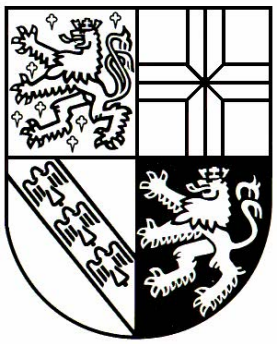


3. Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich

Berichtszeitraum

2005 / 2006

Impressum

Herausgeber: Aufsichtsbehörde für den Datenschutz
im nicht-öffentlichen Bereich beim
Ministerium für Inneres und Sport
Franz-Josef-Röder-Straße 21
66119 Saarbrücken

Hausanschrift:
Mainzer Straße 136
66121 Saarbrücken
Telefon: 0681 / 962 – 1634
Telefax: 0681 / 962 – 1605
E-Mail: datenschutz@innen.saarland.de
Internet: www.saarland.de

VORGELEGT VON

DER AUFSICHTSBEHÖRDE

FÜR DEN DATENSCHUTZ

IM NICHT-ÖFFENTLICHEN BEREICH

BEIM

MINISTERIUM FÜR INNERES UND SPORT

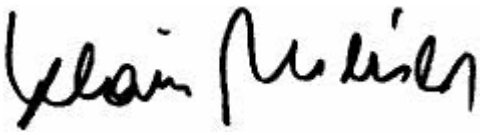
DES SAARLANDES

Liebe Bürgerinnen und Bürger,

die Verarbeitung personenbezogener Daten nimmt im Zeitalter der Informationstechnologie einen immer breiteren Raum ein. Immer mehr Daten können in kürzester Zeit gespeichert, bearbeitet und genutzt werden. Der Gesetzgeber hat im Bundesdatenschutzgesetz, wie auch in anderen datenschutzrechtlichen Vorschriften, versucht, die – teilweise gegenläufigen – Interessen der datenverarbeitenden Stellen und der Betroffenen zu einem Ausgleich zu bringen. Es ist aber nicht nur Aufgabe der Politik, die Datenverarbeitung durch entsprechende Gesetze in geregelte und auf das Notwendige begrenzte Bahnen zu lenken. Auch jeder Einzelne sollte im Rahmen seiner informationellen Selbstbestimmung von seinen Möglichkeiten Gebrauch machen, die Verarbeitung seiner personenbezogenen Daten zu kontrollieren und gegebenenfalls einzudämmen. Eine wesentliche Voraussetzung hierfür ist die Sensibilisierung der Bürgerinnen und Bürger für das Thema Datenschutz.

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich veröffentlicht regelmäßig einen Tätigkeitsbericht, in dem Ausschnitte der im Berichtszeitraum behandelten Probleme sowie Anfragen und Eingaben von Bürgerinnen und Bürgern dargestellt werden. Immer wiederkehrende Fragen und Fallgestaltungen werden erläutert. Das ein oder andere Problem wird vielleicht auch Ihnen schon begegnet sein.

Nutzen Sie das Angebot, sich bei Problemen, Fragen oder Beratungsbedarf an die Datenschutzaufsichtsbehörde zu wenden und von dem für den Bürger kostenlosen Service Gebrauch zu machen.



Klaus Meiser
Minister für Inneres und Sport

Inhaltsverzeichnis Seite

1. Aufsichtsbehörde für den Datenschutz

1.1 Vorbemerkungen

Im Saarland ist die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich beim Ministerium für Inneres und Sport angesiedelt. Die Aufgabe der Aufsichtsbehörde besteht darin, die Einhaltung des Bundesdatenschutzgesetzes (BDSG) und anderer datenschutzrechtlicher Vorschriften durch nicht öffentliche Stellen zu kontrollieren. Dies umfasst vor allem privatrechtlich organisierte Unternehmen, in Ausnahmefällen auch Privatpersonen, die personenbezogene Daten verarbeiten. Für die datenschutzrechtliche Kontrolle öffentlicher Stellen ist hingegen der Landesbeauftragte für Datenschutz und Informationsfreiheit zuständig.

Die Kontrollzuständigkeit der Aufsichtsbehörde erstreckt sich dabei auf die Datenverarbeitungen in dem Unternehmen, gleich, ob die Datenverarbeitung Hauptgeschäftszweck ist oder nur eine Hilfsfunktion hat, wie z. B. bei der Personaldaten- oder Kundendatenverwaltung. Ausschlaggebend ist, dass die Daten entweder in automatisierten Verfahren bzw. in oder aus nicht automatisierten Dateien (z. B. Karteikartensystemen) verarbeitet/genutzt werden.

Bei der Beurteilung der Zulässigkeit von Datenerhebungen, -verarbeitungen und -nutzungen sind immer auch bereichsspezifische Vorschriften zu beachten. Fragen nach dem Schutz personenbezogener Daten werden immer dann aufgeworfen, wenn solche Daten erhoben, verarbeitet oder genutzt werden oder dies beabsichtigt ist. Der Datenschutz kann daher nicht nur einem bestimmten Rechtsgebiet zugewiesen werden.

Die fehlende Zuordnung zu einer bestimmten Rechtsmaterie bedingt, dass allgemeine datenschutzrechtliche Regelungen immer im jeweiligen Kontext, wie z. B. dem Arbeitsrecht, zu betrachten und auch um-

zusetzen sind. Hierbei steht die Prüfung, ob und wie weit die Erhebung, Verarbeitung und Nutzung bestimmter Daten überhaupt erforderlich ist, immer an erster Stelle der Zulässigkeitsvoraussetzungen. Auch sind stets die Interessen der Betroffenen und der verantwortlichen Stelle je nach Vorschrift in unterschiedlicher Gewichtung zu berücksichtigen. Diese gesetzgeberische Entscheidung drückt aus, dass das Recht auf informationelle Selbstbestimmung, das Recht auf Schutz der eigenen Daten, kein absolutes ist. Es muss sich gerade im Spannungsfeld zwischen wirtschaftlichen und privaten Interessen immer wieder neu definieren, da auch die Ausübung eines Gewerbes grundrechtlich geschützt ist.

Es ist daher notwendig, im Sinne aller Beteiligten zu sachgerechten Lösungen und Auslegungen datenschutzrechtlicher Vorschriften zu gelangen. Nur durch gegenseitige Akzeptanz der Datenverarbeiter und der Betroffenen kann ein Verständnis für das Grundanliegen des Datenschutzes gefunden werden: Einen weitest möglichen Schutz personenbezogener Daten unter gleichzeitiger Beachtung des jeweils rechtlich zulässigen Informationsflusses, gehört zu den Aufgaben der Aufsichtsbehörden für den Datenschutz. Klassisch wird dies umgesetzt durch Kontrollen, rechtliche Bewertung der jeweiligen Datenverarbeitungen und dem Erarbeiten von Lösungswegen. Daneben bietet die Aufsichtsbehörde aber auch ihre Hilfe und Beratung bereits im Vorfeld an, um Risiken für das informationelle Selbstbestimmungsrecht zu erkennen und zu vermeiden und so - als weiteres Resultat - auch Rechtssicherheit für die jeweils Verantwortlichen zu schaffen.

1.2 Tätigkeit

Anfragen und Eingaben von Bürgerinnen und Bürgern (auch „Petentinnen/Petenten“ genannt), die telefonisch, schriftlich und per E-Mail an die Aufsichtsbehörde für den Datenschutz herangetragen werden, machen den Hauptteil der praktischen Arbeit aus. Ein großer Teil der tele-

fonischen Anfragen bezieht sich auf die generelle Zulässigkeit der Datenverarbeitung und kann in der Regel unmittelbar beantwortet werden.

Konkret geschilderte Fälle hingegen erfordern eine sog. „Sachverhaltsaufklärung“: Die Aufsichtsbehörde wendet sich in solchen Fällen an die verantwortliche Stelle, die in der Eingabe genannt wurde und bittet um Stellungnahme. Diese darf nur dann verweigert werden, wenn die Gefahr eines Bußgeld- oder Strafverfahrens bestünde. In den meisten Fällen sind die verantwortlichen Stellen durchaus kooperationsbereit und stellen eventuell festgestellte Mängel, die sich hauptsächlich auf Unkenntnis der gesetzlichen Regelungen zurückführen lassen, unverzüglich ab. Ein Bußgeld muss daher nur in den seltensten Fällen angedroht werden.

Ist der Sachverhalt geklärt, erfolgt die datenschutzrechtliche Bewertung, die den Petentinnen/Petenten mitgeteilt wird.

Die Aufsichtsbehörde für den Datenschutz hat für sich das Leitbild einer Verwaltung formuliert, die im Interesse aller Bürgerinnen und Bürger arbeitet. Ziel ist es, Eingaben und Anfragen möglichst umfassend, zeitnah und letztendlich unbürokratisch zu beantworten, soweit dies einer an Recht und Gesetz und damit auch Verfahrensvorschriften gebundenen Verwaltung möglich ist. Durch die Tätigkeit der Aufsichtsbehörde entstehen den Betroffenen keine Kosten, es werden keine Gebühren erhoben. Anwalt der Betroffenen zu sein und gleichzeitig eine objektive Interessenabwägung vorzunehmen, ist das Ziel aller Bemühungen der Aufsichtsbehörde für den Datenschutz.

1.3 Aufgaben und Kompetenzen der Aufsichtsbehörde

- Kontrolle der Rechtmäßigkeit der Datenverarbeitung, auch anlassunabhängig (§ 38 Abs. 1 S. 1 BDSG)

- Führung des Registers meldepflichtiger Verarbeitungen im Rahmen der vorgelagerten Kontrolle (§ 38 Abs. 2 BDSG)
- Betretungs-, Informations- und Einsichtsrechte (§ 38 Abs. 3 und 4 BDSG)
- Genehmigung von Datenübermittlungen in Dritt-Staaten (Nicht-EU-Staaten) ohne angemessenes Datenschutzniveau (§ 4c Abs. 2 BDSG)
- die Herausgabe von Tätigkeitsberichten (§ 38 Abs. 1 S. 6 BDSG)
- Beratung von Unternehmen bei der Erstellung von Unternehmensrichtlinien zum Schutz personenbezogener Daten
- Mitwirkung bei der Vorabkontrolle (§ 4d Abs. 6 S. 3 BDSG)
- Unterstützung der betrieblichen Datenschutzbeauftragten (§ 4g Abs. 1 S. 2 BDSG)
- Prüfung von Unternehmensregelungen zur Verarbeitung personenbezogener Daten (§ 38a BDSG)
- Unterrichtung der Betroffenen, Anzeige bei Verfolgungsbehörden, bei schwerwiegenden Mängeln auch bei der Gewerbeaufsicht (§ 38 Abs. 1 S. 4 BDSG)
- Anordnung zur Beseitigung technischer und organisatorischer Mängel (§ 38 Abs. 5 S. 1 BDSG)
- Zwangsgeld bei unterlassener Mängelbeseitigung (§ 38 Abs. 5 S. 2 BDSG)
- Durchführung von Bußgeldverfahren (§ 43 BDSG)
- Strafantragsrecht bei Verstößen gegen Vorschriften des Bundesdatenschutzgesetzes (§ 44 Abs. 2 BDSG)

1.4 Zusammenarbeit mit anderen Aufsichtsbehörden

„Düsseldorfer Kreis“

Bei dieser Einrichtung handelt es sich um ein Gremium der Vertreter der obersten Aufsichtsbehörden für den Datenschutz in dem alle Bundesländer vertreten sind. Benannt nach seinem ursprünglichen Tagungsort unter dem Vorsitz des Innenministeriums des Landes Nord-

rhein-Westfalen, wechselt der Vorsitz seit 2002 und damit auch das die zwei mal jährlich stattfindenden Tagungen ausrichtende Bundesland. Aufgabe des Düsseldorfer Kreises und seiner bestimmten Fachbereichen zugeordneten Arbeitsgruppen ist es, eine – so weit möglich – bundeseinheitliche Behandlung datenschutzrechtlicher Probleme sicherzustellen. Eine weitere Aufgabe ist die Erörterung datenschutzrechtlicher Grundsatzfragen.

1.5. Beschlüsse des Düsseldorfer Kreises

Im Berichtszeitraum hat der Düsseldorfer Kreis sich unter anderem auch mit den beiden aktuellen Themen der Datenübermittlung im SWIFT-Verfahren in die USA sowie der Entwicklung und Anwendung von RFID-Technologie auseinandergesetzt und die beiden nachfolgenden Beschlüsse gefasst:

1.5.1 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2006 in Bremen

SWIFT: Datenübermittlung im SWIFT-Verfahren in die USA

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespei-

cherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zur Zeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US-Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.

(Anmerkung: Außerhalb des Berichtszeitraumes hat SWIFT im Rahmen einer Presseveröffentlichung nun bekannt gegeben, dass den datenschutzrechtlichen Bedenken durch die Verhinderung eines einfachen Zugriffs der US-Behörden auf die internationalen Überweisungsdaten Rechnung getragen werden soll. Dafür sollen zwei Nachrichtenverarbeitungszonen Europa und Transatlantik geschaffen werden, wobei Nachrichten innerhalb einer Zone künftig in ihrer Ursprungsregion verbleiben sollen.)

1.5.2 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2006 in Bremen

Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich:

Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die

RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen – zum Beispiel mit Hilfe von Hintergrundsystemen – später einer konkreten Person zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird – insbesondere wegen der geringen Größe der RFID-Chips – künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz / Benachrichtigungspflicht

Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht

Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung „hinter dem Rücken“ der Betroffenen darf es nicht geben.

Deaktivierung

Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr erforderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit

Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Verschlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung

Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Einwilligung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

2. Videoüberwachung

2.1 Allgemein

Bereits im zweiten Tätigkeitsbericht wurden die Voraussetzungen einer zulässigen Videoüberwachung dargestellt. Auch im Saarland ist seit einiger Zeit ein Anstieg der Eingaben zur Videoüberwachung festzustellen. Viele der nachgenannten Aspekte und Rechtsfragen werden bei Anfragen zur Videoüberwachung privater Stellen immer wieder erörtert und erklärt.

Grundsätzlich geregelt ist die Videoüberwachung in § 6b Bundesdatenschutzgesetz. Danach dürfen private Stellen öffentlich zugängliche Räume dann mit Videokameras überwachen, wenn dies

- zur Wahrnehmung des Hausrechts oder
- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

2.2 Erforderlichkeit der Videoüberwachung

Allein die Tatsache, dass eine Erlaubnisvorschrift existiert, ermöglicht keine ausufernde Überwachung öffentlich zugänglicher Räume mit Videotechnik. Eine solche Auffassung verkennt, dass der Gesetzgeber die Videoüberwachung an bestimmte Voraussetzungen geknüpft hat, die im Einzelfall auch erfüllt sein müssen: Für nicht-öffentliche Stellen gilt, dass die Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein muss. Gerade dieses Kriterium der Erforderlichkeit wird regelmäßig nur unzulänglich erfüllt. Dem Wortlaut nach muss die Video-

überwachung notwendig sein, um einen bestimmten Zweck zu erfüllen. Dies erfordert, auch bei einem weit gefassten Zweck wie Wahrung des Hausrechts, eine Prognose und eine tragfähige, nachvollziehbare Begründung. Der Begriff der Erforderlichkeit leitet sich nämlich ab aus dem hier auch für private Stellen geltenden Verhältnismäßigkeitsgrundsatz. Danach muss vor jedem Eingriff in die Rechtssphäre anderer geprüft werden, ob nicht ein weniger belastendes Mittel ebenso zielführend eingesetzt werden könnte. Die Videoüberwachung ist demnach nur dann erforderlich, wenn die Aufgabe oder der Zweck anders nicht, nicht vollständig, nicht rechtmäßig oder nicht mit vertretbarem Aufwand erreicht werden kann. Dies ist die Grundüberlegung, die vor jedem Einsatz von Videotechnik stehen muss. In diesem Zusammenhang taucht vielfach der Hinweis auf, dass ein verstärkter Einsatz von Wachpersonal vielfach die Videoüberwachung ersetzen könnte. Denkbare Alternativen müssen allerdings auch unter Kostengesichtspunkten zumutbar sein.

Die Überwachung muss – wenn sie nicht ausschließlich der Wahrung des Hausrechts dient – zudem berechtigten Interessen für konkret festgelegte Zwecke dienen. „Berechtigt“ sind alle von der Rechtsordnung anerkannten Interessen, gleich ob sie ideeller, finanzieller, öffentlicher oder privater Natur sind. Die Vorschrift bietet insofern ein recht großes Spektrum denkbarer Voraussetzungen für eine rechtmäßige Videoüberwachung. Das berechtigte Interesse stellt jedoch nur die erste Stufe der sog. „Tatbestandsvoraussetzungen“ dar, da die Zwecke oder der Zweck der Überwachung konkret festgelegt werden müssen. Dies provoziert immer wieder die Frage, ob der Zweck schriftlich fixiert werden sollte. Aus rein pragmatischen Überlegungen heraus ist das zu bejahen, da „Festlegung“ in diesem Zusammenhang bedeutet, dass sie nicht ohne Weiteres geändert werden kann. Letztlich muss aber auch hier auf den Einzelfall abgestellt werden. Bei der Anwendung der Vorschrift wird oft übersehen, dass hier tatsächlich ein konkreter Zweck, also ein ganz bestimmter, tatsächlicher Zweck verfolgt werden muss. Ist dieser Zweck nachhaltig erfüllt, muss sie eingestellt werden.

2.3 Schutzwürdige Interessen Betroffener

Soweit Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen Betroffener an einer Unterlassung der Videoüberwachung überwiegen, ist diese nicht gestattet. Bei der Prüfung eines solchen möglicherweise bestehenden schutzwürdigen Interesses ist stets das grundrechtlich garantierte Persönlichkeitsrecht, insbesondere das Recht auf Schutz der Privat- und Intimsphäre, zu beachten. So wäre beispielsweise die Überwachung von Umkleidekabinen oder Sanitäranlagen von vornherein ausgeschlossen.

2.4 Anwendbarkeit der Vorschrift

Hierbei ist zu beachten, dass § 6b Bundesdatenschutzgesetz nur die Erfassung öffentlich zugänglicher Räume regelt. Hierunter fallen beispielsweise

- Kaufhäuser,
- Ladenpassagen,
- Tankstellen,
- Räumlichkeiten einer Bank,
- Fitness-Center,
- Videotheken,
- Museen usw.

Die Vorschrift ist jedoch nicht anwendbar, wenn – was häufiger vorkommt – der private Betreiber zum Beispiel

- lediglich sein eigenes Grundstück oder
- Nachbargrundstücke (teilweise) videografiert,

da in beiden Fällen kein öffentlicher Raum erfasst wird. In letzterem Fall hat der betroffene Nachbar jedoch unter Umständen zivilrechtliche

Unterlassungsansprüche nach den §§ 823, 1004 BGB wegen Verletzung seines allgemeinen Persönlichkeitsrechts.

2.5 Abgrenzung des öffentlichen vom privaten Bereich

Nicht erfasst von der gesetzlichen Regelung im Bundesdatenschutzgesetz sind öffentliche Wege, Straßen und Plätze, die nach erfolgter Widmung aufgrund eines öffentlich rechtlichen Rechtsaktes allein dieser Sphäre zuzuordnen und als solche der Verfügung privater Stellen weitestgehend entzogen sind. Diese Bereiche dürfen daher nicht von Privaten, sondern nur von öffentlichen Stellen nach Maßgabe der jeweiligen Landesdatenschutz- und Landespolizeigesetze überwacht werden. Zwischenzeitlich wurde im Saarländischen Datenschutzgesetz eine Befugnis für öffentliche Stellen eingeführt, unter bestimmten Voraussetzungen videografieren zu können.

Problematisch kann sich die Abgrenzung des öffentlichen vom privaten Bereich beispielsweise auch in Ladenpassagen oder vor Kaufhäusern gestalten. Das Amtsgericht Berlin Mitte hat mit einem Urteil vom Dezember 2003 in diesem Punkt insoweit für mehr Klarheit gesorgt, als es befand, dass eine dem Grunde nach zulässige Überwachung der Außenfassade einen Randstreifen von einem Meter Breite ab Hauswand umfassen dürfe. In diesem Bereich sei – so das Amtsgericht – die Überwachung zulässig und hinzunehmen, was im Umkehrschluss bedeutet, dass eine breitflächig angelegte Überwachung öffentlicher Wegeflächen durch Private nicht zulässig ist.

2.6 Speicherung der Daten

Gespeichert (= aufgezeichnet) werden dürfen die erhobenen Daten nur dann, wenn der beabsichtigte Zweck ansonsten nicht verfolgt werden kann. Dies wird regelmäßig dann der Fall sein, wenn es darum geht,

Videotechnik zur Beweissicherung oder zur Täteridentifikation einzusetzen.

Die „klassische“ Verarbeitung personenbezogener Daten bezieht sich in aller Regel auf bestimmte bzw. bestimmbare natürliche Personen, deren Angaben zweckgebunden erhoben, verarbeitet und/oder genutzt werden. Ansatzpunkt ist jedenfalls das Interesse an bestimmten Angaben über einen bestimmten oder bestimmbaren Menschen in einer konkreten Situation.

Gerade dies ist bei der Videoüberwachung nicht der Fall. Gegenstand des Einsatzes von Überwachungstechnik ist üblicherweise nicht der Mensch, sondern der Raum, der überwacht werden soll. Bei der reinen Beobachtung verhindert allein schon die Flüchtigkeit des Augenblicks eine „Erhebung“ personenbezogener Daten. Dieser Vorgang ist bei der Videoüberwachung von der Speicherung in Form der Aufzeichnung von Bildern nicht zu trennen. Auch dann fehlt es immer noch an dem bestimmenden Merkmal der althergebrachten Datenverarbeitung: Genau genommen wird ein Bild erst dann zu einem personenbezogenen Datum, wenn ein solcher Bezug tatsächlich existiert oder zumindest mit vertretbarem Aufwand hergestellt werden kann.

In der Praxis erfolgt die Aufzeichnung meist auf einem sich nach einer bestimmten Zeit selbst überschreibenden Ringspeicher.

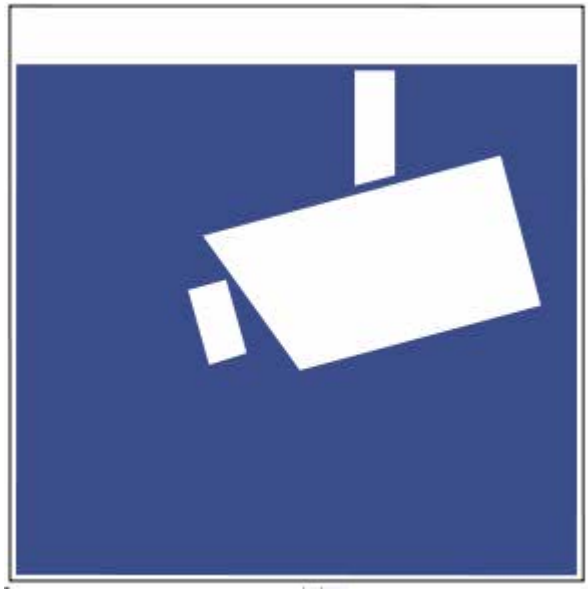
2.7 Benachrichtigung der Betroffenen

Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung zu benachrichtigen. Wie dargestellt, existiert ein solcher Bezug jedoch oftmals nicht.

So ist z. B. bei webcams die Qualität oft nicht ausreichend, einen solchen Personenbezug herzustellen.

2.8 Hinweispflicht

Nach § 6b Absatz 2 BDSG sind sowohl der Umstand der Beobachtung als auch die verantwortliche Stelle durch geeignete Maßnahmen kenntlich zu machen. Zur genauen Ausgestaltung dieses Hinweises äußert sich der Wortlaut des Gesetzes nicht. Einigkeit besteht darüber, dass der Hinweis deutlich und groß genug sein muss, damit potentiell Betroffene den Umstand der Überwachung rechtzeitig erkennen können. Das deutsche Institut für Normung e. V. hat unter der DIN 33450 zwischenzeitlich ein entsprechendes graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen) erstellt.



(Hinweisschild nach DIN 33450)

2.9 Videoüberwachung am Arbeitsplatz

Grundsätzlich gilt das allgemeine Datenschutzrecht auch im Arbeitsverhältnis. Da § 6b des Bundesdatenschutzgesetzes jedoch nur die Videoüberwachung öffentlich zugänglicher Räume regelt, muss im Arbeitsverhältnis differenziert werden: Wird die Arbeitsleistung in einem öffentlich zugänglichen Raum (Ladenlokal o.ä.) erbracht, so ist die Videoüberwachung unter den Voraussetzungen des § 6b zulässig. Ist Publikumsverkehr ausgeschlossen, richtet sich die Rechtmäßigkeit entweder nach § 28 des Bundesdatenschutzgesetzes oder dem Allgemeinen Persönlichkeitsrecht. Im Ergebnis ist in beiden Fallkonstellationen (öffentlich zugängliche/unzugängliche Räume) die Videobeobachtung von Arbeitnehmerinnen und Arbeitnehmern nur unter engen Voraussetzungen zulässig:

- Grundsätzlich muss auch die Überwachung von Arbeitnehmern offen erfolgen.

- Der Schutz des Arbeitgebers vor Verlust von Firmeneigentum durch Diebstahl oder Unterschlagung ist als schutzwürdiges Interesse anerkannt. Vor Betreiben einer Videoüberwachung müssen jedoch Anhaltspunkte und/oder Verdachtsmomente vorliegen, die diesen Eingriff in die Rechte der Betroffenen rechtfertigen.

- Die verdeckte Überwachung ist nur zulässig, wenn sie das letzte verbleibende Mittel darstellt, um einen konkreten objektiven Verdacht einer Straftat oder eines anderen schweren Vergehens aufzuklären.

- Nach der Rechtsprechung des Bundesarbeitsgerichts unterfällt die Einführung einer Videoüberwachung am Arbeitsplatz dem Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz. Die Betriebsparteien haben dabei das grundrechtlich geschützte allgemeine Persönlichkeitsrecht der Arbeit-

nehmer zu beachten. Für die erforderliche Verhältnismäßigkeitsprüfung sind die Gesamtumstände maßgeblich. Mitentscheidend ist insbesondere die Intensität des Eingriffs.

2.10 Aufsichtsbehördliche Überprüfungen

Der Großteil der eingegangenen Eingaben bezog sich auf Videokamerainstallationen an Privathäusern, die der Überwachung des eigenen Grundstücks dienten. Die Petenten fürchteten dabei, selbst von der Überwachung betroffen zu sein. Begründet wurden die Kamerainstallationen von den verantwortlichen Stellen in der Regel mit bereits vorgefallenen Einbrüchen oder Vandalismus. In verschiedenen Fällen war das BDSG nicht anwendbar, da kein öffentlicher Raum erfasst wurde (siehe oben). Die Aufsichtsbehörde verweist diese Petenten in solchen Fällen meistens auf den Zivilrechtsweg.

Trotzdem wird es von Zeit zu Zeit von den Betroffenen gewünscht, dass auch in solchen Fällen die Aufsichtsbehörde ihre Einschätzung abgibt und vermittelnd tätig wird.

So hatten sich in einem hier vorliegenden Fall zwei Nachbarn darauf verständigt, die Aufsichtsbehörde zu einer Begutachtung einer Videokamerainstallation zu bitten, da sich beide unsicher waren, ob hier nicht der zulässige Rahmen überschritten sein könnte. Eine Zuständigkeit der Aufsichtsbehörde konnte auch nicht von vorneherein ausgeschlossen werden, da die Parteien angaben, dass ein im Hintergrund verlaufender öffentlicher Weg teilweise miterfasst würde. Zumindest diese Erfassung des öffentlichen Weges konnte die Aufsichtsbehörde bei einer Vor-Ort-Besichtigung ausschließen. Aufgrund der Entfernung und der Kameraeinstellung wäre auch keine Personenerkennbarkeit gegeben gewesen. Was die Erfassung des nachbarlichen Bereiches betrifft, so konnte die Aufsichtsbehörde vermitteln und darauf hinwir-

ken, dass die Einstellung der Kamera soweit verändert wurde, dass das Bild an der Grenze des Nachbarn abgeschnitten wird.

In anderen Fällen konnte seitens der Aufsichtsbehörde darauf hingewirkt werden, dass den gesetzlichen Bestimmungen – beispielsweise durch Anbringen eines Hinweises oder durch Verändern des Erfassungswinkels – Rechnung getragen wurde.

3. Pflichten datenverarbeitender Stellen

Mit der Änderung des Bundesdatenschutzgesetzes vom 22. August 2006 wurden insbesondere die Schwellenwerte hinsichtlich der Meldepflicht nach § 4d BDSG und der Pflicht, einen betrieblichen Datenschutzbeauftragten nach § 4f BDSG zu bestellen, angehoben.

An die Aufsichtsbehörde für den Datenschutz wird von Unternehmen immer wieder die Frage herangetragen, ob sie einen Datenschutzbeauftragten zu bestellen haben oder ob eine Meldepflicht besteht.

Daher werden im Folgenden noch einmal die generellen Voraussetzungen dieser Vorschriften erläutert.

3.1 Meldepflicht

Grundsätzlich unterliegen zwar alle Verfahren automatisierter Verarbeitungen der Meldepflicht gegenüber der Aufsichtsbehörde. Durch die im Gesetz festgeschriebenen Ausnahmen besteht diese Pflicht jedoch im Ergebnis tatsächlich für die wenigsten Stellen.
Danach entfällt die Meldepflicht, wenn

- die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt,
- hierbei höchstens neun Personen 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.

Die Meldepflicht entfällt außerdem, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

3.2 Bestellung eines betrieblichen Datenschutzbeauftragten

Auch bei der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten gilt der Schwellenwert von neun Personen. Etwas anderes gilt für Unternehmen, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung (Auskunfteien, Adresshändler) oder zum Zweck der anonymisierten Übermittlung speichern (Markt- und Meinungsforschungs-, Sozialforschungs- oder Konsumforschungsinstitute etc.). Diese müssen unabhängig von der Anzahl der Beschäftigten nach § 4f Abs. 1 S. 6 BDSG einen betrieblichen Datenschutzbeauftragten bestellen.

Weiter muss ein betrieblicher Datenschutzbeauftragter bestellt werden, wenn eine sog. „Vorabkontrolle“ durchgeführt werden muss. Eine solche muss nach § 4d Abs. 5 Satz 2 BDSG dann erfolgen, wenn

- besondere Arten personenbezogener Daten verarbeitet werden, oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit der Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,
- es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung der Betroffenen vorliegt oder
- die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Verhältnisses mit den Betroffenen dient.

Der einschränkende Halbsatz hat zur Folge, dass in einer Vielzahl von Fällen keine Vorabkontrolle erfolgen muss, obwohl besondere Arten personenbezogener Daten verarbeitet werden. Bei dieser Konstellation entfällt folglich auch die Verpflichtung, betriebliche Datenschutzbeauftragte zu ernennen. Ärztinnen und Ärzte beispielsweise, wie Angehörige anderer Heilberufe auch, die Gesundheitsdaten auf Grund des Behandlungsvertrags erheben, verarbeiten oder nutzen, müssen erst dann betriebliche Datenschutzbeauftragte bestellen, wenn sie mehr als

neun Personen mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen.

Im Berichtszeitraum hat die Aufsichtsbehörde einen Vortrag vor einem datenschutzrechtlichen Arbeitskreis gehalten, der auch diese Fragen zum Thema hatte.

4. Versicherungen

4.1 Löschung von Daten bei einem nicht zustande gekommenem Vertrag

Im Berichtszeitraum gingen verschiedene Anfragen Betroffener ein, die bei einer Versicherung einen Antrag auf einen Vertrag gestellt hatten, der letztlich aus unterschiedlichen Gründen nicht zustande kam. Häufig fällt den Betroffenen im Zusammenhang mit der Rückforderung eingereichter Unterlagen auf, dass die Versicherung die Daten speichert. Die Betroffenen verlangen dann von der Versicherung eine Bestätigung, dass ihre personenbezogenen Daten gelöscht wurden.

Zwar sind Daten grundsätzlich zu löschen, wenn sie nicht mehr erforderlich sind. Dem Löschungsanspruch stehen hier jedoch gesetzliche Aufbewahrungspflichten gegenüber. Die Rechtsgrundlagen für die Aufbewahrung von Antragsunterlagen sind in § 257 Abs. 1 Nr. 2 Handelsgesetzbuch i. V. m. Absatz 4 der Vorschrift sowie in § 147 Abs. 1 Nr. 2 Abgabenordnung i. V. m. Absatz 3 zu sehen. Danach sind empfangene Handelsbriefe für die Dauer von 6 Jahren aufzubewahren. Diese gesetzlich vorgeschriebene Aufbewahrung der Unterlagen dient der Dokumentation und erlaubt Nachprüfungen, Beweissicherungen und Beweisführungen. Die genannten Vorschriften gehen – deklaratorisch bestätigt durch § 35 Abs. 3 Nr. 1 Bundesdatenschutzgesetz – der Regelung des § 35 Abs. 2 Nr. 3 Bundesdatenschutzgesetz vor, wonach personenbezogene Daten zu löschen sind, wenn sie nicht mehr benötigt werden. Diese Unterlagen werden auch von den Aufsichtsbehörden für den Datenschutz als Handelsbriefe qualifiziert.

Die Aufbewahrungsfristen wurden der AG Versicherungswirtschaft des „Düsseldorfer Kreises“ zuletzt im Januar 2005 seitens des Gesamtverbandes der Deutschen Versicherungswirtschaft bestätigt und von der Datenschutzseite anerkannt.

Im Einzelnen betragen die Aufbewahrungsfristen für Abrechnungsunterlagen 10 Jahre, für Geschäftsbriefe, Schriftwechsel, Versicherungspolicen und Verträge jeweils 6 Jahre.

Eine Löschung wäre daher sogar unzulässig. In Frage kommt statt dieser Löschung eine Sperrung der Daten gemäß § 35 Abs. 3 Nr. 1 Bundesdatenschutzgesetz. Die Versicherung bleibt dabei verpflichtet, sämtliche Unterlagen zwecks externen Kontrollen vorzuhalten. Wegen der Sperrung dürfen die Daten aber nur für diese eingeschränkten Zwecke verwandt werden. Nach Ablauf der Aufbewahrungsfrist müssen sie gelöscht werden.

4.2 Schweigepflichtentbindungserklärung

Ein Betroffener stellte einen Antrag auf Abschluss eines Versicherungsvertrages und sollte in diesem Zusammenhang mittels einer Schweigepflichtentbindungserklärung Ärzten, Krankenhäusern, sonstige Krankenanstalten, Pflegeheimen usw. erlauben, dem Versicherungsunternehmen auf Verlangen Auskunft zu geben. Er wandte sich darauf hin an die Aufsichtsbehörde, mit der Bitte, ihm mitzuteilen, ob er dies so hinnehmen müsse. Die Aufsichtsbehörden kritisieren diese pauschale Einwilligung schon seit längerem, und vertreten die Auffassung, dass jedenfalls mit der Novellierung des Bundesdatenschutzgesetzes die verwandte Schweigepflichtentbindungserklärung nicht mehr den gesetzlichen Anforderungen an eine wirksame Einwilligungserklärung entspricht.

Hierzu hat das Bundesverfassungsgericht mit Beschluss vom 23. Oktober 2006 (1 BvR 2027/02) nun festgestellt, dass wegen der in der Regel sehr weiten Fassung der Erklärungen für die Betroffenen praktisch nicht absehbar sei, welche Auskünfte über sie von wem eingeholt werden können. Zu dem beim Bundesverfassungsgericht konkret vorliegenden Fall führte dieses weiter aus, dass der Versicherungsnehmer

auch nicht auf die Möglichkeit verwiesen werden könne, um des informationellen Selbstschutzes willen einen Vertragsschluss zu unterlassen. Trotzdem bleibt festzuhalten, dass es für die Versicherungsunternehmen von großer Bedeutung ist, den Eintritt des Versicherungsfalles überprüfen zu können. Der Versicherungsnehmer bleibt zur Mitwirkung verpflichtet. Es muss aber geprüft werden, ob nicht andere Vorgehensweisen als eine pauschale Erklärung in Betracht kommen. So könnte das Versicherungsunternehmen im Zusammenhang mit der Mitteilung, welche Informationserhebungen beabsichtigt sind, dem Versicherten die Möglichkeit zur Beschaffung der Informationen oder jedenfalls eine Widerspruchsmöglichkeit einräumen. Laut Gericht wäre es auch unbedenklich, den Versicherten die Kosten tragen zu lassen, die durch einen besonderen Aufwand bei der Bearbeitung des Leistungsantrags entstehen. Die damit verbundenen Kosten dürfen aber nicht so hoch sein, dass sie einen informationellen Selbstschutz unzumutbar machen.

(Anmerkung: Die Aufsichtsbehörden verhandeln zum Zeitpunkt der Vorlage dieses Berichts noch mit der Versicherungswirtschaft mit dem Ziel einer neuen Schweigepflichtentbindungserklärung, die den datenschutzrechtlichen Anforderungen Rechnung trägt.)

5. Auskunfteien

Die Tätigkeit von Auskunfteien ist unter den im Bundesdatenschutzgesetz allgemein genannten Voraussetzungen zulässig. Um die Rechte der Betroffenen zu schützen, haben die Auskunfteien bestimmte Pflichten, z. B. sind Betroffene zu informieren, wenn zum ersten mal eine Auskunft über sie erteilt wurde:

5.1 Benachrichtigungspflicht

Regelmäßig, meist veranlasst durch das Informationsschreiben der Auskunftei, wird an die Aufsichtsbehörde die Frage herangetragen, was es mit einer erhaltenen Benachrichtigung über die erstmalige Übermittlung von Daten auf sich hat.

Auskunfteien speichern personenbezogene Daten, um diese auf Anfrage zu übermitteln. Von der erstmaligen Übermittlung ist der Betroffene nach § 33 Abs. 1 Satz 2 Bundesdatenschutzgesetz zu benachrichtigen.

Nachdem in einem Fall ein Betroffener eine solche Benachrichtigung seitens einer Auskunftei erhalten hatte, fragte er dort nach, wer diese Daten erhalten habe. Die Auskunftei verwehrte ihm die Beantwortung dieser Frage mit dem simplen Hinweis darauf, dass Auskunftsempfänger nicht bekannt gegeben würden. Der Betroffene wandte sich daraufhin an die Aufsichtsbehörde mit der Bitte, dieser Frage nachzugehen.

Grundsätzlich haben Betroffene nach § 34 Abs. 1 Bundesdatenschutzgesetz durchaus einen Anspruch darauf, erfahren zu können, wer ihre Daten erhalten hat. Dies gilt allerdings nur unter der Einschränkung eines möglicherweise überwiegenden Geschäftsgeheimnisses.

Die Auskunftei darf aber aufgrund dieser Vorschrift die Auskunft über Datenempfänger nicht pauschal verweigern. Sie hat vielmehr eine Abwägung der verschiedenen Interessen im Einzelfall vorzunehmen und muss eine Ablehnung des Auskunftsersuchens begründen können.

Die Aufsichtsbehörde für den Datenschutz vertritt in diesem Zusammenhang die Auffassung, dass bei Datenübermittlungen an Unternehmen folgender Branchen stets die Auskunftsempfänger bekannt zu geben sind:

- Banken,
- Factoringgesellschaften,
- konzernangehörige Gesellschaften,
- Leasinggesellschaften,
- Telekommunikationsunternehmen,
- Versicherungen und
- Versandhandel.

Diese Liste basiert auf einem Vorschlag des Verbandes der Handelsauskunfteien (VdH), der von den Aufsichtsbehörden für den Datenschutz angenommen wurde.

Die Aufsichtsbehörde hat die Auskunftei aufgefordert, ihr Verfahren den geltenden Vorschriften anzupassen. Die Auskunftei hat der Aufsichtsbehörde gegenüber dies bestätigt.

5.2 Unternehmensauskünfte

Ein Firmeninhaber hatte von einer Auskunftei einen Auszug aus dem Datenbestand zu seiner Firma und einen Fragebogen erhalten, in welchem er um Auskünfte zu seiner Firma gebeten wurde. Er wandte sich daraufhin an die Aufsichtsbehörde mit der Bitte, zu überprüfen, ob solche Schreiben rechtmäßig seien. Er bemängelte besonders, dass nicht

über die beabsichtigte Datenspeicherung informiert würde und dass die Freiwilligkeit der Angaben nicht deutlich genug gemacht werde. Außerdem träfen die Angaben in dem Auszug nicht zu.

Zu der bemängelten fehlenden Information über die Datenspeicherung ist zu sagen, dass eine Information des Betroffenen bei der Datenspeicherung grundsätzlich nicht erfolgen muss. Erst bei der erstmaligen Abfrage z. B. eines Geschäftspartners erhält der Betroffene eine Benachrichtigung über das Auskunftsersuchen gemäß § 33 Abs. 1 S. 2 Bundesdatenschutzgesetz. In diesem Zusammenhang ist allerdings auch zu beachten, dass die (Schutz-)Vorschriften des Bundesdatenschutzgesetzes nur für personenbezogene Daten und nicht für Firmendaten gelten.

Zu der weiter bezweifelten Freiwilligkeit der Angaben führte die verantwortliche Stelle aus, dass in dem der Auskunft beigefügten Begleitschreiben vermerkt sei, dass die Übermittlung weiterer eigener Angaben nicht verpflichtend sei, sondern auf freiwilliger Basis erfolge.

Es handelte sich bei dem Fragebogen außerdem um Schätzwerte. Angesichts des anerkennenswerten Interesses der Wirtschaft, sich bei Geschäften mit Vorleistungen abzusichern, gibt es gegen die Verwendung solcher Schätzdaten keine datenschutzrechtlichen Bedenken. Überdies betreffen sie den Schutzbereich des Bundesdatenschutzgesetzes wie oben dargelegt nur sehr am Rande. Durch den Hinweis auf die Verwendung der Schätzdaten und die damit verbundene Möglichkeit des Betroffenen, sich durch Bekanntgabe richtiger Daten in der Einschätzung nach außen möglicherweise zu "verbessern", genügt die verantwortliche Stelle den datenschutzrechtlichen Anforderungen.

Die Freiwilligkeit der Auskunft wird auch mittelbar durch diesen Hinweis auf die gespeicherten Schätzdaten deutlich. In diesem Zusammenhang ist zu bedenken, dass es sich um Unternehmensauskünfte handelt und den davon in ihren geschäftlichen Angelegenheiten Betrof-

fenen im Allgemeinen durch ihre Geschäftserfahrung erkennbar ist, dass keine Verpflichtung zu den Angaben besteht. Ein ausdrücklicher Hinweis auf die Freiwilligkeit der Angaben wäre zwar wünschenswert, kann aber, da es sich nicht um personenbezogene Daten handelt, nicht verlangt werden.

6. Banken

Eine Bankkundin wandte sich an die Aufsichtsbehörde mit der Frage, ob es Banken erlaubt sei, Personalausweiskopien zu fertigen. Die Bank berief sich dabei auf Identifizierungspflichten nach dem Geldwäschegesetz.

Dieser Darstellung des Bankinstitutes war im Ergebnis zuzustimmen. Tatsächlich obliegen Banken Identifizierungspflichten sowohl nach der Abgabenordnung als auch nach dem Geldwäschegesetz.

So sind die Banken nach der Abgabenordnung verpflichtet, sich Gewissheit über die Person und Anschrift des Verfügungsberechtigten zu verschaffen und die entsprechenden Angaben in geeigneter Form festzuhalten.

Nach dem Geldwäschegesetz haben die Institute bei Abschluss eines Vertrages zur Begründung einer auf Dauer angelegten Geschäftsbeziehung oder bei geldwäscherelevanten Handlungen den Vertragspartner zu identifizieren.

Diese Identifizierungspflicht umfasst Name, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift, sowie Art, Nummer und ausstellende Behörde des amtlichen Ausweises. Die Feststellungen sind durch Aufzeichnung der Angaben oder durch Anfertigung einer Kopie der Seiten der zur Feststellung der Identität vorgelegten Ausweises, die diese Angaben enthalten, aufzuzeichnen.

Das Anfertigen einer Ausweiskopie ist also nach dem Wortlaut des Gesetzes durchaus vorgesehen und zulässig, so dass ein Verstoß gegen das Bundesdatenschutzgesetz nicht vorlag.

Bundesdatenschutzgesetz

- Auszug -

(zuletzt geändert am 22. August 2006)

§ 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 aufgrund 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.

§ 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 und die Informationsfreiheit 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 neun Personen 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 und die Informationsfreiheit 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 verarbeiten, 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 die nichtöffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung 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 automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen 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. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. 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 Gesetzbuches, 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.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(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 kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. 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. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(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 nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 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 den §§ 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.

§ 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 Geschäftsbezeichnung,
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 für 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 Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von
Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, 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 Zweck der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck 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 zugrunde 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.

§ 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 Zweck 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 Fall 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 Zweck 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 Zwecks 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 Fall 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 Zweck 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.

§ 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. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. 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 Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

Adressen der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und der Landesbeauftragten für den Datenschutz

Bundesland	**Oberste Aufsichtsbehörde**	**Regional zuständige Aufsichtsbehörde**	**Landesbeauftragte/r für Datenschutz**
Baden-Württemberg	Innenministerium Baden-Württemberg Dorotheenstraße 6 70173 Stuttgart 07 11 / 231 – 32 50 Fax: 23 1 – 32 99 datenschutz@im.bwl.de		Der Landesbeauftragte für den Datenschutz in Baden-Württemberg Urbanstraße 32 70178 Stuttgart 07 11 / 61 55 41 – 0 Fax: 61 55 41 – 15 poststelle@lfd.bwl.de
Bayern	Bayerisches Staatsministerium des Inneren Odeonsplatz 3 80539 München 0 89 / 21 92 – 01 Fax: 21 92 – 1 22 66 datenschutz@stmi.bayern.de	Regierung von Mittelfranken Promenade 27 (Schloss) 91522 Ansbach 09 81 / 53-0 Fax: 09 81 / 53-5301 datenschutz@reg-mfr.bayern.de	Der Bayerische Landesbeauftragte für den Datenschutz Wagmüllerstraße 18 80538 München 0 89 / 21 26 72 – 0 Fax 21 26 72 – 50 poststelle@datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4 – 10 10787 Berlin 0 30 / 1 38 89 - 0 Fax: 2 15 - 50 50 mailbox@datenschutz-berlin.de		Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4 – 10 10787 Berlin 0 30 / 1 38 89 - 0 Fax: 2 15 - 50 50 mailbox@datenschutz-berlin.de
Brandenburg	Innenministerium des Landes Brandenburg Henning-von-Tresckow-Straße 9-13 14467 Potsdam 03 31 / 8 66 - 0 Fax: 03 31 / 8 66 – 22 02 poststelle@mi.brandenburg.de		Der Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht Brandenburg Stahnsdorfer Damm 77 14532 Kleinmachnow 03 32 03 / 3 56 – 0 Fax:3 56 – 49 poststelle@lda.brandenburg.de
Bremen	Landesbeauftragter für den Datenschutz Arndtstr. 1 27570 Bremerhaven 04 71 / 9 24 61-0 Fax: 9 24 61-31 office@datenschutz.bremen.de		Landesbeauftragter für den Datenschutz Arndtstr. 1 27570 Bremerhaven 04 71 – 9 24 61-0 Fax: 9 24 61-31 office@datenschutz.bremen.de

Bundesland	**Oberste Aufsichtsbehörde**	**Regional zuständige Aufsichtsbehörde**	**Landesbeauftragte/r für Datenschutz**
Hamburg	Der Hamburgische Datenschutzbeauftragte Klosterwall 6, Block C 20095 Hamburg 0 40 / 4 28 54 – 4040 Fax: -4000 mail-box@datenschutz.hamburg.de		Der Hamburgische Datenschutzbeauftragte Klosterwall 6, Block C 20095 Hamburg 0 40 / 4 28 54 – 4040 Fax: -4000 mail-box@datenschutz.hamburg.de
Hessen	Hessisches Ministerium des Innern und für Sport Friedrich-Ebert-Allee 12 65185 Wiesbaden 06 11 / 3 53 – 0 Fax: 06 11 / 353 – 13 02	Regierungspräsidium Darmstadt Luisenplatz 2 64278 Darmstadt 0 61 51 / 12 – 0 Fax: 12 – 5794 datenschutz@rpda.hessen.de	Der Hessische Datenschutzbeauftragte Uhlandstr. 4 65189 Wiesbaden 06 11 / 14 08 – 0 Fax: 06 11 / 14 08 – 900 poststelle@datenschutz.hessen.de
Mecklenburg-Vorpommern	Innenministerium Mecklenburg-Vorpommern Arsenal am Pfaffenteich Karl-Marx-Straße 1 19048 Schwerin 0385/588-0 Fax: 588-2978 II2Vz@im.mv-regierung.de		Der Landesbeauftragte für Datenschutz Mecklenburg-Vorpommern Schloß Schwerin Johannes-Stelling-Straße 21, 19053 Schwerin 03 85 / 5 94 94 – 0 Fax- 58 datenschutz@mvnet.de
Niedersachsen	Niedersächsisches Innenministerium Lavesallee 6 30169 Hannover 05 11 / 1 20 – 0 datenschutz@mi.niedersachsen.de	Der Landesbeauftragte für den Datenschutz Brühlstraße 9 30169 Hannover 05 11 / 1 20 – 45 00 Fax: 1 20 – 45 99 poststelle@lfd.niedersachsen.de	Der Landesbeauftragte für den Datenschutz Brühlstraße 9 30169 Hannover 05 11 / 1 20 – 45 00 Fax: 1 20 – 45 99 poststelle@lfd.niedersachsen.de
Nordrhein-Westfalen	Innenministerium des Landes Nordrhein-Westfalen Haroldstraße 5 40213 Düsseldorf 02 11 / 8 71 – 01 Fax: 8 71 – 33 55 poststelle@im.nrw.de	Die Landesbeauftragte für Datenschutz und Informationsfreiheit Kavalleriestraße 2-4 40213 Düsseldorf 02 11 / 3 84 24 – 0 Fax: 3 84 24 – 10 poststelle@ldi.nrw.de	Die Landesbeauftragte für Datenschutz und Informationsfreiheit Kavalleriestraße 2-4 40213 Düsseldorf 02 11 / 3 84 24 – 0 Fax: 3 84 24 – 10 poststelle@ldi.nrw.de

Bundesland	**Oberste Aufsichtsbehörde**	**Regional zuständige Aufsichtsbehörde**	**Landesbeauftragte/r für Datenschutz**
Rheinland-Pfalz	Ministerium des Innern und für Sport Schillerstraße 3 – 5 55116 Mainz 0 61 31 / 16 – 0 Fax: 16-33 69	Aufsichts- und Dienstleistungsdirektion Trier Willy-Brandt-Platz 3 54290 Trier 06 51 – 94 94 – 0 Fax: 9 4 94 – 1 70 poststelle@add.rlp.de	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Deutschhausplatz 12 55116 Mainz 0 61 31 / 2 08-24 49 Fax: 2 08-24 97 poststelle@datenschutz.rlp.de
Saarland	Ministerium für Inneres und Sport Franz-Josef-Röder-Straße 21 66119 Saarbrücken 06 81 / 5 01 – 00 06 81 / 9 62 – 16 34 Fax: 9 62 – 16 05 datenschutz@innen.saarland.de		Landesbeauftragter für Datenschutz und Informationsfreiheit Fritz-Dobisch-Straße 12 66111 Saarbrücken 06 81 / 9 47 81 – 0 Fax: 9 47 81 – 29 poststelle@lfdi.saarland.de
Sachsen	Sächsisches Staatsministerium des Innern Wilhelm-Buck-Straße 2 01097 Dresden 03 51 / 5 64 – 0 Fax: 5 64 – 31 99 datenschutz@smi.sachsen.de	Der sächsische Datenschutzbeauftragte Bernhard-von-Lindenau-Platz 1 01067 Dresden 03 51 / 49 35 – 4 01 Fax: 03 51 – 49 35-4 90 saechsdsb@lst.sachsen.de	Der sächsische Datenschutzbeauftragte Bernhard-von-Lindenau-Platz 1 01067 Dresden 03 51 / 49 35 – 4 01 Fax: 03 51 – 49 35-4 90 saechsdsb@lst.sachsen.de
Sachsen-Anhalt	Ministerium des Landes Sachsen-Anhalt Halberstädter Straße 2 39112 Magdeburg 03 91 / 5 67 – 01 Fax: 5 67 – 54 53/ 52 90	Landesverwaltungsamt Willy-Lohmann-Straße 7 06114 Halle 03 45 / 5 14 – 0 Fax: 5 14 -1 444	Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt Berliner Chaussee 9 39114 Magdeburg 03 91 - 8 18 03 – 0 Fax: 03 91 / 8 18 03-33
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel 04 31 / 9 88 – 12 00 Fax: 9 88 – 12 23 mail@datenschutzzentrum.de		Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel 04 31 / 9 88 – 12 00 Fax: 9 88 – 12 23 mail@datenschutzzentrum.de

Bundes-land	**Oberste Aufsichtsbehörde**	**Regional zuständige Aufsichtsbehörde**	**Landesbeauftragte/r für Datenschutz**
Thüringen	Innenministerium des Landes Thüringen Steigerstraße 24 99096 Erfurt 03 61 / 3 79 – 00 Fax: 3 79 – 34 49	Thüringer Landesverwaltungsamt Weimarplatz 4 99423 Weimar 0 361 / 37 70 –0 Fax: 0 361/ 37 73 71 90	Der Thüringer Landesbeauftragte für den Datenschutz Jürgen-Fuchs-Straße 1 99096 Erfurt 03 61 / 3 77 - 19 00 03 61 / 3 77 - 19 04

Bundesbeauftragter für Datenschutz und Informationsfreiheit	Der Bundesbeauftragte für den Datenschutz Husarenstraße 30 53117 Bonn 01888 / 7799 – 0 Fax: -550

Links[1]

Aufsichtsbehörden und Landesbeauftragte

Saarland:
http://www.innen.saarland.de

Baden-Württemberg:
http://www.innenministerium.baden-wuerttemberg.de

Bayern:
http://www.innenministerium.bayern.de
http://www.regierung.mittelfranken.bayern.de

Berlin:
http://www.datenschutz-berlin.de

Brandenburg:
http://www.mi.brandenburg.de

Bremen:
http://www.datenschutz.bremen.de

Hamburg:
http://www.datenschutz-hamburg.de

Hessen:
http://www.hmdi.hessen.de
http://www.rp-darmstadt.hessen.de

Mecklenburg-Vorpommern:
http://www.datenschutz.mvnet.de

Niedersachsen:
http://www.mi.niedersachsen.de
http://www.lfd.niedersachsen.de

Nordrhein-Westfalen:
http://www.ldi.nrw.de

Rheinland-Pfalz:
http://www.ism.rlp.de
http://www.add.rlp.de

[1] Die Links verweisen mit Ausnahme desjenigen zum Angebot des Ministerium für Inneres und Sport auf externe Angebote, für deren Inhalt keine Haftung übernommen wird. Die Liste erhebt auch keinen Anspruch auf Vollständigkeit, ebenso wenig wie sie als Ausdruck einer Präferenz der Aufsichtsbehörde für den Datenschutz verstanden werden darf.

Sachsen:
http://www.sachsen.de/de/bf/staatsregierung/ministerien/smi/
http://www.datenschutz.sachsen.de

Sachsen-Anhalt:
http://www.mi.sachsen-anhalt.de
http://www.landesverwaltungsamt.sachsen-anhalt.de

Schleswig-Holstein:
http://www.datenschutzzentrum.de

Thüringen:
http://www.thueringen.de/de/tim
http://www.thueringen.de/de/tlvwa/

Landesbeauftragte für Datenschutz/Bundesbeauftragter für Datenschutz (soweit nicht bereits oben aufgeführt):

Bundesbeauftragter für den Datenschutz:
http://www.bfdi.bund.de

Landesbeauftragter für Datenschutz und Informationsfreiheit des Saarlands:
http://www.lfdi.saarland.de

Der Hessische Datenschutzbeauftragte:
http://www.datenschutz.hessen.de

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz:
http://www.datenschutz.rlp.de

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt:
http://www.datenschutz.sachsen-anhalt.de

Der Thüringer Landesbeauftragte für den Datenschutz:
http://www.datenschutz.thueringen.de

Sonstige Behörden:

Bundesamt für Sicherheit in der Informationstechnik:
http://www.bsi.de
http://www.bsi-fuer-buerger.de - „Ins Internet – mit Sicherheit“, ein Angebot des BSI nicht nur für Bürger/innen im statusrechtlichen Sinn

Bundesamt für Finanzdienstleistungsaufsicht:
http://www.bafin.de

Datenschutzseite der EU - deutschsprachiges Informationsportal der EU mit ausführlichen Informationen über die Entwicklung des Datenschutzes auf europäischer Ebene:
http://ec.europa.eu/justice_home/fsj/privacy/

Sonstige

Virtuelles Datenschutzbüro, das gemeinsame Portal verschiedener Datenschutzinstitutionen:
http://www.datenschutz.de

Secorvo Security Consulting GmbH © - Datenschutzseminare und News
http://www.secorvo.de

heise online - Technik, Datenschutz, c't, Newsletter
http://www.heise.de

DuD - Datenschutz und Datensicherheit, Fachzeitschrift
http://www.dud.de

Datenschutzberater Online - Fachzeitschrift
http://www.ad-on-line.de/portfolio_dsb.htm

GDD - Gesellschaft für Datenschutz und Datensicherheit
http://www.gdd.de

DATAKONTEXT-Gruppe - Fachverlag
http://www.datakontext.com

INTEREST – Verlag - Fachverlag
http://www.interest-verlag.de

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
http://www.bvdnet.de

COMPUTAS, Service und Konferenzen
http://www.computas.de

Deutsche Vereinigung für Datenschutz
http://www.datenschutzverein.de/

Informationen zum Datenschutz in der katholischen Kirche
http://www.datenschutz-kirche.de/

Informationen zum Datenschutz in der evangelischen Kirche in Deutschland
http://www.ekd.de/datenschutz/1618_4586.html

Datenschutz-Help - Datenschutzberatung für Unternehmen
http://www.datenschutz-help.de

Bundesverband der Verbraucherzentralen:
http://www.vzbv.de

Teletrust Deutschland e.V. - Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik
http://www.teletrust.de

Schufa
http://www.schufa.de

SPAM, Viren, Dialer, Hoaxes etc.

Dialerinformationen des BSI
http://www.bsi.bund.de/dialer/index.htm

BSI für Bürger - Direktlink zu Dialerinformationen
http://www.bsi-fuer-buerger.de/abzocker/05_02.htm

Dialerschutz.de - Hinweise und Aufklärung über Dialer
http://www.dialerschutz.de

Vireninformationen auf SPIEGEL Online
http://www.spiegel.de/netzwelt/0,1518,k-1626,00.html

Vireninformationen des BSI
http://www.bsi.bund.de/av/HinweiseCV.htm

BSI für Bürger - Direktlink zu Vireninformationen
http://www.bsi-fuer-buerger.de/viren/

Verband der deutschen Internet-Wirtschaft - Informationen über SPAM
http://www.eco.de
http://www.internet-beschwerdestelle.de

Deutscher Direktmarketing Verband e.V. – Allgemeine Informationen zum Direktmarketing, nicht nur zu SPAM
http://www.direktmarketing-info.de/datenschutz/index.html

Beschwerdestelle der Wettbewerbszentrale
www.wettbewerbszentrale.de

Datenbanken:

Juris GmbH
http://www.bundesrecht.juris.de

de jure - Gesetze und Rechtsprechung zum europäischen, deutschen und baden-württembergischen Recht
http://www.dejure.org

Saar-Daten-Bank – Frisierte Gesetze (ab 1. Januar 2008 kostenpflichtig)
http://www.sadaba.de

Landesmedienanstalt Saarland
http://www.lmsaar.de

Rechtliches.de - Gesetze im WWW - Suchportal für Rechtsvorschriften
http://www.rechtliches.de

wikipedia.org – wikipedia, die freie Enzyklopädie im Internet
http://de.wikipedia.org/wiki/Hauptseite