibt es Fälle, bei denen Sie keine Löschung verlangen können? Und was können Sie dann tun?

Weitgehend unbekannt ist der Begriff der Sperrung. Sperren bedeutet ein „Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.“ [9] Gemeint ist folgendes: Es gibt Situationen, in denen an und für sich eine Löschung von personenbezogenen Daten erforderlich wäre. Andererseits kann es gute Gründe geben, z. B. weil es ein Gesetz verlangt, oder auch das Interesse des Betroffenen dafür spricht, dass die Daten weiterhin gespeichert werden. In diesem Fall bewirkt eine Sperrung, dass die Daten zwar gespeichert werden, grundsätzlich aber nicht mehr verwendet werden dürfen. Die einzige Nutzungsmöglichkeit besteht in dem Grund, weswegen die Daten nur gesperrt und nicht gelöscht wurden.

Beispiel 18 | Das Abgabenrecht sieht zwingend vor, dass bestimmte steuerrelevante Daten bis zu zehn Jahren aufbewahrt werden.[10] Die weitere Verarbeitung dieser Daten ist aber nicht mehr erforderlich, weil z. B. der Kaufvertrag mit Ihnen längst abgewickelt ist. In diesem Fall muss die verantwortliche Stelle Ihre personenbezogenen Daten sperren. Das bedeutet, die Daten dürfen ausschließlich dazu verwendet werden, der Finanzverwaltung eine Prüfung der Steuerpflicht zu ermöglichen.

Beispiel 19 | Ein Versandhandel hat Sie zu Werbezwecken persönlich angeschrieben. Sie widersprechen der weiteren Nutzung Ihrer Daten.[11] Nun kann es passieren, dass das Unternehmen von kommerziellen Adresshändlern erneut Ihre Adresse erhält. Wenn das Unternehmen alle Ihre Daten gelöscht hat, kann es nicht mehr erkennen, dass Sie einen Widerspruch erklärt haben und keine Werbezuschriften wünschen.Hier „hilft“ die Sperrung: Ihre Adressdaten werden nur dazu aufbewahrt, um zu verhindern, dass Sie erneut zu Werbezwecken angesprochen werden.

Um alle Formen der Datenverwendung rechtlich zu erfassen, sieht das BDSG überdies den Begriff der Nutzung personenbezogener Daten vor. Nutzung sind alle Verwendungen, die nicht Erheben oder Verarbeiten sind.

Beispiel 20 | Die Datenweitergabe innerhalb einer verantwortlichen Stelle ist keine Datenübermittlung (die Daten gehen nicht an einen Dritten), sondern eine Nutzung.

Beispiel 21 | Wenn ein Call Center z. B. für einen Autohändler oder für eine Bank bei Ihnen eine „Zufriedenheitsbefragung“ über Produkte durchführt, die Sie erhalten haben, dann liegt in der persönlichen Ansprache ein Nutzen.

HINWEISE
Für Unternehmen

Was tun, wenn Kunden über ihre Zufriedenheit befragt werden sollen (Kundenzufriedenheitsbefragung)?

Falls Sie beabsichtigen, durch ein Call Center eine Zufriedenheitsbefragung durchführen zu lassen, sind Sie nach § 4 Abs. 3 gehalten, die Betroffenen auch über die Kategorien von Empfängern zu unterrichten. Denn regelmäßig muss ein Kunde nicht mit „Zufriedenheitsbefragungen“ rechnen.
Nach der Rechtsprechung ist die telefonische Kontaktaufnahme mit Endverbrauchern ohne deren ausdrücklichen Einwilligung (Opt-in) regelmäßig unzulässig, weil sie eine erhebliche Beeinträchtigung der Privatsphäre bedeutet.
Überlassen Sie es dem Kunden zu entscheiden, ob er Ihnen eine Rückmeldung über Ihren Service geben will! Formulieren Sie eine Einwilligungserklärung, bei der der Kunde sich für oder gegen eine Kundenzufriedenheitsbefragung entscheiden kann. Erfahrungsgemäß trägt dies erheblich zur Akzeptanz der Befragung bei.[12]
Eine solche Klausel könnte wie folgt lauten: „Wir sind bestrebt, unsere Vertragsleistungen noch stärker an Ihren Bedürfnissen auszurichten. Deshalb würden wir Sie gerne durch ein Call Center (falls der Name des Call Center bereits bekannt ist, sollte er genannt werden) befragen, ob Sie mit unserem Service zufrieden sind. Die Daten werden vertraulich behandelt und nur zur Verbesserung unseres Services verwendet, eine Weitergabe an Dritte findet nicht statt.
Ja, ich bin mit eine Zufriedenheitsbefragung durch die ... einverstanden ☐
(Anrufe erfolgen nur, wenn Sie Ihre Zustimmung durch Ankreuzen ausdrücklich erteilen.)

Wann schützt Sie das BDSG? (§ 1 Abs. 2)

Es gibt viele Datenschutzgesetze, die zu Ihrem Schutz gelten. Für öffentliche Stellen (also vor allem Behörden) des Landes Schleswig-Holstein gilt beispielsweise das Landesdatenschutzgesetz vom 9.2.2000, das zahlreiche moderne Datenschutzprinzipien verwirklicht und Sie daher weitgehend und wirksam schützt. Das BDSG sieht vor allem Regelungen für Bundesbehörden und für so genannte „nicht-öffentliche Stellen" vor. Mit diesem Begriff sind in erster Linie Unternehmen der Privatwirtschaft und Vereinigungen gemeint.[13]

Menschen können auch „nicht-öffentliche Stelle" sein, wenn sie nicht nur für rein private oder familiäre Tätigkeiten personenbezogene Daten verarbeiten.[14] Ob eine solche Tätigkeit vorliegt, richtet sich nach den Wirkungen und den Verarbeitungszwecken.

Beispiel 22 | Wenn Sie sich auf Ihrem Rechner für private Zwecke ein Telefonbuch anlegen, verarbeiten Sie zwar personenbezogene Daten, das BDSG findet aber keine Anwendung.

Beispiel 23 | Wenn Sie im Internet eine private Website anlegen, mag dies privat motiviert sein. Sie richten sich aber an ein weltweites Publikation. Dem entsprechend unterliegen auf der Website veröffentlichte Daten über andere Personen zumeist dem BDSG.

Sind Sie auch geschützt, wenn Ihre Daten nicht per Computer verarbeitet werden?

Benutzt eine private Stelle keinen Computer, wenn es Ihre Daten verwendet, kann Sie das BDSG rechtlich auch nur eingeschränkt schützen. Ein besonderes Risiko wird dann vom Gesetzgeber offenbar nur gesehen, wenn Ihre Daten in einem strukturierten Datenbestand erfasst sind (nicht automatisierte Datei).[15] In diesem Fall können nämlich die personenbezogenen Daten regelmäßig zügig unter bestimmten Gesichtspunkten ausgewertet werden.

Beispiel 24 | Wenn Sie bei einer Tankstelle Ihr Portemonnaie vergessen haben, verlangt der Tankstellenpächter häufig, dass Sie Ihren Personalausweis vorzeigen. Er notiert dann Name, Adresse und Personalausweisnummer. Solange er diese Angaben nur auf einem losen Zettel notiert und nicht eine Kartei über alle Personen anlegt, die schon einmal ihr Portemonnaie vergessen haben, findet das BDSG keine Anwendung.

Beispiel 25 | Kreditinstitute verlangen bei der Eröffnung von Konten regelmäßig die Vorlage des Personalausweises. Sie kopieren den Personalausweis, weil dies vom Geldwäschegesetz in bestimmten Fällen verlangt wird. Wird diese Personalausweiskopie nicht nur zu Ihren Kontounterlagen genommen, sondern in einen so genannten „Geldwäscheordner" geheftet, in dem die Personalausweiskopien alphabetisch sortiert sind, liegt regelmäßig eine nicht automatisierte Datei vor, sodass das BDSG dann regelmäßig Anwendung findet.

TIPP
Für Verbraucher

Personalausweiskopien

Nach neuer Rechtslage müssen Sie es meistens dulden, dass Kreditinstitute zur Geldwäscheprävention Ihren Personalausweis kopieren. Denn das Geldwäschegesetz sieht eine Verpflichtung der Kreditinstitute zur Identifizierung des Bankkunden vor, wenn eine „auf Dauer angelegte Geschäftsbeziehung" begründet wird. Eine solche Geschäftsbeziehung ist insbesondere gegeben, wenn ein Konto eröffnet und geführt wird.[16] Wenn Sie als Bankkunde bereits persönlich bekannt sind (z. B. schon ein Konto bei Ihrer Bank unterhalten), ist eine Kopie des Personalausweises allerdings überflüssig und rechtlich nicht geboten.
Bei anderen Unternehmen ist das Kopieren des Personalausweis aber grundsätzlich nicht vorgesehen!

HINWEISE
Für Kredidinstitute

Personalausweiskopien:

Rückfragen beim Unabhängigen Landeszentrum für Datenschutz zeigen, dass die Anfertigung von Personalausweiskopien für zahlreiche Bankkunden befremdlich ist. Unabhängig von datenschutzrechtlichen Unterrichtungspflichten wird deshalb empfohlen, die Kunden vor der Anfertigung der Kopien auf die gesetzliche Verpflichtung nach § 9 Geldwäschegesetz hinzuweisen.

Wer muss das BDSG überhaupt beachten?

Meistens führen die Beispiele in dieser Broschüre Unternehmen auf, die Ihre personenbezogenen Daten verarbeiten. Auch Vereine oder einzelne Menschen kommen als Datenverarbeiter in Betracht. Das BDSG nennt solche Datenverarbeiter „verantwortliche Stellen“. Das sind alle Menschen, Unternehmen, Vereine oder Gruppierungen, die personenbezogene Daten für sich verwenden oder andere dazu beauftragen.

[1]

Rechtmäßigkeit der Verarbeitung personenbezogener Daten (§ 4, §§ 27-30)

Teil I

Rechtmäßigkeit der Verarbeitung personenbezogener Daten (§ 4, §§ 27-30)

Die Grundregel des Datenschutzrechts lautet: Eine Verarbeitung personenbezogener Daten ist nur zulässig, wenn sie durch eine Rechtsvorschrift oder durch die Einwilligung des Betroffenen erlaubt wird.[17]

Einwilligung (§ 4a)

Eine wichtige Form der Rechtfertigung ist die Einwilligung. Der Theorie nach gibt sie Ihnen als betroffenen Bürger die Möglichkeit zu bestimmen, wann und unter welchen Bedingungen Sie eine Datenverarbeitung zulassen oder nicht zulassen. Ob Sie im wirklichen Leben tatsächlich eine Gestaltungsmöglichkeit haben, hängt allerdings von den Umständen des Einzelfalls ab.

Beispiel 26 | Kreditinstitute verlangen bei der Kontoeröffnung regelmäßig, dass Sie eine so genannte SCHUFA-Klausel unterschreiben. Diese SCHUFA-Klausel besagt, dass Sie das Kreditinstitut dazu ermächtigen, bestimmte Daten an die SCHUFA zu übermitteln, obwohl dies für die eigentliche Vertragserfüllung mit Ihnen nicht notwendig ist. Verweigern Sie die Unterschrift, wird das Kreditinstitut u.U. kein Konto eröffnen. Da weit über 90 % aller deutschen Kreditinstitute Vertragspartner der SCHUFA sind, haben Sie oft faktisch keine andere Wahl, als der SCHUFA-Klausel zuzustimmen.

TIPP
Für Verbraucher

SCHUFA-Klausel

Kreditinstitute haben kein berechtigtes Interesse an einer SCHUFA-Klausel, wenn sie nicht in Vorleistung treten. Es ist also unzulässig, wenn Sie bei einem Sparbuch angehalten werden, eine SCHUFA-Klausel zu unterschreiben. Manche Kreditinstitute bieten auch ein Girokonto auf Guthabenbasis an. Da Ihnen dabei grundsätzlich keine Kreditlinie eingeräumt wird, erfordert ein solches Konto zumindest keine Übermittlungen an die SCHUFA. Hier sollte auf eine SCHUFA-Klausel verzichtet werden können. Falls sie Ihnen gleichwohl abverlangt wird, können Sie sich an Ihre Aufsichtsbehörde wenden.
Die Kreditinstitute nehmen allerdings bei der Eröffnung eines solchen Kontos häufig eine SCHUFA-Abfrage vor (Datenerhebung), um feststellen zu können, ob Sie Konten missbräuchlich genutzt haben. Die rechtliche Zulässigkeit einer solchen Abfrage ist derzeit umstritten. Das Hauptargument der Kreditinstitute stellt auf die Möglichkeit des Kunden ab, Konten vertragswidrig zu überziehen. Dem wird entgegenhalten, dass nicht jedes wirtschaftliche Risiko zu einer SCHUFA-Abfrage berechtigt.

Beispiel 27 | Wenn Sie ein Handy erstehen wollen, verlangen auch Telekommunikationsunternehmen häufig die Unterschrift unter eine SCHUFA-Klausel. Da Sie nicht von einem bestimmten Handy abhängig sind, haben Sie in diesem Fall eine echte Wahlmöglichkeit. Sie können die Unterschrift ablehnen und einen anderen Anbieter suchen, der kein SCHUFA-Vertragspartner ist. Oder Sie kaufen ein Prepaid-Handy, bei dem das Telekommunikationsunternehmen kein kreditorisches Risiko trägt.

TIPP
Für Verbraucher

Allgemeine Geschäftsbedingungen

Wie bei jedem Vertragsabschluss sollten Sie auf das Kleingedruckte achten. Jedes oder zumindest fast jedes Telekommunikationsunternehmen prüft in irgendeiner Weise die Kreditwürdigkeit ihres Neukunden.
Wie das erfolgt, ergibt sich zumeist aus den „Datenschutzklauseln“ (was eigentlich ein Wortmissbrauch ist, weil es nicht um Datenschutz, sondern um Datenverarbeitung geht!)
Wenn Sie ohne großen Aufwand verschiedene Anbieter aufsuchen können, nutzen Sie die Vergleichsmöglichkeit! Sind Sie z. B. wirklich damit einverstanden, dass ein Unternehmen mit der SCHUFA und drei weiteren Auskunfteien zusammenarbeitet und mit allen diesen Stellen Daten über Sie austauscht? Die Frage, ob eine Kooperation des Telekommunikationsanbieters mit der SCHUFA oder mit einer Auskunftei günstiger für Sie ist, hängt von Ihrer Einschätzung ab.

Eine Einwilligung ist nur wirksam erteilt, wenn sie auf der freien Entscheidung des Betroffenen beruht.[18] Das setzt zunächst voraus, dass der Betroffene die Tragweite seiner Entscheidung überblicken kann.

Beispiel 28 | Zur Gewinnung künftiger Kunden veranstalten (nicht nur) Krankenkassen Gewinnspiele für Schülerinnen und Schüler, bei denen die Teilnehmer ihre Adressdaten und ihr Alter sowie weitere Angaben preisgeben sollen. Die so erhobenen personenbezogenen Daten werden anschließend zur gezielten Ansprache der Betroffenen (Werbung) genutzt. Die Zulässigkeit solcher „Gewinnspiele" hängt unter anderem davon ab, ob die Schüler bereits die nötige Einsichtsfähigkeit besitzen, welche Folgen eine Teilnahme am Gewinnspiel hat. Bei einem 15jährigen Schüler kann man sie häufig voraussetzen, bei einem 12jährigen hingegen nicht.

Die Tragweite einer Entscheidung können Sie aber auch als Erwachsener nur überschauen, wenn Sie hinreichend informiert werden. Eine Vertragsklausel, die ein Unternehmen zu einer Datenverarbeitung berechtigen soll, muss dem entsprechend klar den Zweck der Verarbeitung beschreiben. Wenn eine Datenübermittlung an andere Unternehmen nicht selbstverständlich ist, muss eine Einwilligungsklausel auch beschreiben, an wen Ihre Daten übermittelt werden.
Außerdem müssen Sie zumindest eine ungefähre Vorstellung haben, in welchem Umfang personenbezogene Daten über Sie verarbeitet werden.

Beispiel 29 | Zahlreiche Unternehmen bieten Rabattkarten/Kundenkarten[19] an. Solche Karten werden in Kundenbindungsprogrammen eingesetzt. Sie dienen nicht nur dazu, Sie als Verbraucher mit Rabatten zu locken. Ihre Umsatzdaten werden auch erfasst und ausgewertet, ohne dass dies dem Kunden oft klar ist. Meist sind die eingeräumten Rabatte relativ gering, der erhoffte Nutzen für die Unternehmen aber sehr groß.

TIPP
Für Verbraucher

Rabattkarten / Kundenkarten

Datenschutzrechtlich sind Kundenbindungsprogramme häufig kritisch zu sehen. **Insbesondere wenn die Antragsformulare für die Rabattkarte/Kundenkarte keine klaren Informationen darüber enthalten, welche Daten über Sie gespeichert werden und was mit diesen Daten geschieht, sollten Sie die Finger von der Rabattkarte lassen!**
Häufig wird Ihr Kaufverhalten ausgewertet, um über Sie Nutzungsprofile und/oder Persönlichkeitsprofile zu erstellen. Das heißt: Es wird geprüft, welche Waren Sie mit der Karte kaufen, wie oft Sie die Karte benutzen, welche Geschäfte Sie bevorzugt aufsuchen usw.. Je nach Ausgestaltung des Systems werden Sie dann gezielt zu Werbezwecken angesprochen.
Besondere Vorsicht, wenn Sie beim Antrag Ihr Einkommen offenlegen sollen! Einige Kundenbindungsprogramme verwenden Ihre Daten sogar zu Bonitätsprüfungen (Kreditwürdigkeitsprüfungen). Es ist dann nicht auszuschließen, dass Ihr Konsumverhalten mit Ihren Einkommensverhältnissen abgeglichen wird.
Sind die Daten erst einmal erfasst, werden sie bis zu 30 Jahre lang (!) gespeichert. Fadenscheiniges Argument der Kartenverwender: Das Zivilrecht sehe eine solch lange Verjährungsfrist vor, also müsste man so lange mit Forderungen der Kunden rechnen.
Lesen Sie die Geschäftsbedingungen einer solchen Karte genau durch!
Zu welchen Zwecken werden Ihre Daten verarbeitet: Werden die Vertragspartner der Rabattkarte / Kundenkarte genannt? Erhalten diese Vertragspartner Ihre Daten oder (besser) nur anonymisierte Auswertungen? Welche Daten werden vom Kartenbetreiber verarbeitet?
Bei manchen Rabattkartensystemen können Sie bestimmte Kaufbeträge nachträglich einreichen, sodass Ihnen nichts verloren geht, wenn Sie sich Zeit lassen. Lassen Sie sich vor Allem nicht vom Kassenpersonal dazu überreden, den Antrag auf eine Rabattkarte gleich an der Kasse auszufüllen: Natürlich ist das Personal angehalten, möglichst viele Kunden für solche Programme zu gewinnen. Überdies hat es regelmäßig kein oder nur wenig Wissen darüber, was mit Ihren Daten geschieht. Es weiß also eigentlich nicht, was es Ihnen empfiehlt.

Unternehmen verwenden häufig Allgemeine Geschäftsbedingungen, um die Rechte und Pflichten aus einem Vertrag festzulegen. Unter Allgemeine Geschäftsbedingungen werden vor allem Vertragsformulare/Vordrucke verstanden. Hier werden die Vertragsbedingungen nicht mehr besonders ausgehandelt, sondern vom Unternehmen gestellt. Nicht ohne Grund ist dabei vom „Kleingedruckten" die Rede. Man kann bei solchen Vertragsformularen eine Vielzahl von Regelungen „verstecken". Das BDSG sieht vor, dass Einwilligungen in Datenverarbeitungsvorgänge **optisch hervorgehoben** werden müssen, wenn sie mit anderen Erklärungen abgegeben werden.[20] Das BDSG soll so das „Verstecken" von Einwilligungsklauseln verhindern.

Beispiel 30 | Die meisten Supermärkte und Kaufhäuser ermöglichen mittlerweile die Zahlung mit EC-Karte. Falls Sie dabei nicht Ihre Geheimzahl verwenden müssen, sehen die Kassenbons auf der Rückseite Lastschriftermächtigungen vor. Für den Fall, dass die Lastschrift nicht erfolgreich ist, wird das Unternehmen „ermächtigt", von Ihrer Bank Ihre Adressdaten zu verlangen. Schauen Sie sich bei Gelegenheit einmal an, welche Kassenbons diese Ermächtigung zur Datenerhebung im Druckbild hervorheben!

TIPP
Für Verbraucher

Lastschriftermächtigung

Lastschriftermächtigungen auf dem Kassenbon und andere Allgemeine Geschäftsbedingungen fassen häufig mehrere Erklärungen zusammen. Einwilligungen in eine Datenverarbeitung sind häufig dabei, **ohne dass sie hervorgehoben sind.** Obwohl dann Ihre Einwilligungserklärung **nicht wirksam** erteilt worden ist, nehmen die Unternehmen diese Einwilligung als Grundlage für die Verarbeitung Ihrer Daten.
Überdies schalten manche Unternehmen bei dem Forderungseinzug dritte Stellen ein, ohne Sie hierüber zu informieren. Zum Beispiel werden damit Inkassounternehmen und manchmal sogar Banken/Sparkassen (Kreditinstitute) beauftragt. Solange Sie als Verbraucher damit rechnen müssen (bei Inkassounternehmen), kann das rechtmäßig sein. Soweit Sie nicht damit rechnen müssen (bei Kreditinstituten), ist die Datenbeschaffung durch den Beauftragten unzulässig, wenn Sie nicht vor Ihrer Einwilligung darüber informiert werden.

TIPP
Für Verbraucher

Verbrauchertipp: Lastschriftermächtigung

Ihr Kreditinstitut kann sich aufgrund des Wettbewerbsdrucks genötigt sehen, Auskünfte an solche Unternehmen selbst dann zu erteilen, wenn es die Einwilligungserklärung als mängelbehaftet ansieht. Wenn Ihr Kreditinstitut die Auskünfte konsequent verweigert, läuft es Gefahr, dass seine EC-Karten vom Handel nicht mehr akzeptiert werden.
Das wäre unfair, weil die entsprechenden Supermärkte bzw. Warenhäuser das Risiko der datenschutzwidrigen Ausgestaltung ihrer Einwilligungserklärungen auf die Kreditinstitute verlagern. Sollten Sie im Zusammenhang mit einer Lastschriftermächtigung Bedenken hinsichtlich der Rechtmäßigkeit der Einwilligung haben, können Sie sich also ohne moralische Bedenken an Ihre Aufsichtsbehörde wenden. Sie überprüft dann deren Übereinstimmung mit dem Datenschutzrecht. Alternative natürlich immer: wieder mehr in bar bezahlen.

Gesetzliche Rechtsgrundlagen für eine Datenverarbeitung im BDSG (§§ 28-30)

Auch wenn keine Einwilligung des Betroffenen vorliegt, kann die Verarbeitung personenbezogener Daten rechtsmäßig sein. Die Verarbeitung wird unter bestimmten Voraussetzungen durch allgemeine Vorschriften gestattet, sie ergeben sich für nicht–öffentliche Stellen aus dem BDSG[21] oder aus anderen Gesetzen (so genannte „bereichsspezifische Regelungen").

Das BDSG unterscheidet zwischen der Verarbeitung zu eigenen Geschäftszwecken[22] und der geschäftsmäßigen Verarbeitung zum Zwecke der Übermittlung.[23] Eine geschäftsmäßige Verarbeitung zum Zweck der Übermittlung liegt immer dann vor, wenn ein Unternehmen Daten sammelt, nur um sie Dritten zur Verfügung zu stellen. Dient eine Verarbeitung (auch) eigenen Belangen, liegt eine Verarbeitung zu eigenen Geschäftszwecken vor.

Beispiel 31 | Eine Handels- und Wirtschaftsauskunftei sammelt und speichert bonitätsrelevante Daten über Unternehmen und Personen, die am Wirtschaftsverkehr teilnehmen. Die Speicherung erfolgt ausschließlich zu dem Zweck, diese Daten ihren Kunden auf Anfrage zu übermitteln. Für jede Übermittlung verlangt die Auskunftei ein Entgelt. Hier liegt eine geschäftsmäßige Erhebung und Verarbeitung personenbezogener Daten zum Zweck der Übermittlung vor.

Beispiel 32 | Die Personalabteilung einer Auskunftei verarbeitet auch personenbezogene Daten ihrer Mitarbeiter. Diese Daten sollen aber nicht an Dritte verkauft werden, sondern dienen unmittelbar dem eigenen Geschäftsbetrieb. Hier liegt eine Datenverarbeitung für eigene Geschäftszwecke vor.

Beispiel 33 | Ein Warenversandhandelsunternehmen ist Vertragspartner der SCHUFA (oder einer anderen Auskunftei). Es übermittelt personenbezogene Daten über eine Forderung an die SCHUFA. Diese Übermittlung ist eine Datenverarbeitung für eigene Geschäftszwecke, weil die Daten nicht ausschließlich erhoben wurden, um sie anderen zur Verfügung zu stellen, sondern auch für die eigene Vertragsabwicklung. Die SCHUFA selbst verarbeitet die Daten für fremde Zwecke.

Generell gilt, dass ein Unternehmen die Zwecke der beabsichtigten Verarbeitung konkret festlegen muss.[24]

HINWEISE
Für Unternehmen

Festlegung von Verarbeitungszwecken

Grundsätzlich ist es schon aus Beweiszwecken zu empfehlen, Verarbeitungszwecke schriftlich festzulegen. Verarbeiten Sie eine Vielzahl von gleich gearteten Datenkategorien, kann dies auch in der Verfahrensübersicht nach § 4e/in der Verfahrensmeldung nach § 4d geschehen. Voraussetzung hierfür ist allerdings, dass diese hinreichend konkret ausgestaltet ist.
„Hinreichend" heißt: Anhand Ihrer Angaben muss eine kursorische Rechtmäßigkeitsprüfung möglich sein.

Verarbeitung zur Abwicklung eines Vertrags mit dem Betroffenen (§ 28 Abs. 1 Nr. 1)

Eigentlich ist es eine Selbstverständlichkeit, dass Unternehmen Ihre personenbezogenen Daten verarbeiten, die erforderlich sind, um einen Vertrag mit Ihnen abzuwickeln. Da das BDSG von der Grundregel des Datenschutzes ausgeht (keine Verarbeitung personenbezogener Daten ohne besondere Rechtfertigung), sieht es aber eine besondere Rechtsvorschrift vor, die die Datenverarbeitung zur Vertragsabwicklung erlaubt.[25] Die Datenverarbeitung muss allerdings auch zur Vertragsabwicklung notwendig sein (Erforderlichkeitsprinzip).

Beispiel 34 | Viele Unternehmen verlangen routinemäßig (in Vertragsformularen) Angaben, die zur Vertragsabwicklung nicht notwendig sind. Notwendig ist beispielsweise häufig der Name und die Adresse des Kunden, in der Regel nicht erforderlich sind hingegen Telefonnummer, Telefaxnummer und E-Mailadresse. Ob die Angabe des Geburtsdatums wirklich erforderlich ist, ist häufig auch fraglich. Gleichwohl werden solche Angaben zumeist nicht als freiwillig gekennzeichnet.

Beispiel 35 | Wenn ein Kunde bei einer Bank oder Sparkasse einen Kredit aufnehmen will, so wird von ihm häufig jährlich eine detaillierte Vermögensaufstellung, ein Einkommensteuerbescheid und eine Einkommensteuererklärung mit Anlagen abverlangt. Bei einer Kreditsumme über 250.000 Euro dürfen Kreditinstitute in der Regel solche Informationen einholen.[26] Wenn der Gesamtkredit aber erheblich niedriger ausfällt und genügend Sicherheiten angeboten werden, ist eine solche Datensammlung grundsätzlich nicht erforderlich – vorausgesetzt, der Kunde kommt seinen Zahlungspflichten ordnungsgemäß nach.[27]

TIPP
Für Verbraucher

Angaben auf Vertragsformularen

Wenn Vertragsformulare überflüssige Angaben vorsehen, müssen Sie diese nicht ausfüllen. Gerade bei Telefon/Telefax/E-Mail sollten Sie immer prüfen, ob Sie eine Kontaktaufnahme auf diesem Wege durch den Vertragspartner wirklich wünschen. An der fehlenden Angabe zu Telefon/Telefax/E-Mail scheitert im Normalfall kein Vertragsschluss.
Sie können deshalb ruhig auch „Kleinigkeiten" berücksichtigen: Halten Sie Mittagsschlaf? Dann sollten Sie vielleicht sparsam mit Ihrer Telefonnummer sein, denn es ist nicht auszuschließen, dass Sie in der Mittagszeit angerufen werden – Unternehmen machen häufig keine festen Mittagspausen.
Prüfen Sie dabei auch, ob das Unternehmen Sie zu Werbezwecken kontaktieren will (dazu siehe unten mehr).
Wenn ein Unternehmen bestimmte Angaben als freiwillig kennzeichnet (Kennzeichnung der Freiwilligkeit), heißt das zwar noch nicht zwingend, dass die anderen verlangten Angaben wirklich erforderlich sind, immerhin dokumentiert es aber, dass das Unternehmen sich Gedanken um Ihr Selbstbestimmungsrecht gemacht hat (ein Pluspunkt für Sie?).

Speziell das Geburtsdatum ist ein wichtiger Bestandteil von Datensammlungen und Datenauswertungen. Nicht alle, aber viele Unternehmen bilden daraus Persönlichkeitsprofile ihrer Kunden. Das konkrete Geburtsdatum dient damit der eindeutigen Feststellung der Person. Beispielsweise kann Ihnen die Datenverarbeitung besser „nachfolgen", wenn Sie umziehen. Daraus folgt allerdings nicht zwingend, dass die Information „Geburtsdatum" generell datenschutzwidrig verlangt wird.

Beispiel 36 | Bei der Kontoeröffnung ist die Erfassung des Geburtsdatums datenschutzrechtlich nicht zu beanstanden, soweit sie zur Identifizierung des Kontoinhabers beiträgt. Ohne eine klar formulierte Einwilligung darf das Geburtsdatum allerdings grundsätzlich nicht zu Zwecken der Kundenbindung (Customer-Relationship-Management) verwendet werden.[25]

Beispiel 37 | Im Zusammenhang mit dem Jugendschutz oder beim Eingehen finanzieller Verpflichtungen ist in einigen Fällen die Angabe des Geburtsdatums – bzw. genauer: des Alters - erforderlich, um sicherzustellen, dass der Besteller volljährig bzw. handlungsfähig ist.

TIPP
Für Verbraucher

Angabe des Geburtsdatums

Leuchtet Ihnen nicht ein, warum ein Unternehmen von Ihnen die Angabe des Geburtsdatums oder anderer Informationen verlangt, fragen Sie einfach nach dem Zweck der Datenerhebung! Das Unternehmen **ist verpflichtet**, Ihnen den Zweck mitzuteilen.

HINWEISE
Für Unternehmen

Erhebung von personenbezogenen Daten

Prüfen Sie vor der Gestaltung von Vertragsformularen, welche Informationen Ihrer Kunden Sie wirklich benötigen! Beachten Sie, dass der Zweck der Datenverarbeitung **konkret festzulegen** ist (Zweckbindung)[29]. Kennzeichnen Sie freiwillige Angaben – Fairness gegenüber den Kunden zahlt sich aus.

Das BDSG setzt bestimmte Verarbeitungsvorgänge der Datenverarbeitung zur Vertragsabwicklung gleich. Das Gesetz spricht von „vertragsähnlichen Vertrauensverhältnissen". Voraussetzung hierfür ist eine Beziehung zwischen Ihnen und einer Stelle, die in ihrer Art und Weise einem Vertragsverhältnis gleicht.

Beispiel 38 | Eine Mitgliedschaft in einem Verein wird rechtlich meist nicht als „Vertragsverhältnis" bezeichnet, weil regelmäßig kein vertragstypisches Leistungs-Gegenleistungsverhältnis besteht. Datenschutzrechtlich ist das Mitgliedschaftsverhältnis aber „vertragsähnlich", weil ähnlich wie bei einem Vertrag bestimmte Datenverarbeitungsprozesse erforderlich sind, um den gemeinsamen Vereinszweck zu fördern.[30]

Beispiel 39 | Ein vertragsähnliches Vertrauensverhältnis kann auch vorliegen, wenn zwischen Ihnen und einem Unternehmen noch kein Vertragsverhältnis besteht, Sie aber bereits Kontakte unterhalten, z. B. konkrete Vertragsverhandlungen führen. Regelmäßig ist dafür aber erforderlich, dass Sie den Anstoß für den Kontakt gegeben haben (zum Beispiel: Bewerbung auf einen Arbeitsplatz).

Sonstige Datenverarbeitung für eigene Geschäftszwecke (§ 28 Abs. 1 Nr. 2)

Liegt kein Vertragsverhältnis vor oder ist eine Datenverarbeitung nicht erforderlich, um ein Vertragsverhältnis mit Ihnen als Betroffenem abzuwickeln, kann sich ein Unternehmen unter Umständen darauf berufen, dass es ein sonstiges berechtigtes Interesse an der Datenverarbeitung hat. Hierfür sind allerdings besondere Rechtmäßigkeitsbedingungen zu erfüllen.

Zunächst muss die Verarbeitung für einen eigenen, berechtigten Zweck erforderlich sein.

Beispiel 40 | Typisch ist die Datenverarbeitung zur Vorbeugung bestimmter Geschäftsrisiken. Ein Unternehmen kann hierfür eine hausinterne Warndatei einrichten, um Betrugsversuchen unredlicher Kunden vorzubeugen. Eine Warndatei ist nicht zur Vertragsabwicklung erforderlich, kann aber berechtigten (Eigenschutz-) Interessen des Unternehmens dienen.

Beispiel 41 | Eine Datenverarbeitung im Interesse eines Dritten ist keine Datenverarbeitung im eigenen berechtigten Interesse (hierfür gibt es eine gesonderte Rechtsgrundlage[31] mit anderen Rechtmäßigkeitsbedingungen).

Hinweise **Für Unternehmen**

Einrichtung einer Warndatei

Die Einrichtung einer Warndatei unterliegt dem strikten Gebot der Erforderlichkeit! Sie müssen einen konkreten Zweck festlegen[32], für den die Nutzung der Warndatei zulässig sein soll. Daten dürfen nur bei konkreten und eindeutigen Missbrauchsfällen gespeichert werden. Zu empfehlen ist, dass den Bearbeitern lediglich vorgegebene Begriffe zur Auswahl gegeben werden. Persönliche, abwertende Anmerkungen haben in einer Warndatei nichts zu suchen, sie dienen nicht zur Abwehr von Missbrauchsfällen. Beachten Sie, dass Missbrauchsdaten nicht unbegrenzt gespeichert werden dürfen[33]. Bei allen Vorbehalten gegenüber festen Speicherfristen können Ihnen die Vorschriften über das Schuldnerverzeichnis der Amtsgerichte (§ 915 ff. der Zivilprozessordnung) einen **Anhaltspunkt** für eine zulässige Speicherfrist bieten: Sie gehen von einer Speicherfrist von maximal drei Jahren aus.

Wenn ein Unternehmen personenbezogene Daten für eigene Zwecke verarbeitet, darf kein Grund zu der Annahme bestehen, dass schutzwürdige Belange des Betroffenen der Verarbeitung entgegenstehen.[34]

Beispiel 42 | (Klingt absurd, ist aber tatsächlich geschehen!) Ein Sauna- und Schwimmbadbetreiber plant wegen einiger vorangegangener Diebstähle, seine Umkleidekabinen mithilfe von Videokameras überwachen zu lassen. Es liegt auf der Hand, dass die meisten Menschen darin ihre Intimsphäre auf das Gröbste verletzt sehen, selbst wenn Hinweisschilder „Achtung Videoüberwachung!“ aufgehängt werden.

Beispiel 43 | Sie erfahren durch Zufall, dass ein Unternehmen Ihre Hobbies speichert, um Sie besser umwerben zu können. Sie legen bei dem Unternehmen Widerspruch gegen die weitere Speicherung ein. Schon aus diesem Grund steht Ihr schutzwürdiges Interesse einer weiteren Speicherung zu Werbezwecken entgegen.

Erleichterte Datenverarbeitung bei allgemein zugänglichen Daten (§ 28 Abs. 1 Nr. 3)

Verarbeitet ein Unternehmen Ihre Daten zur Vertragsabwicklung oder, um damit eigene berechtigte Interessen zu verfolgen, muss es prüfen, welche Daten es für diese Datenverarbeitung benötigt. Diese Prüfpflicht entfällt, wenn das Unternehmen allgemein zugängliche Daten verwendet. Allgemein zugänglich sind Informationen nur, wenn sie einem nicht bestimmbaren Personenkreis zugänglich gemacht wurden.

Beispiel 44 | Ein Unternehmen ermittelt anhand des Telefonbuchs Ihre Adresse. Damit liegt eine Verwendung allgemein zugänglicher Daten vor.

Beispiel 45 | Das Rundschreiben eines Vereins vermittelt noch keine allgemein zugänglichen Daten, weil sich das Schreiben regelmäßig nur an die Mitglieder richtet.

Liegen allgemein zugängliche Daten vor, muss das Unternehmen für die Datenverarbeitung nur prüfen, ob möglicherweise Ihre überwiegenden schutzwürdigen Interessen der Verarbeitung Ihrer Daten entgegenstehen.

Anschreiben zu Werbezwecken (§ 28 Abs. 3 Nr. 3, Abs. 4)

Ärgern Sie sich bisweilen auch darüber? Sie erhalten persönlich an Sie adressierte Schreiben und stellen fest: Schon wieder nur Werbung? Bei Post von Unternehmen, mit denen Sie Verträge abgeschlossen haben, sollten Sie gleichwohl jeden Brief öffnen (es könnten vertragsrelevante Unterlagen beigefügt sein). Selbst bei Schreiben, die erkennbar von fremden Unternehmen stammen, kann man nicht unbedingt riskieren, sie ungelesen wegzuwerfen.

Beispiel 46 | Sie haben einen Vertrag mit einem Telefonanbieter abgeschlossen. Dieser wird von einem anderen Unternehmen aufgekauft. Dieses Unternehmen teilt Ihnen mit, dass es Rechtsnachfolger Ihres ursprünglichen Vertragspartners ist und macht zugleich eine Forderung gegen Sie geltend.

Auch wenn das deutsche Recht verlangt, dass Werbung nicht klar feststehende Unwahrheiten verbreiten darf, sehen manche Unternehmen die Maßstäbe an die Wahrheitspflicht recht „locker“.

TIPP
Für Verbraucher

Anschreiben zu Werbezwecken / Gewinnmitteilungen

Vorsicht bei Gewinnmitteilungen! Sollten Sie von Ihnen unbekannten Unternehmen die Mitteilung erhalten haben, dass Sie gewonnen haben: seien Sie vorsichtig! Im Zweifel holen Sie am besten Rat bei Ihrer Verbraucherzentrale. Häufig wird der Gewinn nicht ausgeschüttet, weil an verborgener Stelle auf die Unverbindlichkeit der Gewinnmitteilung hingewiesen wird. Andere Mitteilungen knüpfen die Ausschüttung des „Gewinns“ an bestimmte Bedingungen, die den Vorteil des „Gewinns“ aufheben.
Insbesondere wenn als Absender ausschließlich eine Postfachadresse oder eine ausländische Adresse angegeben wird, ist besondere Zurückhaltung angebracht, weil hierdurch eine Geltendmachung von Rechten erschwert wird.
So verlockend eine Mitteilung auch klingen mag, denken Sie daran: Kein Ihnen fremdes Wirtschaftsunternehmen verschenkt etwas ohne die Aussicht auf erheblichen Mehrgewinn!

Zurzeit gestattet der Gesetzgeber die Nutzung Ihrer Daten zu Werbezwecken zu erleichterten Bedingungen. Solange ein Unternehmen „nur“ Ihren Namen, eine Gruppenzugehörigkeit, Ihre Adressdaten und Ihr Geburtsjahr zu Werbezwecken verwendet, darf es grundsätzlich ganze Listen personenbezogener Daten beliebig an dritte Unternehmen verkaufen (so genanntes Listenprivileg der Adressdatenverarbeitung). Voraussetzung ist nur, dass „kein Anhaltspunkt zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat“.[35]

Beispiel 47 | Eine Gruppenzugehörigkeit kann darin bestehen, dass Sie Kunde eines bestimmten Unternehmens sind oder an einer ganz bestimmten Informationsveranstaltung teilgenommen haben.

HINWEISE
Für Unternehmen

Gruppenzugehörigkeit bei Werbeansprache

Die E-Mailadresse, die Telefonnummer, die Telefaxnummer und das genaue Geburtsdatum unterliegen nicht dem Listenprivileg des § 28 Abs. 3 Nr. 3 BDSG!

Eine Gruppenzugehörigkeit liegt nicht vor, wenn Sie mehrere Eigenschaften in einen Sammelbegriff zu verknüpfen suchen.

Beispiel 48 | Die Information „Herr Müller gehört zu den solventen Kunden des Unternehmens A“ geht über das Erfordernis einer Gruppenzugehörigkeit hinaus:
Denn eine Gruppenzugehörigkeit ergibt sich aus der Tatsache, dass Herr Müller Kunde des A ist. Die Zahlungskraft ist eine weitere Information, die zusätzlich gegeben wird. Eine andere Interpretation des § 28 Abs. 3 Nr. 3 BDSG ist nicht möglich. Ansonsten wäre dem Missbrauch des so genannten Listenprivilegs Tür und Tor geöffnet (man bräuchte nur noch Gruppenzugehörigkeit um beliebige Informationen zu ergänzen: „Herr Müller gehört zu der Gruppe, die Kunde des A ist, eine gute Zahlungsmoral hat, gerne Pizza mit Oliven isst und die ihren Urlaub in Italien verbringt usw.“).

Der wichtigste Anhaltspunkt, der gegen die Inanspruchnahme des Listenprivilegs spricht, ist Ihr Widerspruch.

TIPP
Für Verbraucher

Widerspruch gegen Werbung bereits bei Vertragsschluss

Zögern Sie nicht, bei Vertragsabschlüssen auf Vertragsformularen folgenden handschriftlichen Vermerk anzubringen:
„Bitte keine Übermittlung oder Nutzung meiner Daten zu Werbezwecken!“
Seriöse Vertragspartner respektieren diesen Vermerk.
Unternehmer, die Ihre Anmerkung ignorieren, verhalten sich nicht nur unseriös, sondern möglicherweise auch ordnungswidrig oder strafbar.[36]

HINWEISE
Für Unternehmen

Widerspruch gegen Werbung bereits bei Vertragsschluss

Finden Sie bei Vertragsabschlüssen auf Vertragsformularen folgenden (oder einen ähnlichen) handschriftlichen Vermerk vor: „Bitte keine Übermittlung oder Nutzung meiner Daten zu Werbezwecken!“, dann sind Sie **verpflichtet**, dies als Widerspruch gegen die Datenverwendung zu Werbezwecken zu werten. Immer dann wenn ein solcher Widerspruch vorliegt, ist eine Datenauswertung im Rahmen von Data -Warehouse- und Data-Mining-Systemen schon deshalb unzulässig (und zwar unabhängig von sonstigen datenschutzrechtlichen Bedenken gegen solche Systeme).
Falls Sie den Hinweis Ihres Vertragspartners vernachlässigen und die Daten Ihres Vertragspartners zu Werbezwecken verwenden (insbesondere an Dritte übermitteln), verhalten Sie sich vorsätzlich datenschutzrechtswidrig und können mit empfindlichen Geldbußen (bis zu 250.000 Euro pro Verstoß) belegt werden.

TIPP
Für Unternehmen

Widerspruch gegen Werbung bereits bei Vertragsschluss

Ermöglichen Sie Ihren Kunden **bereits bei Vertragsschluss**, der Verwendung ihrer Daten zu Werbezwecken zu widersprechen.
Hierzu bedarf es lediglich einer Textzeile und eines Ankreuzkästchens „Falls Sie unsere Werbung wünschen, kreuzen Sie bitte das nebenstehende Kästchen an. ☐“ Weniger datenschutzfreundlich, aber wohl auch datenschutzkonform wäre die Formulierung: „Falls Sie keine Werbung wünschen, kreuzen Sie bitte das nebenstehende Kästchen an: ☐“).
Auf diese Weise ermöglichen Sie Ihren Kunden, unbürokratisch das diesen gesetzlich zustehende Widerspruchsrecht auszuüben. Zugleich erhalten Sie eine Rückmeldung zur Akzeptanz Ihrer Werbezuschriften: Sollte Ihre Einschätzung zutreffen, dass die meisten Kunden von Ihnen Werbe- und Informationszuschriften wünschen, ändert sich für Sie nichts Wesentliches. Gleichwohl fördern Sie hiermit die Akzeptanz Ihrer Dienstleistungen. Falls Ihre Einschätzung nicht zutreffen sollte, reduzieren Sie die Kosten im Direktmarketingbereich, weil Sie überflüssige Werbung einsparen.

Werden Sie von Unternehmen zu Werbezwecken angesprochen, müssen Sie darauf hingewiesen werden, dass Sie das Recht haben, der Nutzung Ihrer Daten zu Werbezwecken zu widersprechen (Unterrichtungspflicht bei Ansprache zu Werbezwecken)[37]. Sie müssen dabei tatsächlich in die Lage versetzt werden, Ihren Widerspruch effektiv auszuüben.

Beispiel 49 | Ein Unternehmen schreibt Sie persönlich an und wirbt für ein Produkt. Am Ende des Anschreibens steht (meist in kleiner Schrift): „Sie haben das Recht, der Nutzung Ihrer Daten zu Werbezwecken zu widersprechen." Eine Adresse, an die Sie den Widerspruch richten können, wird nicht angegeben. Wenn Sie Ihren Widerspruch nicht effektiv bei der im Briefkopf angegebenen Adresse ausüben können, ist die Unterrichtung nutzlos. Dann genügt diese auch nicht den datenschutzrechtlichen Anforderungen.

TIPP
Für Verbraucher

Unterrichtung über Widerspruchsrecht bei Werbeansprache

Jedes Unternehmen, das Sie persönlich zu Werbezwecken anschreibt, **ist verpflichtet,** Sie über Ihr Widerspruchsrecht zu informieren. Persönlich angesprochen sind Sie immer dann, wenn das Unternehmen bei der Anrede Ihren Namen verwendet oder wenn auf dem Briefumschlag Ihre Postadresse angegeben ist. Wenn Sie sich über eine solche Werbezuschrift ärgern und diese Unterrichtung nicht erfolgt, können Sie sich an Ihre Datenschutzaufsichtsbehörde wenden.

Die derzeitige Rechtslage ist aus Sicht des Unabhängigen Landeszentrums für Datenschutz unbefriedigend. Denn sie zwingt den Verbraucher dazu, stets auf bereits erfolgte Belästigungen zu reagieren. Überdies ist der Erfolg Ihres Widerspruchs nicht immer gewiss (falls es Schwierigkeiten gibt: nehmen Sie die Hilfe der Datenschutzaufsichtsbehörden in Anspruch!). Bei einer Straßenumfrage hat das Unabhängige Landeszentrum für Datenschutz festgestellt, dass die überwältigende Mehrheit der befragten Bürgerinnen und Bürger Schleswig-Holsteins mehr Selbstbestimmung bei der Verarbeitung personenbezogener Daten zu Werbezwecken einfordert.

Aus diesen Gründen setzen sich das Unabhängige Landeszentrum für Datenschutz und der VZBV für eine Änderung des BDSG ein:
Künftig soll die Zulässigkeit der Verarbeitung zu Werbezwecken von der Einwilligung des betroffenen Verbrauchers abhängen.[38]

TIPP
Für Verbraucher

Robinson-Liste gegen Werbezuschriften

Der private Deutsche Direkt-Marketing-Verband (DDV) bietet Verbrauchern an, sich in die so genannte Robinsonliste eintragen zu lassen (der Name Robinsonliste lehnt sich an den Romanhelden Robinson Crusoe an, der jahrelang auf einer einsamen Insel verbracht hat).
Die dem DDV angeschlossenen Unternehmen erhalten dann die Nachricht, dass Sie keine Werbezuschriften wünschen. Angeblich soll die Eintragung Werbezuschriften um bis zu vierzig Prozent verringern. Die Eintragung gilt allerdings nur für fünf Jahre.
Ein Formular für die Aufnahme in die Robinsonliste erhalten Sie bei: DDV, Robinson-Liste, Postfach 1401, 71243 Ditzingen.

Das oben erwähnte Listenprivileg (mit den genannten Einschränkungen!) gilt auch für Markt- und Meinungsforschungsinstitute.

TIPP
Für Verbraucher

Markt- und Meinungsforschungsinstitute

Grundsätzlich machen Sie nichts falsch, wenn Sie die Bitte zur Beantwortung von Meinungsumfragen nicht beantworten. Markt- und Meinungsforschungsinstitute verfolgen zumeist nicht wissenschaftliche Interessen, sondern sammeln Ihre Daten, um sie an Dritte zu verkaufen. Natürlich gibt es auch Verbraucherbefragungen, die nicht kommerziellen Interessen dienen. Ihnen sind meistens Empfehlungsschreiben von Behörden beigefügt. Solche Empfehlungsschreiben sind ein Indiz (meist aber auch nicht mehr!) dafür, dass das Institut seriös arbeitet und Ihre Daten nicht kommerziell ausbeutet.

Wenn Sie prinzipiell gerne an Meinungsumfragen teilnehmen, achten Sie in Ihrem eigenen Interesse dennoch darauf, ob das Institut Sie darüber informiert, was mit Ihren Daten geschieht. Wenn es um „rein statistische Angaben" gehen soll, wozu müssen Sie Ihren Namen nennen?

Werbefaxe

Sie sind Faxbesitzer? Dann kennen Sie vielleicht das Problem: Sie werden zu jeder Tages- und Nachtzeit gestört, weil Ihr Faxgerät anspringt und unerwünschte Werbefaxe ausdruckt.[39] In Deutschland ist die Zusendung von unerwünschten Werbefaxen nach der Rechtsprechung unzulässig. Das wird Ihnen regelmäßig wenig helfen. Insbesondere stammen die Werbefaxe häufig von ausländischen Firmen, die man mit deutschen aufsichtsbehördlichen Maßnahmen kaum schrecken wird.

TIPP
Für Verbraucher

Verhalten bei Werbefaxen

Regel 1:
Beantworten Sie niemals per Fax ein Werbefax!
Die dort angegebenen Nummern sind in der Regel kostenpflichtig.

Regel 2:
Prüfen Sie, ob Sie Telefaxe von Mehrwertdienstenummern (0180, 0190 usw.) wirklich benötigen. Falls nicht, sprechen Sie mit Ihrem Telefonanbieter über die Möglichkeiten der Sperrung des Empfangs von Absendern, die diese Nummern verwenden. Sie dürfte allerdings kostenpflichtig sein und würde den Nachteil mit sich bringen, dass Sie selbst auch "positive" Mehrwertdienste nicht mehr in Anspruch nehmen können. Diese Methode ist vor allem dann zu empfehlen, wenn die Zusendung von Werbefaxen überhand nimmt.

Regel 3:
Gehen Sie sparsam mit der Veröffentlichung Ihrer Telefaxnummer um.

Regel 4:
Sollten Sie Werbefaxe erhalten, schalten Sie nachts das Faxgerät ab.

TIPP
Für Verbraucher

Robinsonliste für Werbefaxe

Auch für Telefaxanschlüsse gibt es eine Robinsonliste. Sie wird von der Retarus Network Services GmbH für den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. betrieben. Der Eintrag bei dieser Firma ist kostenlos (es sei denn, Sie wählen den Faxabruf: Dann fällt eine Gebühr von 12 Cent/Minute an). Angeblich soll dies zu einer erheblichen Reduzierung der deutschen Werbefaxe führen. Die Adresse lautet:
Retarus Network Services GmbH - Telefax-Robinsonliste – Fax: 01805-000 761.
Achtung! Lassen Sie sich nicht auf kostenpflichtige „Robinsonlisten“ ein! Missbrauch ist hier nicht ausgeschlossen!

Kein Widerspruch bei Werbefaxen!

Wenn Sie Telefaxwerbung erhalten, ist der Weg des Widerspruchs meistens nicht zu empfehlen. Er ist zu lang, zu aufwändig und überdies selten von Erfolg gekrönt, weil die werbenden Firmen meist eine kurze Lebensdauer haben.

Gibt es Datenarten, die besonders geschützt sind? (§ 3 Abs. 9, § 28 Abs. 6-9)

Ob sich eine Datenverarbeitung nachteilhaft für Sie auswirkt, hängt immer von den konkreten Bedingungen des Verarbeitungsvorganges ab. Insofern gibt es keine „ungefährlichen“ Daten. So kann sich Ihre Nationalität oder Ihr Alter in bestimmten Zusammenhängen ungünstig auswirken.

Beispiel 50 | Die Merkmale „Alter“, „Nationalität“, manchmal auch Wohnadressen spielen bei so genannten „Scorewerten“ (oder Ergebnisse von speziellen „Ratingverfahren“) eine Rolle. Diese Scorewerte werden von kreditgebenden Unternehmen (Banken, Versandhandel), von Versicherungen oder von Auskunfteien erstellt und dienen dazu, Ihre (wahrscheinliche) Kreditwürdigkeit oder ein sonstiges Vertragsrisiko in einer einzigen Zahl zu veranschaulichen. Dabei werden Ihre persönlichen Merkmale (z. B. 37 Jahre alt, Deutscher, wohnhaft in Kiel) mit den Erfahrungen abgeglichen, die das Unternehmen mit allen anderen Menschen gemacht hat, die ein gleiches Merkmal erfüllen (z. B. 2,4 % aller 37 Jährigen zahlen ihre Rechnungen unzuverlässig usw.).

Es gibt aber auch Daten, die erfahrungsgemäß ein höheres Risikopotential für die Betroffenen mit sich bringen. Der Gesetzgeber bezeichnet sie als „besondere Arten personenbezogener Daten“ [40] und stellt sie unter einen besonderen Schutz. Solche Daten dürfen nur mit Ihrer ausdrücklichen Einwilligung oder aber in engen Ausnahmefällen verarbeitet werden.[41]

Beispiel 51 | Wenn Sie Mitglied in einer Gewerkschaft sind, so kann sich diese Information in bestimmten Situationen negativ für Sie auswirken (etwa bei einer Bewerbung um einen Arbeitsplatz). Deshalb darf Ihre Gewerkschaft Ihre Daten zwar für Gewerkschaftszwecke verarbeiten, muss sie aber im Übrigen vertraulich behandeln.[42]

Beispiel 52 | Es liegt auf der Hand, dass ein Arzt bestimmte Krankheitsdaten verarbeiten können muss, um Sie gut behandeln zu können. Deshalb darf er die für die konkrete Behandlung notwendigen Daten verarbeiten. Es ist aber auch zu beachten, dass Krankheitsdaten sehr sensibel sind und nicht in unberufene Hände gehören. Der Arzt ist daher verpflichtet, Ihre Patientendaten vertraulich zu behandeln (Arztgeheimnis/Patientengeheimnis). Es geht niemanden etwas an, ob Sie wegen einer Erkältung oder wegen einer anderen Krankheit (z. B. Aids) behandelt werden!

TIPP
Für Verbraucher

Auf der Webseite des Unabhängigen Landeszentrums finden Sie ausführliche Informationen über Datenschutz in Krankenhäusern und Arztpraxen unter: www.datenschutzzentrum.de/medizin/

Gibt es besondere Verfahren der Datenverarbeitung, vor denen Sie besonders geschützt sind? (§§ 6a- 6c)

Bestimmte Arten der Verarbeitung unterliegen besonderen Rechtmäßigkeitsbedingungen. Dies sind Regelungen zu so genannten automatisierten Einzelentscheidungen[43], zur Videoüberwachung[44] und zu Chipkarten[45]. In der Praxis werden Sie vor allem der Videoüberwachung sehr häufig begegnen. Ausdrücklich geregelt ist nur die Videoüberwachung „öffentlich zugänglicher Räume“. Das sind räumliche Bereiche, die der Allgemeinheit zugänglich sind. Ein öffentlich zugänglicher Raum ist immer dann gegeben, wenn ihn jeder ohne besondere Voraussetzungen betreten kann.

Beispiel 53 | Warenhäuser während der Öffnungszeiten; Schalterräume von Banken und Sparkassen, Fußgängerzonen, Bahnhöfe usw.

Eine Überwachung durch private Stellen ist normalerweise nur in zwei Fällen zulässig: 1. wenn sie zur Wahrung des Hausrechts erforderlich ist, oder 2. wenn sie „zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ erforderlich ist. In beiden Fällen darf das schutzwürdige Interesse der Betroffenen nicht der Überwachung entgegenstehen.

Beispiel 54 | Das Hausrecht kann nur herangezogen werden, wenn sich der Beobachtete in dem räumlichen Bereich des Beobachters befindet. Typisch: Schalterhalle eines Kreditinstituts, Geschäftsräume eines Supermarktes usw., nicht hingegen die Fußgängerzone vor der Eingangstür.

Beispiel 55 | Berechtigte Interessen sind nur solche Interessen, die objektiv begründbar sind. Dazu gehört vor allem der Eigentumsschutz (aber nicht uneingeschränkt!! Die Abwehr von Bagatellschäden rechtfertigt nach der Rechtsprechung keine Videoüberwachung) und der Schutz vor Angriffen anderer Art (Sachbeschädigung, Unfallgefahr usw.).

Überwachung heißt nicht Aufzeichnung und erst recht nicht Veröffentlichung von Personenbildern. Letzteres kann sogar **strafbar**[46] sein!

TIPP

Für Verbraucher

Videoüberwachung

Sie werden videoüberwacht und sind neugierig, was dahinter steckt? Dann machen Sie doch einmal von Ihrem Recht auf Auskunft Gebrauch. Grundsätzlich muss Ihnen jede verantwortliche Stelle Auskunft über die Verarbeitung von Bilddaten erteilen, wenn Sie betroffen sind.

HINWEISE

Für Unternehmen

Videoüberwachung

Bei der Beurteilung der Erforderlichkeit einer Videoüberwachung ist ein strenger Maßstab anzulegen. Die Abwehr von Bagatellschäden rechtfertigt nach der Rechtsprechung keine Videoüberwachung. Es muss die begründete Erwartung bestehen, dass ohne eine Videoüberwachung Schäden eintreten. Die Aufzeichnung von Personenbildern ist nur zulässig, wenn sie „zum Erreichen des verfolgten Zwecks" erforderlich ist. Das heißt: Die Bildaufzeichnung muss notwendig sein, um Schäden abzuwehren oder Schadensersatzpflichtige ausfindig zu machen usw.
Ihre Interessen an der Videoüberwachung sind mit den Interessen der Betroffenen abzuwägen: Ist eine Videoüberwachung überhaupt erforderlich? Muss eine Bildaufzeichnung erfolgen oder genügt eine bloße Beobachtung (Monitoring)? Wie scharf müssen die Bilder sein: Müssen Personen wirklich erkennbar sein oder genügen Übersichtsaufnahmen?
Bildaufzeichnungen sind unverzüglich zu löschen, sobald sie für den erreichten Zweck nicht mehr erforderlich sind. Regelmäßig ist die Unverzüglichkeit nach mehr als drei Arbeitstagen nicht mehr gegeben, nur in Ausnahmefällen sind längere Speicherfristen zulässig.
Beachten Sie Ihre Verpflichtung, den Umstand der Beobachtung und die verantwortliche Stelle geeignet kenntlich zu machen. Maßgeblich ist dabei, ob der Betroffene durch die Unterrichtung in die Lage versetzt wird, seine Auskunftsrechte geltend zu machen. Häufig ist es nicht ausreichend, wenn nur eine Kamera sichtbar angebracht ist. Meistens sind Hinweisschilder („Vorsicht Videoüberwachung!" oder ein entsprechendes Kamerasymbol) erforderlich. Erfolgt durch Sie eine Identifizierung von Personen auf den Videoaufnahmen, so sind diese Personen entsprechend der allgemeinen Benachrichtungspflichten hierüber zu informieren.

[2]

Transparenz der Datenverarbeitung

Teil 2

Transparenz der Datenverarbeitung

In dem vorangegangenen Teil war schon öfter die Rede von Benachrichtigungs-, Unterrichtungs- und Informationspflichten und Auskunftsrechten. Alle diese Rechte und Pflichten dienen dazu, Ihnen als Betroffenen einen Überblick zu verschaffen, wer welche Informationen über Sie speichert. Man kann auch davon sprechen, dass personenbezogene Datenverarbeitung „transparent" (durchsichtig, durchschaubar) gemacht werden soll. Im Folgenden sollen diese Transparenzregeln in einen systematischen Zusammenhang gebracht werden.

Informationen, die Sie in der Regel erfahren können

In der Regel können Sie von einem Unternehmen Antwort auf folgende Fragen verlangen:

1. Werden Daten über Sie gespeichert und wenn ja, welche („gespeicherte Daten")?
2. Wer verarbeitet Ihre Daten („Identität der verantwortlichen Stelle")?
3. Von wem hat der gegenwärtige Datenverarbeiter Ihre Daten („Herkunft der der gespeicherten Daten")?
4. Zu welchen Zwecken sollen Ihre Daten verarbeitet werden („Zweckbestimmung")?
5. An welche Empfänger werden Ihre Daten weitergegeben („Datenempfänger")?

Das BDSG schreibt allerdings nicht ausdrücklich vor, dass ein Unternehmen Sie zu jeder Verarbeitungsphase über diese fünf Punkte informieren muss. Vielmehr trifft das Gesetz eine Vielzahl von Unterrichtungs-, Informations-, Benachrichtigungs- und Auskunftspflichten, die scheinbar im Umfang des Informationsgehalts erheblich von einander abweichen.[47] Warum ist das so? Dafür gibt es im Wesentlichen zwei Gründe. Erstens kann eine Information unterbleiben, wenn Sie auf Grund bestimmter Umstände ohnehin wissen, wer welche Daten wie verarbeitet (eine Grundregel der Transparenz). Zweitens geht es davon aus, dass es meistens genügt, wenn Sie wissen, dass eine Datenverarbeitung **durch eine bestimmte Stelle** erfolgt. Nur wenn Sie selbst mehr wissen wollen, sollen Sie auch mehr erfahren. Dazu müssen Sie allerdings selbst tätig werden.

Dementsprechend gestaltet das BDSG die Transparenzregeln situationsangepasst aus. Die folgenden Abschnitte zeigen Ihnen, in welchen Situationen Sie von Unternehmen welche Informationen erhalten müssen. Um Ihnen die Übersicht zu erleichtern, wird dabei zumeist auf die oben genannten fünf Punkte Bezug genommen.

Ein Unternehmen erhebt bei Ihnen Daten (§ 4 Abs. 3)

Ein Unternehmen beschafft sich bei Ihnen selbst personenbezogene Daten (Unterrichtung bei Datenerhebung).

> Beispiel 56 | Sie bestellen ein Sofa und müssen dazu einen Bestellschein ausfüllen.

Welche Informationen müssen Ihnen gegeben werden? Es gilt wieder die Grundregel, dass eine Information unterbleiben kann, wenn Sie aus anderen Umständen wissen, wer welche Daten wie verarbeitet.[48]
Also: Informationen über:

1. gespeicherte Daten: Nein. Da das Unternehmen die personenbezogenen Daten bei Ihnen selbst beschafft, wissen Sie, dass diese Daten gespeichert werden sollen. In Beispiel 56 muss Sie das Möbelunternehmen folglich nicht darüber informieren, dass es die im Bestellschein angegebenen Daten speichert!
2. die Identität der verantwortlichen Stelle: Ja. Das Unternehmen muss Sie über seine Identität aufklären. Sie glauben, dass sei selbstverständlich und deshalb überflüssig? Das Unabhängige Landeszentrum für Datenschutz hat bereits Unternehmen angetroffen, die unter acht verschiedenen Identitäten (Unternehmensnamen) aufgetreten sind![49] Gegen welches dieser Unternehmen wollen Sie im Streitfall Ihre Ansprüche geltend machen? Meistens reicht allerdings der Briefkopf des Bestellscheins aus, um die Identität eines Unternehmens festzustellen. Wenn das Möbelunternehmen im Beispiel 56 seinen Geschäftssitz im Briefkopf seiner Schreiben ordnungsgemäß angibt, genügt das zumeist als Information.

3. die Herkunft der gespeicherten Daten: Nein. Sie sind ja die Datenquelle!
4. die Zweckbestimmung: Ja. Sie können höchstens vermuten, aber nicht genau wissen, zu welchen Zwecken das Unternehmen Ihre Daten verwenden will. Deshalb muss über die beabsichtigten Zwecke der Verarbeitung unterrichtet werden.
5. die Datenempfänger: Jein.Bei der Datenerhebung genügt es, wenn das Unternehmen Ihnen mitteilt, an welche Empfängerkategorien Ihre Daten weitergeleitet werden sollen.

Beispiel 57 | Im Rahmen der Bestellung Ihres Sofas wünschen Sie, dass das Möbelunternehmen Sie beliefert. Wenn das Möbelunternehmen einen Spediteur mit der Anlieferung betraut, muss es Sie zumindest darüber informieren, dass es Ihre Adressdaten an einen Spediteur weitergibt, nicht unbedingt, welche Firma beauftragt wird.

TIPP
Für Verbraucher

Unterrichtungsklauseln bei Datenerhebung

Wenn Sie eine Unterrichtungsklausel vorfinden, achten Sie vor allem darauf, zu welchen Zwecken Ihre Daten verarbeitet und an wen sie übermittelt werden sollen. Hier liegen die meisten Missbrauchsmöglichkeiten und hier können Sie bereits Ihre Rechte geltend machen!
Wenn Sie bereits öfter Ärger mit Datenmissbrauch hatten und den eigentlichen Verursacher nicht ausfindig machen konnten, variieren Sie bei Bestellungen usw. Ihren Namen geringfügig (z. B.: Thomas A. Mustermann; Thomas B. Mustermann, Thomas C. Mustermann usw.). Ordnen Sie bestimmte Varianten bestimmten Unternehmen zu. Solche geringfügigen Variationen haben auf die Zustellbarkeit von Schreiben in der Regel keinerlei Auswirkungen, Sie erhalten aber eine Kontrolle darüber, wer bestimmte Daten zu welchen Zwecken an wen weitergegeben hat.

HINWEISE
Für Unternehmen

Unterrichtungsklauseln

Der Hinweis auf die Zweckbestimmung der künftigen Verarbeitung ist datenschutzrechtlich nicht geboten, wenn Sie die Daten ausschließlich zur Vertragsabwicklung verwenden wollen. Überflüssig ist der Hinweis aber nicht; insbesondere wenn Sie in einer Branche tätig sind, in der Kundendaten häufig zu Zwecken des Adresshandels verwendet werden. Rückmeldungen zeigen immer wieder, dass Kunden die Weiterveräußerung ihrer Daten als Vertrauensbruch empfinden („das sind doch meine Daten!“). Hier können Sie mit dem Satz „Wir verwenden Ihre Daten ausschließlich zur Vertragsabwicklung“ auf die Bedürfnisse das Vertrauen Ihrer Kunden eingehengewinnen.
Sie machen nichts falsch, wenn Sie die Betroffenen nur über die Kategorien von Empfängern unterrichten (Beispiel 57). Pflegen Sie langjährige Vertragsbeziehungen mit einem anderen Unternehmen, kann es aber auch sinnvoll sein, den konkreten Namen des Datenempfängers zu benennen. Eine kleine Geste, nicht Ihrem betroffenen Kunden, sondern auch Ihrem Geschäftspartner gegenüber!

Ein Unternehmen beschafft sich bei Dritten Ihre Daten, um sie für sich zu gebrauchen (§ 4 Abs. 2 S. 2, § 33 Abs. 1 S. 1)

Grundsätzlich müssen Unternehmen personenbezogene Daten beim Betroffenen, also bei Ihnen, erheben.[50] Diese Verpflichtung soll Sie in die Lage versetzen zu beurteilen, ob Sie gerade der anfragenden Stelle Informationen über sich preisgeben wollen oder nicht. Allerdings sieht das Gesetz Ausnahmen vor, die dazu geführt haben, dass viele Daten verarbeitende Unternehmen den Grundsatz der Direkterhebung beim Betroffenen missachten.

Eine Datenbeschaffung ohne Ihre Mitwirkung als betroffene Person ist zulässig, wenn das gesetzlich vorgesehen ist, der Geschäftszweck eine Informationserhebung bei Dritten erfordert oder eine Direkterhebung bei Ihnen einen unverhältnismäßigen Aufwand bedeuten würde. Dabei dürfen allerdings „keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.“[51]

Beispiel 58 | Eine Detektei soll Informationen über Sie herausfinden. In diesem Fall steht der Geschäftszweck Ihrer direkten Befragung entgegen. Aber: Wenn der Detektiv aus nichtigen Gründen eingeschaltet wird und sensible Informationen erforscht werden (z. B. Ihr Gesundheitszustand) wäre das unzulässig, weil Ihre schutzwürdigen Interessen das Ermittlungsinteresse des Auftraggebers offensichtlich überwiegen.

Beispiel 59 | Sie wollen von einer Bank einen Kredit erhalten. Die Bank holt Informationen über Ihre Kreditwürdigkeit (Bonität) bei der SCHUFA oder einer Handels- und Wirtschaftsauskunftei ein. Wenn der Aufwand für die Bank unverhältnismäßig groß wäre, von Ihnen selbst den Nachweis Ihrer Bonität zu erhalten, ist die Abfrage gerechtfertigt.

Speichert das Unternehmen Ihre personenbezogenen Daten zum ersten Mal „für eigene Geschäftszwecke", muss es Sie benachrichtigen (Benachrichtigung bei erster Speicherung).

Beispiel 60 | Ein Versandhandel (Quelle, Otto-Versand usw.) erhält von einem Adresshändler Ihren Namen und Ihre Adresse mitgeteilt. Er speichert diese Daten in seiner Kundendatei.

Welche Informationen muss das Unternehmen Ihnen mitteilen?

1. Gespeicherte Daten: Ja.
   Da Sie bislang keine Kenntnis von der Speicherung haben, muss Ihnen mitgeteilt werden, welche Informationen über Sie gespeichert werden.
2. Identität der verantwortlichen Stelle: Ja.
   Das Unternehmen muss Sie natürlich auch über seine Identität aufklären.
3. Herkunft der gespeicherten Daten: Nein.
   Sie muss nicht mitgeteilt werden – offenbar sieht der Gesetzgeber das für zu aufwändig an.
4. Zweckbestimmung: Ja.
   Eine ganz wichtige Verpflichtung des Unternehmens! Es muss Ihnen mitteilen, zu welchen Zwecken die Daten verwendet werden.
5. Datenempfänger: Nein.
   Diese müssen nicht mitgeteilt werden – offenbar sieht der Gesetzgeber auch das für zu aufwändig an.

Während die Information über eine künftige Datenverarbeitung relativ oft erteilt wird, benachrichtigen Unternehmen von einer erstmaligen Speicherung sehr selten – oder haben Sie schon einmal eine solche Benachrichtigung erhalten?

Woran liegt das? Vielleicht kennen die meisten Unternehmen die Rechtslage nur unzureichend. Es gibt aber auch einige Fälle, bei denen eine Speicherung nicht mitgeteilt werden muss. Einen Ausnahmefall kennen Sie bereits: es ist die Grundregel, dass eine Benachrichtigung nicht erfolgen muss, wenn der Betroffene ohnehin von der Speicherung weiß. Eine Benachrichtigung muss aber beispielsweise auch nicht erfolgen, wenn Ihre Daten aus „allgemein zugänglichen Quellen" entnommen sind und eine Benachrichtigung für das Unternehmen wegen der Vielzahl der Fälle unverhältnismäßig wäre.

Beispiel 61 | Ein Versandhandel wertet Telefonbücher aus und gewinnt dadurch rund 100.000 für ihn interessante Adressdaten. Eine Benachrichtigung dürfte hier unverhältnismäßig sein.

Beispiel 62 | Ein Unternehmen erhält von einem Arbeitgeber die Liste von dessen Beschäftigten. Diese Liste ist keine allgemein zugängliche Quelle, weil nur der Arbeitgeber über sie verfügt. Deshalb muss benachrichtigt werden.

HINWEISE
Für Unternehmen

Benachrichtigungspflicht nach § 33
(bei Datenverarbeitung für eigene Geschäftszwecke)

1. Bitte beachten Sie: § 33 Abs. 1 Satz 1 **verpflichtet** Sie grundsätzlich zur Benachrichtigung der Betroffenen. Eine Missachtung der Benachrichtigungspflicht ist ordnungswidrig und kann mit Bußgeldern bis zu 25.000 Euro belegt werden!
2. Verändert sich der Verarbeitungszweck wesentlich, so löst dies ebenfalls eine Benachrichtigungspflicht aus (Beispiel: Sie speichern personenbezogene Kundendaten ausschließlich zur Vertragsabwicklung und teilen dies dem Kunden mit. Später wollen Sie die Adressdaten Ihrer Kunden an andere Unternehmen veräußern).

3. Zulässige Ausnahmen von der Benachrichtigungspflicht sind **ausschließlich** die in § 33 Abs. 2 genannten Fälle. Die Ansprache zu Werbezwecken ersetzt **nicht** ohne Weiteres die Benachrichtigung!
4. Eine Benachrichtigungspflicht entfällt insbesondere, wenn eine Speicherung ausdrücklich gesetzlich vorgesehen ist. Das gilt auch für gesetzliche Aufbewahrungspflichten (zum Beispiel steuerrelevante Daten), wenn die Benachrichtigung einen unverhältnismäßigen Aufwand bedeuten würde.
5. Eine Benachrichtigungspflicht entfällt gemäß § 33 Abs. 2 Nr. 7a auch, wenn personenbezogene Daten „aus allgemeinen Quellen entnommen sind“ und die Benachrichtigung „wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.“ Entnommen heißt, dass Sie den Nachweis führen müssen, dass die Daten **tatsächlich** aus diesen Quellen stammen. Der Nachweis, dass die Daten aus allgemeinen Quellen entnommen werden **können**, reicht nicht aus!

Ein Unternehmen beschafft sich bei Dritten Ihre Daten, um sie Dritten zur Verfügung zu stellen (§ 33 Abs. 1 S. 2)

Noch weniger muss Ihnen mitgeteilt werden, wenn das Unternehmen die Daten nur speichert, um sie anderen Unternehmen zur Verfügung zu stellen (geschäftsmäßige Verarbeitung zum Zweck der Übermittlung, vgl. auch Beispiel 28). Da das Unternehmen kein Eigeninteresse an Ihren Daten hat, geht der Gesetzgeber davon aus, dass eine nachhaltige Gefährdung Ihrer Rechte erst bei der Übermittlung an einen interessierten Dritten eintritt. Dann muss Sie das Unternehmen von der erstmaligen Übermittlung benachrichtigen.

Beispiel 63 | Eine Auskunftei sammelt Schuldnerdaten, zum Beispiel zu einer Verbraucherinsolvenz, einem Offenbarungseid usw.. Gerade die genannten Daten werden von Amtsgerichten unter strengen gesetzlichen Auflagen[52] Unternehmen zur Verfügung gestellt. Wenn Sie nun mit einem Kunden der Auskunftei einen Vertrag abschließen, kann es passieren, dass dieses Unternehmen die Auskunftei befragt, ob gegen Sie irgend etwas vorliegt. Gibt die Auskunftei erstmalig Ihre Informationen weiter, muss sie Sie darüber benachrichtigen.

Auch gibt es Ausnahmefälle, die im Wesentlichen dem oben Gesagten entsprechen.

Wie Sie sehen, sind hier von der Benachrichtigungspflicht nur wenige Daten erfasst. Vermutlich hängt dies auch damit zusammen, dass die betroffenen Bürger ein Interesse, umfassend über Verarbeitungsvorgänge informiert zu werden, regelmäßig nicht zum Ausdruck bringen. Wenn Sie aber ein Interesse haben, sollen Sie auch einen Überblick über die gespeicherten Informationen erhalten.

TIPP
Für Verbraucher

Benachrichtigung

Sie haben eine „Benachrichtigung gemäß § 33 Bundesdatenschutzgesetz“ erhalten? Dann hat sich ein Unternehmen zumindest insoweit rechtmäßig verhalten, als es Sie informiert hat. Sie können aber auch die Zulässigkeit der gespeicherten Daten überprüfen, indem Sie von Ihrem Auskunftsrecht Gebrauch machen (wie das geht, folgt im nächsten Verbrauchertipp).
Wenn es sich um eine **Handels- und Wirtschaftsauskunftei** handelt, **sollten** Sie **unbedingt** von **Ihrem Auskunftsrecht** Gebrauch machen! Auskunfteien geben Bonitätsdaten weiter, das heißt: Wahrscheinlich hat sich ein Vertragspartner von Ihnen über Sie und Ihre Kreditwürdigkeit erkundigt. Für Sie geht es dann um den Abschluss oder Nichtabschluss eines Vertrags.
Bei Adresshändlern müssen Sie häufig damit rechnen, dass Ihre Daten an andere Unternehmen veräußert werden, die Sie dann zu Werbezwecken anschreiben.

Ihr Trumpf: Das Auskunftsrecht (§ 34 Abs. 1)

Ihr Auskunftsanspruch umfasst alle folgenden Informationen

1. Werden Daten über Sie gespeichert und wenn ja, welche?
2. Wer verarbeitet Ihre Daten?
3. Von wem hat der gegenwärtige Datenverarbeiter Ihre Daten?
4. Zu welchen Zwecken sollen Ihre Daten verarbeitet werden?
5. An welche Empfänger werden Ihre Daten weitergegeben?

Um dem speichernden Unternehmen die Beauskunftung zu erleichtern, sollten Sie Ihr Auskunftsbegehren so konkret wie möglich fassen. Eine Pflicht zur konkreten Bestimmung gibt es jedoch nicht.

Beispiel 64 | Wenn Sie Ihre Hausbank anschreiben und „Auskunft nach § 34 BDSG über meine Daten“ verlangen, stellen Sie Ihre Bank vor eine schwierige Aufgabe. Denn alle gespeicherten Daten umfassen den Stammdatensatz, Kontoverbindungsdaten, Akten usw. – das ist eine Unmenge an personenbezogenen Daten!

Beispiel 65 | Ein Unternehmen benachrichtigt Sie, dass es über Sie erstmalig Daten gespeichert oder weitergegeben hat? Dann können Sie Ihr Auskunftsbegehren in der Regel gar nicht genau fassen.

TIPP
Für Verbraucher

Auskunftsanspruch

Sie möchten wissen, ob ein Unternehmen personenbezogene Daten über Sie speichert? Dann zögern Sie nicht, Auskunft zu verlangen – Sie haben einen Anspruch darauf zu erfahren, welche Informationen zu welchen Zwecken über Sie gespeichert werden!

Machen Sie Ihren Auskunftsanspruch schriftlich geltend und setzen Sie eine angemessene Frist (zwei bis drei Wochen sind fast eine immer angemessene Frist).

Fassen Sie Ihren Auskunftsanspruch dabei so genau wie möglich. An welchen Informationen sind Sie interessiert? Sind es alle Daten? Dann schreiben Sie „alle Daten.“ Sind es nur bestimmte Daten? Dann beschreiben Sie, an welchen Informationen Sie interessiert sind.

Adressieren Sie Ihren Auskunftsanspruch an den „betrieblichen Datenschutzbeauftragten“ des Unternehmens. Alle größeren Unternehmen sind verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Er müsste die Gesetzeslage kennen und für eine ordnungsgemäße Auskunfterteilung sorgen.

Sollte sich das Unternehmen weigern oder überhaupt nicht reagieren – wenden Sie sich ruhig an Ihre Datenschutz-Aufsichtsbehörden. Sie sind zu Ihrem Schutz geschaffen eingerichtet worden!

Nur in Ausnahmefällen darf das Unternehmen Ihnen die Auskunft verweigern.[53] Insbesondere kommt es nicht darauf an, ob Sie bereits Kenntnis über gespeicherte Daten haben oder nicht.

Beispiel 66 | Nur in besonderen Fällen kann Sie ein Unternehmen darauf hinweisen, dass die Geltendmachung des Auskunftsanspruches missbräuchlich ist. So etwa, wenn Sie wöchentlich mehrfach in kurzen Abständen Auskunft über die gespeicherten Daten verlangen, obwohl wesentliche Änderungen des gespeicherten Datensatzes nicht zu erwarten sind. Aber wer macht so etwas schon?

HINWEISE
Für Unternehmen

Auskunftserteilung

Das Auskunftsrecht soll den Betroffenen unter anderem in die Lage versetzen zu beurteilen, ob alle über ihn gespeicherten Daten rechtmäßig gespeichert sind. Es genügt also **nicht**, die gespeicherten Datenarten zu beschreiben. Beispiel: Unzureichend ist die Mitteilung „Wir haben über Sie Ihren Namen, Ihre Adresse usw. gespeichert“.

Vielmehr müssen Sie die konkret gespeicherten Daten mitteilen.

Beispiel 67 | Die Auskunft könnte etwa wie folgt aussehen: „Über Sie haben wir folgende Informationen gespeichert: Name: Andreas C. Mustermann, Adresse: Musterweg 22, 23456 Musterstadt“ usw.

In der Regel ist die Auskunft kostenlos und schriftlich zu erteilen. Es gibt allerdings eine Ausnahme: Wenn Sie eine so genannte „Selbstauskunft“ von einem Unternehmen einholen, das diese Daten geschäftsmäßig speichert, um sie an andere Unternehmen zu übermitteln, kann ein Entgelt verlangt werden. Voraussetzung dafür allerdings ist, dass diese Selbstauskunft wirtschaftlich verwertbar ist.

Beispiel 68 | Die SCHUFA verlangt für die Zusendung einer Selbstauskunft zur Zeit 7,60 Euro zuzüglich Porto. Sie vertritt dazu die Auffassung, dass die Betroffenen die erteilten Selbstauskünfte gegenüber Dritten stets wirtschaftlich nutzen können. Diese Auffassung ist zumindest fragwürdig, wenn die Selbstauskunft ausschließlich aus datenschutzrechtlichen Gründen erfolgt.

Ergibt sich aus der Selbstauskunft, dass der gespeicherte Datensatz unrichtige oder unzulässige Daten enthält, darf kein Entgelt verlangt werden.[54]

HINWEISE
Für Verbraucher

SCHUFA-Selbstauskunft gibt es nicht bei den Datenschutz-Aufsichtsbehörden

Die SCHUFA-Selbstauskunft ist nicht bei den Datenschutz-Aufsichtsbehörden, sondern nur direkt bei der SCHUFA erhältlich. Die Adresse der für Sie zuständigen SCHUFA-Niederlassung findet sich im Internet (www.schufa.de unter „Kontakt“) und im Telefonbuch. Sie können sich aber auch an das so genannte „SCHUFA-Verbraucherservicezentrum Hannover“ wenden.
(Adresse: Georgstraße 11, 30159 Hannover, Tel.: 0511/12396).

Was Auskunfteien über Sie wissen

Haben Sie schon einmal ein Schreiben wie dieses erhalten?

ABC Wirtschaftsinformationen
DE Straße 123
12345 Musterstadt

Benachrichtigungsschreiben nach § 33 Bundesdatenschutzgesetz

Sehr geehrte Damen und Herren,
die Firma... ist eine der führenden Handelsauskunfteien / Kreditschutzorganisationen... in der Bundesrepublik...

Zu unseren Kunden zählen...

In unserer Datenbank werden insbesondere Angaben gespeichert über den Namen, die Firmierung, die Anschrift, den Familienstand, die berufliche Tätigkeit, Bankverbindung, Vermögensverhältnisse, etwaige Verbindlichkeiten sowie Hinweise zum Zahlungsverhalten. Hiermit unterrichten wir Sie gemäß § 33 Abs. 1 Satz 2 Bundesdatenschutzgesetz darüber, dass erstmals Daten der oben beschriebenen Art zu Ihrer Person / Firma übermittelt wurden.

Mit freundlichen Grüßen

(Unterschrift)

Zumeist sind solche Schreiben mit einem „Informationsblatt“ versehen, auf dem in enger Schrift juristische Ausführungen zum BDSG abgedruckt sind. Den Inhalt dieses Schreibens könnte man in einem Satz zusammenfassen: Der Absender (meistens eine Auskunftei) hat geschäftsmäßig kreditrelevante Informationen über Sie gespeichert und an einen Kunden weitergegeben.

Wie sollten Sie auf ein solches Schreiben reagieren?

Eine solche Praxis ist grundsätzlich datenschutzrechtsgemäß. Es gibt im BDSG mit § 29 sogar eine Vorschrift, die die Speicherung durch Auskunfteien relativ ausführlich regelt.

Sie sind dabei aber nicht schutzlos, insbesondere haben Sie grundsätzlich das Recht zu erfahren, welche Informationen über Sie gespeichert sind. Zunächst sollten Sie sich einen Überblick darüber verschaffen, welche Daten über Sie weitergegeben worden sind und wer der Datenempfänger ist. In der Regel ist der Datenempfänger ein Unternehmen, mit dem auch Sie einen Vertrag abschließen wollen oder wollten. Deshalb ist es immer günstig für Sie zu wissen, was dieses Unternehmen über Sie weiß.

Wenn die Auskunft über Sie günstig ausgefallen ist, haben Sie keine Veranlassung, dagegen vorzugehen. Ist die Auskunft ungünstig oder gar unrichtig, können Sie darauf reagieren - bei unrichtigen Daten die Berichtigung oder Löschung verlangen, den Sachverhalt aufklären usw.

Machen Sie also von Ihrem Auskunftsrecht Gebrauch! Dazu können Sie das auf der nächsten Seite folgende Musterschreiben verwenden.

Absender:

Name, Vorname:
Straße:
PLZ, Ort:
Geburtsdatum:

An die Auskunftei:
Betrieblicher Datenschutzbeauftragter
Straße:
PLZ, Ort:

Betreff: Auskunfterteilung gemäß § 34 Abs. 1 Bundesdatenschutzgesetz

Sehr geehrte Damen und Herren,
ich nehme Bezug auf Ihr Schreiben vom.... und bitte Sie um Auskunft über

a) die bei Ihnen über mich gespeicherten personenbezogenen Daten
b) die Herkunft meiner Daten
c) den oder die Empfänger (bitte mit Namen und Adresse), an den Sie meine Daten übermittelt haben.

Bitte erteilen Sie mir die Auskunft bis zum....

Mit freundlichen Grüßen

.....
(Unterschrift)

Transparenzregeln bei besonderen Formen der Datenverarbeitung

Bei bestimmten Verfahren sind besondere Transparenzregeln vorgesehen. Die Informationspflichten bei der Videoüberwachung wurden ja bereits vorgestellt (siehe ab Beispiel 44). So genannte automatisierte Einzelentscheidungen[55] und Chipkarten[56] zeichnen sich durch komplexe Datenverarbeitungsprozesse aus, die für Sie technisch schwer durchschaubar sind.

Deshalb wird Ihr Informationsanspruch um die Beschreibung technischer Details erweitert. Eine automatisierte Einzelentscheidung liegt vor, wenn Entscheidungen mit negativen Folgen für Sie **ausschließlich** auf eine automatisierte Verarbeitung gestützt werden.

Beispiel 69 | Ein Mobilfunkunternehmen weist seine Mitarbeiter an, Mobilfunkverträge nur abzuschließen, wenn der SCHUFA-Scorewert (oder der Scorewert einer anderen Auskunftei) einen bestimmten Wert erreicht. Wenn der Mitarbeiter keinerlei Entscheidungsspielraum hat, liegt bei einer Ablehnung des Vertragsabschlusses eine „automatisierte Einzelentscheidung" vor, weil tatsächlich allein der Computer die maßgebliche Entscheidung trifft.

Eine solche automatisierte Einzelentscheidung ist nur zulässig, wenn Sie die Chance haben, die Entscheidung des Computers durch eine Überprüfung in Frage zu stellen. Diese Regelung beruht auf dem Grundgedanken, dass Entscheidungen, die die Bewertung einer Person beinhalten und daher das Persönlichkeitsrecht zentral berühren, nicht einem Computerprogramm überlassen werden dürfen, sondern stets „menschenverantwortet" sein müssen.

HINWEISE
Für Unternehmen

Automatisierte Einzelentscheidung/Scoringverfahren (§ 6a)

Wie das Beispiel 69 dokumentiert, gilt die Einschränkung automatisierter Entscheidungen nicht nur, wenn der Anwender des Scoring-Verfahrens und der Nutzer des Ergebnisses identisch sind.[57]

Bei **negativen Entscheidungen** müssen nach § 6a Abs. 2 Nr. 2 BDSG geeignete Maßnahmen gewährleisten, dass die **berechtigten Interessen des Betroffenen** gewahrt werden. Eine Interessenwahrung liegt insbesondere vor, wenn der Betroffene die Möglichkeit hat, seinen Standpunkt geltend zu machen und die verantwortliche Stelle ihre Entscheidung daraufhin erneut überprüft. Es können auch Aspekte vorgetragen werden, die in dem automatisierten Verfahren nicht berücksichtigt wurden. Die erneute Überprüfung der verantwortlichen Stelle kann sich im Anschluss daran nicht darauf beschränken, „den Computer noch einmal anzuwerfen" und dem Betroffenen das Ergebnis noch einmal mitzuteilen.

Nach § 6a Abs. 3 hat der Betroffene das Recht auf Auskunft bezüglich des logischen Aufbaus der automatisierten Verarbeitung der ihn betreffenden Daten. Die verantwortliche Stelle ist allerdings nicht verpflichtet, Angaben zur Gewichtung der gescorten Daten sowie ihrer wechselseitigen Abhängigkeit zu machen.

Wenn eine automatisierte Einzelentscheidung vorliegt, haben Sie neben dem normalen Auskunftsanspruch auch das Recht zu erfahren, wie die automatisierte Verarbeitung logisch aufgebaut ist (vgl. auch oben stehenden Hinweis für Unternehmen). Das Hauptproblem der Regelung ist, dass es meistens nicht beweisbar ist, dass eine automatisierte Einzelentscheidung vorliegt.

Beispiel 70 | Die SCHUFA Auskunfteien weisen stets darauf hin, dass in ihren Vertragsbedingungen vorgesehen ist, dass der SCHUFA-Scorewert nicht alleinige Entscheidungsgrundlage für eine Kreditvergabe sein darf. Trotzdem gibt es bei dem Unabhängigen Landeszentrum für Datenschutz immer wieder (inoffizielle) Rückmeldungen von Bankmitarbeitern, die von anderslautenden mündlichen Weisungen ihrer Vorgesetzten berichten. Doch niemand wird dies öffentlich zugeben.

Einfacher zu erkennen ist die so genannte Chipkarte. Das BDSG spricht etwas umständlich von einem „mobilen personenbezogenem Speicher- und Verarbeitungsmedium". Anders als die normale EC-Karte, bei der bestimmte Daten gespeichert werden können, enthalten Chipkarten Prozessoren, die über den bloßen Speichervorgang hinaus besondere Verarbeitungsprozesse **auf der Karte** ermöglichen.

Beispiel 71 | Typisch für eine Chipkarte ist die „Geldkarte" der Banken und Sparkassen, bei denen Sie Guthabenbeträge aufladen können.

Hier muss Sie der Verwender von sich aus darüber informieren, wie die Karte funktioniert, wie Sie sich verhalten sollen, wenn die Karte kaputt geht und wie Sie Ihre Auskunftsrechte wahrnehmen können. Wichtig ist auch, dass erkennbar sein muss, dass eine Datenverarbeitung auf der Karte ausgelöst wird.

Beispiel 72 | Normalerweise müssen Sie die Chipkarte in ein Lesegerät einführen, damit eine Verarbeitung Ihrer Daten stattfinden kann. Bei der Geldkarte sind dies die Selbstbedienungsautomaten der Sparkassen. Wenn nun ein Ladevorgang Ihrer Geldkarte angestoßen wird, zeigt Ihnen der Automat das an.

Noch sind Chipkarten dieser Art relativ selten, ihre Zahl nimmt aber zu.

Information der Betroffenen bei der Ansprache zu Werbezwecken

Für werbetreibende Unternehmen, Adresshändler und Markt- und Meinungsforschungsinstitute ist insbesondere § 28 Abs. 4 Satz 2 BDSG von großer Bedeutung. Die Ansprache zu den Zwecken der Werbung, der Markt- oder Meinungsforschung erfordert nach § 28 Abs. 4 BDSG eine Unterrichtung des jeweils Betroffenen, dass er dieser Nutzung seiner personenbezogenen Daten widersprechen darf. Diese **Unterrichtung** muss dem Betroffenen einen **effektiven Widerspruch ermöglichen.**

Beispiel 73 | Die Klausel „Sie können der Verwendung Ihrer Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung jederzeit widersprechen" genügt nicht den gesetzlichen Anforderungen, wenn der Betroffene keine Adresse zur Verfügung gestellt bekommt, an die er seinen Widerspruch richten kann und die seinen Widerspruch auch beachtet.

Beispiel 74 | Werbefaxe oder SPAM-Mails enthalten manchmal den Hinweis, falls man keinen weiteren Informationen des Versenders wünsche, solle man eine entsprechende Nachricht an die angegebene Telefaxnummer oder Mailadresse senden. Da die Gefahr des Missbrauchs (Kostenpflichtigkeit der angebotenen Nummer! Niemals antworten!) droht, ist dies keine ausreichende Unterrichtung.

Die **Benennung einer Kontaktperson/Telefonnummer** ist zwar nicht ausdrücklich gesetzlich vorgesehen, aber aus Akzeptanzgründen dringend zu empfehlen. Die bei den Aufsichtsbehörden eingehenden Beschwerden betreffen meistens nicht die Tatsache der Ansprache als solche, sondern die Missachtung des Widerspruchs.

Hinweise
Für Unternehmen

Einwilligungsklauseln für die Nutzung zu Werbezwecken

Ist für eine bestimmte Datenverarbeitung oder Nutzung zu Kundenbindungszwecken die Einwilligung des betroffenen Kunden erforderlich, genügt es nach der Rechtsprechung in der Regel nicht immer, eine Streichoption anzubieten (Unzulässigkeit eines bloßen opt-out).

Beispiel 75 | Unzureichende Einwilligung in die Nutzung von Daten zu Werbezwecken:

„Mit Ihrer Unterschrift geben Sie Ihre Einwilligung, dass wir Sie auch per Fax, E-Mail oder Telefon kontaktieren sowie Ihre Daten mit anderen Unternehmen (isb. der X-GmbH) in Deutschland zu Zwecken der Werbung austauschen dürfen. Sollten Sie die Einwilligung nicht in dieser Form geben wollen, so streichen Sie bitte entsprechende Satzteile oder setzen Sie sich mit uns in Verbindung (Telefon: 0123/456789). Diese Einwilligung kann jederzeit widerrufen werden. Sie können der Verwendung Ihrer Daten zu den genannten Zwecken jederzeit widersprechen."

Hinweise
Für Unternehmen

Einwilligungsklauseln für die Nutzung zu Werbezwecken

Die soeben gewählte Streichoption setzt ein aktives Handeln voraus, um den Werbekontakt zu unterbinden. Die Rechtsprechung billigt hingegen regelmäßig nur Erklärungen, bei denen Sie Werbefaxe oder Werbeanrufe ausdrücklich wünschen (also „aktiv" werden, um Anrufe oder Telefaxe zu erhalten, so genanntes opt-in).
Anderes gilt selbstverständlich, wenn Sie dem Kunden bereits bei Vertragsabschluss auf sein Recht auf Widerspruch gegen persönlich adressierte Werbeschreiben nach § 28 Abs. 4 hinweisen wollen.

Beispiel 76 | Zulässige Unterrichtung über das Widerspruchsrecht nach § 28 Abs. 4 bei Vertragsschluss:

„Die X-AG ist berechtigt, Ihre Adressangaben zu nutzen, um Sie über ihre Produkte zu informieren. Sie haben jederzeit das Recht, der Nutzung Ihrer Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung zu widersprechen. Falls Sie von diesem Recht Gebrauch machen wollen, kreuzen Sie bitte den nebenstehenden Kasten an ☐ oder wenden Sie sich bitte an..."

Tipp
Für Verbraucher

Abschließende Verbrauchertipps zu Transparenzregeln:

Manche Informationen werden Sie im geschäftlichen Alltag häufig vermissen. Fordern Sie sie ruhig ein, Sie haben einen Anspruch darauf! Wenn Unternehmen einen Bedarf ihrer Kunden erkennen, reagieren sie häufig in der Regel gerne und schnell. Wenn Datenschutzrechte nicht eingefordert werden, werden sie schnell auch nicht beachtet.
Wussten Sie schon, dass die meisten deutschen Unternehmen verpflichtet sind, ein Verzeichnis ihrer automatisierten Verfahren zu führen, bei denen personenbezogene Daten verarbeitet werden? Nach dem Bundesdatenschutzgesetz haben die Unternehmen die Pflicht, auf Antrag die dort getroffenen Angaben jedermann (also auch Ihnen!) „in geeigneter Form" verfügbar zu machen.
Mehr zu diesem Verfahrensverzeichnis erfahren Sie im vierten Teil dieser Broschüre.

[3]

Korrekturrechte und Rechtsbehelfe (§ 6, § 35)

Teil 3

Korrekturrechte und Rechtsbehelfe (§ 6, § 35)

Das BDSG lässt im weiten Umfang zu, dass Unternehmen Ihre personenbezogenen Daten verarbeiten. Dafür räumt es Ihnen aber auch bestimmte Rechte ein, mit denen Sie die Verarbeitungsbefugnisse von Unternehmen einschränken können.

Neben dem bereits erwähnten Kontrollrecht der Auskunft sind es vor allem Ihre Rechte auf Berichtigung, Löschung und Sperrung, die besonders geschützt sind.[58] Diese Rechte dürfen durch Vertrag nicht eingeschränkt oder ausgeschlossen werden, sie sind „unabdingbar."

Berichtigung

Speichert ein Unternehmen über Sie unrichtige Daten, so muss es diese unrichtigen Daten berichtigen.[59] In den allermeisten Fällen haben Unternehmen ein großes Eigeninteresse an der richtigen Speicherung Ihrer korrekter personenbezogenern Daten.

Beispiel 77 | Ein Weinhändler beliefert Sie jährlich mit mehreren Kisten Wein. Naturgemäß hat er ein großes Interesse, Ihre richtige Adresse zu speichern. Sobald er erfährt, dass Sie umgezogen sind, wird er von sich aus Ihre neue Adresse speichern.

In anderen Fällen ist die Interessenlage nicht ganz so eindeutig. Eine Interesse an der Korrektur Ihrer Daten liegt meist dann nicht vor, wenn ein Unternehmen eine Berichtigung nur mit großen Aufwand vornehmen kann oder wenn es kein wirtschaftliches Interesse an korrekten Daten mehr hat.

Beispiel 78 | Eine Auskunftei hat einem ihrer Kunden mitgeteilt, dass Sie als Einzelkaufmann einen Jahresumsatz von 1 Millionen Euro erzielen. Ein Vierteljahr später erfährt sie, dass Ihr Umsatz wesentlich höher ist. Die Gebühr, die sie für die Auskunft verlangt, hat sie aber bereits erhalten.

Ein wirtschaftliches Interesse an einer nachträglichen Korrektur der Auskunft liegt also nur noch bedingt vor.

Wenn ein Unternehmen unrichtige Daten über Sie an ein anderes Unternehmen übermittelt hat, verlangt das Datenschutzrecht, dass es den Datenempfänger über diese Unrichtigkeit aufklärt. Im Beispiel 78 müsste die Auskunftei also eigentlich ihren Kunden über die Unrichtigkeit der Auskunft informieren. Man spricht insoweit von einer Nachberichtspflicht der Auskunftei. Allerdings gilt diese Pflicht nur im Rahmen der Verhältnismäßigkeit. Außerdem darf diese nachträgliche Berichtigung nicht gegen Ihre schutzwürdigen Interessen verstoßen.[60]

Beispiel 79 | Eine Auskunftei teilt ihrem Kunden mit, dass Sie eine hohe Kreditwürdigkeit haben und dass insbesondere keine Vertragsverletzungen durch Sie bekannt sind. Ein Jahr später erfährt sie nachträglich, dass Sie einige Kaufpreisforderungen nicht beglichen haben. Hier dürfte ein Nachbericht unzulässig sein, weil der Kunde seinen Vertrag mit Ihnen wahrscheinlich längst abgewickelt hat und Sie überflüssig schlecht beleumundet würden.

Löschen

Um von vornherein Irrtümern vorzubeugen: Sie haben leider keinen uneingeschränkten Anspruch, von jedermann die Löschung Ihrer personenbezogenen Daten zu verlangen. Ein subjektives Recht auf Löschung steht Ihnen in vier Fallgruppen zu. Diese Löschpflichten sind an und für sich von der verantwortlichen Stelle ohnehin zu beachten. Sie können die Löschung dann aber auch als persönlichen Anspruch fordern, wenn das Unternehmen Ihre Daten nicht von sich aus vernichtet.

1) Speichert ein Unternehmen unzulässig personenbezogene Daten über Sie, muss es diese Daten löschen.[61]

Beispiel 80 | Ihr Arbeitgeber speichert ohne Ihre Einwilligung Informationen über Ihre Freizeitbeschäftigungen. Das ist in der Regel unzulässig, solange die Freizeitbeschäftigung ohne Belang für den Arbeitsplatz ist. Der Arbeitgeber muss diese Daten löschen.

Beispiel 81 | Ein Immobilienmakler speichert Sie versehentlich als

Eigentümer eines bestimmten Grundstücks. Wenn Sie mit dem Grundstück überhaupt nichts zu tun haben, muss er diese Information löschen: Die Information ist zwar unrichtig, eine Berichtigung ist aber nicht sinnvoll, weil kein berechtigtes Interesse an der Speicherung der korrigierten Information besteht („Herr Mustermann ist nicht Eigentümer des Grundstücks“ ist normalerweise eine sinnlose Information, weil diese Aussage auf rund sechs Milliarden andere Menschen auch zutrifft).

2) Bei besonders sensitiven Daten muss eine Stelle Ihre Daten löschen, wenn sie die Richtigkeit der Daten nicht beweisen kann.

   Beispiel 82 | Ein Verkehrsunternehmen unterhält eine Warndatei. Darin werden alle Kunden gespeichert, die schwarzgefahren oder sonst negativ aufgefallen sind. Ihnen wird in dieser Datei vorgeworfen, die Sitze mit einem Taschenmesser aufgeschlitzt zu haben. Sie bestreiten das (hoffentlich zu Recht!). Das Unternehmen darf diese Behauptung nur dann weiterhin speichern, wenn es ihre Richtigkeit beweist.

3) Der häufigste Fall der Löschpflicht dürfte sein, dass ein Unternehmen Ihre personenbezogenen Daten zunächst „für eigene Geschäftszwecke“ speichert. Wenn der Zweck der Speicherung erreicht worden ist oder überhaupt nicht mehr erreichbar ist, muss das Unternehmen Ihre Daten löschen.

   Beispiel 83 | Sie haben eine Bestellung bei einem Buchhandel aufgegeben und dazu Ihren Namen und Ihre Telefonnummer hinterlassen. Die Buchhandlung hat das Buch besorgt, Sie haben das Buch bezahlt und abgeholt. Sie haben Ihre Daten nur zur Abwicklung der Buchbestellung zurückgelassen. Die weitere Speicherung der Daten ist für die Abwicklung der Bestellung nicht mehr erforderlich. Also muss die Buchhandlung die Daten löschen.

Allerdings kann es passieren, dass das Unternehmen den Zweck der Speicherung ändert. Grundsätzlich ist eine solche Zweckänderung möglich, wenn die Speicherung auch unter dem neuen Verarbeitungszweck zulässig ist. Im Beispiel 83 kann der Buchhandel Ihre personenbezogenen Daten auch für die Abwicklung einer weiteren Bestellung verwenden. Oder er kann Ihre Telefonnummer dazu benutzen, Sie zu Autorenlesungen einzuladen, wenn Sie damit einverstanden sind usw.

4) Unternehmen, die geschäftsmäßig Ihre Daten verarbeiten, um sie Dritten zur Verfügung zu stellen, unterliegen insoweit weniger strengen Löschpflichten. Der Gesetzgeber geht davon aus, dass solche Unternehmen Daten von so vielen Menschen speichernt, dass eine laufende Überprüfung der Erforderlichkeit eine unverhältnismäßige Belastung darstellen würde. Deshalb sind solche Unternehmen nur verpflichtet, nach dem Ablauf des vierten Jahres nach der ersten Speicherung zu überprüfen, ob Ihre Daten auch weiterhin benötigt werden.

   Beispiel 84 | Man geht davon aus, dass personenbezogene Markt- und Meinungsforschungsergebnisse durchschnittlich nach drei Jahren mehr als die Hälfte ihres Wertes verloren haben (weil Sie als Verbraucher Ihr Konsumverhalten ändern, Ihre Adresse veraltet usw.). Zumindest für schnelllebige Branchen sind solche Umfragedaten nach vier Jahren nicht mehr von aktueller Relevanz.

Sperrung, Berichtigung durch Gegendarstellung

Was passiert eigentlich, wenn Sie der Meinung sind, eine bestimmte Information über Sie sei falsch – das Unternehmen meint aber, dass die gespeicherte Information richtig ist?

Beispiel 85 | Eine Auskunftei speichert über Sie, dass Sie einen Offenbarungseid abgegeben haben (also vor Gericht erklärt haben, dass Ihr Vermögen nicht mehr genügt, um Ihre Schulden zu begleichen). Sie sind empört, weil diese Behauptung nicht stimmt. Die Auskunftei lässt sich aber nicht davon überzeugen.

In solchen Fällen hat das Unternehmen in der Regel Ihre Daten zu sperren, das heißt, die Daten dürfen für den „normalen Gebrauch“ nicht mehr verwendet werden.[62] Diese Sperrung ist so lange beizubehalten, bis der Sachverhalt aufgeklärt ist.

TIPP
Für Verbraucher

Berichtigung unrichtiger Daten/Sperrung

In der Praxis genügt es meist nicht zu behaupten, dass eine bestimmte gespeicherte Information unrichtig ist. Gerade Auskunfteien, die ihr Geld damit verdienen, dass sie kreditrelevante Daten an Dritte verkaufen, verlangen häufig von Ihnen, dass Sie die Unrichtigkeit der Daten **beweisen**.
Andererseits wäre es unzumutbar, wenn Sie die unrichtigen Datensätze von Auskunfteien korrigieren müssten. Es genügt daher, wenn Sie **Anhaltspunkte** dafür benennen, dass die gespeicherten Daten unrichtig sind. Die korrekten Daten müssen Sie nicht benennen, um eine Sperrung zu erreichen.
Hier hilft es möglicherweise, wenn Sie sich an die Datenschutz-Aufsichtsbehörden wenden. Wenn Sie der Behörde die richtigen Daten mitteilen, kann sie auf eine Sperrung hinwirken.
Eine Besonderheit gilt für sensitive Daten (Daten über Weltanschauungen, über den Gesundheitszustand, Straftaten oder Ordnungswidrigkeiten usw., vgl. Beispiel 51, 52 und 82): Hier genügt die bloße Behauptung der Unrichtigkeit. Wenn ein Unternehmen die Richtigkeit der gespeicherten Daten nicht beweisen kann, muss sie es sie löschen[63].

Herausgabe von Unterlagen

Im BDSG nicht geregelt ist die Herausgabe von Unterlagen. Sie können aber aus anderen Rechtsgründen einen Anspruch auf Herausgabe von Unterlagen haben. Der wichtigste Rechtsgrund hierfür ist, dass Sie der Eigentümer von Unterlagen sind und diese nur für bestimmte Zwecke aus der Hand gegeben haben.

Beispiel 86 | Weil Sie von Ihrer Bank einen Kredit haben wollen, legen Sie dem Kreditinstitut bestimmte Unterlagen vor. Die Bank prüft Ihre Unterlagen und will das Kreditgeschäft nicht abschließen. Dann ist das Kreditinstitut grundsätzlich verpflichtet, Ihnen die Unterlagen zurückzugeben. Anderes kann allenfalls gelten, wenn Sie ausdrücklich vereinbart haben, dass die Unterlagen beim Kreditinstitut verbleiben dürfen. Datenschutzrechtlich könnten Sie allerdings allenfalls die Löschung der Unterlagen verlangen.

Beispiel 87 | Entsprechendes gilt für Bewerbungsunterlagen, die Sie an einen Arbeitgeber schicken, wenn Sie den Arbeitsplatz nicht bekommen haben. Auch hier gilt, dass die Unterlagen zurückgesendet werden müssen, wenn Sie es verlangen.

Die Datenschutzaufsichtsbehörden (§ 38) – Sie helfen Ihnen gerne!

Ärgern Sie sich darüber, dass jemand Ihre personenbezogene Daten illegal verarbeitet? Oder haben Sie als Bürgerin oder Bürger Fragen zum Datenschutz? Dann können Sie sich kostenfrei an Ihre Aufsichtsbehörden wenden, die Ihnen gerne helfen. Auch Unternehmen können sich mit Beratungsgesuchen an die Datenschutzbehörden wenden. Dann gilt allerdings die Einschränkung, dass eine Beratung kostenpflichtig sein kann, wenn sie das Unternehmen für kommerzielle Zwecke nutzt.[64]

Die örtliche Zuständigkeit der Datenschutz-Aufsichtsbehörden orientiert sich daran, in welchem Bundesland die Daten verarbeitende Stelle ihren Geschäftssitz hat. Ausnahmen gelten für Post- und Telekommunikationsunternehmen: Für sie ist der Bundesbeauftragte für den Datenschutz zuständig.

Beispiel 88 | Eine Versicherung hat ihren Geschäftssitz in Kiel. Dann ist das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein die örtlich zuständige Datenschutz-Aufsichtsbehörde.

TIPP
Für Verbraucher

Aufsichtsbehörden

Falls Sie sich nicht sicher sind, welche Behörde zuständig ist, wenden Sie sich einfach an die Datenschutzbehörde Ihres Bundeslandes. Sie leitet Ihr Anliegen an die richtige Stelle weiter.
Falls Sie nur Informationsmaterial suchen und über einen Webanschluss verfügen – das gemeinsame Internetportal zahlreicher deutscher und ausländischer Datenschutzbehörden www.datenschutz.de bietet eine Fülle von Material!

Anschriften

Bundesbeauftragter für den Datenschutz
Landesbeauftragte für den Datenschutz
Aufsichtsbehörden für den Datenschutz

Der Bundesbeauftragte für den Datenschutz

Husarenstr. 30, 53117 Bonn
Telefon: (0228) 8 19 95 - 0 / Telefax: (0228) 8 19 95 - 550
E-Mail: poststelle@bfd.bund400.de

Landesbeauftragte für den Datenschutz

Baden-Württemberg

Der Landesbeauftragte
für den Datenschutz Baden-Württemberg
Marienstr. 12, 70178 Stuttgart
Telefon: (0711) 61 55 41 - 0 / Telefax: (0711) 61 55 41 - 15
E-Mail: poststelle@lfd.bwl.de

Bayern

Der Bayerische Landesbeauftragte für den Datenschutz
Wagmüllerstr. 18/II, 80538 München
Telefon: (089) 21 26 72 - 0 / Telefax: (089) 21 26 72 - 50
E-Mail: poststelle@datenschutz-bayern.de

Berlin

Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4-10,10787 Berlin
Telefon: (030) 1 38 89 - 0 / Telefax: (030) / 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de

Brandenburg

Der Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77 Haus 2, 14532 Kleinmachnow
Telefon: (033203) 3 56 - 0 / Telefax: (033203) 356 - 49
E-Mail: poststelle@lda.brandenburg.de

Bremen

Landesbeauftragter für den Datenschutz Bremen
Arndtstr. 1, 27570 Bremerhaven
Telefon: (0471) 9 24 61 - 0 / Telefax: (0471) 9 24 61 - 31
E-Mail: office@datenschutz.bremen.de

Hamburg

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg
Telefon: (040) 4 28 41 - 20 44, 45 / Telefax: (040) 4 28 41 - 23 72
E-Mail: mailbox@datenschutz.hamburg.de

Hessen

Der Hessische Datenschutzbeauftragte
Uhlandstr. 4, 65189 Wiesbaden
Telefon: (0611) 14 08 - 0 / Telefax: (0611) 14 08 - 900 / 921
E-Mail: poststelle@datenschutz.hessen.de

Mecklenburg-Vorpommern

Der Landesbeauftragte
für den Datenschutz Mecklenburg-Vorpommern
Schloß Schwerin, Johannes-Stelling-Str. 21, 19053 Schwerin
Telefon: (0385) 5 94 94 - 0 / Telefax: (0385) 5 94 94 - 58
E-Mail: datenschutz@mvnet.de

Niedersachsen

Der Landesbeauftragte für den Datenschutz Niedersachsen
Brühlstr. 9, 30169 Hannover
Telefon: (0511) 120 - 45 00 / Telefax: (0511) 120 - 45 99
E-Mail: mail@lfd.niedersachsen.de

Nordrhein-Westfalen

Die Landesbeauftragte
für den Datenschutz Nordrhein-Westfalen
Reichsstr. 43, 40217 Düsseldorf
Telefon: (0211) 3 84 24 - 15 / Telefax: (0211) 3 84 24 - 10
E-Mail: datenschutz@lfd.nrw.de

Rheinland-Pfalz

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz
Deutschhausplatz 12, 55116 Mainz
Telefon: (06131) 208 - 24 49 / Telefax: (06131) 208 - 24 97
E-Mail: poststelle@datenschutz.rlp.de

Saarland

Der Landesbeauftragte für den Datenschutz Saarland
Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Telefon: (0681) 9 47 81 14 / Telefax: (0681) 9 47 81 29
E-Mail: lfd-saar@t-online.de

Sachsen

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1, 01067 Dresden
Telefon: (0351) 49 35 - 400 / Telefax: (0351) 49 35 - 490
E-Mail: saechsdsb@slt.sachsen.de

Sachsen-Anhalt

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Berliner Chaussee 9, 39114 Magdeburg
Telefon: (0391) 8 18 03 - 0 / Telefax: (0391) 8 18 03 - 33
E-Mail: poststelle @lfd.lsa-net.de

Schleswig-Holstein

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
Telefon: (0431) 988 - 12 00 / Telefax: (0431) 988 - 12 23
E-Mail: mail@datenschutzzentrum.de

Thüringen

Der Thüringer Landesbeauftragte für den Datenschutz
Johann-Sebastian-Bach-Str. 1, 99096 Erfurt
Telefon: (0361) 3 77 19 - 00 / Telefax: (0361) 3 77 19 - 04
E-Mail: poststelle@datenschutz.thueringen.de

Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich

Baden-Württemberg

Innenministerium - Baden-Württemberg
Dorotheenstr: 6, 70173 Stuttgart
Telefon: (0711) 2 31 32 50 / Telefax: (0711) 2 31 32 99

Bayern

Regierung von Mittelfranken
Promenade 27, 91522 Ansbach
Telefon: (0981) 53 - 0 / -301 / Telefax: (0981) 53 - 206
E-Mail: datenschutz@reg-mfr.bayern.de

Berlin

Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4-10,10787 Berlin
Telefon: (030) 13 889 - 0 / Telefax: (030) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de

Brandenburg

Ministerium des Inneren des Landes Brandenburg
Henning-von-Tresckow-Str. 9-13, 14467 Potsdam
Telefon: (0331) 8 66 23 - 60 / Telefax: (0331) 8 66 23 - 02
E-Mail: poststelle@mi.brandenburg.de

Bremen

Landesbeauftragter für den Datenschutz Bremen
Arndtstr. 1, 27570 Bremerhaven
Telefon: (0471) 9 24 61 - 0 / Telefax: (0471) 9 24 61 - 28
E-Mail: office@datenschutz.bremen.de

Hamburg

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg
Telefon: (040) 4 28 41 - 20 44 / Telefax: (040) 4 28 41 - 23 72
E-Mail: mailbox@datenschutz.hamburg.de

Hessen

Hessisches Ministerium des Innern und für Sport
F.-Ebert-Allee 12, 65185 Wiesbaden
Telefon: (0611) 353 - 0 / Telefax: (0611) 353 - 17 66
E-Mail: poststelle@hmdi.hessen.de

Regierungspräsidium Darmstadt
WilhelminenStr. 1/3, 64278 Darmstadt
Telefon: (06151) 120 / Telefax: (06151) 12 68 34

Regierungspräsidium Kassel
Steinweg 6, 34117 Kassel
Telefon: (0561) 106 - 0 / Telefax: (0561) 106 - 16 31

Regierungspräsidium Gießen
Landgraf-Philipp-Platz 3-7, 35390 Gießen
Telefon: (0641) 303 - 0 / Telefax: (0641) 303 - 21 97

Mecklenburg-Vorpommern

Innenministerium Mecklenburg-Vorpommern
Arsenal am Pfaffenteich Karl-Marx-Str.1, 19055 Schwerin
Telefon: (0385) 58 82 - 2021 / Telefax: (0385) 58 82 - 978
E-Mail: poststelle@im.mv-regierung.de

Niedersachsen

Niedersächsisches Innenministerium
Lavesallee 6, 30169 Hannover
Telefon: (0511) 1 20 47 -53, -72, -73 / Telefax: (0511) 1 20 45 91

Der Landesbeauftragte für den Datenschutz Niedersachsen
Brühlstr. 9, 30169 Hannover
Telefon: (0511) 12 04 - 45 52 / Telefax: (0511) 12 04 - 45 91
E-Mail: mail@lfd.niedersachsen.de

Nordrhein-Westfalen

Die Landesbeauftragte
für den Datenschutz Nordrhein-Westfalen
Reichsstr. 43, 40217 Düsseldorf
Telefon: (0211) 3 84 24 - 15 / Telefax: (0211) 3 84 24 - 10
E-Mail: datenschutz@mail.lfd.nrw.de

Rheinland-Pfalz

Ministerium des Innern und für Sport Rheinland-Pfalz
Schillerplatz 3-5, 55116 Mainz
Telefon: (06131) 163 - 259 / Telefax: (06131) 163 - 595
Aufsichts- und Dienstleistungsdirektion
Willy-Brandt-Platz 3, 54290 Trier
Telefon: (0651) 94 94 - 0 / Telefax: (0651) 94 94 - 170

Saarland

Ministerium für Inneres und Sport
Mainzer Str. 136, 66024 Saarbrücken
Telefon: (0681) 9 62 - 0 / Telefax: (0681) 9 62 - 16 05
E-Mail: abtb@mdi.x400.saarland.de

Sachsen

Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Str. 2, 01097 Dresden
Telefon: (0351) 564 - 0 / Telefax: (0351) 564 - 31 99
E-Mail: datenschutz@smi.sachsen.de

Regierungspräsidium Chemnitz
Altchemnitzer Str. 41, 09120 Chemnitz
Telefon: (0371) 532 - 11 43 / Telefax: (0371) 532 - 21 49

Regierungspräsidium Dresden
Staufenbergallee 2, 01099 Dresden
Telefon: (0351) 825 - 14 20 / Telefax: (0351) 825 - 99 99
E-Mail: datenschutz@rpdd.sachsen.de

Regierungspräsidium Leipzig
Braustr. 2, 04107 Leipzig
Telefon: (0341) 977 - 14 41 / Telefax: (0341) 977 - 14 99

Sachsen-Anhalt

Regierungspräsidium Halle
Willy-Lohmann-Str. 7, 06114 Halle
Telefon: (0345) 51 40 / Telefax: (0345) 5 14 14 44
E-Mail: poststelle@rph.mi.lsa-net.de

Schleswig-Holstein

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
Telefon: (0431) 988 - 12 00 / Telefax: (0431) 988 - 12 23
E-Mail: mail@datenschutzzentrum.de

Thüringen

Innenministerium des Landes Thüringen
Steigerstr. 24, 99096 Erfurt
Telefon: (0361) 379 - 00 / Telefax: (0361) 379 - 31 11

Thüringer Landesverwaltung, Referat 202
Carl-August-Allee 2a, 99423 Weimar
Telefon: (03643) 587 - 258 / Telefax: (03643) 587 - 190

Der Verbraucherzentrale Bundesverband e.V. (vzbv) vertritt die Interessen der Verbraucher in der Öffentlichkeit und gegenüber Politik, Wirtschaft und Zivilgesellschaft. Der vzbv ist die bundesweite Dachorganisation der 16 Verbraucherzentralen und von 23 weiteren verbraucherorientierten Verbänden. Er ist nach dem Unterlassungsklagengesetz berechtigt, Unternehmen, die unzulässige Datenverarbeitungsklauseln verwenden, auf Unterlassung in Anspruch zu nehmen (nähere Informationen unter: www.vzbv.de).

[4]

Die wichtigsten Regeln zur Gewährleistung des Datenschutzes

Hinweise an Kleine und Mittlere Unternehmen (KMU) zur Datenschutzorganisation:

Teil 4

Hinweise an Kleine und Mittlere Unternehmen (KMU) zur Datenschutzorganisation:

Die wichtigsten Regeln zur Gewährleistung des Datenschutzes

Diese Broschüre kann Ihnen den Aufbau eines effektiven Datenschutzmanagements nicht abnehmen. Hier werden nur einige Denkanstöße und Hinweise gegeben, die Ihnen Ihre Arbeit die Erfüllung Ihrer datenschutzrechtlichen Pflichten erleichtern sollen.

Haben Sie eine Datenschutzvision?

Diskretion, Vertraulichkeit und Vertrauen spielen in bestimmten Wirtschaftsbranchen für Kunden eine wichtige Rolle. Dies zu gewährleisten ist auch Aufgabe des Datenschutzes. Wie wäre es also, Datenschutzrecht nicht nur als gesetzliche Verpflichtung zu begreifen, sondern als Orientierungspunkt für Vertrauensstandards, mit denen man Kunden an sich bindet?

Hat man ein gutes Datenschutzangebot erst einmal als ein zeitgemäßes Mittel zur Werbung und Überzeugung von Kunden erkannt, dann ergeben sich plötzlich ganz neue Perspektiven. Dann ist der Datenschutz nicht eine auferlegte Last, sondern wird zur Chance, Kunden langfristig an sich zu binden. So kommen immer häufiger Beratungsanfragen an das Unabhängige Landeszentrum für Datenschutz, wie man sich auf den Wettbewerb um den bestmöglichen Datenschutz einstellen soll.

Beispiel 89 | Datenschutzfreundliche IT-Produkte können bei dem Unabhängigen Landeszentrum für Datenschutz ein Datenschutz-Gütesiegel erlangen. Dieses Gütesiegel bescheinigt, dass das Produkt in datenschutzrechtlicher Sicht für den Einsatz bei öffentlichen Stellen des Landes geeignet ist. Und was für öffentliche Stellen datenschutzrechtlich gut ist, kann eigentlich für Private nicht schlecht sein. Niemand hindert Unternehmen also, mit dem Datenschutz-Gütesiegel um das Vertrauen der Kunden zu werben (nähere Informationen unter www.datenschutzzentrum.de).

Doch selbst wenn Sie ein solches Konzept als das Wunschdenken einiger Datenschützer abtun, sollten Sie sich im Klaren sein, welche Nutzen und welche Nachteile der Datenschutzstandard Ihres Unternehmens konkret hat. Manche Unternehmen fragen immer nur: „Was kostet der Datenschutz?“ Wenn man weiterdenkt, kommt man zu der Frage: „Was kostet es ohne Datenschutzvorkehrungen?“

Empfehlung
Für kleine und mittlere Unternehmen

Nehmen Sie sich etwas Zeit (je nach Größe Ihres Unternehmens genügt unter Umständen hierfür schon eine Stunde), um festzulegen, welche Datenschutzziele Sie verfolgen: Wollen Sie lediglich so viel tun, dass Sie von aufsichtsbehördlichen Sanktionen oder Unterlassungsklagen von Verbraucherschutzverbänden verschont zu bleiben? Wollen Sie die gesetzlichen Vorgaben erfüllen? Oder wollen Sie – vielleicht im Sinne eines Total-Quality-Ansatzes – einen überdurchschnittlich qualitativ guten Datenschutz anbieten? Können Sie damit sogar neue Kunden werben?

Wie setzen Sie Ihre Datenschutzvision um?

In einem nächsten Schritt sollten Sie Ihre Vorstellungen von einem Ihrem betrieblichen Datenschutz in abstrakte Zielsetzungen fassen und diesen konkrete Umsetzungsmaßnahmen zuordnen.

Beispiel 90 | Ihre abstrakten Vorstellungen von einem „guten Datenschutz“ können Sie in eine „Privacy Policy“ oder „Datenschutzerklärung“ fassen. Sie kann für Ihre Mitarbeiter einen wichtige Orientierung geben, was Ihre Datenschutzziele sind. Hier sollten Sie allerdings die Interessen Ihrer Mitarbeiter einbeziehen. Dabei kommt es gar nicht auf Menge und Kompliziertheit an. Wie wäre es beispielsweise mit „Zehn Punkten zum Datenschutz in unserem Unternehmen“?

Tipp
Für Unternehmen

Umsetzung von Datenschutzzielen/Datenschutzvisionen

Bilden Sie eine Datenschutzgruppe, bei denen derVertreter der Geschäftsleitung, aber auch der Mitarbeiter sowie der Datenschutzbeauftragte mitwirken. Auf diese Weise erhalten Sie einen Überblick über die Bedürfnisse und Interessen aller maßgeblichen Gruppen des Unternehmens.

Setzen Sie sich zunächst abstrakte Ziele, die Sie dann in konkrete Vorgaben umformulieren. Machen Sie die Motive für bestimmte Regelungen/Absprachen transparent, denn nur dann werden die Mitarbeiter sie auf Dauer befolgen.

Gesetzliche Mindestanforderungen an die Datenschutzorganisation

Wie auch immer Ihre Zielsetzung für den Datenschutz in Ihrem Unternehmen aussieht: Die wesentlichen gesetzlichen Datenschutzregeln müssen Sie beachten, um Sanktionen zu vermeiden. Einige Vorschriften werden nachfolgend vorgestellt.

Meldepflicht und Verfahrensübersicht (§ 4d, § 4e, § 4g Abs. 2)

Nicht-öffentliche verantwortliche Stellen haben grundsätzlich ihre Verfahren automatisierter Verarbeitungen vor der Inbetriebnahme den zuständigen Aufsichtsbehörden zu melden. Die Aufsichtsbehörden sind verpflichtet, ein entsprechendes Register zu führen. Dieses Register ist für jedermann einsehbar, mit Ausnahme der Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit.[65]

Die Meldepflicht entfällt grundsätzlich, sobald die Stelle einen betrieblichen Datenschutzbeauftragten bestellt.[66] Der Datenschutzbeauftragte hat allerdings in diesem Fall eine Übersicht der an und für sich meldepflichtigen Daten zu führen; zusätzlich muss die Übersicht Angaben der zugriffsberechtigten Personen erhalten. Die Aufsichtsbehörde kann die Einhaltung dieser Vorschrift überprüfen, indem sie im Rahmen einer Prüfung von dem Datenschutzbeauftragten die Vorlage der Übersicht verlangt.[67]

Eine Meldung kann auch entfallen, wenn eine verantwortliche Stelle personenbezogene Daten für eigene Geschäftszwecke verwendet und dabei höchstens vier Mitarbeiter mit der Datenverarbeitung beschäftigt. Allerdings muss die Datenverarbeitung dann entweder ausschließlich auf der Einwilligung der Betroffenen beruhen oder ausschließlich zur Abwicklung eines Vertrags oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erfolgen.

Beispiel 91 | Ein Einmann-Unternehmen verarbeitet personenbezogene Daten ausschließlich im Auftrag anderer Unternehmen (§ 11). Für eigene Geschäftszwecke verwendet es nur Kundendaten und auch nur zur Vertragsabwicklung. Es besteht keine Meldepflicht. Der Unternehmer ist auch nicht zum Führen einer Verfahrensübersicht (nach § 4g) verpflichtet.

Hinweise
Für Unternehmen

So sollte eine Meldung / Verfahrensübersicht nicht aussehen (Auszug: Angaben zu § 4e Nr. 4-9):

Nr. 4)
Zweckbestimmung der Verarbeitung: Gegenstand des Unternehmens ist der Betrieb von Geschäften aller Art und von damit zusammenhängenden Geschäften (vgl. §... der Satzung). Die Datenerhebung, -verarbeitung und –nutzung erfolgt zur Ausführung der oben genannten Zwecke.

Nr. 5)
Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien: Kundendaten, Personaldaten sowie Daten von Lieferanten, sofern diese zur Erfüllung der unter 4) genannten Zwecke erforderlich sind.

Nr. 6)
Empfänger oder Kategorien von Empfängern: Öffentliche Stellen bei Vorliegen vorrangiger Rechtsvorschriften sowie externe Stellen und interne Stellen der X–AG zur Erfüllung der unter 4) genannten Zwecke.

Nr. 7)
Regelfristen für die Löschung: Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und –fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten gelöscht. Sofern keine gesetzlichen Aufbewahrungspflichten bestehen, werden die Daten gelöscht, sobald die Verarbeitungszwecke entfallen.

Nr. 8)
Geplante Datenübermittlung an Drittstaaten: Eine Übermittlung an Drittstaaten ist zur Erfüllung der unter 4) genannten Zwecke vorgesehen.

Nr. 9)
Allgemeine Beschreibung der Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung: Die technischen und organisatorischen Maßnahmen nach § 9 BDSG sind getroffen.“

Kommentar

Eine Verfahrensübersicht wie die soeben Vorgestellte ist überflüssig, sie stellt einen Bürokratismus ohne praktischen Mehrwert dar. Nachfolgend werden einige Kritikpunkte aufgeführt:

zu Nr. 4): Der Zweck der Verarbeitungen ist derart komprimiert, dass er mit dem Unternehmenszweck deckungsgleich ist. Selbst eine Groborientierung, welche Verarbeitungszwecke verfolgt werden, ist so nicht möglich.

zu Nr. 5 und 4): Da „der Verfahrenszweck" zu unbestimmt ist, lassen sich die betroffenen Personengruppen nicht feststellen; die Kategorien der verarbeiteten Daten sind nicht aussagekräftig.

zu Nr. 6): Wissen Sie, wer mit „externen Stellen" als Datenempfänger gemeint sein soll?

zu Nr. 7): Es wird Bezug auf gesetzliche Regelungen genommen, § 4e Nr. 7 verlangt aber die Angabe von Regelfristen.

zu Nr. 8) Dieser Angabe nur zu entnehmen, dass solche Übermittlungen vorgesehen sind, nicht aber unter welchen Umständen.

zu Nr. 9): Die verwendete Klausel ist eine Behauptung, verlangt wird aber die Bezeichnung der tatsächlich umgesetzten Maßnahmen.

HINWEISE
FÜR UNTERNEHMEN

Hinweise für Unternehmen

Ein (anonymisiertes) Praxisbeispiel, kein Muster: Anlage Personaldatenverwaltung eines mittelständigen Unternehmens (ca. 200 Beschäftigte; Angaben gem. § 4e Nr. 4-8):

NR. 4)

Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung: Personalverwaltung; Erfüllung sozialversicherungsrechtlicher gesetzlicher Verpflichtungen.

NR. 5)

Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
Nr. 5.1: Betroffene Personengruppen: Beschäftigte und ehemalige Beschäftigte.
Nr. 5.2: Datenkategorien: Name, Personalnummer, Staatsangehörigkeit, Adressdaten, Geburtsdatum, Angaben zur Qualifikation, Ein – und Austritt in das bzw. aus dem Beschäftigungsverhältnis, Lohn- und Gehaltsdaten, Renten- und Sozialversicherungsdaten, Bankverbindung, Abmahnungen, Zeugnisse, Bewerbungsunterlagen.

NR. 6)

Empfänger oder Empfängerkategorien, denen die Daten mitgeteilt werden können: Personalabteilung, Vorgesetzte des Betroffenen, Kreditinstitute (zur Durchführung der Gehaltsüberweisungen). Bei Lohn- und Gehaltspfändungen: Gläubiger. Bei sozialversicherungsrechtlichen und steuerlichen Fragestellungen: Sozialversicherungsträger, Finanzamt.

NR. 7)

Regelfristen für die Löschung der Daten:
Abmahnungen: 6 Jahre; Bewerbungsunterlagen unverzüglich nach Auflösung des Vertragsverhältnisses mit dem Betroffenen; Lohn- und Gehaltsdaten: 10 Jahre; Sonstige Daten; 30 Jahre.

NR. 8)

Geplante Datenübermittlung in Drittstaaten: USA (XXX Inc., Nevada).

Kommentar

Nr. 4) ist relativ knapp gefasst, man kann ihr aber immerhin entnehmen, dass es um eine Verfahrensgruppe geht (Personaldatenverwaltung).
In seiner ihrer Ausführlichtkeit nahezu vorbildlich ist die Ausgestaltung von **Nr. 5)** Allerdings birgt dies die Gefahr in sich, dass einzelne Datenkategorien vergessen werden.
Nr. 6) passt sehr gut auf ein KMU, wäre in der vorliegenden Form allerdings für eine datenbankgestützte Übersicht (z. B. Großunternehmen) kaum praktikabel: Die Angabe der Zweckbestimmungen bei Kreditinstituten und Gläubigern helfen zu verstehen, aus welchen Gründen diese Stellen als Adressaten in Betracht kommen. Gestatten Sie im Rahmen einer umfangreichen Datenbank einem zugriffsberechtigten Sachbearbeiter die dezentrale Eingabe von Freitexten dieser Art, würde die Verfahrensübersicht ihre Übersichtlichkeit verlieren!
Nr. 7) Die Angabe der Regelfristen bieten einen Anhaltspunkt zur Nachfrage: Wieso muss eine Abmahnung 6 Jahre aufbewahrt werden?
Der Klammerzusatz in **Nr. 8)** ist hilfreich: Der Name des Datenempfängers ermöglicht z. B. die Überprüfung, ob das Unternehmen dem Safe Harbor Abkommen beigetreten ist.

Datenschutzbeauftragter

Das Bundesdatenschutzgesetz verpflichtet Unternehmen, einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn eine der folgenden Varianten erfüllt sind:

- unabhängig von der Zahl der Beschäftigten, wenn die verantwortliche Stelle personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung nutzt (z. B. Auskunfteien, Adressverlage, Markt- und Meinungsforschungsinstitute)[68],
- unabhängig von der Zahl der Beschäftigten, wenn die verantwortliche Stelle automatisierte Datenverarbeitungsvorgänge vornimmt, die eine Vorabkontrolle verlangen (etwa Scoringverfahren, soweit sie selbst eine Entscheidung enthalten)[69],
- sonstige verantwortliche Stellen, die mindestens fünf Arbeitnehmer[70] mit automatisierter Datenerhebung, -verarbeitung oder –nutzung beschäftigen[71],
- sonstige verantwortliche Stellen, die mindestens zwanzig Arbeitnehmer mit nichtautomatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigen[72].

Abgesehen von der rechtlichen Verpflichtung kann es auch für sonstige verantwortliche Stellen sinnvoll sein, einen betrieblichen Datenschutzbeauftragten zu bestellen. So haben nichtöffentliche Stellen grundsätzlich ihre Verfahren automatisierter Verarbeitungen vor der Inbetriebnahme den zuständigen Aufsichtsbehörden zu melden. Diese Meldepflicht entfällt, sobald die Stelle einen eigenen betrieblichen Datenschutzbeauftragten bestellt.[73]

Der betriebliche Datenschutzbeauftragte ist in der Ausübung seiner Aufgabe weisungsfrei.[74] Er genießt in Bezug auf seine Tätigkeit als Datenschutzbeauftragter einen **besonderen Kündigungsschutz**. Dieser privilegierte Kündigungsschutz erstreckt sich aber weithin nur auf Entlassungsgründe aufgrund der Funktionswahrnehmung[75] und bleibt damit z. B. hinter dem Kündigungsschutz des Betriebsrates[76] zurück.

> Beispiel 92 | Ein Bankmitarbeiter wird mit der Funktion des Datenschutzbeauftragten betraut. Er soll etwa ein Drittel seiner Arbeitszeit für den Datenschutz, zwei Drittel für den Wertpapierhandel verwenden. Der Mitarbeiter kann wegen schlechter Arbeitsleistungen im Wertpapierhandelbereich ordentlich gekündigt werden.

Neben der Überwachung der ordnungsgemäßen Datenverarbeitung und der Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen hat der betriebliche Datenschutzbeauftragte mehrere neue Aufgaben wahrzunehmen:

Er nimmt die Aufgabe eines Ansprechpartners für die Beschäftigten in Datenschutzfragen wahr. Von einer Datenverarbeitung betroffene Arbeitnehmer können sich nun direkt und jederzeit an den betrieblichen Datenschutzbeauftragten wenden. Die Verschwiegenheitspflicht des Datenschutzbeauftragten[77] gewährleistet dabei die Vertraulichkeit und sichert das Vertrauensverhältnis zwischen dem betroffenen Arbeitnehmer und dem Datenschutzbeauftragten.

Er führt ein Verzeichnis der automatisierten Verarbeitungen der verantwortlichen Stelle. Dieses Verzeichnis muss (mit Ausnahme der Beschreibung der Datensicherheitsmaßnahmen) jedermann auf Anfrage verfügbar gemacht werden.[78]

Er ist für die Vorabkontrolle zuständig (siehe oben). Dazu hat die Leitung der verantwortlichen Stelle dem Beauftragten eine Übersicht über die Verfahren automatisierter Verarbeitungen zur Verfügung zu stellen. In der Praxis wird der betriebliche Datenschutzbeauftragte häufig selbst im Zusammenwirken mit anderen Beschäftigten (EDV-Abteilung) die Verfahrensübersicht erstellen.

Verpflichtung auf das Datengeheimnis, § 5

Grundsätzlich ist jede Person in Ihrem Unternehmen verpflichtet, das Datenschutzrecht zu beachten. Da Menschen in Beschäftigungsverhältnissen häufig mit der Verarbeitung fremder personenbezogener Daten betraut werden, sieht das BDSG vor, dass nicht-öffentliche Arbeitgeber ihre Mitarbeiter auf das Datengeheimnis verpflichten. Die Verpflichtung der Beschäftigten hat „bei der Aufnahme ihrer Tätigkeit“ zu erfolgen, also bei Aufnahme des Arbeitsverhältnisses.

Mustererklärung: Verpflichtungserklärung nach § 5 BDSG

Verpflichtungserklärung
nach § 5 des Bundesdatenschutzgesetzes (BDSG)

.....
Name der Firma

Sehr geehrte(r) Frau/Herr.....,
aufgrund Ihrer Aufgabenstellung in unserem Unternehmen gilt für Sie das Datengeheimnis nach § 5 des Bundesdatenschutzgesetzes (BDSG). Nach dieser Vorschrift ist es Ihnen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.
Gem. § 5 BDSG sind Sie verpflichtet, das Datengeheimnis zu wahren. Diese Verpflichtung besteht auch über das Ende Ihrer Tätigkeit in unserem Unternehmen hinaus.
Wir weisen Sie darauf hin, dass Verstöße gegen das Datengeheimnis nach §§ 44, 43 Abs.2 BDSG und anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden können. Abschriften der genannten Vorschriften des BDSG (§§ 5 und 44, 43 Abs.2) sind beigefügt.
Ihre sich ggf. aus dem Arbeits- bzw. Dienstvertrag und der Arbeitsordnung ergebende allgemeine Geheimhaltungsverpflichtung wird durch diese Erklärung nicht berührt. Geben Sie bitte die beigefügte Zweitschrift dieses Schreibens nach Vollzug Ihrer Unterschrift an die Personalabteilung zurück.

.....
Ort, Datum

.....
Unterschrift der Firma

Über die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes wurde ich unterrichtet. Die sich daraus ergebenden Verhaltensweisen wurden mir mitgeteilt. Meine Verpflichtung auf das Datengeheimnis nach § 5 BDSG habe ich hiermit zur Kenntnis genommen.

.....
Ort, Datum

.....
Unterschrift der Mitarbeiterin
bzw. des Mitarbeiters

Auszug aus dem Bundesdatenschutzgesetz (Abzudrucken sind die Vorschriften der §§ 5,43,44 BDSG)

Gesetzliche Mindeststandards hinsichtlich der Datenverarbeitung - Vorabkontrolle

Bestimmte automatisierte Verfahren sind für die Betroffenen besonders riskant. Würde man bei ihnen erst die konkrete Datenverarbeitung betrachten, würden den Betroffenen unter Umständen irreparable Schäden erwachsen. Deshalb muss vor der Einrichtung solcher Verfahren eine besondere Rechtmäßigkeitsprüfung vorgenommen werden, die Vorabkontrolle. Sie ist insbesondere in zwei Fällen durchzuführen:

1. bei der Verarbeitung besonderer Arten personenbezogener Daten,
2. bei Verfahren, die zur Bewertung der Persönlichkeit des Betroffenen dienen; ausdrücklich eingeschlossen ist dabei die Bewertung seiner Leistungen, Fähigkeiten oder seines Verhaltens.

BEISPIEL 93 | Einrichtungen, die der Überwachung des Sozial- und Leistungsverhaltens von Arbeitnehmern dienen (Videoüberwachung am Arbeitsplatz), erfordern neben der Mitwirkung des Betriebsrates[79] auch eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten.

Diese Aufzählung ist nicht abschließend. In Betracht kommen beispielsweise Verfahren, bei denen mehrere verantwortliche Stellen einen gemeinsamen Datenbestand pflegen und verwenden. In einer solchen Fallkonstellation ist für den Betroffenen weniger überschaubar, wer über seine personenbezogenen Daten verfügt. Aus gleichen Erwägungen dürften im Regelfall automatisierte Abrufverfahren ein besonderes Risiko für die Betroffenen darstellen. Die Beteiligung mehrerer Stellen wirft überdies stets die Frage nach einer besonderen Sicherung gegenüber der unbefugten Kenntnisnahme durch Dritte auf.

Eine Vorabkontrolle muss nicht stattfinden, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen in die Verwendung vorliegt. Sie ist ferner nicht erforderlich, wenn sich die Datenverwendung im Rahmen eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses bewegt.

BEISPIEL 94 | Selbst bei der Verarbeitung sensitiver Daten muss eine Vorabkontrolle nicht vorgenommen werden, wenn der Betroffene der

verantwortlichen Stelle selbst einen Vertragsabschluss anträgt und diese Stelle im Rahmen des vorvertraglichen Vertrauensverhältnisses die Daten des Betroffenen verarbeitet (z. B. Bearbeitung eines Antrags auf Abschluss einer privaten Krankenversicherung).

Aus den Ausnahmen zum Erfordernis der Vorabkontrolle ergibt sich, dass diese in erster Linie eine Rechtskontrolle ist. Da sie sich überdies auf Datenverarbeitungsvorgänge bezieht, die besondere Risiken für die Betroffenen aufweisen, hat die Vorabkontrolle auch im besonderen Maße die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten. Ergeben sich Zweifel an der Rechtmäßigkeit geplanter Verarbeitungsverfahren, hat sich der betriebliche Datenschutzbeauftragte an die zuständige Aufsichtsbehörde zu wenden.[80]

TIPP
Für Unternehmen

Hinweise zur Vorabkontrolle gibt es auch unter www.datenschutzzentrum.de (unter „Infos für die Wirtschaft" – Betriebliche Datenschutzorganisation – Betriebliches Datenschutzmanagement).

Internationaler Datenverkehr (§ 1 Abs. 5, §§ 4 b, c)

Bislang war nur von dem Normalfall die Rede, dass Unternehmen personenbezogene Daten innerhalb der Bundesrepublik Deutschland verarbeiten. Der internationale Datenaustausch gewinnt jedoch in Schleswig-Holstein zunehmend an Bedeutung. Die Datenbeschaffung ist dabei nach den üblichen Regeln zu beurteilen. Besondere Rechtmäßigkeitsvoraussetzungen sind aber bei Datenübermittlungen in Staaten zu beachten, die nicht Mitglied der Europäischen Union oder des Europäischen Wirtschaftsraums sind.

Wann ist das BDSG auf ausländische Stellen anwendbar? (§ 1 Abs. 5)

Das BDSG kann auch Anwendung finden, wenn von einem anderen Land aus in Deutschland personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Zu unterscheiden ist danach, ob sich die jeweils verantwortliche Stelle in einem EU-Land (oder einem anderen dem Europäischen Wirtschaftsraum (EWR) zuzurechnenden Land: also auch Island, Norwegen, Liechtenstein) befindet oder in einem Drittland. Leitgedanke dieser Differenzierung ist, dass - solange sich Datenverarbeitungsvorgänge innerhalb des europäischen, mit einheitlichem Datenschutzniveau versehenen Binnenmarktes abspielen - jedes EU-Land sein eigenes Datenschutzrecht zur Anwendung bringt, wenn dort eine Niederlassung besteht.[81] Umgekehrt wird bei einer vom Drittland ausgehenden Datenverarbeitung in Europa das jeweilige europäische Recht angewendet.[82]
Verarbeitet eine Stelle innnerhalb der Europäischen Union gelegene Stellenpersonenbezogene Daten, findet das BDSG Anwendung, wenn die in einem anderen EU-Land gelegene verantwortliche Stelle durch eine Niederlassung in Deutschland tätig wird. Ohne eine Niederlassung in Deutschland gilt das Recht desjenigen Mitgliedsstaates, in dem die verantwortliche Stelle ihren Sitz hat.

Beispiel 95 | Führt ein französisches Markt- und Meinungsforschungsinstitut in Deutschland eine Umfrageaktion durch, ohne hier eine eigene Niederlassung zu betreiben oder auf Datenverarbeitungsmöglichkeiten zurückzugreifen, die hier belegen sind, dann ist deutsches Datenschutzrecht nicht anwendbar. Vielmehr gilt französisches Datenschutzrecht, das durch die deutsche Aufsichtsbehörde (notfalls mit Unterstützung durch die französischen Kollegen) anzuwenden ist.[83]

Das Recht der in der Europäischen Union befindlichen verantwortlichen Stelle gilt auch dann, wenn für sie gerade keine Niederlassung, sondern ein Auftragnehmer mit Sitz in der Europäischen Union tätig wird: Auf dessen Tätigkeit findet trotzdem das Recht der verantwortlichen Stelle Anwendung, deren Teil er ist [84]. Dies gilt allerdings nur für diejenige Datenverarbeitung, die tatsächlich im Auftrag getätigt wird; für die Eigenverarbeitung bleibt das eigene nationale Recht anwendbar.

Auf die Rechtsform der Niederlassung kommt es nicht an. Als Interpretationshilfe kann auf § 42 Abs. 2 Gewerbeordnung zurückgegriffen werden. Danach besteht eine Niederlassung, wenn der Gewerbetreibende einen zum dauernden Gebrauch eingerichteten, ständig oder in regelmäßiger Wieder-

kehr von ihm benutzten Raum für den Betrieb seines Gewerbes besitzt. Sofern die Datenverarbeitung (-erhebung, -nutzung) in Deutschland von einer Stelle ausgeht, die ihren Sitz außerhalb der Europäischen Union hat, ist das BundesdatenschutzgesetzDSG anzuwenden.[85]

Beispiel 96 | Ein im südpazifischen Inselstaat Tonga ansässiger Internet Service Provider bietet in Deutschland Dienste an und erhebt über seine von Deutschland aus abrufbare Website von sich aus personenbezogene (Kunden-) Daten (z. B. durch Cookies). Insbesondere sind dann die §§ 28 ff. Vorschriften des BDSG anwendbar. Von der Durchsetzung der datenschutzrechtlichen Bestimmungen vor Ort dürften die Aufsichtsbehörden allerdings nur träumen.

Im Gegensatz zur Europäischen Datenschutzrichtlinie (Art. 4 Abs. 1c) ist nach deutschem Recht für dessen Anwendbarkeit nicht entscheidend, dass auf in Deutschland belegene (automatisierte) Mittel zurückgegriffen wird, die sich in der Verfügungsgewalt des (im Drittland ansässigen) Anbieters befinden. Gleichwohl wird ein Mindestmaß an Einwirkungsmöglichkeit des Providers auf die in Deutschland stattfindende Verarbeitung vorliegen müssen. Dies zeigt, dass Service Provider, die ihren Geschäftssitz in ein Drittland ohne angemessenes Datenschutzniveau verlegen, dadurch nicht etwa in einen datenschutzfreien Raum flüchten können. Wenn die verarbeitende Stelle zu nennen ist (z. B. bei der Benachrichtigung nach § 33), müssen Angaben über einen Vertreter im Inland gemacht werden (Satz 3).[86] Ausnahmsweise soll das Bundesdatenschutzgesetz nicht geltengilt das BDSG nicht, wenn Datenträger nur zum Zweck des Transits durch Deutschland eingesetzt werden.[87] Das setzt voraus, dass Übertragungswege benutzt werden, ohne dass von den personenbezogenen Daten Kenntnis genommen wird (z. B. bei Telekommunikationsleitungen).

Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen (§ 4 b)

Übermittlungen von Daten an Empfänger im EWR sowie an Organe und Einrichtungen der Europäischen Gemeinschaften (z. B. Europäische Kommission, Europäisches Parlament) sind nach den allgemeinen Datenverarbeitungsregeln zu beurteilen, also insbesondere nach §§ 28 bis 30. Datenübermittlungen innerhalb des europäischen Binnenmarktes werden nach den gleichen Zulässigkeitsvoraussetzungen beurteilt wie Datenübermittlungen innerhalb Deutschlands. Dies gilt aber nicht für alle Daten, sondern nur für solche, die ganz oder teilweise in den „Anwendungsbereich des Rechts der Europäischen Gemeinschaften“ fallen. Die privilegierende Regelung bezieht sich also in erster Linie auf das EG-Wirtschaftsrecht, in der Regel nicht aber auf die gemeinsame Außen- und Sicherheitspolitik, oder die Zusammenarbeit in der Innen- und Rechtspolitik.

Beispiel 97 | Ein selbständiges Tochterunternehmen in Deutschland möchte Arbeitnehmerdaten an das französische Mutterunternehmen übermitteln. Mit den §§ 28 bis 30 BDSG gelten für die Datenübermittlung die gleichen Regelungen wie bei einem Datentransfer innerhalb Deutschlands.

Für Datenübermittlungen an europäische Stellen außerhalb der Europäischen Union sowie an Drittländer gelten die §§ 28 bis 30 BDSG, jedoch mit einer Einschränkung: Die Übermittlung der Daten darf nicht stattfinden, wenn der Betroffene ein „schutzwürdiges Interesse“ an der Nichtübermittlung hat. Dies ist insbesondere der Fall, wenn beim Datenempfänger ein angemessenes Datenschutzniveau nicht gewährleistet ist.

Die verantwortliche Stelle (also das Unternehmen) ist verpflichtet, das Datenschutzniveau des Empfängers zu beurteilen. Wann ein angemessenes Schutzniveau tatsächlich vorliegt, ergibt sich hieraus der gesetzlichen Regelung jedoch nicht. Die maßgeblichen Beurteilungskriterien sind in einem Arbeitspapier WP 12 der Gruppe nach Art. 29 Europäische Datenschutzrichtlinie aufgeführt (abrufbar unter http://www.datenschutz-berlin.de, Datenschutz in Europa).

Ob beim Empfänger ein angemessenes Datenschutzniveau vorliegt, muss innerhalb der Europäischen Union einheitlich beurteilt werden. Die Europäische Kommission unternimmt verschiedene Überprüfungen hinsichtlich der Angemessenheit des Datenschutzes in Drittländern. Positiv festgestellt

wurde sie bereits z. B. für die Schweiz und Ungarn. Die Kommission trifft die Feststellung nach Art. 25 Abs. 6 Europäische Datenschutzrichtlinie zumeist auf Grund der jeweiligen innerstaatlichen Rechtsvorschriften (so geschehen für die Schweiz und Ungarn). Eine andere Möglichkeit ist die Feststellung des angemessenen Schutzniveaus aufgrund von Verhandlungen mit dem Drittstaat. Dieser Weg wurde in Bezug auf die USA beschritten. Da dort die Selbstregulierung einer umfassenden Datenschutzgesetzgebung vorgezogen wird, kann von einem angemessenen Schutzniveau nicht von vornherein ausgegangen werden. Nur wenn ein US-Unternehmen sich den zwischen der Europäischen Kommission und der US-Regierung ausgehandelten „Safe Harbor"-Prinzipien unterworfen hat und diese beachtet, gilt es als in dieser Hinsicht mit angemessenem Datenschutzniveau versehen, eben als „sicherer Hafen". Eine Liste der bislang beigetretenen US- Unternehmen ist unter http://www.export.gov/safeharbor abrufbar.

Die Verantwortung für die Zulässigkeit der Datenübermittlung trägt die „übermittelnde" also die deutsche Stelle.[88] Daraus ergibt sich, dass diese Stelle selbst für die nach Abs. 3 durchzuführende Überprüfung der Angemessenheit des Schutzniveaus beim Empfänger zuständig ist. Dabei können auch branchenspezifische Regelungen im Drittland berücksichtigt werden. Vorrangig zu beachten hat die übermittelnde Stelle die positiven Entscheidungen der Europäischen Kommission zur Angemessenheit des Datenschutzniveaus im Drittland (s. o.). Datenübermittlungen in Drittstaaten unterliegen einer strikten Zweckbindung. Darauf sind die Datenempfänger hinzuweisen.

Beispiel 98 | Die deutsche Tochter eines US-amerikanischen Konzerns möchte Daten aus ihren Kundendateien an die Mutterfirma weiterleiten, damit den Kunden Informationsmaterial aus bestimmten Tätigkeitsbereichen der Mutterfirma zugesendet werden kann. Es sollen personenbezogene Daten von einem Unternehmen an ein anderes außerhalb der Europäischen Union versendet werden. Anzuwenden ist § 4b Abs. 2. Die Übermittlung unterbleibt, wenn das Datenschutzniveau beim Empfänger nicht angemessen ist (Satz 2). Ist es angemessen, so müssen zusätzlich die materiellen Voraussetzungen, die auch für eine innerdeutsche oder innereuropäische Datenübermittlung vorliegen müssen, erfüllt sein (Satz 1); sonst wäre eine Datenübermittlung in die USA leichter zu realisieren als im europäischen Binnenmarkt oder innerhalb Deutschlands.

Ausnahmen: Datenübermittlung trotz unangemessenem Datenschutzniveau im Drittstaat (§ 4c)

§ 4c BDSG benennt die Ausnahmen, bei denen trotz unangemessenen Datenschutzniveaus im Drittland eine Datenübermittlung erfolgen darf. Da die Feststellungen über angemessene Datenschutzniveaus bisher nicht sehr zahlreich sind, wird sich die Zulässigkeit des internationalen Datentransfers im unternehmerischen Alltag weitestgehend nach diesen Regelungen richten. § 4c Absatz 1 Satz 1 benennt sechs Ausnahmen, bei denen die Datenübermittlung zulässig ist, obwohl ein angemessenes Datenschutzniveau beim Empfänger nicht vorliegt.

Hierzu zählt zunächst die Einwilligung des Betroffenen, die vor der Datenübermittlung einzuholen ist (Nr. 1). Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 4a Abs.1 Satz 3 BDSG). Immer muss zweifelsfrei feststehen, dass der Betroffene der Datenübermittlung tatsächlich zugestimmt hat. Insbesondere aber muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Angesichts des Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer ist diese Rechtsgrundlage für die Übermittlung von Arbeitnehmerdaten problematisch. Ob stattdessen auf eine Betriebsvereinbarung zurückgegriffen werden kann, ist ebenfalls fraglich.

Nr. 2 und 3 erlauben die Datenübermittlung im Rahmen der geschäftlichen Verbindung. Als maßgebliche Voraussetzung ist hier der Grundsatz der Erforderlichkeit zu beachten. Bei Nr. 2 muss eine vertragliche oder vorvertragliche Basis zwischen dem Betroffenen und dem Datenübermittler bestehen. Bei Nr. 3 ist der Betroffene nicht selbst Vertragspartei.

Wenn ein Betroffener einen Vertrag für eine Reise in ein Drittland abschließt, wird der Reiseveranstalter die Unterbringung im Drittland arrangieren müssen, so dass zu diesem Zweck die erforderlichen Daten des Betroffenen dorthin übermittelt werden dürfen. Eine solche Datenweitergabe ist durch § 4c Abs. 1 Satz 1 Nr. 2 oder Nr. 3 gedeckt. Sollen die Daten im Drittland über den ursprünglichen Vertragszweck hinaus noch weiterverarbeitet werden, so ist hierfür die Einwilligung des Betroffenen erforderlich.

Beispiel 99 | Sie buchen bei einem Reiseveranstalter eine Rundreise in den Vereinigten Staaten von Amerika (USA). Sollen Ihre Daten an Ausflugsunternehmen vor Ort gegeben werden, damit diese Sie als Reisenden gezielt mit Angeboten umwerben können, so ist das vom Vertragszweck nicht mit erfasst. Der Veranstalter muss Ihre Einwilligung einholen.

Wichtige öffentliche Interessen im Sinne von Nr. 4 werden im privatwirtschaftlichen Sektor kaum vorliegen. Im Hinblick auf lebenswichtige Interessen im Sinne von Nr. 5 kommen medizinische Daten in Frage, wenn der Betroffene nicht einwilligen kann. Nr. 6 meint die Übermittlung aus öffentlichen (behördlichen) Registern wie z. B. das Handelsregister. Wiederum ist der Datenempfänger darauf hinzuweisen, dass die Daten nur zu dem Zweck verarbeitet werden dürfen, zu dem sie übermittelt wurden.

Liegt keine der genannten Ausnahmen vor, kann die zuständige Aufsichtsbehörde die Datenübermittlung genehmigen, wenn das verantwortliche deutsche Unternehmen ausreichende Datenschutzgarantien vorweist.[89] Die Garantien können sich insbesondere (aber nicht ausschließlich) aus einem Vertrag zwischen dem Datenexporteur und dem -importeur ergeben. Damit wird der (wenn überhaupt vorhandene) Datenschutz beim im Drittland befindlichen Datenimporteur gewissermaßen auf ein angemessenes Niveau „gehoben“. Welche inhaltlichen Anforderungen ein derartiger Vertrag mindestens erfüllen muss, hat die Europäische Kommission bereits entschieden (vgl. Art. 26 Abs. 4 Europäische Datenschutzrichtlinie). Zugleich hat sie Mustervertragsklauseln entworfen (ABl. EG, L 181/19 v. 4.7.2001). Ihre Verwendung ist nicht zwingend, eigene vertragliche Ausgestaltungen sind zulässig. Die Verwendung der Mustervertragsklauseln hat jedoch den Vorteil, dass die Aufsichtsbehörde die Genehmigung nicht mit der Begründung versagen darf, es seien ausreichende Datenschutzgarantien nicht vorhanden; sie wird vielmehr die Genehmigung in Aussicht stellen unter der Voraussetzung, dass die beabsichtigten Übermittlungen der Aufsichtsbehörde mitgeteilt werden.

Ein Verstoß gegen (aufgrund von Verträgen oder Unternehmensregelungen) genehmigte Datenübermittlungen führt - mangels Befugnisregelung im BDSG - zwar nicht zur Aussetzung der Vollziehung des Datentransfers durch die Aufsichtsbehörde. Er kann aber die Rücknahme der Genehmigung oder die Verhängung eines Bußgeldes gegen den Datenexporteur nach sich ziehen.[90]

Bundesdatenschutzgesetz (BDSG)

in der Neufassung des Bundesdatenschutzgesetzes (BDSG)
vom 14.01.2003 (BGBl. I S.66)

Dieses Gesetz dient der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281, S. 31 ff.).

Inhaltsübersicht

Erster Abschnitt: Allgemeine und gemeinsame Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn:

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.
(3) Erheben ist das Beschaffen von Daten über den Betroffenen.
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.
(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter istjede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

§ 3a Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen,

soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.
(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen
Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.
(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.
(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.
(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.
(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

§ 4c Ausnahmen

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.
(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b

Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.
(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz nach Maßgabe von § 4e zu melden.
(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.
(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.
(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung oder
2. zum Zweck der anonymisierten Übermittlung

gespeichert werden.
(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.
(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz zu wenden.

§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

§ 4f Beauftragter für den Datenschutz

(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für nicht-öffentliche Stellen, die höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen, haben sie unabhängig von der Anzahl der Arbeitnehmer einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz die

Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar. Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.
(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt,
personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.
(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

§ 6a Automatisierte Einzelentscheidung

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.
(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitgeteilt wird. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

(3) Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend §§ 19a und 33 zu benachrichtigen.
(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 7 Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.
(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt §254 des Bürgerlichen Gesetzbuchs.
(6) Auf die Verjährung finden die für unerlaubteHandlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 9a Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig,
soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.
(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesministerium zugestimmt hat.
(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.
(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.
(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich von der Einhaltung der beim

Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs.1 Nr. 2, 10 und 11, Abs.2 Nr.1 bis 3 undAbs.3 sowie §44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,
2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder
2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.
(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse erhoben, verarbeitet oder genutzt, gelten an Stelle der §§ 13 bis 16, 19 bis 20 der § 28 Abs. 1 und 3 Nr. 1 sowie die §§ 33 bis 35, auch soweit personenbezogene Daten weder automatisiert verarbeitet noch in nicht automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden.

§ 13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.
(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft vepflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.
(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblichüberwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient.

Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.
(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.
(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder
2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.
(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.
(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.
(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.
(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.
(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwür-

diges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§17 (weggefallen)

§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens, sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Zweiter Unterabschnitt: Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bun-

desnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 bis 4 gilt entsprechend.

§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.
(6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.
(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.
(9) §2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21 Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt: Bundesbeauftragter für den Datenschutz

§ 22 Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muss bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.
(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:
"Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe."
Der Eid kann auch ohne religiöse Beteuerung geleistet werden.
(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.
(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.
(5) Der Bundesbeauftragte wird beim Bundesministerium des

Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.
(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz
beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Der Bundespräsident entlässt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.
(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.
(3) Der Bundesbeauftragte hat dem Bundesministerium des Innern Mitteilung über Geschenke zu machen, die er in Bezug auf sein Amt erhält. Das Bundesministerium des Innern entscheidet über die Verwendung der Geschenke.
(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet.Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.
(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministeriums des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für den Bundesbeauftragten und seine Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, § 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um

vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.
(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.
(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, dass an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.
(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.
(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs, und
2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.
(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,
4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.
(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.
(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.
(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.
(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.
(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit denöffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 3 und 4 gilt entsprechend.

Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

§ 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.

(3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder
2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder
3. für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf
   a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   b) Berufs-, Branchen- oder Geschäftsbeziehung,
   c) Namen,
   d) Titel,
   e) akademische Grade,
   f) Anschrift und
   g) Geburtsjahr

   beschränken

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

In den Fällen des Satzes 1 Nr. 3 ist anzunehmen, dass dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

1. auf strafbare Handlungen,
2. auf Ordnungswidrigkeiten sowie
3. bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten nach Absatz 3 übermittelt werden, der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.
(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.
(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme
   besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafge-

setzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet odergenutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.
(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.
(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.

§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

§ 28 Abs. 1 Satz 2 ist anzuwenden.
(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. a) der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
   b) es sich um listenmäßig oder sonst zusammengefasste Daten nach § 28 Abs. 3 Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden.
(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zu Grunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.
(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.
(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben

über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 32 (weggefallen)

Zweiter Unterabschnitt: Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen,
4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,
5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
7. die Daten für eigene Zwecke gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder

b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder

8. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und

   a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

   b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b)

   und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

   Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie weder in einer automatisierten Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über

Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt: Aufsichtsbehörde

§ 36 (weggefallen)

§ 37 (weggefallen)

§ 38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Die Aufsichtsbehörde

darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.
(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.
(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.
(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.
(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.

§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.
(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Vierter Abschnitt: Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.
(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.
(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.
(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. An Stelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42 Datenschutzbeauftragter der Deutschen Welle

(1) Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. Die § 4f und 4g bleiben unberührt.

Fünfter Abschnitt: Schlussvorschriften

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,
3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,
4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,
5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,
8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfundzwanzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu zweihundertfünfzigtausend Euro geahndet werden.

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.

Sechster Abschnitt: Übergangsvorschriften

§ 45 Laufende Verwendungen

Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

§ 46 Weitergeltung von Begriffsbestimmungen

(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.
(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Stichwortverzeichnis

O

P

R

S

T

U

V

W

Z

Fußnoten und Literaturhinweise

1 Diese Informationsweitergabe ist nur eingeschränkt zulässig. Grundsätzlich ist hierfür der Nachweis des Datenempfängers erforderlich, dass er zum Erhalt der Kontoinformationen berechtigt ist. Ein solcher Nachweis ist in der Regel nur durch den Erbschein zu erbringen (vgl. § 2365 BGB). Einen Fall dazu finden Sie im ULD-Tätigkeitsbericht 2002, S. 82, 83 (unter 6.3).

2 Zur grundsätzlichen Unzulässigkeit der umfassenden Speicherung der IP-Nummer über den eigentlichen Vorgang der Diensterbringung hinaus vgl. die Pressemitteilung des ULD vom 16. Januar 2003, veröffentlicht im Internet (www.datenschutzzentrum.de unter Presse).

3 Der offizielle Titel dieser Richtlinie lautet: „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr".

4 Dazu Art. 249 EG-Vertrag: „Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel."

5 § 3 Abs. 3.

6 § 3 Abs. 4.

7 § 3 Abs. 5.

8 Das leitet man aus der Tatsache ab, dass eine ältere Fassung des BDSG (Gesetz vom 20.12.1990) für vorübergehende Speicherung nur eingeschränkt anwendbar war (§ 1 Abs. 3 Nr. 1 BDSG 1990). Diese Einschränkung des Anwendungsbereichs ist in der Neufassung von 2003 entfallen, weil die EG-DSRL auch zur Regelung vorübergehender Speicherungen verpflichtet.

9 § 3 Abs. 4 Nr. 4.

10 § 147 Abgabenordnung.

11 § 28 Abs. 3, 4.

12 Vgl. dazu auch ULD-Tätigkeitsbericht 2003, S. 81 (unter 6.3.6).

13 § 2 Abs. 4.

14 § 1 Abs. 2 Nr. 3.

15 Genauer: „Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann", § 3 Abs. 2 S. 2.

16 § 9 Abs. 1 Satz 2, § 2 Abs. 1 Geldwäschegesetz seit der Änderung vom 8.8.2002 (BGBl. I S. 3105).

17 § 4 Abs. 1.

18 § 4a Abs. 1 Satz 1.

19 Dazu auch ULD-Tätigkeitsbericht 2002, S. 83, 84.

20 § 4a Abs. 1 Satz 3.

23 §§ 6a-6c, 28-30.

24 § 28.

25 § 29. Soll die Verarbeitung zum Zweck der anonymisierten Übermittlung erfolgen, ist § 30 anzuwenden.

26 § 28 Abs. 1 Satz 2; ggf. in Verbindung mit § 29 Abs. 1 Satz 2.

27 § 28 Abs. 1 Nr. 1.

28 § 18 Kreditwesengesetz.

29 Dazu ULD Tätigkeitsbericht 2001, S. 87 (unter 6.6.).

30 Das Geburtsjahr darf nach Maßgabe des § 28 Abs. 3 Nr. 3 zu Werbezwecken verwendet werden.

31 § 28 Abs. 1 Satz 2.

32 Mehr zum Thema Datenschutz in Vereinen kann man aus einer Broschüre „Datenschutz im Verein" erfahren, die von den Datenschutzbehörden der Länder Berlin, Bremen, Hamburg, Niedersachsen und Nordrhein-Westfalen herausgegeben wird. Natürlich gibt es auf dem gemeinsamen Internetportal der Datenschutzsbehörden www.datenschutz.de und auf der Webseite des ULD www.datenschutzzentrum.de (unter Infos für die Wirtschaft) ebenfalls zahlreiche Informationen.

33 § 28 Abs. 3 Nr. 1.

34 § 28 Abs. 1 Satz 2.

35 Vgl. § 35 Abs. 2.

36 § 28 Abs. 1 Nr. 2.

37 § 28 Abs. 3 Nr. 3.

38 Ob das der Fall ist, richtet sich vor allem nach § 43 Abs. 2, § 44 Abs. 1.

39 § 28 Abs. 4.

40 Einzelheiten zu der Straßenumfrage auf der ULD-Website www.datenschutzzentrum.de unter Presse: Bürger ärgern sich über Werbesendungen (8.November 2002). Der Verband Deutscher Direktmarketing (DDV) hat sich erfolglos mit diversen Schreiben über diese Umfrage beschwert. Informationen darüber finden Sie auf der genannten Website unter „Infos für die Wirtschaft"/„Vorträge und Stellungnahmen".

41 Vgl. dazu ULD TB 2001, S. 80, 81 (Abschnitt 6.3.3).

42 § 3 Abs. 9.

43 Vgl. § 28 Abs. 6-9.

44 Vgl. § 28 Abs. 9.

45 § 6a. Gemeint sind nachteilige Entscheidungen, die ausschließlich von Computern erzeugt werden.

46 § 6b.

47 § 6c. Gemeint sind Chipkarten, die über bloße Speichervorgänge hinaus auf der Karte Verarbeitungsprozesse ermöglichen (z. B. aufladbare Geldkarten der Sparkassen).

48 §§ 23, 33 Kunsturhebergesetz.

49 Vgl. §§ 4 Abs. 3, 28 Abs. 4, 33 Abs. 1, 34 Abs. 1.

50 § 4 Abs. 3 erster Halbsatz.

51 Dazu ULD TB 2003, S. 82 (Abschnitt 6.4.2).
52 § 4 Abs. 2.
53 § 4 Abs. 2 Satz 2 am Ende.
54 §§ 915 ff. Zivilprozessordnung und Schuldnerverzeichnisverordnung.
55 Vgl. § 34 Abs. 4.
56 § 34 Abs. 5 S. 4.
57 § 6a. Gemeint sind nachteilige Entscheidungen, die ausschließlich von Computern erzeugt werden.
58 § 6c. Gemeint sind Chipkarten, die über bloße Speichervorgänge hinaus auf der Karte Verarbeitungsprozesse ermöglichen (z. B. aufladbare Geldkarten der Sparkassen).
59 Eine solche Einschränkung ist der EU-DSRL nicht zu entnehmen. Dementsprechend ist der Bundestags-Innenausschuss zu Recht der im Regierungsentwurf zu § 6a BDSG geäußerten, gegenteiligen Rechtsauffassung nicht gefolgt. Vgl. hierzu Beschlussempfehlung und Bericht des Innenausschusses vom 4. April 2001, BT-Drs. 14/5793, S. 65.
60 § 6 Abs. 1.
61 § 35 Abs. 1.
62 § 35 Abs. 7.
63 § 35 Abs. 2 Nr. 1.
64 § 35 Abs. 4.
65 § 35 Abs. 2 Nr. 2.
66 Dazu vgl. § 43 Abs. 4 Landesdatenschutzgesetz Schleswig-Holstein. Andere Bundesländer verfügen über vergleichbare Regelungen.
67 § 38 Absatz 2.
68 § 4d Absatz 2. Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung erheben und verarbeiten, sind weiterhin zur Meldung verpflichtet.
69 § 38 Absatz 4 Satz 2.
70 § 4f Abs. 1 S. 6.
71 § 4f Abs. 1 S. 6.
72 Dem Schutzzweck entsprechend ist der Arbeitnehmerbegriff funktional zu verstehen und umfasst diejenigen Beschäftigten eines Unternehmens, die organisatorisch in die verantwortliche Stelle eingegliedert sind. Vgl. dazu bereits Simitis in Dammann/Simitis, BDSG, 3. Auflage 1981, § 28 Rn. 36.
73 § 4f Abs. 1 S. 1, 4.
74 § 4f Abs. 1 S. 1, 3.
75 § 4d Absatz 2.
76 Die Wortlaut-Änderungen des § 4f Absatz 3 Satz 2 gegenüber der Vorgängervorschrift (§ 36 Absatz 3 Satz 2 BDSG 1990) sind lediglich redaktioneller Art, vgl. Begründung des zum Regierungsentwurfs, BT-Drs. 14/ 4329, S. 36, zu § 4f.
77 § 4f Absatz 3 Satz 4.
78 § 15 Absatz 1 KSchG.
79 Nach § 4f Absatz 4.
80 § 4 g Absatz 2 Satz 2 in Verbindung mit § 4 e Nrn. 1-8.
81 Vgl. § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz.
82 § 4 d Abs. 6 Satz 3.
83 § 1 Abs. 5 S. 1.
84 Bei § 1 Abs. 5 S. 2 also deutsches Recht.
85 § 38 Abs. 1 Satz 1 a. E.
86 § 3 Abs. 8 Satz 3.
87 § 1 Abs. 5 S. 2.
88 § 1 Abs. 5 S. 3.
89 § 1 Abs. 5 S. 4.
90 § 4b Abs. 5.
91 § 4c Abs. 2.
92 § 43 Abs. 2 Nr. 1.

Impressum

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Holstenstraße 98
D – 24103 Kiel
Telefon: 0431/988 - 1200 | Fax: 0431/988 - 1223
E-Mail: mail@datenschutzzentrum.de
Hompage: http://www. datenschutzzentrum.de

vzbv Verbraucherzentrale Bundesverband e.V.
Markgrafenstraße 66
D – 10969 Berlin
Telefon: 030/25800-0 | Fax: 030/25800-218
E-Mail: info@vzbv.de
Homepage: http://www.vzbv.de

Verbraucherzentrale Schleswig-Holstein e.V.
Bergstraße 24
D – 24103 Kiel
Telefon: 0431/590 99 0 | Telefax: 0431/590 99 77
E-Mail: info@verbraucherzentrale-sh.de
Hompage: http://www.verbraucherzentrale-sh.de