September 2003

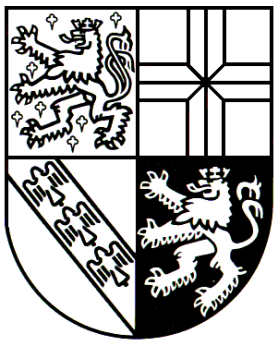
Datenschutz im Saarland

1. Tätigkeitsbericht der Aufsichtsbehörde für Datenschutz im nicht öffentlichen Bereich

Berichtszeitraum 2001 / 2002

Saarland

Ministerium für Inneres und Sport



1. TÄTIGKEITSBERICHT
DER AUFSICHTSBEHÖRDE
FÜR DEN DATENSCHUTZ
IM NICHT ÖFFENTLICHEN BEREICH

BERICHTSZEITRAUM 2001 / 2002

VORGELEGT VON

DER AUFSICHTSBEHÖRDE FÜR DEN DATENSCHUTZ

IM NICHT ÖFFENTLICHEN BEREICH

BEIM

MINISTERIUM FÜR INNERES UND SPORT

DES SAARLANDES

1. TÄTIGKEITSBERICHT DER 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
TEL.: 06 81 / 9 62 – 16 30, 16 34, FAX: 06 81 / 9 62 – 16 05
E-MAIL: DATENSCHUTZ@INNEN.SAARLAND.DE

Liebe Bürgerinnen und Bürger,

im Zeitalter der Informationstechnologie und den damit verbundenen Möglichkeiten der Datenverarbeitung hat der Schutz des informationellen Selbstbestimmungsrechtes einen neuen Stellenwert erlangt. Wir alle sind wesentlich sensibler geworden, wenn unsere persönlichen Daten erhoben, gespeichert und genutzt werden sollen. Täglich kommen wir mit Geschäftspartnern in Verbindung, die neben dem eigentlichen Vertragsabschluss auch Interesse an den verschiedensten Daten ihrer Kunden haben, sei es weil sie diese für eigene Zwecke benötigen oder aber auch weil diese an Dritte weitergegeben werden sollen. Sich im Dschungel der Datenschutzgesetzgebung und der Allgemeinen Geschäftsbedingungen der Unternehmen zurecht zu finden, bereitet den meisten von uns Probleme. Um so erfreulicher, dass eine öffentliche Stelle, die Aufsichtsbehörde für den Datenschutz, angesiedelt beim Ministerium für Inneres und Sport, die Betroffenen kostenlos berät und bei Bedarf auch bei der Durchsetzung ihrer Rechte unterstützt. Jeder – auch das datenverarbeitende Unternehmen - kann sich an die Aufsichtsbehörde für den Datenschutz wenden und sich über seine Rechte und Pflichten informieren.

Ihre

Annegret Kramp-Karrenbauer

Vorwort[1]

Datenschutz in der Informationsgesellschaft?

Wir leben in einer Informationsgesellschaft! Dieser Satz scheint wie in Stein gemeißelt. Information, der Singular als ultimativer Plural des Wortes „Informationen“, sichert - so die offenbar einhellige Meinung – wissenschaftlichen Vorsprung, wirtschaftliches und technisches Können, treibt die wissenschaftliche Forschung voran, setzt - wie ein heute oft verwandter Begriff lautet - „Benchmarks“[2].

So absolut scheint diese Aussage, dass sich die Frage nach ihrem Inhalt kaum noch zu stellen lohnt. Doch was sind Informationen oder was ist Information überhaupt? Können oder dürfen wir Behauptungen wie die obige aufstellen, ohne uns über die Bedeutung des Begriffs und damit die Reichweite dieses Apodiktums im Klaren zu sein.

Eine erste Annäherung an den Begriff scheint über die Negativabgrenzung möglich, Informationen sind unwidersprochen nichts Materielles. Diese Feststellung allein bringt uns jedoch dem Kern der Frage nicht wesentlich näher, sagt sie doch nichts darüber aus, was Informationen sind. In die naturwissenschaftlich-technische Sprache übertragen, könnte man Informationen als Atome oder Bauteilchen des Wissens bezeichnen. Semantisch beschreibend könnte man Information auch als „... jede Kenntnisbeziehung zu jedem realen und irrealen Gegenstand der Welt...“ definieren[3]; wie der Zitierte selbst zugesteht, eine konturen- und grenzenlose Begrifflichkeit. Informationen lassen sich daher wohl nur von Ihrem Nutzen bzw. Ihren Auswirkungen her beurteilen:

Information/en als Kenntnis von irgendetwas oder irgendjemandem, als Teil des Wissens. Allerdings ist/sind Information/en zunächst wertneutral, sie bedarf/bedürfen der Umsetzung: Die Renaissance zum Beispiel wird allgemein als Beginn der Neuzeit angenommen, die Wiederentdeckung längst vergessenen Wissens gab den Anstoß zu einer geistigen und technischen Weiterentwicklung. Informationen mithin und somit Wissen, das längst existierte, jedoch vergessen war.

Wenn wir nach diesem Beispiel davon ausgehen, dass Informationen keinen Wert an sich besitzen, sondern ihr Wert ganz entscheidend von ihrer Verfüg- und Verwertbarkeit abhängt, so relativiert sich der Eingangssatz in seiner Bedeutung. Wir leben nicht in der Informationsgesellschaft, sondern in einer Gesellschaft, welche die technischen Voraussetzungen geschaffen hat, eine Vielzahl von Informationen verfügbar zu machen. War in der Vergangenheit die Suche nach Informationen sowie das Erforschen der Grenzen zwischen Tatsachen und Glauben Grundvoraussetzung für Entscheidungen, so besteht heute das Problem zumeist in der Auswahl der Informationen, denn diese sind – Fluch und Segen des Internets - vielfach weltweit verfügbar. Überschussinformationen – informationeller Abraum – stellen kontextbezogen nutzloses, nicht verwertbares Wissen dar. So hat beispielsweise die im Internet mit Sicherheit recherchierbare Preisliste einer Garküche in Taipeh hier eher einen geringen Informationswert; das Wissen hierum ist nutzlos, da es bei uns nicht verwertbar ist, noch nicht einmal als Argu-

---

[1] Hinweis in eigener Sache: Alle Links in diesem Text verweisen auf externe frei zugängliche Quellen. Eine Haftung für eventuelle Datenschutz- und sonstige Rechtsverletzungen in anderen Angeboten, auf die wir einen Link gesetzt haben, übernehmen wir nicht.

[2] Fixpunkte, Bezugspunkte, übertragen: Maßstäbe

[3] s. Thomas Hoeren, Internetrecht, S.1
Quelle: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript_Maerz.pdf

ment für den Wettbewerbsnachteil der inländischen Gastronomie in Folge hoher Lohnnebenkosten und der fortschreitenden Globalisierung auch auf diesem Sektor.

Die Verwertbarkeit ist es demnach vor allem, die in unserem Informationszeitalter Informationen die Bedeutung verleiht, die ihnen zugesprochen wird; Verfügbarkeit wird zur Voraussetzung. Herrschaftswissen definiert sich demnach künftig nicht mehr ausschließlich über das Wissen selbst, sondern auch über die Möglichkeiten zur Auswertung, zur Analyse von Informationen. Verwertbarkeit setzt voraus, dass die Informationen einer Person, einer Sache oder auch anderen Informationen zugeordnet werden können. Dies ist eine Erkenntnis, die dem Datenschutzrecht immanent ist. Personenbezug oder Personenbeziehbarkeit sind die Schlüsselbegriffe. Personenbezogene Daten, Informationen, sind Einzelangaben über bestimmte oder bestimmbare natürliche Personen, so § 3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG).

Der Personenbezug der einzelnen Information macht ihren Wert und die ihr immanente Gefahr aus - eine Gefahr, die darin liegt, dass nicht Offenkundiges „bekannt“ wird. Verstärkt wird die Gefährdung des Individuums, besser: seiner informationellen Privat- oder Intimsphäre, zum einen in der Tat durch die weite Verfügbarkeit großer Datenmengen und zum anderen durch immer neue Verfahren der Auswertung von Informationen. Data-Mining lautet einer der Schlüsselbegriffe: Verfahren, die selbsttätig ablaufend neue Erkenntnisse aus vorhandenen Daten filtern, um neue Informationen zu gewinnen, zu speichern und nutzbar machen.

Diese - aus der modernen Datenverarbeitung resultierenden - Gefahren hat das Bundesverfassungsgericht bereits in seinem Volkszählungsurteil vom 15. Dezember 1983 erkannt und das sog. *„Grundrecht auf informationelle Selbstbestimmung“* formuliert. Das Recht auf Schutz der eigenen Daten wurde so als Abwehrrecht gegen den Staat formuliert; ein Recht, dem zufolge jede/r frei bestimmen könne, wer ihre/seine Daten wo und wie verarbeitet.

Doch die Geschichte des Datenschutzes selbst beginnt nicht erst zu diesem Zeitpunkt:

Datenschutzgesetze existieren in der Bundesrepublik seit Beginn der 70er Jahre; das Hessische Datenschutzgesetz von 1970 war das erste der Welt. Auch im Saarland wurde bereits 1978 das erste Saarländische Datenschutzgesetz erlassen. Die Datenschutzgesetze des Bundes und der Länder stellen sicher, dass eine Verarbeitung personenbezogener Daten, diese sind nichts anderes als Informationen über einen bestimmten oder zumindest bestimmbaren Menschen, nur unter genau definierten Voraussetzungen erfolgen darf. Unterschiedlich sind die Regelungsbereiche der verschiedenen Vorschriften:

Die Landesdatenschutzgesetze richten sich an die Behörden und öffentlichen Stellen des jeweiligen Landes. Das Bundesdatenschutzgesetz hingegen gilt für Einrichtungen des Bundes sowie nicht öffentliche Stellen. Letztere sind i.S.d. Gesetzes vor allem private Unternehmen und Personengesellschaften, die personenbezogene Daten verarbeiten.

Behörden und öffentliche Stellen werden von den jeweiligen Landesbeauftragten bzw. dem Bundesbeauftragten für Datenschutz kontrolliert, private Stellen hingegen von den regional zuständigen Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich.[4]

Im Saarland ist das Ministerium für Inneres und Sport Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich. Rechtsgrundlage für diese Tätigkeit ist § 38 BDSG.

[4] Eine Auflistung der Kontrollbehörden finden Sie im Anhang.

Am 23. Mai 2001 ist das geänderte Bundesdatenschutzgesetz in Kraft getreten. Die neue Vorschrift des § 38 Abs. 1 BDSG schreibt in Umsetzung des Artikels 28 Absatz 5 der EG-Datenschutzrichtlinie den Aufsichtsbehörden für den Datenschutz erstmals vor, regelmäßig – spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit zu veröffentlichen. Das Ministerium für Inneres und Sport folgt dieser Vorgabe und legt hiermit den ersten Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz vor.

Inhaltsverzeichnis

Aufsichtsbehörde für den Datenschutz

Das Ministerium für Inneres und Sport ist im Saarland traditionell seit In-Kraft-Treten des ersten Bundesdatenschutzgesetzes 1977 Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich. Die Aufgabe der Aufsichtsbehörde besteht darin, die Einhaltung des BDSG und anderer datenschutzrechtlicher Vorschriften durch sog. „nicht öffentliche Stellen“ zu kontrollieren. Gemeint sind mit dieser etwas sperrig anmutenden Formulierung vor allem privatrechtlich organisierte Unternehmen, in Ausnahmefällen auch Privatpersonen, die personenbezogene Daten in irgendeiner Form verarbeiten. Hierbei kommt es nicht darauf an, ob die Datenverarbeitung (Haupt-) Geschäftszweck des Unternehmens 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. Es reicht bereits aus, wenn die Daten für einen der genannten Zwecke erhoben werden.

Datenschutz ist eine Querschnittsmaterie, die nicht nur einem bestimmten Rechtsgebiet zugewiesen werden kann. Fragen nach dem Schutz personenbezogener Daten werden immer dann aufgeworfen, wenn solche Daten erhoben, verarbeitet oder genutzt werden oder dies beabsichtigt ist.

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 umzusetzen 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 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.

Ausgleich ist gefragt. In einer Welt, in der Daten und Informationen immer wichtiger werden, ja mittlerweile selbst zur Ware geworden sind, ist es notwendig, im Sinne aller Beteiligten zu sachgerechten und realitätsnahen 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 und gleichzeitig den jeweils notwendigen Informationsfluss zu sichern 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.

Aufgaben und Kompetenzen der Aufsichtsbehörden lassen sich im wesentlichen in drei Bereiche gliedern:

1. Kontrolle
   - Kontrolle der Rechtmäßigkeit der Datenverarbeitung, auch ohne konkreten Anlass (§ 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) und,
- 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) als Ausfluss der Kontrolle im weitesten Sinne

2. Beratung

- 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)

3. Sanktionen

- 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)

Durch die Novellierung des BDSG hat die Aufsichtsbehörde die Möglichkeit erhalten, selbst Strafantrag zu stellen. Nach alter Rechtslage war dies den Betroffenen vorbehalten. Strafanzeigen wie auch Bußgeldverfahren stellen in der Arbeit der Aufsichtsbehörden eher die Ausnahme dar, im Saarland wie auch in den anderen Bundesländern. Im Berichtszeitraum jedenfalls wurden hier lediglich zwei Strafanträge gestellt, Antragsteller waren in beiden Fällen die Betroffenen selbst. Einer dieser Anträge wurde direkt bei der Staatsanwaltschaft gestellt, die jedoch keine strafbare Handlung erkennen konnte und den Fall an die Aufsichtsbehörde weiterreichte. Über den Stand des zweiten Verfahrens ist der Aufsichtsbehörde für den Datenschutz nicht bekannt. Bußgelder hingegen mussten in der Vergangenheit, allerdings nicht im Berichtszeitraum, mehrfach angedroht werden. Die Ursachen lagen in jedem Fall in einer verspäteten Auskunft an die Aufsichtsbehörde.

Anfragen und Eingaben von Bürgerinnen und Bürgern (auch „Petentinnen/Petenten“ genannt), die telefonisch, schriftlich und verstärkt auch per E-Mail an die Aufsichtsbehörde für den Datenschutz herangetragen werden, machen den Hauptteil der praktischen Arbeit aus. Ein großer Teil der telefonischen 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[5]. Ist der Sach-

[5] Genauer: Die/der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung sie/ihn selbst oder eine/n der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichnete/n An-

verhalt geklärt, erfolgt die datenschutzrechtliche Bewertung, die den Petentinnen/Petenten mitgeteilt wird. In der Regel werden im Saarland die verantwortlichen Stellen nur dann informiert, wenn die Datenverarbeitung zu beanstanden ist.

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.

Zusammenarbeit mit anderen Aufsichtsbehörden

Düsseldorfer Kreis und Arbeitsgruppen

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 Nordrhein-Westfalen, wechselt der Vorsitz seit 2002 und damit auch das ausrichtende Bundesland. Aufgabe des Düsseldorfer Kreises ist es, eine – so weit wie möglich – bundeseinheitliche Behandlung datenschutzrechtlicher Probleme sicherzustellen. Eine weitere Aufgabe ist die Erörterung datenschutzrechtlicher Grundsatzfragen.

Im Berichtszeitraum hat sich der Düsseldorfer Kreis u.a. mit folgenden Schwerpunktthemen befasst:

Die zweite Stufe der Novellierung des Bundesdatenschutzgesetzes

Die Änderung des Bundesdatenschutzgesetzes 2001 beschränkte sich vor allem auf die Anpassung von Bundesrechts an EG-Vorgaben. Die von vielen gewünschte und als notwendig erachtete umfassende Novellierung des deutschen Datenschutzrechts konnte und wollte der Gesetzgeber mit dieser Änderung nicht leisten. Anerkannt war bereits seit langem, dass die Unübersichtlichkeit datenschutzrechtlicher Regelungen, die immer noch fehlende Reflektion technischer Entwicklungen sowie die sich aus dem gestiegenen Datenexport ergebenden Probleme dringend einer Lösung bedürfen, die sich nicht in einer selbst Juristen kaum verständlichen Auslegung komplexer Rechtsvorschriften erschöpft.

Ein im Auftrag des Bundesinnenministeriums erstelltes und im September 2001 vorgelegtes Gutachten befasst sich umfassend eben mit der Modernisierung des Datenschutzrechts. Obwohl die dort vorgetragenen Thesen zum Teil äußerst kontrovers diskutiert werden, steht außer Frage, dass das gesamte deutsche Datenschutzrecht dringend überarbeitet werden muss. Der Gedankenaustausch im Düsseldorfer Kreis stellt sicher, dass die Praxiserfahrungen mit dem BDSG letztendlich auch in die Gesetzgebung einfließen wird.

Nutzung von Rezeptdaten durch Apothekenrechenzentren

Apothekenrechenzentren übernehmen für ihre Kunden die Abrechnung mit den Krankenkassen. Die hierfür erforderliche Weitergabe personenbezogener Daten durch die Apotheken ist durch die Vorschriften des Sozialgesetzbuches 5. Teil (SGB V) zugelas-

---

gehörige/n der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde (§ 38 Abs. 3 S. 2 BDSG).

sen. Nicht zugelassen hingegen ist die weitere Nutzung dieser Daten. Hierzu bedarf es einer Rechtsgrundlage. Kontrovers diskutiert wurde und wird zwischen der Mehrheit des Düsseldorfer Kreises einerseits und dem Bundesministerium für Gesundheit und Soziales andererseits die Frage, ob weitere Datennutzungen auf Grundlage einer Einwilligung der Betroffenen zulässig seien. Gedacht ist hierbei u.a. an Zuzahlungsbescheinigungen für Patientinnen und Patienten oder an Möglichkeiten der Rezeptrecherche für die Betroffenen, Ärzte und Krankenkassen. Grundsätzlich ist jede Datenerhebung, -verarbeitung oder –nutzung nur zulässig, wenn sie durch Rechtsvorschrift erlaubt ist oder die Betroffenen eingewilligt haben. Dieses Recht auf informationelle Selbstbestimmung, das auch gesetzlich nicht vorgesehene Nutzungen erlauben kann, besteht nach mehrheitlicher Auffassung der Aufsichtsbehörde für den Datenschutz auch hier. Patientinnen und Patienten können danach grundsätzlich frei entscheiden, in welchem Umfang ihre Daten von den Rechenzentren genutzt werden dürfen. Das Bundesministerium für Gesundheit und soziale Sicherung hält dem allerdings entgegen, dass die genannten Nutzungsmöglichkeiten nicht im SGB V zugelassen seien. Zum Zeitpunkt der Schlussredaktion dieses Tätigkeitsberichts war die Diskussion allerdings noch nicht abgeschlossen.

Schufa-Verträge mit Wohnungsunternehmen und Mieterwarndateien

Das Mietausfallrisiko und die Notwendigkeit einer Wohnung stellen zwei Fixpunkte einer von den Aufsichtsbehörden für den Datenschutz begleiteten Diskussion dar: Sind Mieterwarndateien zulässig und darf gar die Schufa Verträge mit Wohnungsunternehmen abschließen? Jenseits aller ideologischen Motivation können dies letzten Endes durchaus Fragen von existenzieller Bedeutung sein. Eine Wohnung ist Voraussetzung für einen Arbeitsplatz, eine Kontoeröffnung ohne Anschrift ist undenkbar, selbst das elementarste Recht in der Demokratie, das Wahlrecht, ist bei fehlendem Eintrag im Melderegister erschwert. Dem halten Vermieter das gestiegene Mietausfallrisiko entgegen, das durch genauere Informationen über die Bonität der Mieterinnen und Mieter minimiert werden könne.

Wohnungsunternehmen zählten in der Vergangenheit nicht zu den Geschäftspartnern der Schufa. Daher sind Vermieter in der Vergangenheit immer häufiger dazu über gegangen, von Mietinteressenten sog. „Schufa-Selbstauskünfte“ zu fordern. Auf diese Weise sollte die Bonität der Wohnungsinteressenten und somit auch das Mietrisiko beurteilt werden. Diese Praxis war den Aufsichtsbehörden für den Datenschutz ein wahrer Dorn im Auge, da hier von einer freiwilligen Vorlage der Informationen nicht die Rede sein konnte. Die Zwangslage der Betroffenen verhinderte deren freie Entscheidung. Hinzu kam, dass in der Selbstauskunft alle bei der Schufa gespeicherten Informationen über den Betroffenen enthalten sind, auch solche, die für eine Risikoabschätzung nicht relevant sind.

Mittlerweile hat die Schufa ihr Vertragsangebot erweitert, so das Wohnungsunternehmen jetzt „B-Vertragspartner“ werden können. Diese erhalten auf Anfrage eingeschränkte Auskünfte, nämlich ausschließlich Information über nicht vertragsgemäßes Verhalten wie z. B. titulierte Forderungen. Gemeldet werden dürfen nur Informationen, die tatsächlich Rückschlüsse auf die Bonität der Betroffenen zulassen.

Ob dieses Verfahren, das die Datenübermittlung an alle Schufa-Partner erlaubt, zulässig ist, ist noch strittig. Aus datenschutzrechtlichen Grundüberlegungen heraus wird bisweilen gefordert, eine geschlossene Benutzergruppe zu bilden. Hierbei würden mietrelevante Daten nur an Vermieter übermittelt. Strittig ist weiter, welche Daten konkret eingemeldet werden dürfen.

Die Idee, eine geschlossene Benutzergruppe zu bilden, leitet sich von den sog. „Warndateien“ ab. Im Versicherungsbereich existieren bereits seit langem solche Dateien, die

Hinweise auf Versicherungsbetrüger etc. enthalten. Diese Warnsysteme sind unter bestimmten Voraussetzungen zulässig. Im Düsseldorfer Kreis besteht Übereinstimmung darin, dass auch Mieterwarndateien unter bestimmten Voraussetzungen zulässig sind. Die Diskussion dieses Gesamtkomplexes ist ebenfalls noch nicht abgeschlossen.

Der Düsseldorfer Kreis hat zu mehreren Themenschwerpunkten Arbeitsgruppen gebildet. Die Arbeitsgruppen „Internationaler Datenverkehr", „Tele- und Mediendienste", „Auskunfteien", „Kreditwirtschaft" und „Versicherungswirtschaft" tagen in der Regel einmal jährlich. Hierbei werden Grundsatzfragen mit den Vertretern der Wirtschaft erörtert. Insbesondere die Arbeitsgruppen *Auskunfteien*, *Versicherungswirtschaft* und *Kreditwirtschaft* arbeiten seit Jahren mit den jeweiligen Dachorganisationen *Verband der Handelsauskunfteien, Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV)* und dem *Zentralen Kreditausschuss (ZKA)* zusammen. Die Arbeitsgruppe Auskunfteien weist eine Besonderheit auf, hat sie doch zum ständigen Ansprechpartner neben dem Verband der Handelsauskunfteien noch die Schufa.

Workshop der Aufsichtsbehörden

Bei diesen Veranstaltungen, die turnusmäßig veranstaltet werden, steht die praktische Anwendung datenschutzrechtlicher Vorschriften im Vordergrund. Teilnehmer und Ausrichter sind die jeweils vor Ort prüfenden („unteren") Aufsichtsbehörden, nicht wie beim Düsseldorfer Kreis die obersten Aufsichtsbehörden[6]. Intention ist es, auch hier eine möglichst bundeseinheitliche Prüfpraxis bzw. Beurteilung konkreter datenschutzrechtlicher Fragen zu ermöglichen.

Anlassbezogene Zusammenarbeit

Die Kontrollkompetenz der Aufsichtsbehörden für den Datenschutz endet an den jeweiligen Landesgrenzen. Durch die jüngste Novellierung des Bundesdatenschutzgesetzes wurde der Begriff der „verantwortlichen Stelle" eingeführt. Ging man bisher von der Zuständigkeit der Aufsichtsbehörde vor Ort aus, so richtet sich die Kontrollkompetenz jetzt nach dem Sitz der verantwortlichen Stelle, meist des „Mutterkonzerns". Für alle Aufsichtsbehörden hat dies zur Folge, dass Anlasskontrollen nicht immer vor Ort durchgeführt werden können, sondern die jeweiligen Vorgänge an die nunmehr zuständige Behörde weitergeleitet werden müssen[7]. Anlassbezogen arbeiten Aufsichtsbehörden auch zusammen, wenn verschiedene Unternehmen in unterschiedlichen Sitzländern betroffen sind.

Kontrolldualismus

Das BDSG kennt bereits seit 1977 die Institution des betrieblichen Datenschutzbeauftragten. Durch diese Institution wurde ein Kontrolldualismus von interner „Datenschutzrevision" und externer staatlicher Kontrolle geschaffen. Nach unserem Staats- und Bürger/innenverständnis ist zunächst jede/r selbst für sich und sein rechtmäßiges Handeln verantwortlich, niemand nimmt ihr/ihm die Verantwortung für eine Beachtung der geschriebenen und ungeschriebenen Normen unserer Gesellschaft ab. Dies gilt ebenso für juristische Personen; auch diesen wird durch die Gesamtheit des Rechts ein Normen- und Wertegerüst vorgegeben, an dem sie sich eigenverantwortlich orientieren müssen. Ein solches Konzept berechtigt folglich nicht nur zur freien Entfaltung der eigenen – auch Unternehmer - Persönlichkeit, sondern verpflichtet auch zur Beachtung der

[6] In manchen größeren Bundesländern wird die praktische Arbeit von nachgeordneten Aufsichtsbehörden („unteren") wahrgenommen. Im Saarland fallen untere und oberste Aufsichtsbehörde zusammen.

[7] Eine Besonderheit in diesem System stellt die Schufa dar, die als verantwortliche Stelle ihren Sitz in Wiesbaden hat. Zwischen der Schufa und den Aufsichtsbehörden wurde vereinbart, dass die Vor-Ort-Kontrolle weiterhin von den bisher zuständigen Aufsichtsbehörden durchgeführt wird.

Rechte anderer. Das Bundesdatenschutzgesetz gibt daher ein duales System der Kontrolle vor:

Staatliche Aufsicht – externe Kontrolle

Die Verarbeitung personenbezogener Daten durch private Unternehmen wird durch die Aufsichtsbehörde für den Datenschutz kontrolliert. Hierbei handelt es sich jedoch nicht um eine dauerhafte Überwachung im Sinne einer Art Monitorkontrolle, sondern in der Regel um eine Anlasskontrolle. Das Bundesdatenschutzgesetz gibt den Kontrollstellen zwar die Möglichkeit, anlassfrei zu kontrollieren, in der Praxis lässt sich dies jedoch allein schon wegen der großen Zahl der Unternehmen kaum durchführen. Die Aufsichtsbehörde kann jedes Unternehmen, das personenbezogene Daten erhebt, verarbeitet oder nutzt, jederzeit um die erforderlichen Auskünfte bitten. Die Mitarbeiter/innen der Aufsichtsbehörde haben weiter das Recht die Geschäftsräume zu betreten und alle mit der Datenverarbeitung in Zusammenhang stehenden Unterlagen einzusehen; dies gilt auch für personenbezogene Daten, die einem Berufs[8]- oder besonderen Amtsgeheimnis unterliegen. Diese umfassenden Kontrollrechte können mit Hilfe von Bußgeldern durchgesetzt werden.

Eigenverantwortung – interne Kontrolle

Das Datenschutzrecht hat wie beschrieben den Gedanken der internen Kontrolle aufgegriffen und eine/n intern Verantwortliche/n in Form der/des betrieblichen Datenschutzbeauftragten institutionalisiert. Diese/r hat im Binnenverhältnis auf die Einhaltung datenschutzrechtlicher Vorschriften hinzuwirken, die Datenverarbeitung zu überwachen und die Mitarbeiter/innen zu schulen. Darüber hinaus ist sie/er Schnittstelle zu den Betroffenen und zu der Aufsichtsbehörde für den Datenschutz. Die Institution „betriebliche/r Datenschutzbeauftragte/r“ hat sich seit 1977 so bewährt, dass sie Eingang in die EG-Datenschutzrichtlinie gefunden hat.

[8] So beispielsweise dem Arzt- oder Anwaltsgeheimnis

Häufig gestellte Fragen– „FAQs[9]“

Die folgenden Ausführungen stellen den Versuch dar, häufig an die Aufsichtsbehörde für den Datenschutz gestellte Fragen knapp, präzise und verständlich zu beantworten. Die Auswahl erhebt selbstverständlich keinen Anspruch auf Vollständigkeit, repräsentativ ist sie nur insofern, als alle diese Fragen mehr oder weniger häufig an die Aufsichtsbehörde für den Datenschutz gerichtet wurden, sei es in abstrakter Form aus reinem Interesse oder im Rahmen der konkreten Fallbearbeitung. Für Anregungen zu weiteren Themen sind wir dankbar.

Was ist Datenverarbeitung?

Datenverarbeitung nach dem Bundesdatenschutzgesetz meint die *Speicherung*, *Veränderung*, *Übermittlung*, *Sperrung* und *Löschung* personenbezogener Daten (§ 3 Abs. 4). Übermittlung ist die Weitergabe gespeicherter personenbezogener Daten an einen Dritten durch die verantwortliche Stelle. Werden personenbezogene Daten zur Einsichtnahme bereitgehalten oder von einem Dritten z.B über das Internet abgerufen, stellt dies ebenfalls eine Übermittlung dar.

Der im Bundesdatenschutzgesetz verwandte Verarbeitungsbegriff beschränkt sich auf die rein technischen Phasen der Datenverarbeitung und umfasst im Gegensatz zu dem Saarländischen Datenschutzgesetz (SDSG) und anderen Landesdatenschutzgesetzen nicht das *Erheben*, obwohl dieses die unabdingbare Voraussetzung einer jeden weiteren Datenverarbeitung ist.

Auch die über die rein technischen Phasen der Verarbeitung hinausgehende Verwendung, die Nutzung im Wortsinne, also der tatsächliche Gebrauch des Informationsgehalts der Daten, ist nicht vom Verarbeitungsbegriff umfasst. Hier ist das Saarländische Datenschutzgesetz ebenfalls weitergehender.

Was sind personenbezogene Daten?

Personenbezogene Daten sind Einzelangaben/Informationen über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Es genügt, wenn aus einer Angabe mit Hilfe zusätzlicher Informationen auf einen bestimmten Menschen geschlossen werden kann; damit ist bereits das Merkmal „bestimmbar“ erfüllt. Es müssen nicht zwangsläufig offen zugängliche Erkenntnisse sein, es reicht aus, wenn sich die Stelle, die über die „Basisinformationen“ verfügt, das erforderliche Zusatzwissen verschaffen kann.

Informationen über persönliche Verhältnisse umfassen beispielsweise Daten wie Namen, Geburtsdatum, Beruf, persönliche Vorlieben etc. Sachliche Angaben hingegen können Grundbucheintragungen oder Hinweise auf eventuell vorhandenes sonstiges Vermögen sein. Eine klare Trennung ist hier nicht möglich, daher hat der Gesetzgeber beide Bereiche gleichgestellt.

Weiter müssen die Angaben schon oder noch lebende Menschen betreffen, da weder Tote noch Ungeborene die vom Bundesverfassungsgericht formulierten Rechte (Selbstbestimmung) wahrnehmen können. Informationen über Verstorbene fallen nicht unter das allgemeine Persönlichkeitsrecht, da dieses mit dem Tode erlischt. Das allgemeine Datenschutzrecht als Ausfluss des Persönlichkeitsrechts schützt daher Informationen über Tote nicht. Daten Verstorbener unterliegen allerdings den aus Artikel 1 Absatz 1 des Grundgesetzes abgeleiteten Grundsätzen der Unverletzlichkeit der Men-

[9] **F**requently **a**sked **q**uestions: Häufig gestellte Fragen, mittlerweile sehr oft verwandter Begriff aus der (Service-)Technikspräche

schenwürde. Auch gehen spezielle Regelungen – wie z.B. das Arztgeheimnis, das nicht mit dem Tod der/des Patientin/Patienten endet – den allgemeinen Bestimmungen des Datenschutzrechts vor.

Da der Begriff der „personenbezogenen Daten“ nur natürliche Personen meint, umfasst der Schutzbereich datenschutzrechtlicher Regelungen keine juristischen Personen.

Grundsätzlich kennt das deutsche Datenschutzrecht keine Unterscheidung zwischen „sensiblen“ und weniger „sensiblen“ Daten, da es stets auf den Verarbeitungskontext und die Nutzungsabsicht ankommt. Das Bundesverfassungsgericht hat hierzu bereits im Volkszählungsurteil ausgeführt, dass nicht allein auf die Art der Daten abgestellt werden kann. *„...Entscheidend sind ihre Nutzbarkeit und Verwendbarkeit... Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr.“*

Durch die 2001 erfolgte Umsetzung der EG-Datenschutzrichtlinie wurde allerdings der Begriff der besonderen Arten personenbezogener Daten eingeführt, es sind dies Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diesen Datenkategorien wird eine größere Schutzbedürftigkeit zugestanden. Dem erhöhten Schutzbedarf wird bereits im Vorfeld der Verarbeitung dadurch Rechnung getragen, dass die automatisierte Verarbeitung solcher Angaben stets einer Vorabkontrolle[10] zu unterziehen ist.

Unter welchen Voraussetzungen dürfen personenbezogene Daten verarbeitet werden?

Datenverarbeitung oder die Verarbeitung personenbezogener Daten sowie deren Erhebung und Nutzung sind nur dann zulässig, wenn dies durch Rechtsvorschrift erlaubt ist oder Betroffene eingewilligt haben (§ 4 des Bundesdatenschutzgesetzes). Diese Regelung findet sich auch in allen Landesdatenschutzgesetzen. Sie ist zurückzuführen auf das Volkszählungsurteil, wonach jede Einschränkung des Grundrechts auf informationelle Selbstbestimmung zwingend eine klare gesetzliche Vorschrift erfordert.

Fehlt es an einer Rechtsvorschrift, bleibt nur noch die Einwilligung der Betroffenen als Grundlage für eine rechtmäßige Datenverarbeitung. Die Einwilligung muss grundsätzlich schriftlich erfolgen, nur in begründeten Ausnahmefällen ist eine andere Form der Zustimmung erlaubt. Eine wirksame Einwilligung setzt zunächst die freie Entscheidung der Betroffenen voraus, eine unter Zwang abgegebene Einwilligungserklärung ist wirkungslos. Weiter müssen Betroffene über den Zweck der Erhebung, der Verarbeitung und der Nutzung informiert werden. Nur wer in der Lage ist zu verstehen, wie die jeweiligen Daten weiter verarbeitet und genutzt werden, kann abschätzen, ob sie/er dies wirklich möchte.

Was meint der Begriff „Verantwortliche Stelle“?

Verantwortliche Stelle ist nach § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies im Auftrag vornehmen lässt. Die verantwortliche Stelle ist Adressat datenschutzrechtlicher Vorschriften und für deren Einhaltung verantwortlich. Bei Konzernen und Filialunternehmen rich-

[10] Soll ein EDV-Verfahren eingesetzt werden, das mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann, so ist zuvor eine Vorabkontrolle durchzuführen. Das Verfahren darf erst dann zum Einsatz kommen, wenn feststeht, dass solche Risiken entweder gar nicht bestehen oder sie sich durch technische oder organisatorische Maßnahmen vermeiden lassen. Das Ergebnis der Vorabkontrolle sowie dessen Begründung sind schriftlich zu dokumentieren.

tet sich die Verantwortlichkeit in aller Regel nach dem Organisationsaufbau und dürfte meist beim Mutterunternehmen liegen.

Worin liegt der Unterschied zwischen einem Datenempfänger und einem Dritten?

Datenempfänger sind alle natürlichen Person und alle Stellen, die personenbezogene Daten erhalten, unabhängig davon, ob die Daten innerhalb der verantwortlichen Stelle einfach weitergegeben oder übermittelt werden (§ 3 Abs. 8 BDSG). Dritte/r hingegen ist nach § 3 Abs. 8 Satz 2 BDSG jede Person oder Stelle außerhalb der verantwortlichen Stelle. Nicht gemeint sind hiermit die von der Datenverarbeitung Betroffenen selbst. Die Datenweitergabe an einen Dritten erfordert stets eine Übermittlung.

Einen Sonderfall stellt die Auftragsdatenverarbeitung dar. Bei der Auftragsdatenverarbeitung werden Daten physisch an eine fremde Stelle weitergegeben. Der Auftragnehmer darf personenbezogene Daten allerdings nur im Rahmen der Weisungen des Auftragsgebers erheben, verarbeiten oder nutzen. Verantwortliche Stelle im datenschutzrechtlichen Sinn bleibt der Auftraggeber (§ 11 Abs. 1 BDSG). Der Auftragnehmer ist also kein „Dritter“ im datenschutzrechtlichen Sinne, da eine Datenübermittlung nicht erfolgen kann, wenn die ursprüngliche Verantwortlichkeit gewahrt bleibt. Diese Konstruktion hat für die verantwortlichen Stellen den Vorteil, dass sie die Datenverarbeitung auslagern können, ohne die strengen Vorschriften über die Datenübermittlung beachten zu müssen.

Welche Rechte haben Betroffene?

Das Bundesdatenschutzgesetz regelt die Datenverarbeitung durch nicht öffentliche Stellen im dritten Abschnitt. Die Rechte der Betroffenen sind im zweiten Unterabschnitt in den §§ 33 bis 35 geregelt. Sie umfassen

- das Recht auf Benachrichtigung (§ 33),
- das Recht auf Auskunft (§ 34),
- das Recht auf Berichtigung, Löschung und Sperrung (§ 35) und
- das Widerspruchsrecht (§ 35 Abs. 5).

Die beiden erstgenannten sind Ausfluss des Transparenzgebots: Jede/r soll gerade unter den Bedingungen einer modernen EDV-gestützten Datenverarbeitung wissen, wer wo welche personenbezogenen Daten über sie/ihn erhebt, verarbeitet und/oder nutzt.

Benachrichtigung

Grundsätzlich ist jede verantwortliche Stelle verpflichtet, Betroffene zu informieren, wenn erstmals personenbezogene Daten ohne deren Kenntnis gespeichert werden. Werden die Daten allerdings zum Zweck der Übermittlung (durch eine Auskunftei oder die Schufa) gespeichert, muss die Benachrichtigung bei der ersten Übermittlung erfolgen. Weitere Mitteilungen sind nicht erforderlich. Um dem Transparenzgebot zu genügen muss die Benachrichtigung zumindest folgende Angaben umfassen:

- Anschrift der verantwortlichen Stelle,
- Art der Daten,
- Zweckbestimmung der Erhebung, Verarbeitung und Nutzung sowie
- mögliche Datenempfänger bzw. Kategorien von Empfängern, wenn die/der Betroffene nicht mit einer Übermittlung an diese rechnen müssen.

Auskunfteien und Schufa müssen in der Mitteilung auch den Hinweis aufnehmen, dass erstmals Daten der/des Betroffenen übermittelt wurden (s.o.)

Die Verpflichtung, Betroffene zu benachrichtigen, kann für die verantwortlichen Stellen u. a. entfallen, wenn

- Betroffene auf andere Weise von der Speicherung oder Übermittlung erfahren haben,
- Speicherung und Übermittlung durch eine gesetzliche Vorschrift ausdrücklich vorgesehen sind,
- besondere Geheimhaltungspflichten bestehen, oder
- die Benachrichtigung mit einem unverhältnismäßig hohen Aufwand verbunden wäre.

Ein Anspruch auf Benachrichtigung besteht nicht, wenn personenbezogene Daten mit Kenntnis des Betroffenen erhoben werden. Weitere Ausnahmen von der Benachrichtigungspflicht sind in § 33 Abs. 2 BDSG aufgeführt.

Auskunft

Das mit der Benachrichtigungspflicht Hand in Hand gehende Auskunftsrecht ist in § 34 BDSG geregelt. Betroffene können jederzeit Auskunft darüber verlangen,

- welche Daten über sie gespeichert sind,
- woher diese Daten stammen,
- an wen die Daten weitergegeben werden (sollen) und
- wozu die Daten überhaupt gespeichert sind.

Neu an der Vorschrift ist, dass nunmehr auch Auskunfteien verpflichtet sind, Herkunft und Empfänger mitzuteilen, außer wenn das Interesse an der Wahrung der Geschäftsgeheimnisse überwiegt. Weiter besteht die Auskunftsverpflichtung dann nicht, wenn unter bestimmten Voraussetzungen (§ 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 BDSG) nicht zu benachrichtigen ist. Die Auskunftsverweigerung muss begründet werden, hierbei ist auch die Rechtsgrundlage anzugeben.

Die Auskunft ist schriftlich zu erteilen. Es empfiehlt sich, diese auch schriftlich zu beantragen. Seriöse Unternehmen erteilen keine telefonischen Vorabauskünfte über personenbezogene Daten, da auf diesem Wege keine sichere Identifikation der Anruferin/des Anrufers möglich ist.

Grundsätzlich ist die Auskunft kostenfrei. Anders verhält es sich lediglich, wenn schriftliche Auskünfte von Auskunfteien, Schufa etc. zu wirtschaftlichen Zwecken genutzt werden können (Nachweis der Kreditwürdigkeit, Bonitätsnachweis). In solchen Fällen dürfen die direkt zurechenbaren Kosten als Gebühr erhoben werden. Bei dieser Konstellation müssen Betroffene allerdings darauf hingewiesen werden, dass sie persönlich kostenfrei Einsicht in die Datensätze nehmen können.

Berichtigung, Löschung, Sperrung

Betroffene haben das Recht auf Berichtigung ihrer gespeicherten personenbezogenen Daten (§ 35 Abs. 1 BDSG). Die verantwortlichen Stellen müssen die Berichtigung vornehmen.

Personenbezogene Daten **können** außer in besonders geregelten Fällen[11] jederzeit gelöscht werden. Gelöscht werden **müssen** personenbezogene Daten, wenn

- 1. ihre Speicherung unzulässig ist,
- 2. es sich um besondere Arten personenbezogener Daten handelt[12], deren Richtigkeit nicht von der verantwortlichen Stelle bewiesen werden kann,

[11] Hierunter fallen spezielle Aufbewahrungsvorschriften wie z.B. im Versicherungs- oder Handelsrecht, aber auch Dokumentationspflichten wie sie z.B. für ärztliche Unterlagen gelten.

- 3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist[13], 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 länger währende Speicherung nicht erforderlich ist. (§ 35 Abs. 2 Nr. 1 – 4 BDSG).

An Stelle der Löschung tritt in den Fällen des § 35 Abs. 3 BDSG die Sperrung. Danach sind Daten dann zu sperren, wenn

- 1. sie eigentlich gelöscht werden müssten, aber wegen gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen noch gespeichert bleiben müssen,
- 2. Grund zur Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden, oder
- 3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Abgesehen von den in § 35 Abs. 3 genannten Fallgruppen müssen personenbezogene Daten auch dann gesperrt werden, wenn Betroffene ihre Richtigkeit bestreiten und sich weder Richtig- noch Unrichtigkeit nachweisen lassen (§ 35 Abs. 4 BDSG). Bei einer solchen Konstellation sind die Daten bereits während des Prüfvorgangs zu sperren.

Widerspruchsrecht

Hierbei handelt es sich um ein bei der jüngsten Novellierung des Bundesdatenschutzgesetzes neu geschaffenes Betroffenenrecht:

Personenbezogene Daten dürfen dann nicht für eine automatisierte Verarbeitung oder Verarbeitung in einer nicht automatisierten Datei erhoben, verarbeitet oder genutzt werden, wenn die/der Betroffene dem widerspricht und eine Prüfung durch die verantwortliche Stelle ergibt, dass das schutzwürdige Interesse der/des Betroffenen in der speziellen persönlichen Situation das Interesse an der Verarbeitung überwiegt (§ 35 Abs. 5 BDSG). Mit anderen Worten: Selbst eine rechtmäßige Datenerhebung, -verarbeitung und –nutzung kann, je nach persönlicher Situation der/des Betroffenen, zu einer rechtswidrigen werden. Betroffene müssen bei diesem Verfahren nachvollziehbar darlegen, worin die besondere Beeinträchtigung liegt. Die Aufsichtsbehörde vertritt hierzu die Auffassung, dass Nachteile gemeint sind, die wesentlich schwerer wiegen als üblicherweise bei der jeweiligen Datenerhebung, -verarbeitung und –nutzung zu erwarten ist. Ist die Erhebung, Verarbeitung oder Nutzung durch Rechtsvorschrift vorgeschrieben, kommt ein Widerspruchsrecht nicht in Betracht.

Was ist das Bankgeheimnis?

Das Bankgeheimnis ist nahezu eine Legende, deren eigentlicher Inhalt eher ernüchternd wirkt. Gemeint ist hiermit nicht ein ehernes Schweigen bis zum Zeigen der Folterinstrumente des Gerichtsvollziehers oder des Staatsanwalts: Es handelt sich vielmehr um eine vertragliche Nebenpflicht, die erst 1993 in den Allgemeinen Geschäftsbedingungen der Kreditinstitute festgeschrieben wurde. Die Banken sind durch das Bankgeheimnis zur Verschwiegenheit über Kundendaten verpflichtet. Diese Verschwiegen-

[12] Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. S.a. „Was sind personenbezogene Daten?“

[13] Vereinfacht: Die Daten sind zu löschen, wenn sie für den ursprünglichen Zweck nicht mehr benötigt werden.

heitspflicht beginnt bereits vor Abschluss eines Vertrags während der Geschäftsanbahnung und endet nicht mit Vertragsablauf. Das besondere Vertrauensverhältnis zwischen Bank und Kundinnen/Kunden ist allerdings auch gesetzlich anerkannt. § 30a der Abgabenordnung enthält beispielsweise besondere Bestimmungen zum Schutz der Bankkundinnen und -kunden, wenngleich eine Definition des Bankgeheimnisses auch an dieser Stelle fehlt.

Ob das Bankgeheimnis darüber hinaus ein besonderes Berufsgeheimnis wie z.B. die ärztliche Schweigepflicht darstellt, ist fraglich. Es beruht schließlich nicht auf einer Berufsordnung oder sonst kodifiziertem Standesrecht, sondern auf vertraglichen und vorvertraglichen Rechtsbeziehungen zwischen Kundinnen/Kunden und Bank. Letztlich ist eine solche Unterscheidung jedoch unbeachtlich, da das Schutzniveau vergleichbar ist und vor allem von der Einhaltung der vertraglichen Pflichten, nicht von deren systematischer Einordnung in das Rechtssystem abhängt.

Was muss bei der Ahnenforschung beachtet werden?

Die Genealogie oder auch Familien-/Ahnenforschung ist eine Wissenschaft, die mittlerweile sehr weit verbreitet ist. Immer wieder diskutiert, jedoch selten gelöst ist das Problem des Verhältnisses zwischen Datenschutz und Ahnenforschung. So wird dem „Datenschutz“ oftmals die Schuld zugewiesen, wenn Informationen nicht oder nicht in der gewünschten Form erhoben werden können. Ursache hierfür ist oftmals ein falsches Verständnis dessen, was „Datenschutz“ eigentlich bedeutet. Rein datenschutzrechtliche Vorschriften beziehen sich in aller Regel ausschließlich auf natürliche, also lebende Personen, da Tote die vom Bundesverfassungsgericht formulierten Rechte nicht geltend machen können.

Anders ist die Rechtslage, wenn die Angaben sich auch auf Lebende beziehen („Die Mutter/Der Vater von ...“). Für diese Fälle gilt grundsätzlich, dass die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn sie durch Rechtsvorschrift erlaubt ist oder die Betroffenen wirksam - i.d.R. schriftlich - eingewilligt haben (§ 4 Abs. 1 BDSG). Unausgesprochene Voraussetzung ist natürlich, dass die Daten rechtmäßig erhoben wurden. Da genealogische Daten nur selten direkt von den Betroffenen selbst stammen - und somit meist keine Einwilligung in die Verwendung vorliegt - und auch nicht - wie im Geschäftsleben üblich - im Rahmen einer Vertragserfüllung bekannt wurden, kommt den Möglichkeiten der Datenerhebung und deren rechtlicher Beurteilung erhebliche Bedeutung zu. Hierbei sind hauptsächlich die folgenden Themenkomplexe zu unterscheiden:

- 1. Die Erhebung personenbezogener Daten aus Kirchenbüchern,
- 2. Nutzung bereits veröffentlichter Familienbücher und Sterbeanzeigen,
- 3. Bestände anderer Genealogen.

Zu 1.:

Kirchenbücher sind als Quelle für die Familienforschung nur für den Zeitraum von 1500 bis zum 31.12.1875 geeignet. Ab dem 1.1.1876 wurden die Angaben fast ausschließlich in Personenstandsbüchern geführt. Die Auswertung der Kirchenbücher ist weitgehend unproblematisch, da hierfür der Nachweis eines berechtigten Interesses ausreicht. Die kirchlichen Archivanordnungen sehen regelmäßig die Erforschung der eigenen bzw. der Familienherkunft als ausreichend für den Nachweis eines solchen Interesses an.

Eine auf den Zeitraum nach dem 1.1.1876 ausgerichtete Familienforschung kann jedoch mit dem Personenstandsrecht kollidieren, da dieses Auskünfte nur unter den en-

gen Voraussetzungen des § 61 Abs. 1 des Personenstandsgesetzes (PStG)[14] erlaubt. Die Einsicht in die Personenstandsbücher, deren Durchsicht und die Erteilung von Personenstandsurkunden können demnach nur von den Personen verlangt werden, auf die sich der Eintrag bezieht sowie von deren Ehegatten, Vorfahren und Abkömmlingen, also von Nachfahren in gerader Linie. Andere Personen - zu diesen zählen auch Verwandte in Seitenlinien - dürfen die Personenstandsbücher nur dann nutzen, wenn sie ein rechtliches Interesse glaubhaft machen können. Demzufolge müssen die Nutzung der Unterlagen durch spezielle Rechtsvorschriften erlaubt oder die Nutzer auf die Kenntnis der Daten zur Verfolgung eines ihnen zustehenden Rechts angewiesen sein. Diesen Voraussetzungen genügt das Forschungsinteresse der Genealogen allein nicht. Die Rechtsprechung hat dementsprechend in der Vergangenheit mehrfach bestätigt, dass die Familienforschung kein rechtliches Interesse begründet. In solchen Fällen bleibt nur noch der Weg über eine durch einen nach § 61 Abs. 1 Satz 1 PStG Berechtigten ausgestellte Vollmacht.

Was die Veröffentlichung der aus Kirchen-/Personenstandsbüchern erhobenen Daten anbetrifft, bestehen aus datenschutzrechtlicher Sicht bei einer rechtmäßigen Erhebung keine Hinderungsgründe, soweit es sich um Angaben über bereits Verstorbene handelt. Soweit Daten Lebender veröffentlicht werden sollen, sollte aus Gründen der Rechtssicherheit eine Einwilligung der Betroffenen eingeholt werden.

Zu 2.:

Bereits veröffentlichte Familienbücher stellen ebenso wie Sterbeanzeigen allgemein zugängliche Quellen dar. Einschlägig für die Nutzung solcher „offenen“ Quellen ist § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Demnach gilt, dass eine weitere Veröffentlichung (als Sonderfall der Übermittlung) grundsätzlich zulässig ist, es sei denn, dass das schutzwürdige Interesse Betroffener an einem Übermittlungsverbot offensichtlich überwiegt. Das heißt: Es bedarf keiner - auch nur summarischen - Erforschung des Interesses Betroffener, es muss vielmehr quasi „ins Auge springen“, dass eine weitere Veröffentlichung den Interessen der Genannten offensichtlich zuwider läuft.

Zu 3.:

Am schwierigsten zu beurteilen ist die Nutzung der Forschungsergebnisse anderer Familienforscher. Hierbei wird es entscheidend darauf ankommen, ob es sich um bereits veröffentlichte Unterlagen handelt oder nicht. Soweit es sich hier um allgemein zugängliche Quellen handelt, gilt das unter 2.) Gesagte mit der Folge, dass die Veröffentlichung unter der Maßgabe des § 28 Abs. 1 Satz 1 Nr. 3 BDSG zulässig ist. Andernfalls bedarf es auch hier der Einwilligung der Betroffenen in die Veröffentlichung.

Nach alledem bleibt festzuhalten, dass vorwiegend personenstandsrechtliche Regelungen der Informationserhebung zu Zwecken der Familienforschung entgegenstehen. Soweit es sich bei den zu Nennenden um bereits Verstorbene handelt, ist die Veröffentlichung in aller Regel datenschutzrechtlich gesehen unbedenklich.

---

[14] § 61
(1) Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden kann nur von den Behörden im Rahmen ihrer Zuständigkeit und von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Behörden haben den Zweck anzugeben. Andere Personen haben nur dann ein Recht auf Einsicht in die Personenstandsbücher, auf Durchsicht dieser Bücher und auf Erteilung von Personenstandsurkunden, wenn sie ein rechtliches Interesse glaubhaft machen.

Wann muss ein/e betriebliche/r Datenschutzbeauftragte/r bestellt werden?

Die Systematik des Bundesdatenschutzgesetzes sieht die Bestellung einer/eines betrieblichen Datenschutzbeauftragten als Regelfall vor. Immer dann, wenn personenbezogene Daten automatisiert verarbeitet werden, muss eine solche Bestellung erfolgen (§ 4f Abs. 1 S. 1 BDSG). Allerdings kennt auch diese Regel Ausnahmen: Stellen, die höchstens vier Arbeitnehmer/innen dauerhaft mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, müssen keine/n betriebliche/n Datenschutzbeauftragte/n bestellen (§ 4f Abs. 1 S. 4 BDSG). Werden personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt (nicht automatisiert) muss ein betrieblicher Datenschutzbeauftragter erst bestellt werden, wenn mindestens 20 Personen regelmäßig hiermit beschäftigt sind (§ 4f Abs. 1 S. 3 BDSG)

Das Bundesdatenschutzgesetz kennt nun jedoch nicht nur Ausnahmen von der Regel, sondern auch Ausnahmen von der Ausnahme („Rückausnahmen“):

Unternehmen, die geschäftsmäßig personenbezogene Daten

- 1. zum Zweck der Übermittlung speichern (Auskunfteien, Adresshändler) oder
- 2. zum Zweck der anonymisierten Übermittlung speichern (Markt- und Meinungsforschungs-, Sozialforschungs- oder Konsumforschungsinstitute etc.),

müssen unabhängig von der Anzahl der Beschäftigten eine/n betriebliche/n Datenschutzbeauftragte/n bestellen (§ 4f Abs. 1 S. 6 BDSG). Weiter muss ein/e betriebliche/r Datenschutzbeauftragte/r bestellt werden, wenn eine sog. „Vorabkontrolle“ durchgeführt werden muss. Eine solche muss dann erfolgen, wenn

- 1. besondere Arten personenbezogener Daten verarbeitet werden, oder
- 2. 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 (§ 4d Abs. 5 BDSG).

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 vier Personen mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. Für andere Arten der Erhebung, Verarbeitung und Nutzung gilt auch hier die „20-Personen-Regel“.

Wie arbeiten Schufa und Auskunfteien?

Sowohl Kreditschutzorganisationen wie die Schufa (Schutzgemeinschaft für allgemeine Kreditsicherung) als auch Auskunfteien sind in der Regel partnerschaftlich organisiert. Ihr Zweck besteht darin, personenbezogene Daten sowie Daten über Unternehmen zu erheben und zu speichern, um diese auf Anfrage an ihre Vertragspartner zu übermitteln. Die Schufa beschränkt sich auf Auskünfte über natürliche Personen. Datenempfänger sind meist Unternehmen, die in irgendeiner Form ein Kreditrisiko tragen oder die mit Waren oder Dienstleistungen in Vorlage treten. Durch eine Auskunft soll versucht werden, die Bonität der jeweiligen Kunden einzuschätzen, um so finanzielle Verluste zu vermeiden.

Die Datenquellen von Auskunfteien sind vielfältig. Ein Teil der Angaben stammt aus allgemein zugänglichen Quellen wie Telefon- oder Adressbüchern, denkbar ist aber auch, dass bei Aufnahme eines Kredits oder bei Bestellungen im Versandhandel eine Einwilligung zur Weitergabe der Daten („Schufa-Klausel“) unterschrieben wurde. Informationen über nicht-vertragsgemäßes Verhalten[15] (sog. „Negativmerkmale“) dürfen nach einer Einzelfallprüfung auch ohne Einwilligung der/des Betroffenen an Auskunfteien übermittelt werden. Des Weiteren erhalten Auskunfteien Abdrucke aus den Schuldnerverzeichnissen der Amtsgerichte. Aus datenschutzrechtlicher Sicht kritisch ist die bisweilen immer noch anzutreffende Praxis, Nachbarschaftsbefragungen durchzuführen, vor allem, wenn Fragen zu eventuell vorhandenem Grundbesitz geklärt werden sollen. Auch Auskünfte von Geschäftspartnern werden oftmals gespeichert und übermittelt. Die bei der Schufa gespeicherten Daten werden durch Auswertung öffentlicher Verzeichnisse (Schuldnerverzeichnis) sowie der Mitteilungen ihrer Vertragspartner, zu denen diese vertraglich verpflichtet sind, gewonnen.

Datenschutzrechtlich gesehen ist die Tätigkeit von Auskunfteien unter bestimmten Voraussetzungen zulässig. Das Bundesdatenschutzgesetz hat dies im dritten Abschnitt geregelt und der Kontrolle durch die Aufsichtsbehörden für den Datenschutz unterstellt.

Nach § 29 Abs. 1 BDSG sind Auskunfteien im Rahmen ihrer Tätigkeit berechtigt, personenbezogene Daten zu erheben, zu speichern und zu verändern, wenn kein Grund zu der Annahme ersichtlich ist, dass Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung haben. Darüber hinaus ist dies auch dann zulässig, wenn die Daten allgemein zugänglichen Quellen entnommen wurden. Voraussetzung für eine Datenübermittlung ist, dass der Empfänger ein berechtigtes Interesse, dies kann auch ein wirtschaftliches sein, an der Auskunft glaubhaft machen kann (§ 29 Abs. 2 Nr. 1a BDSG). Gleichzeitig darf kein Grund zu der Annahme bestehen, dass Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben (§ 29 Abs. 2 Nr. 2 BDSG). Dies erfordert keine Nachforschungen, es reicht vielmehr aus, wenn die Interessen Betroffener nicht offensichtlich stärker zu gewichten sind.

Bei großen Auskunfteien ist die Datenübermittlung ein Massengeschäft. Um sicherzustellen, dass auch dort die Rechte der Betroffenen gewahrt bleiben, bestehen die Aufsichtsbehörden auf einer stichprobenartigen Nachprüfung des angegebenen berechtigten Interesses.

Nach § 34 Abs. 2 BDSG haben Betroffene jederzeit Anspruch auf Auskunft über die zu ihrer Person gespeicherten Daten. Die Auskunft ist grundsätzlich unentgeltlich, es sei denn, sie könnte gegenüber Dritten zu wirtschaftlichen Zwecken genutzt werden (§ 34 Abs. 5 BDSG). Einen Anspruch, Herkunft und Empfänger von Daten zu erfahren, haben Betroffene nur dann, wenn das Interesse an der Wahrung des Geschäftsgeheimnisses der Auskunftei nicht überwiegt oder wenn begründete Zweifel an der Richtigkeit der Daten geltend gemacht werden können.

Auch gegen Schufa und Auskunfteien können Betroffene die bereits beschriebenen Rechte geltend machen („Welche Rechte haben Betroffene“).

Muss die „Schufa-Klausel“ unterschrieben werden?

Die Schufa-Klausel, ursprünglich nur bei der Eröffnung von Girokonten verwandt, begegnet uns mittlerweile in vielen Bereichen des täglichen Lebens. Grundsätzlich kann

[15] Mahnbescheide bei unbestrittener Forderung, Saldo nach Verzug, Titulierung etc.

nahezu jedes Unternehmen[16], das in irgendeiner Form Geld- oder Warenkredite gewährt, Mitglied der Schufa werden. Je nach Vertragsausgestaltung sind die Schufapartner verpflichtet, Daten ihrer Kunden an die Schufa zu übermitteln. Da nicht für jede vorgesehene Datenweitergabe eine Rechtsgrundlage existiert, sind die Unternehmen auf die Einwilligung ihrer Kunden in die Datenweitergabe angewiesen. Mit der Unterschrift unter die Schufa-Klausel wird die erforderliche Zustimmung zu der Datenübermittlung abgegeben. Ein formeller Zwang, diese Einverständniserklärung abzugeben, existiert nicht. Allerdings ist es dem Unternehmen auch freigestellt, in diesem Fall den gewünschten Kredit nicht zu gewähren oder kein Girokonto zu eröffnen. Zumindest im letzteren Fall besteht allerdings noch die Alternative eines Guthabenkontos, denn hierbei ist mangels Kreditrisikos keine Schufa-Klausel erforderlich. Die Datenschutzaufsichtsbehörden haben das Interesse der Kreditwirtschaft an Daten, die Rückschlüsse auf die Bonität zulassen, anerkannt, auch im Interesse aller Kunden. Das hier beschriebene Verfahren wird daher grundsätzlich akzeptiert.

Wozu dient die Einwilligungsklausel der Versicherungsunternehmen?

Versicherungen erheben, verarbeiten und nutzen personenbezogene Daten in sehr großem Umfang. Insbesondere die Kranken-, Unfall-, Renten- und Lebensversicherer unterhalten große Bestände an besonders sensiblen Daten; Daten, die teils bei den Versicherten selbst, teils bei den behandelnden Ärztinnen und Ärzten erhoben wurden und werden. Wer eine private Krankenversicherung, eine Unfall- oder Berufsunfähigkeitsversicherung oder eine Lebensversicherung abschließen möchte, muss daher dem Versicherungsunternehmen Angaben über bisherige Krankheiten, behandelnde Ärzte und besondere Risiken mitteilen. Dies soll die Versicherer in die Lage versetzen, das individuelle Risiko zu beurteilen. Eine gesetzliche Grundlage hierfür existiert jedoch nicht, so dass die erbetenen Angaben allesamt freiwillig gemacht werden. Die Versicherungen verwenden hierzu je nach Vertragstyp und angebotenem Produkt unterschiedliche standardisierte Einwilligungsklauseln. Diese Klauseln, die von den Aufsichtsbehörden für den Datenschutz und dem Gesamtverband der Versicherungswirtschaft in zum Teil langwierigen Prozessen erarbeitet und abgesprochen wurden, erlauben den Versicherungen die Verarbeitung personenbezogener Daten, insbesondere die Übermittlung an Rückversicherungen und andere Versicherungen. Die Einwilligungsklauseln dienen so letztlich auch dem Ausgleich zwischen den Interessen der Versicherungsunternehmen und den der Betroffenen.

Versicherungsunternehmen wandeln sich in zunehmendem Maße zu Finanzdienstleistern, die eine Vielzahl von Produkten im Bereich Vermögensbildung und Altersvorsorge anbieten. Das geschäftliche Interesse der Versicherungen gilt daher nicht nur der Risikoabschätzung, sondern auch der Information der Kundinnen und Kunden über andere Produkte, vor allem eben Finanzdienstleistungen. Die Versicherungsverträge enthalten daher eine sog. „Allfinanzklausel“, mittels derer sich die Versicherungsnehmer/innen damit einverstanden erklären, dass ihre allgemeinen Antrags-, Vertrags- und Leistungsdaten auch für solche Zwecke genutzt werden. Diese lautet:

„Ohne Einfluss auf den Vertrag und jederzeit widerrufbar willige ich weiter ein, dass die Vermittler meine allgemeinen Antrags-, Vertrags- und Leistungsdaten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen dürfen.“

[16] z.B. Banken und Sparkassen, Bausparkassen, Leasinggesellschaften, Kreditkartenemittenten, Einzelhandels- und Versandhandelsunternehmen, Telekommunikationsunternehmen, Versicherungen, Wohnungswirtschaft, Energieversorger, Internet-Handel (eCommerce)

Die Einwilligungsklausel kann ohne Auswirkungen auf den Versicherungsvertrag gestrichen und jederzeit widerrufen werden.

Werbung/Direktwerbung

Die zunehmende Werbeflut, konventionell oder per E-Mail, wirft immer wieder datenschutzrechtliche Probleme auf. Insbesondere die persönliche Adressierung provoziert geradezu die Frage nach der Zulässigkeit.

Grundsätzlich ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift dies erlaubt/anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Die Einwilligung stellt begrifflich eine Form der Zustimmung dar, die vor der Verwendung der Daten zu erfolgen hat.

Von dem Verbot der Datenverarbeitung und –nutzung ist die Nutzung oder Übermittlung personenbezogener Daten zu Werbezwecken bzw. zur Markt- und Meinungsforschung ausgenommen. Personenbezogene Daten dürfen bereits dann für Marketingzwecke (Werbung, Markt- und Meinungsforschung) übermittelt und genutzt werden, wenn Betroffene dem nicht widersprechen (§ 28 Abs. 4 Satz 1 des Bundesdatenschutzgesetzes). Mit dieser Regelung ist der Gesetzgeber nur scheinbar von der Grundentscheidung des § 4 Abs. 1 BDSG abgewichen. Eine solche Auslegung übersieht, dass die Übermittlung und Nutzung zu Werbezwecken immer auch an die für alle Phasen der Datenerhebung, -verarbeitung und –nutzung geltenden rechtlichen Voraussetzungen gebunden ist. Es geht hier nicht darum, die Verwendung von Daten zu Werbezwecken bis zu einem Widerspruch hinzunehmen, vielmehr muss bereits für die Erhebung und Speicherung eine Rechtsgrundlage existieren. Es bedarf lediglich keiner ausdrücklichen Einwilligung in die Übermittlung zu Werbezwecken. Als Korrektiv hat der Gesetzgeber weitgehende Aufklärungspflichten des Werbenden vorgesehen. In der Praxis erweist sich dies allerdings oft als problematisch.

Die Betroffenen sind

- über ihr Widerspruchsrecht sowie
- über die (für die Werbung) verantwortliche Stelle

zu informieren. Fehlen diese Informationen bei der Ansprache, dürfen personenbezogene Daten nicht für die genannten Zwecke verwandt werden. Kommen die werbenden Unternehmen diesen Informationspflichten nicht nach, kann dies als Ordnungswidrigkeit mit einer Geldbuße bis zu einer Höhe von 25.000 € geahndet werden kann.

Diese Ausführungen betreffen allerdings nur die Zulässigkeit der Datenverwendung, sie sagt nichts über die der Werbung, insbesondere der E-Mail-Werbung, aus. Die herrschende Meinung in der Rechtsprechung hierzu ist relativ eindeutig:

Die Zusendung unverlangter E-Mails ist ein Eingriff in die Privatsphäre, dem sich die Betroffenen ebenso wenig entziehen können wie telefonischer Werbung. Wegen dieses vergleichsweise weitgehenden Eingriffs ist E-Mail-Werbung in den meisten Fällen nicht zulässig und es besteht ein Unterlassungsanspruch nach den §§ 1004 und 823 BGB. Unzulässig ist E-Mail-Werbung insbesondere auch dann, wenn sie ein aktives Handeln der Betroffenen erfordert, um sich ihrer zu erwehren. Die Rechtsprechung stellt mittlerweile hohe Ansprüche auch an die Wirksamkeit der Einwilligung.

Der Briefkasten ist voll! - Was kann dagegen unternommen werden?

Datenquellen

Eine der häufigsten Fragen im Zusammenhang mit Direktwerbung ist die nach der Herkunft der Adresse. Die Datenquellen sind mannigfaltig: Die Werbewirtschaft erhebt Adressen oft aus Telefonbüchern oder im Zusammenhang mit Preisausschreiben, wenn

der Verwendung der Daten zu Werbezwecken nicht ausdrücklich widersprochen wurde. Personenbezogene Daten werden auch im Zusammenhang mit sog. „Kundenbindungsprogrammen“ („Rabattsystemen“) erhoben. Weitere Datenquellen können Adresshändler sein oder auch Unternehmen, die ihre Kundenliste vermieten. Grundsätzlich wird dies zulässig sein, es sei denn die Betroffenen haben der Nutzung ihrer Daten zu Werbezwecken widersprochen. Wie bereits erläutert, bedarf es keiner ausdrücklichen Einwilligung in die Verwendung der personenbezogenen Daten zu Werbe- und Marketingzwecken. Eine Ausnahme stellen Tele- und Mediendienste („Internet“) dar; hier ist die Nutzung der Nutzerdaten zu Werbezwecken grundsätzlich nur mit Einwilligung zulässig.

Schutzmöglichkeiten

Betroffene können bei jedem einzelnen Versender der Nutzung ihrer Daten zu Werbezwecken widersprechen. Es empfiehlt sich, einen solchen Widerspruch bereits dann einzulegen, wenn bei dem ersten Kontakt, z. B. beim Anfordern von Informationsmaterial, personenbezogene Daten angegeben werden müssen. Dieser präventive Widerspruch verhindert, dass mit den Daten gehandelt wird. Weiter besteht die Möglichkeit, sich beim Deutschen Direkt-Marketing-Verband kostenlos in die sog. „Robinson-Liste“ eintragen zu lassen. Die dem Verband angeschlossenen Unternehmen gleichen ihre Adressbestände mit dieser Sperrliste ab und verzichten darauf, den dort Aufgeführten Direktwerbung zu schicken. Der Eintrag gilt für fünf Jahre.

Informationen können unter folgender Adresse angefordert werden:

DDV - Robinson-Liste
Postfach 14 01
71243 Ditzingen
Tel.: 0 71 56 / 95 10 10

Was kann gegen unerwünschte E-Mails (Spam) unternommen werden?

Was ist Spam und wie kann man sich dagegen wehren?

Der Ursprung und die genaue Definition des Ausdrucks sind umstritten. Spam ist ursprünglich eine Konservenfleischmarke (**http://www.spam.com/**). Warum dieser Ausdruck für unverlangte E-mails verwandt wird, ist nicht ganz ersichtlich. Der Legende nach sind die Ursprünge in einem Sketch von Monty Python zu sehen, in dem es in einem Restaurant nichts als Spam gibt - niemand will Spam, aber alle werden davon überflutet.

Spam wird nicht durch den Inhalt definiert, sondern alleine durch die Tatsache, dass er unverlangt und in großer Menge versandt wird. Da es auf den Inhalt nicht ankommt, gelten auch sog. „Newsletter“, die oftmals getarnte Werbeangebote darstellen, dann als Spam, wenn sie unverlangt zugeschickt werden.

Werbung per E-Mail setzt – soweit keine vertraglichen Beziehungen zu der/dem Beworbenen bestehen – deren/dessen Einwilligung voraus. Verlangt wird mittlerweile eine sog. doppelte „Opt-in-Lösung“, d.h. auch bei angeforderten Mails wie z.B. Newslettern, muss sich der Anbieter unter der Mailadresse des mutmaßlichen Anfragers die Bestellung bestätigen lassen, ansonsten sind die Adressen zu löschen.

Auch die von der Bundesrepublik noch umzusetzende Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, Amtsblatt der Europäischen Gemeinschaften, Amtsblatt Nr. L 201 vom 31/07/2002 S. 37-47) greift dieses Problem auf und regelt in Artikel 13, dass die Verwendung der elektronischen Post zur Direktwerbung nur bei Einwilligung der Betroffenen gestattet werden darf.

Die Adressaten der E-Mail-Werbung erhalten diese oft nicht gezielt als natürliche Person. Die Mailadressen werden vielmehr durch spezielle Programme generiert, künstlich erzeugt[17]. Hierzu werden die Adressen der Mailbox-Anbieter (AOL, Freenet, GMX, t-online, web.de, etc.) mit Ziffernfolgen kombiniert[18]. Die so entstandenen Adressen werden ohne weitere Identifikationsversuche zum Mailing verwandt. Bei diesen virtuell erzeugten „Putativ-Adressen" handelt es sich nach der reinen Lehre noch nicht um personenbezogene Daten i.S.d. Datenschutzrechts, da jeder Personenbezug fehlt; dies dürfte auch für die Personenbeziehbarkeit gelten. Erfolgt nun eine Rückmeldung, sei es auch in Form eines Widerspruchs oder eines Hinweises auf eine erfolgreiche Zustellung wird die künstliche Adresse zur echten – wertvollen – Adresse. Diese kann – wenn kein Widerspruch nach § 28 Abs. 4 BDSG erfolgt – grundsätzlich weiterhin zu Werbezwecken verwandt werden.

Die Erfahrung hat gezeigt, dass die Mehrzahl der unseriösen Anbieter weder im Inland noch in der EU ansässig ist, so dass die Einleitung eines Bußgeldverfahrens bzw. Zivilklagen wenig erfolgversprechend sind. In aller Regel werden diese Maßnahmen bereits daran scheitern, dass die verantwortliche Stelle kaschiert ist. Eine strafrechtliche Relevanz wird der Mail-Werbung nur in Bezug auf die Inhalte zugesprochen, die reine Belästigung durch die Werbung als solche ist lediglich zivil- sowie evtl. datenschutzrechtlich von Belang.

Wirkungsvolle Abhilfe können daher zur Zeit lediglich Spam-Filter schaffen. Bewährt hat sich auch das einfache Wegklicken ohne die Nachrichten überhaupt zu öffnen. Wird die E-Mail doch geöffnet, ist es nur dann sinnvoll der Werbung zu widersprechen, wenn die nach § 28 Abs. 4 BDSG erforderlichen Informationen ersichtlich sind. Ansonsten sollte eine wie auch immer formulierte Antwort unterbleiben, um die künstlichen Adressen nicht zu echten und damit für die Absender auch wertvollen Adressen werden zu lassen.

Der Verband der deutschen Internet-Wirtschaft e.V. (eco) hat zu dem Thema Spam eine ausführliche Informationsschrift, die unter

http://www.eco.de/servlet/PB/show/1165913/SPAM_ger_100.pdf

abgerufen werden kann, veröffentlicht. Als zusätzlichen Service hat eco eine Beschwerdestelle für alle Spam-Opfer eingerichtet, die unter **hotline@eco.de** oder **http://www.eco.de** erreichbar ist.

[17] Ein vergleichbares Problem besteht auch im Bereich des Mobilfunks. Dort wird bei der SMS-Werbung ähnlich verfahren.

[18] Die „eigentliche" Mailadresse besteht aus einer Ziffernabfolge, die in Leseform „übersetzt" wird.

Ausgewählte Einzelprobleme

Der folgende Abschnitt gibt einen konkreteren Einblick in die praktische Arbeit der Aufsichtsbehörde für den Datenschutz. Die ausgewählten Fälle spiegeln die Bandbreite sowohl der möglichen Datenverarbeiter (verantwortliche Stellen im Sinne des BDSG) als auch der hierbei entstehenden Probleme und Missverständnisse wieder. Im Berichtszeitraum war im Gegensatz zu den Vorjahren kein eindeutiger Schwerpunkt auszumachen. Allerdings hat sich auch in den Jahren 2001 und 2002 bestätigt, dass mit der Zahl der Betroffenen auch die Zahl der Eingaben anwächst. Versicherer, Banken, Auskunfteien und Schufa erheben, verarbeiten und nutzen in besonders hohem Maße personenbezogene Daten. Dies schlägt sich auch im Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz nieder: Die Bereiche „Schufa“ und „Versicherungen“ stellen zwei der thematischen Schwerpunkte dar. Weitere Themen sind Adresshandel, Direktwerbung, Datenverarbeitung im Zusammenhang mit dem world-wide-web, Medizin und Datenschutz sowie Ordnungswidrigkeiten und Straftaten.

Registermeldung

Bei der Aufsichtsbehörde für den Datenschutz wird ein Register bestimmter Unternehmen, die personenbezogene Daten Dritter[19] im weitesten Sinne erheben, verarbeiten und/oder nutzen, geführt. Dieses Register steht zwar für jedermann zur Einsicht offen, im Berichtszeitraum jedoch interessierte sich niemand hierfür.

Bis zur Novellierung des Bundesdatenschutzgesetzes 2001 waren nach § 32 Abs. 1 Unternehmen, die Daten

- 1. zum Zwecke der Übermittlung speichern (vor allem Auskunfteien und Adresshändler),
- 2. zum Zwecke der anonymisierten Übermittlung speichern (vor allem Markt- und Meinungsforschungsinstitute) sowie
- 3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen,

bei der Aufsichtsbehörde für den Datenschutz meldepflichtig. In dem Register waren überwiegend Stellen, die unter 3.) fielen, enthalten. Es handelte sich hierbei vor allem um klassische Auftragsdatenverarbeiter wie Schreibbüros, Datenerfassungszentren, Aktenvernichtungsunternehmen oder privatärztliche Verrechnungsstellen. Durch die Änderung des Bundesdatenschutzgesetzes wurde die Meldepflicht auf die oben unter 1.) und 2.) genannten Unternehmen beschränkt.

Nach der fälligen Bereinigung des Registers sind bei der Aufsichtsbehörde für den Datenschutz lediglich noch fünf Unternehmen gemeldet. Es handelt sich hierbei um drei Auskunfteien sowie zwei Markt- und Meinungsforschungsinstitute.

Adresshandel

Die verschlungenen Wege des Adresshandels[20]

Der Bundesgesetzgeber hat bei der Novellierung des Bundesdatenschutzgesetzes eine neue Regelung in § 28 Absatz 4 aufgenommen, um sicherzustellen, dass gerade bei der Direktwerbung das Transparenzgebot stärker beachtet wird. Nunmehr müssen die

[19] Dritte/r ist nach § 3 Abs. 8 Satz 2 BDSG jede Person oder Stelle außerhalb der verantwortlichen Stelle. Nicht gemeint sind hiermit die von der Datenverarbeitung Betroffenen selbst sowie Personen oder Stellen, die im Inland oder einem anderen Mitgliedstaat der EU bzw. des europäischen Wirtschaftsraumes personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen („Auftragsdatenverarbeiter“).

[20] s. hierzu auch: „Häufig gestellte Fragen – Werbung/Direktwerbung“

Werbenden auch dafür Sorge tragen, dass die Betroffenen erfahren können, woher ihre Daten stammen.

Ein Petent hatte persönlich adressierte Werbung von einem anscheinend in Baden-Württemberg ansässigen Unternehmen erhalten, ohne ersehen zu können, woher seine Adresse stammte. Das Anschreiben enthielt zwar eine Service-Nummer, die aber offenbar nicht zu erreichen war. Aufgeführt war allerdings auch eine Kontaktadresse im Saarland. Die Aufsichtsbehörde für den Datenschutz hat daraufhin das im Saarland ansässige Unternehmen um Stellungnahme gebeten und Folgendes erfahren:

Das baden-württembergische Unternehmen hatte dem hiesigen Adressen für eine Werbeaktion zur Verfügung gestellt. Die Adressen selbst stammten ursprünglich von einem Adresshandels- und Direktwerbeunternehmen in Hessen. Gewonnen – oder technisch ausgedrückt: erhoben - wurden die Daten des Petenten durch dessen Teilnahme an einem Gewinnspiel. Dieser hatte sich – wie viele andere auch – an einem kostenlosen Gewinnspiel in einer Zeitschrift oder Ähnlichem beteiligt und – ansonsten wäre die Teilnahme auch ziemlich sinnlos - seine Adresse angegeben. Weiter war der Hinweis auf eine mögliche Datenweitergabe (=Adresshandel!) nicht gestrichen worden.

Im Falle des Petenten war die Möglichkeit des Widerspruchs auf der Teilnahmekarte vorgesehen, wenngleich an nicht sehr exponierter Stelle. Auch die Schriftgröße lag – wie leider üblich in solchen Fällen – etwas unter der Norm. Rechtswidrig war die Datenübermittlung allerdings nicht. Da nach dem Wortlaut des § 28 Abs. 4 Satz 2 des BDSG lediglich sichergestellt sein muss, dass Betroffene die Herkunft ihrer Daten erfahren können, konnte hier kein Verstoß gegen datenschutzrechtliche Vorschriften festgestellt werden.

Direktwerbung

Der übersehene Widerspruch

Direktwerbung kann – dies beweisen zahlreiche Eingaben und telefonische Anfragen – lästig sein. Umso lästiger ist es, wenn der Werbung unverzüglich widersprochen, der Widerspruch jedoch nicht beachtet wird.

Ein Petent hatte mehrfach Werbung einer Bank erhalten, über die er ungefähr 4 Jahre zuvor einen Warenkredit finanzierte. Nachdem er mehrfach erfolglos per E-Mail der weiteren Nutzung seiner Daten zu Werbezwecken widersprochen hatte und zudem erfahren wollte, welche Daten die Bank über ihn gespeichert habe, wandte sich der Betroffene an die Aufsichtsbehörde für den Datenschutz.

Nach mehrfachem Nachfragen und Hinweis auf ein mögliches Bußgeldverfahren konnte dann der etwas merkwürdige Ablauf dieser Geschichte rekonstruiert werden:

Die Adressdaten stammten tatsächlich aus dem Kreditvertrag. Die erstmalige Nutzung der Daten zu Werbezwecken war nicht zu beanstanden, da der Petent dem nicht vorher bereits widersprochen hatte[21]. Allerdings hätte der später eingelegte Widerspruch beachtet werden müssen. Dass dies nicht geschah, war schlicht und ergreifend auf ein Organisationsversagen der Bank zurückzuführen. In den Finanzierungsangeboten war eine E-Mail-Adresse aufgeführt, die – so die Überlegung des Betroffenen – eigentlich einen direkten Zugang zur angegebenen Sachbearbeiterin herstellen müsste. Doch weit gefehlt: Dieser E-Mail-Zugang war ausschließlich dazu bestimmt, einen Kreditantrag innerhalb von zwei Wochen widerrufen zu können. Dies war allerdings nicht ohne weiteres ersichtlich. Die an die E-Mail-Adresse gerichteten Widersprüche gegen die Daten-

[21] s.a. „Häufig gestellte Fragen – Werbung/Direktwerbung“

nutzung wurden sogar abgerufen, allerdings – obwohl offenbar eine anderweitige Weisung bestand – nicht an den betrieblichen Datenschutzbeauftragten weitergeleitet mit der Folge, dass die Rechte des Betroffenen nicht beachtet wurden.

Der Vorfall zeigt, wie wichtig eine funktionierende Datenschutzorganisation für ein Unternehmen ist. Die hier offenbar vorliegende Priorität von Marketing und Verkauf/Vertrieb jedenfalls hatte letzten Endes dazu geführt, dass aus einer zulässigen Nutzung personenbezogener Daten zu Werbezwecken eine rechtswidrige wurde. Spätestens nach dem Abruf der ersten E-Mail des Betroffenen durften seine personenbezogenen Daten nicht mehr zur Werbung verwandt werden. Selbstredend hätte die Bank ihm auch mitteilen müssen, welche Angaben gespeichert sind und woher diese stammen.

Die alles in allem schleppende Bearbeitung der Anfragen der Aufsichtsbehörde für den Datenschutz unterstützte die These, dass das Datenschutzmanagement insgesamt verbesserungswürdig war. Der Bank war nur eines zu gute zu halten: Der betriebliche Datenschutzbeauftragte verfügte unverzüglich, die Daten des Betroffenen nicht mehr für Werbezwecke zu nutzen. Ob die zugesagte Sensibilisierung der Mitarbeiterinnen und Mitarbeiter solche Vorfälle vermeiden kann, muss die Zukunft zeigen.

World-wide-web - Internet

Datenspeicherung im Internet-Café

Internet-Cafés erfreuen sich wachsender Beliebtheit. Das nahezu anonyme Surfen im world-wide-web und die für Benutzerinnen und Benutzer kostengünstige Infrastruktur sowie – oft jedenfalls – die kompetente Beratung machen den Reiz dieser Einrichtungen aus. Mittlerweile werden solche Internet-Cafés nicht nur gewerblich, sondern auch von gemeinnützigen Unternehmen betrieben. Diese verfolgen hiermit vor allem das Ziel, ihre Kundinnen und Kunden schnell und umfassend zu informieren. Geradezu maßgeschneidert erscheint dies für Organisationen, die Dienstleistungen für Arbeitssuchende anbieten. Auch im Saarland existieren solche Internet-Cafés. Arbeitssuchende können sich hier im Internet über Arbeitsplatzangebote informieren, Bewerbungsschreiben erstellen und online versenden. Das hiermit verbundene Erlangen von Medienkompetenz ist ein willkommener Nebeneffekt.

Durch eine Eingabe wurde die Aufsichtsbehörde für den Datenschutz darauf hingewiesen, dass in einer solchen Einrichtung das Surfverhalten der Nutzerinnen und Nutzer jederzeit überprüft werden könne.

Die gemeinnützige Betreibergesellschaft des Internet-Cafés hat die Aufsichtsbehörde auf Nachfrage darüber informiert, dass man alle Nutzerinnen und Nutzer auf die Nutzungsbestimmungen hinweise, auch auf die Möglichkeit, deren Einhaltung jederzeit zu kontrollieren. Konkret werde u.a. darüber informiert, dass die EDV-Anlagen zum Suchen nach Stellenangeboten, zum Erstellen von Bewerbungsunterlagen sowie zur Bewerbung selbst genutzt werden dürften. Das Personal der Einrichtung stehe jederzeit bereit, den Nutzerinnen und Nutzern hierbei zu helfen. Leider habe sich in der Vergangenheit immer wieder gezeigt, dass dieses Angebot nicht nur genutzt sondern auch ausgenutzt werde, indem die Anlagen zweckentfremdet würden. Vor allem das stundenlange Surfen und Suchen nach faschistischen und pornografischen Inhalten habe - so der Träger - nicht länger geduldet werden können. Aus diesem Grund sei eine Überwachungssoftware eingesetzt worden, die auf Anforderung den Mitarbeiterinnen und Mitarbeitern eine Kontrolle der aktuellen Bildschirmanzeige der Nutzerinnen und Nutzer ermögliche. Weiter wurde dargelegt, dass die hierbei ersichtlichen Daten nicht gespeichert würden, ebenso wenig sei es möglich, vorher genutzte Programme oder Internetseiten zu rekonstruieren. Seit Einführung des Überwachungsprogramms und der ent-

sprechenden Hinweise sei die missbräuchliche Nutzung jedenfalls signifikant zurückgegangen.

Aus datenschutzrechtlicher Sicht ist die Einführung der Überwachungssoftware in diesem Fall nicht zu beanstanden, zumal keine Speicherung erfolgt. Die Nutzerinnen und Nutzer der Einrichtung werden eindeutig über die Nutzungsbeschränkungen und die Möglichkeit der Kontrolle informiert, so dass es hier der individuellen Entscheidung obliegt, ob und wie die Anlagen genutzt werden. Jedenfalls besteht für jede und jeden Klarheit über die möglichen Konsequenzen eines regelwidrigen Verhaltens.

Domain-Registrierung

Dass das Internet ein rechtsfreier Raum sei, gehört ins Reich der Sagen und Mythen. Dies wird allein schon daran sichtbar, dass jede „Domain", also jede „Homepage", registriert sein muss. Wer eine Internetseite erstellen und betreiben will, braucht eine sog. „Domain" und einen „Domainnamen". So ist gewährleistet, dass jeder Name nur einmal vergeben wird und bestehende Namens- und Markenrechte geschützt werden.

Registriert werden die Domainnamen durch sog. „Registrare", Unternehmen die durch die Dachorganisation **ICANN** (Internet Corporation for Assigned Names and Numbers) akkreditiert und berechtigt wurden, Domainnamen zu vergeben und zu registrieren.

Bei einem im Saarland ansässigen Registrar hatte ein Kunde einen Domainnamen vorbestellt. Für diese Vorbestellung wurde eine „Vorgebühr" in Höhe von 20 € berechnet. Aus verschiedenen Gründen trat der Besteller in der Folge von dem Vertrag zurück und bat das Unternehmen, seine dort gespeicherten personenbezogenen Daten zu löschen. Dies wurde ihm auch umgehend zugesagt.

In der Folge erhielt der Betroffene jedoch erneut eine Rechnung, diesmal über eine Gesamtsumme von 40 €. Daraufhin wandte er sich an die Aufsichtsbehörde für den Datenschutz und wies insbesondere auf die zwar zugesagte, jedoch unterbliebene Datenlöschung hin.

Das Unternehmen hat ausgeführt, dass dort die personenbezogenen Daten des Betroffenen in der Tat umgehend gelöscht worden seien. Die „Vorbestellung" sei jedoch bereits mitsamt den Daten an das „Global Name Registry", eine Art Zentralregister, übermittelt worden. Dies wiederum sei dem für die Löschung der Daten zuständigen Mitarbeiter des hier ansässigen Registrars nicht bekannt gewesen. Als später nun die Vorbestellungen fest registriert worden seien, „tauchte" offenbar die vorbestellte und nicht anbezahlte Domain wieder auf. Da - so das Unternehmen – eine lückenlose manuelle Überprüfung aller Geschäftsvorgänge nicht möglich sei und eine sog. „Plausibilitätskontrolle" auch nicht im Wege der Abgleichung vorgenommen werde, habe der vermeintliche Kunde die auf Grund der Registrierung erstellte Rechnung erhalten.

Das Unternehmen bedauerte diesen Vorfall und versicherte, dass keine personenbezogenen Daten absichtlich gegen den Willen eines Kunden gespeichert werden. Datenschutzrechtlich liegt hier kein allzu grober Verstoß vor, allerdings muss sich das Unternehmen ein Organisationsversagen zurechnen lassen.

Unverlangte E-Mail-Werbung – Spam

Ein Petent hatte E-Mail-Werbung in Form eines Newsletters erhalten und bat darauf hin das werbende Unternehmen um Auskunft, welche Daten über ihn gespeichert seien und verlangte außerdem deren Löschung.

Der Auskunftsanspruch ist ein nahezu absoluter Anspruch und kann nur unter sehr engen Voraussetzungen eingeschränkt werden[22]. Somit auf den ersten Blick ein in der Theorie einfacher Fall: Werbung – Auskunftsverlangen – Mitteilung und Löschung der Daten. In der Praxis jedoch stellte sich das Unterfangen komplizierter dar, weil das Unternehmen auf die Anfrage des Betroffenen gar nicht erst reagierte. So wandte sich der Petent an die Aufsichtsbehörde für den Datenschutz. Das Unternehmen wurde um eine Stellungnahme und um Mitteilung, welche Daten über den Betroffenen gespeichert sind, gebeten.

Dargelegt wurde, dass der Mitarbeiter, welcher die E-Mails versandte, nicht mehr bei dem Unternehmen beschäftigt sei und auch nicht mehr nachvollzogen werden könne, woher die E-Mail-Adresse des Petenten stamme. Es sei möglich, dass ein Dritter diese Adresse an sie weitergegeben habe. Mittlerweile werde jedoch Sorge dafür getragen, dass sich im Newsletterbestand auch nur tatsächliche Abonnenten befänden. Diese hätten - so eine Verlautbarung auf der Homepage des Unternehmens – jederzeit die Möglichkeit, sich aus dieser Liste löschen zu lassen.

Im Ergebnis unbefriedigend, konnten diese Ausführungen von der Aufsichtsbehörde weder bestätigt noch widerlegt werden. Es entspricht jedoch den Erfahrungen der Aufsichtsbehörden, dass Newsletter bisweilen unter falschem Namen oder falscher E-Mail-Adresse bestellt werden. Von daher konnte das Verhalten des Unternehmens nicht beanstandet werden[23]. Gerügt wurde allerdings das Auskunftsverhalten, da zumindest in diesem Punkt das Fehlverhalten eindeutig war.

Medizin und Datenschutz

Umfang des Auskunftsrechts von Patientinnen und Patienten

Ein Schwerpunktthema war im Berichtszeitraum der Komplex „Einsicht in Patientenunterlagen und Krankenakten, Umfang des Einsichtsrechts der Patientinnen und Patienten“. Auf die Anfrage einer (privat-rechtlich organisierten) Klinik hin hat die Aufsichtsbehörde folgende Rechtsauffassung vertreten:

Für die Beantwortung der Frage nach dem Auskunftsrecht von Patientinnen und Patienten sowie der Aushändigung von Kopien des Entlassungsberichts durch die behandelnden Kliniken an diese sind die Berufsordnung für Ärztinnen und Ärzte des Saarlandes und das BDSG einschlägig. § 1 Abs. 3 Satz 2 BDSG regelt, dass die Verpflichtung besondere Geheimhaltungsvorschriften – wie etwa die Berufsordnung der Ärztinnen und Ärzte - zu wahren, unberührt von den Vorschriften des Bundesdatenschutzgesetzes bleibt. Dies bedeutet, dass beide Vorschriften parallel gelten und besondere Geheimhaltungsvorschriften immer dann zu beachten sind, wenn sie eine vergleichbare oder gar restriktivere Datenerhebung, -verarbeitung oder –nutzung regeln. Das Bundesdatenschutzgesetz gibt in diesem Zusammenhang den Minimalstandard an, der für jede Datenverarbeitung auch nach Berufsordnungen einzuhalten ist.

§ 10 der Berufsordnung für Ärztinnen und Ärzte des Saarlandes [24] regelt die ärztliche Dokumentationspflicht. Nach § 10 Abs. 2 hat der Arzt den Patientinnen und Patienten

---

[22] s.a. „Häufig gestellte Fragen – Welche Rechte haben Betroffene?“

[23] Zum damaligen Zeitpunkt waren die von der Rechtsprechung geforderten Voraussetzungen für den Versand von Werbe-Mails, insbesondere Newslettern, noch nicht so eindeutig definiert wie zum Zeitpunkt der Erstellung dieses Tätigkeitsberichts. Die Hinweise zu E-Mail-Werbung in den „Häufig gestellten Fragen – Was kann gegen unerwünschte E-Mails (Spam) unternommen werden?“ geben den aktuellen Stand der Rechtsprechung zum Zeitpunkt der Schlussredaktion wieder.

[24] § 10 Dokumentationspflicht
1. Der Arzt hat über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maß-

grundsätzlich Einsicht in die sie betreffenden Krankenunterlagen zu gewähren; Kopien der Unterlagen sind gegen Erstattung der Kosten herauszugeben. Die Vorschrift erfährt zwei Einschränkungen:

Zum einen gilt das Einsichtsrecht von Patientinnen und Patienten nur für die sie direkt betreffenden Unterlagen. Sind in den Krankenakten Angaben zu Dritten enthalten, gilt diesen gegenüber die ärztliche Schweigepflicht. Solche Daten dürfen nur mit schriftlicher Einwilligung aller Betroffenen offenbart werden, ansonsten ist eine Schwärzung erforderlich.

Zum anderen kann lt. Rechtsprechung des Bundesverfassungsgerichts der Einsichtsanspruch in begründeten Einzelfällen beschränkt werden. Eine solche Einschränkung wird bei psychiatrischen Behandlungsunterlagen regelmäßig eher zu begründen sein als bei solchen, die sich auf den physischen Zustand der Patientinnen und Patienten beziehen. Gerade bei psychischen Störungen oder Erkrankungen kann durchaus ein medizinisch begründetes Patientenschutzinteresse bestehen, das allerdings im Einzelfall zu prüfen und ggf. auch nachzuweisen ist[25].

Die genannte Berufsordnung verzichtet auf einen in der Musterberufsordnung für die deutschen Ärztinnen und Ärzte, dort ebenfalls in § 10 Abs. 2, enthaltenen Hinweis, wonach vom Einsichtsrecht diejenigen Teile der Patientenunterlagen ausgenommen sind, welche subjektive Eindrücke oder Wahrnehmungen der Ärztin/des Arztes enthalten. Nach ständiger Rechtsprechung des Bundesgerichtshofes ist eine solche Beschränkung des Einsichtsrechts auf objektive Befunddaten durchaus zulässig. Das Bundesverfassungsgericht hat diese Auffassung grundsätzlich bestätigt, allerdings mit der Einschränkung, dass eine pauschale Restriktion der Patientenrechte verfassungsrechtlich bedenklich sei. Über den Umfang des Einblicks in Patientenakten, die subjektive Wertungen enthalten, sollte demnach stets im Einzelfall entschieden werden. Die Aufsichtsbehörde für den Datenschutz hält eine generelle Beschneidung der Rechte Betroffener jedenfalls für unzulässig.

Da § 10 der Berufsordnung nur das Einsichtsrecht regelt, ist neben dem Einsichtsrecht nach der Berufsordnung auch ein dem Wortlaut der Vorschrift nach weitergehender Auskunftsanspruch nach § 34 Abs. 1 BDSG denkbar. Demnach können Betroffene Auskunft verlangen über

- die zu ihrer Person gespeicherten Daten, auch über deren Herkunft,
- Empfänger oder Kategorien von Empfängern und
- den Zweck der Speicherung.

Von einer Auskunft kann hier nur unter sehr engen Voraussetzungen abgesehen werden, diese sind in § 34 Abs. 4 BDSG geregelt.

§ 34 Abs. 1 BDSG bedarf der weiteren Auslegung unter den Vorgaben der Rechtsprechung. Die Möglichkeit, den Betroffenen nur objektive Daten mitzuteilen bzw. zu offenbaren, kann demzufolge auch dem Auskunftsanspruch nach dem BDSG Grenzen setzen. Zudem gilt inzident auch hier, dass schutzwürdige Belange Dritter zu beachten sind.

---

nahmen die erforderlichen Aufzeichnungen zu machen. Diese sind nicht nur Gedächtnisstützen für den Arzt, sie dienen auch dem Interesse des Patienten an einer ordnungsgemäßen Dokumentation.

2. Der Arzt hat dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren. Auf Verlangen sind dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben.

[25] Dies bedeutet in der Praxis, dass in solchen Fällen die Patientinnen und Patienten vor ihren eigenen Daten „geschützt“ werden müssen.

Entlassungsberichte dienen der Dokumentation des Behandlungsergebnisses und enthalten in der Regel mehr objektive Informationen über die Betroffenen als beispielsweise eine subjektiv ergänzte Krankenakte. Was die Einsichtnahme in Entlassungsberichte betrifft, gelten dieselben Regelungen wie für die Auskunft aus den Krankenakten. Grundsätzlich besteht somit nach § 10 Abs. 2 der Berufsordnung für Ärztinnen und Ärzte im Saarland wie auch nach § 34 Abs. 1 BDSG ein Anspruch sowohl auf Kenntnisnahme durch die Betroffenen wie auch auf Anfertigung von Kopien, ein Recht auf deren Übersendung wird hierdurch allerdings nicht statuiert. Auch für Entlassungsberichte gilt, dass eine pauschal festgelegte Nichtherausgabe unzulässig ist.

Einsicht in die Krankenakte – Ein konkreter Fall

Wie oben erläutert, haben Patientinnen und Patienten ein sehr weit reichendes Einsichtsrecht in die Krankenakten. Keineswegs handelt es sich hierbei um geistiges Eigentum der Ärzte, sondern vorrangig um personenbezogene Daten der Behandelten.

Im Berichtsraum wandte sich ein Betroffener an die Aufsichtsbehörde für den Datenschutz und gab an, ein Arzt, bei dem er kurzfristig in Behandlung gewesen sei, verweigere ihm die Einsicht in die Krankenakte. Auf Nachfrage bei dem Arzt stellte sich heraus, dass der Petent vor einigen Jahren vom Vorgänger des jetzigen Praxisinhabers behandelt wurde. Ob dieser dem Betroffenen seinerzeit die Einsicht in die Krankenakte verweigerte, ließ sich nicht mehr nachvollziehen. Allerdings war dem Petenten bereits angeboten worden, die jetzt für eine gerichtliche Auseinandersetzung erforderlichen Unterlagen auf Anforderung des Gerichts dorthin zu übersenden. Der Arzt erklärte weiter, dass er dem Petenten auch jederzeit die Einsicht in die Unterlagen ermögliche, wenn dies gewünscht sei.

Letztlich hatte die Aufsichtsbehörde für den Datenschutz eine Reihe von Missverständnissen aufzuklären:

Nach der Darstellung des Arztes fordert das Gericht üblicherweise die Unterlagen an, die daraufhin übersandt werden; dies war dem Betroffenen so auch angeboten worden. Der Arzt wartete folglich auf die Anforderung des Gerichts und gab die Unterlagen eben nicht an den ehemaligen Patienten weiter. Dieser vermutete allerdings wohl, der Arzt weigere sich, die Patientenakte an ihn herauszugeben und wandte sich an die Aufsichtsbehörde für den Datenschutz. Der Schilderung des Betroffenen zufolge wiederum wurde hier die Akteneinsicht ohne erkennbaren Grund verweigert. Nach Klärung dieser Missverständnisse konnten keine Verstöße gegen datenschutzrechtliche Vorschriften festgestellt werden.

Ärztliches Inkasso

Viele Ärztinnen und Ärzte rechnen die Behandlung von Privatpatientinnen und Patienten nicht selbst ab, sondern überlassen die Rechnungslegung und das Inkasso privatärztlichen Verrechnungsstellen. Hierbei existieren grundsätzlich zwei verschiedene Modelle:

- 1. Abrechnung und Inkasso werden übertragen und die/der jeweilige Ärztin/Arzt bleibt Forderungsinhaber/in. Vorteil dieses Verfahrens ist, dass sich der Verwaltungsaufwand in der Praxis verringert und die Kosten in Form eines Abschlags zu Gunsten der Verrechnungsstelle vergleichsweise niedrig sind.
- 2. Die Forderung selbst wird abgetreten („Zession“) und die Inkassostelle wird Inhaberin der Forderung. Der Vorteil für die jeweilige Ärztin/den Arzt liegt neben dem ebenfalls geringeren Verwaltungsaufwand darin, dass die Rechnungen in jedem Fall beglichen werden und zwar durch die Inkassostelle. Ein sog. „Forderungsausfall“ wird dadurch vermieden.

Datenschutzrechtlich zulässig sind beide Modelle, wenn die betroffenen Patientinnen und Patienten in die Datenübermittlung an die Abrechnungs-/Inkassostelle eingewilligt haben. Ansonsten liegt ein Bruch der ärztlichen Schweigepflicht vor, der nach § 203 des Strafgesetzbuches mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft werden kann.

In einem Fall wandte sich ein Petent aus einem anderen Bundesland an die Aufsichtsbehörde für den Datenschutz. Diesem wurde von seinem behandelnden Arzt die Bekanntgabe des Untersuchungsbefundes mit der Begründung verweigert, er sei offensichtlich nicht ausreichend solvent. Unter solchen Umständen könne er ihm das Ergebnis nur gegen Bar- bzw. Scheckzahlung mitteilen. Im Verlaufe des Gesprächs zwischen Arzt und Patient habe sich dann herausgestellt, dass der Arzt seine Forderung einer saarländische Inkassostelle angeboten habe, wobei zeitgleich noch eine Art Online-Bonitätsprüfung vorgenommen worden sei. Hierbei sei dem Arzt durch einen „gelben Punkt“ signalisiert worden, dass es mit der Bonität des Betroffenen nicht zum Besten bestellt sei.

Die Nachforschungen der Aufsichtsbehörde für den Datenschutz zeigten dann, dass diese Darstellung nicht ganz zutraf. Das hiesige Unternehmen kauft tatsächlich bundesweit Forderungen von Vertragsärztinnnen und -ärzten an. Das Procedere ist so ausgestaltet, dass die Ärztin bzw. der Arzt zu Beginn der Behandlung online eine Kaufanfrage stellt, über die das Inkassounternehmen entscheidet. Hierbei werden dem Unternehmen bestimmte personenbezogene Daten übermittelt. Entschließt es sich zum Ankauf, wird im wahrsten Sinne des Wortes „grünes Licht“ auf dem Bildschirm gegeben, wird die Kaufanfrage negativ beschieden, erfolgt die Antwort in Form eines roten Punktes; gelb bedeutet nach Auskunft des Unternehmens lediglich einen vorläufigen Status, der keine Schlüsse auf die endgültige Antwort zuließe.

Datenschutzrechtlich ist dieses Verfahren dann zulässig, wenn die Betroffenen vorher in die Übermittlung ihrer personenbezogenen Daten eingewilligt haben. Dem war hier so. Der betroffene Patient hatte der Datenweitergabe zu Abrechnungszwecken zugestimmt. Ebenfalls zulässig ist nach Ansicht der Aufsichtsbehörde die sog. „Bonitätsprüfung“ durch das hiesige Unternehmen. Bei dieser Bonitätsprüfung werden die vom Anbieter übermittelten Daten mit dem Datenbestand des Inkassounternehmens sowie unter Umständen mit externen Informationen abgeglichen. Auf Basis des so erlangten Wissens erfolgt die Entscheidung über den Ankauf.

Bedenklich hingegen erscheint das Verhalten des behandelnden Arztes, der – unabhängig von einem möglichen Verstoß gegen die für ihn geltende Berufsordnung und seine Pflichten aus dem Behandlungsvertrag – dem Patienten auch dessen Recht auf Kenntnis der Krankenakte verweigerte.

Gesund oder krank - Datenschutz bei Angehörigen anderer Heilberufe

Heilberufe im weitesten Sinn sind alle Berufsausübungen, die sich mit der Vorbeugung sowie dem Erkennen und Behandeln von Krankheiten befassen. Hierbei fallen wie bei der Behandlung durch Ärztinnen und Ärzte medizinische Daten an, Angaben also, die nach § 3 Abs. 9 BDSG immer als besonders sensibel gelten. Die Regelungen zum Schutz medizinischer Daten sind jedoch alles andere als eindeutig und leicht verständlich. Die bereits erwähnte Schweigepflicht der „Berufsordnung für Ärztinnen und Ärzte des Saarlandes“ gilt beispielsweise nicht für Heilpraktiker/innen, Masseurinnen und Masseure, Krankengymnasten/innen, Ergotherapeuten/innen, orthopädische Schuhma-

cher/innen oder medizinische Fußpfleger/innen[26]. Die Datenverarbeitung richtet sich daher hauptsächlich nach dem Bundesdatenschutzgesetz. Danach ist das Erheben, Verarbeiten und Nutzen personenbezogener Daten zulässig, wenn es für die Gesundheitsvorsorge, die Diagnostik, die Gesundheitsverwaltung, die Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist. Bestimmend für die Datenverarbeitung ist hier der Zweck, also die zu erbringende medizinische Leistung. Wird eine solche Leistung durch Angehörige einer anderen Berufsgruppe erbracht als durch ärztliches Personal oder durch Personen, die einer vergleichbaren Geheimhaltungspflicht unterliegen, müssen sich diese strikt an die für Ärzte geltenden Vorschriften halten (§ 28 Abs. 7 BDSG).

Kreditschutzorganisationen/Auskunfteien

In wirtschaftlich schwierigen Zeiten mit hoher Arbeitslosigkeit rückt die Arbeit von Kreditschutzorganisationen und klassischen Wirtschaftsauskunfteien stärker in den Blickpunkt der Aufsichtsbehörde für den Datenschutz. Hohe private Schulden und die hohe Arbeitslosigkeit auch unter Darlehensnehmern bedingen häufiger Zahlungsunfähigkeiten und Insolvenzen als zu Zeiten wirtschaftlichen Wohlstandes. Diese Erkenntnis zwingt die Banken als Darlehensgeber zu möglichst genauen Bonitätseinschätzungen, perspektivisch realistischer Abwägungen des Kreditrisikos. Von nicht zu unterschätzender Bedeutung sind hierbei die Informationen von Kreditschutzorganisationen und Auskunfteien, da sie mittlerweile häufig allein ausschlaggebend für die Entscheidung der Darlehensgeber sind. Richtige Daten, zutreffender: Informationen, sind folglich vielfach Hauptgrundlage für Kreditentscheidungen. Die folgenden beiden Fälle lassen erahnen, wie Fehler in einem komplexen Informationssystem entstehen können.

Der fehlerhafte Eintrag 1

Eine Petentin musste feststellen, dass sie bei ihrer eigenen Hausbank plötzlich unter einer anderen Adresse geführt wurde. Wäre sie tatsächlich umgezogen, hätte diese Erkenntnis sie nicht weiter überrascht. Da dem jedoch nicht so war, bat sie die Bank um eine Erklärung für diesen plötzlichen virtuellen Wohnungswechsel. Es stellte sich heraus, dass eine Kreditschutzorganisation der Bank den vermeintlichen Umzug mitgeteilt hatte. Bei der „neuen“ Adresse handelte es sich um die eines Arbeitskollegen der Petentin. Mit diesem unterhielt sie die Betriebskaffeekasse in Form eines Sparkontos bei einer anderen Bank. Beide waren offenbar im Besitz einer Kontovollmacht, als Adresse war jedoch lediglich die des Arbeitskollegen angegeben. Diese Adresse wurde nun Jahre später als Adresse der Petentin an die Kreditschutzorganisation übermittelt. Jene informierte ihrerseits die Hausbank der Betroffenen über die vermeintliche Adressänderung.

Der Fehler lag hier in der ungeprüften Adressweitergabe durch die Bank, bei der das Sparkonto geführt wurde. Diese ist auf Grund vertraglicher Verpflichtungen gehalten, auch Adressänderungen an die Kreditschutzorganisation zu melden. Diese wiederum hat bei der Vielzahl der ihr gemeldeten Datensätze nicht die Möglichkeit, jede einzelne Meldung zu verifizieren, sondern muss sich letztlich darauf verlassen (können), dass die Vertragspartner nur zutreffende Informationen weitergeben. Liegt wie hier ein Organisationsversagen der Bank vor, bleibt der Kreditschutzorganisation nur, den fehlerhaften Eintrag nachträglich zu korrigieren. Die Ursache für den Fehler konnte im Übrigen nicht ergründet werden, weil die falsch meldende Bank ihren Sitz nicht im Saarland hat.

[26] Sie fallen allerdings teilweise unter die Strafvorschriften des § 203 des Strafgesetzbuches, der unter anderem den Bruch der ärztlichen Schweigepflicht unter Strafe stellt.

Der fehlerhafte Eintrag 2

Der vorstehend beschriebene Falscheintrag ist möglicherweise auf eine unsensible EDV-Routine bei dem Partnerunternehmen einer Kreditschutzorganisation zurückzuführen, die bei Abweichungen ohne weitere Prüfung Korrekturbefehle veranlasste. Beim folgenden Sachverhalt dagegen liegt die Verantwortung ausschließlich bei der Kreditschutzorganisation.

Ein Haftbefehl zur Abgabe einer eidesstattlichen Versicherung über die persönlichen Vermögensverhältnisse ist kein Anzeichen für eine besonders gute Bonität oder eine hohe Zahlungsmoral, bedeutet er doch nichts anderes, als dass gegen die betreffende Schuldnerin oder den Schuldner ein erfolgloses Mahnverfahren betrieben wurde und auch die Zwangsvollstreckung bereits im Ansatz wegen fehlender Mitwirkung scheiterte. Ein sichererer Kreditverhinderer als ein solcher Eintrag ist kaum denkbar. Umso verhängnisvoller, wenn der Eintrag falsch ist.

Wohnen Mutter und Tochter zusammen in einem Haushalt, ist dies sicherlich nicht weiter bemerkenswert, tragen beide ähnliche Vornamen, kann dies – wenn das Geburtsdatum nicht bekannt ist – unter Umständen zu Verwechselungen führen. In der Regel ist dies unproblematisch, lassen sich doch solche Irritationen relativ leicht beheben. Kritisch wird es jedoch, wenn gegen eine der beiden ein Haftbefehl zur Abgabe einer eidesstattlichen Versicherung erlassen wird, der jedoch durch die Kreditschutzorganisation der anderen zugeordnet wird. So in einem der Aufsichtsbehörde für den Datenschutz vorgetragenen Fall:

Ein Amtsgericht in einem anderen Bundesland hatte gegen eine der beiden Frauen einen Haftbefehl erlassen. In der Verfügung waren Vornamen, Namen und Adresse aufgeführt, offenbar nicht jedoch das Geburtsdatum. Der Haftbefehl wurde danach ins Schuldnerverzeichnis aufgenommen. Die Kreditschutzorganisation wiederum hatte nach Auswertung der Schuldnerverzeichnisdaten den Haftbefehl der anderen Frau zugeordnet.

Sowohl das Amtsgericht als auch die Kreditschutzorganisation selbst bestätigten, dass der Haftbefehl nicht die Petentin beträfe, sondern die namensähnliche Verwandte. Hier lag ganz eindeutig ein Fehler der Kreditschutzorganisation vor. Die Falschzuordnung war nach deren Auffassung auf die teilweise identischen Vornamen und die identischen Adressen zurückzuführen. Solchen Fehlern kann allerdings vorgebeugt werden, indem die Datenquellen – hier: die Abdrucke und Listen aus dem Schuldnerverzeichnis – genauer ausgewertet werden und in Zweifelsfällen nachgeforscht wird. Die möglichen weit reichenden Folgen eines Falscheintrags rechtfertigen diesen Mehraufwand.

Verträge sind einzuhalten

„Pacta sunt servanda – Verträge sind einzuhalten“. So lautet einer der wichtigsten Grundsätze im Rechtsverkehr. Dass dieser Grundsatz nicht immer beachtet wird, belegen die beiden nachfolgend geschilderten Fälle.

Autokauf und Kreditvertrag

Ein Petent hatte den Kauf eines neuen Wagens über die Hausbank des Händlers finanziert. Bereits nach kurzer Zeit gab er den Wagen, mit dem er nicht zufrieden war, an den Händler zurück. Der Wagen jedoch war der Bank sicherungsübereignet, ein Verkauf hätte also nur mit deren Zustimmung erfolgen können. Die Rolle des Händlers erschöpfte sich hier zunächst darin, auf seinem Hof Platz für den Wagen zur Verfügung zu stellen. Folgenschwer war, dass der Petent die Zahlung der Kreditraten einfach einstellte. Auch nach mehrmaliger Mahnung kam er diesen Verpflichtungen nicht nach, so dass die Bank den Kredit kündigte und die Gesamtsumme fällig stellte, also die Zahlung

der Gesamtrestsumme aus dem Darlehensvertrag verlangte. In der Folge einigten sich Bank und Petent darüber, dass das Fahrzeug verkauft werden und der Petent eine eventuelle Differenz zwischen Verkaufspreis und Restschuld tragen sollte.

Die tatsächlich entstandene Restschuld wurde dem Petenten in Rechnung gestellt und eine Vereinbarung über eine Ratenzahlung getroffen. Dieser neuen Verpflichtung kam der Betroffene auf Grund seiner wirtschaftlichen Situation ebenfalls nicht nach. Die Bank beantragte daraufhin bei dem zuständigen Amtsgericht einen Mahnbescheid, gegen den kein Einspruch eingelegt wurde. Da der Schuldner die Forderung auch dann noch nicht beglich, wurde letztlich ein Vollstreckungsbescheid erlassen. Die Bank hatte einer Kreditschutzorganisation auf Grund ihrer vertraglichen Informationspflichten mitgeteilt, dass ein Mahnbescheid beantragt worden sei, woraufhin ein entsprechender Hinweis im Datensatz des Petenten aufgenommen wurde.

Im Zuge einer späteren Kreditanfrage erfuhr dieser von dem Eintrag in den Datenbeständen einer Kreditschutzorganisation, der einem Hypothekenkredit im Wege stand. Der Petent bestritt, dass er jemals einen Mahnbescheid erhalten habe. Die Nachforschungen der Aufsichtsbehörde für den Datenschutz haben Folgendes ergeben:

Der Mahnbescheid wurde tatsächlich beantragt und nach den Unterlagen der Bank auch zugestellt. Bei einer formellen Zustellung muss nicht durch persönliche Übergabe zugestellt werden, vielmehr kann die Zustellung auch durch Übergabe an einen anderen erwachsenen Familienangehörigen, der ebenfalls im Haushalt des Betroffenen wohnt, erfolgen. Äußerstenfalls besteht auch die Möglichkeit, ein Schriftstück durch Niederlegen an der angegebenen Adresse zuzustellen.

Für den Eintrag bei der Kreditschutzorganisation spielt allerdings der tatsächliche Zugang des Mahnbescheids keine Rolle; hier reicht es bereits aus, wenn der Mahnbescheid beantragt wurde. Eine Klausel im Vertrag zwischen Kreditgeber und –nehmer enthält einen eindeutigen Hinweis darauf, dass Daten über nicht vertragsgemäßes Verhalten an die Kreditschutzorganisation übermittelt werden dürfen. Die nötigen Voraussetzungen, einen Mahnbescheid zu beantragen, lagen vor und somit auch die für eine entsprechende Meldung an die Kreditschutzorganisation. Der Eintrag musste auch nicht gelöscht werden: Mitteilungen der Vertragspartner über nicht vertragsgemäßes Verhalten werden erst nach drei Kalenderjahren gelöscht, datenschutzrechtlich ist dies nicht zu beanstanden, da nach § 35 Abs. 1 Nr. 4 des Bundesdatenschutzgesetzes auch eine Speicherung für vier Kalenderjahre zulässig wäre. Erledigt sich die Forderung, wird ein sog. „Erledigungsvermerk“ [27] in die Auskunft aufgenommen.

Letzten Endes war der Eintrag darauf zurückzuführen, dass der Betroffene seinen Verpflichtungen aus dem Kreditvertrag und der anschließenden neuen Ratenzahlungsvereinbarung nicht nachgekommen ist. Wenn sich – wie hier letztlich offenbar auch - die wirtschaftlichen Bedingungen verschlechtern, sollte versucht werden, zusammen mit der Kredit gebenden Bank eine einvernehmliche Lösung zu finden. Ein solches Versäumnis ist - wie die folgende Schilderung zeigt - kein Einzelfall.

Bürogeräte und Kreditvertrag

In diesem Fall kaufte der Petent Bürogeräte, die er vollständig über einen Ratenkredit finanzierte. Kurz darauf wurde er arbeitslos und war nicht mehr in der Lage, die fälligen Raten zu zahlen. Auch dieser Kreditnehmer stellte die Zahlungen ein ohne die Bank über die Hintergründe zu informieren. Auf die erste Mahnung hin reagierte er mit einem

[27] Wenn Forderungen ausgeglichen sind, jedoch noch gespeichert und übermittelt werden dürfen, nimmt die Kreditschutzorganisation einen Hinweis auf die Erledigung in den Datensatz auf, den sog. „Erledigungsvermerk“.

Zahlungsvorschlag, der von der Bank nicht akzeptiert wurde. Wegen seiner finanziellen Lage konnte er auch weiterhin seinen Verpflichtungen nicht nachkommen. Nachdem auch die zweite Mahnung erfolglos blieb, wurde der Kredit gekündigt und die Gesamtforderung fällig gestellt. Die Auseinandersetzung mit der Bank endete schließlich in einem Vergleich, allerdings erst nach Abschluss des gerichtlichen Mahnverfahrens und nach Zustellung des Vollstreckungsbescheids.

Die Bank hatte einer Kreditschutzorganisation sowohl die Kündigung des Kredits als auch die offene Forderung (Saldo) mitgeteilt, ebenso dass ein Mahnbescheid beantragt worden sei. Die Kreditschutzorganisation führte die entsprechende Information mit Erledigungsvermerk noch in dem Datensatz des Betroffenen. Hiergegen wandte sich der Petent, mit dem Hinweis darauf, dass es ihm auf Grund des Negativeintrags unmöglich sei, eine neue Existenz zu gründen oder auch nur ein neues Girokonto zu eröffnen.

Verständlich das Bestreben, sich durch Tilgung der Negativauskunft eine Chance auf einen Neubeginn zu eröffnen. Aus Sicht der Aufsichtsbehörde für den Datenschutz liegt hier allerdings kein Verstoß gegen datenschutzrechtliche Bestimmungen vor. Das Verfahren selbst ist mit den Aufsichtsbehörden für den Datenschutz abgesprochen und als solches nicht zu beanstanden. Die Datenübermittlung durch die Bank und die Speicherung erfolgte rechtmäßig, dem Betroffenen wurde gar noch vor Kreditkündigung formularmäßig angeboten, den (Kredit-)Vertrag neu zu verhandeln. Weiter wurde auf die Möglichkeit eines gerichtlichen Mahnverfahrens und die Meldung bei der Kreditschutzorganisation hingewiesen. Ursächlich für die beanstandete Datenspeicherung war ausschließlich die Nichtzahlung der vereinbarten Raten.

Der Betroffene widersprach – nachdem die Aufsichtsbehörde keinen Verstoß feststellen konnte – der Speicherung seiner personenbezogenen Daten bei der Kreditschutzorganisation[28]. Die Prüfung durch die Kreditschutzorganisation ergab allerdings, dass hier kein besonderes schutzwürdiges Interesse vorliegt, das zu einer vorzeitigen Löschung führen könnte. Auch die Aufsichtsbehörde konnte eine solche Belastung nicht erkennen, da die Nichtgewährung von Krediten gerade keine außergewöhnliche Belastung in einer solchen Situation darstellt, sondern vielmehr zur Regel geworden ist.

[28] S. Hierzu auch „Häufig gestellt Fragen – Welche Rechte haben Betroffene?“

Versicherungen

Die Einwilligungsklausel

Verstöße gegen datenschutzrechtliche Vorschriften gehen häufig auf Unkenntnis, Bequemlichkeit oder unterschiedliche Auslegung der Rechtsgrundlagen zurück. Solche Erfahrungen machen alle Aufsichtsbehörden. Vor diesem Hintergrund war es für die Aufsichtsbehörde für den Datenschutz erstaunlich, dass eine Versicherung offen gegen ihre vertragliche Selbstverpflichtung verstieß.

Ein Petent wollte einen Unfallversicherungsvertrag abschließen und unterschrieb auch die Einwilligungsklausel[29] nach dem Bundesdatenschutzgesetz. Nicht einverstanden war er mit der weitergehenden Datennutzung für Finanzdienstzwecke und strich folglich die Allfinanzklausel[30]. Daraufhin verweigerte die Versicherung den Vertragsabschluss unter Hinweis auf eben diese Klausel. Diese sei Vertragsbestandteil und müsse vollständig akzeptiert werden, da ansonsten der Antrag nicht angenommen werden könne. Der Antragsteller verwies angesichts dessen auf die Formulierung in der Klausel selbst, wonach diese ohne Wirkung auf den Vertrag selbst gestrichen werden könne. Dieser Hinweis blieb jedoch vorerst erfolglos. Erst auf Initiative der Aufsichtsbehörde für den Datenschutz hin erklärte sich das Versicherungsunternehmen dazu bereit, künftig die Streichung der Allfinanzklausel zu akzeptieren, zumal diese ja auch jederzeit widerrufbar sei.

Bonitätsprüfungen bei Versicherungen

„Pacta sunt servanda – Verträge sind einzuhalten“, dies gilt auch für den Versicherungsbereich. Dort ist das Augenmerk der Versicherer selbst nicht nur auf den Vertragsabschluss gerichtet, sondern auch darauf, ob die Versicherungsnehmer/innen auch ihren Verpflichtungen – vor allem Mitwirkungspflichten und Prämienzahlung – nachkommen (können). Persönliche finanzielle Leistungsfähigkeit und subjektiver Leistungswille werden in aller Regel bereits vor Vertragsabschluss geprüft oder können zumindest geprüft werden.

Das Ergebnis einer solchen Bonitätsprüfung kann auch zur Ablehnung eines Vertrages führen, wie ein Petent erfahren musste. Dieser hatte sich an die Aufsichtsbehörde für den Datenschutz gewandt, weil eine Versicherung sich weigerte, einen Vertrag mit ihm abzuschließen. Der Betroffene vermutete, die Ablehnung sei auf einen Verstoß gegen datenschutzrechtliche Bestimmungen zurückzuführen.

Die Versicherung hingegen hatte hierzu dargelegt, dass im Rahmen der Antragsprüfung eine Bonitätsprüfung vorgenommen wurde. Zur Wahrung berechtigter Interessen aller Versicherten sei man gehalten, die gesetzlich zulässigen Mittel zur Erfüllung eigener Geschäftszwecke auszuschöpfen. Gemeint ist hiermit, dass „schlechte“ Risiken möglichst vermieden werden sollen. Im Ergebnis habe die Bonitätsprüfung im hier angesprochenen Fall dazu geführt, dass der Antrag des Petenten nicht angenommen wurde. Die Bonitätsprüfung selbst wurde durch eine Anfrage bei einer bundesweit tätigen Auskunftei vorgenommen.

Aus datenschutzrechtlicher Sicht war das Verhalten des Versicherers nicht zu beanstanden, da das Erheben personenbezogener Daten – auch zur Bonitätsbewertung – zulässig ist, wenn es der Zweckbestimmung eines Vertrages oder vertragsähnlichen

---

[29] S. hierzu auch „Häufig gestellte Fragen - Wozu dient die Einwilligungsklausel der Versicherungsunternehmen?“

[30] s. hierzu auch: „Häufig gestellte Fragen –
Wozu dient die Einwilligungsklausel der Versicherungsunternehmen?“

Vertrauensverhältnisses dient. Hierzu zählt auch die Entscheidung über ein Vertragsangebot.

Zivilrecht oder Datenschutzrecht

Bisweilen offenbart erst eine Gesamtschau die hinter einer Eingabe steckende Absicht und die einschlägige Rechtsmaterie. Versicherungen erheben für Ihre Aufgabenerfüllung personenbezogene Daten, sei es dass sie tatsächlich erforderlich sind für die Risikoabschätzung, sei es für die Ausarbeitung eines Angebots z.B. in Form einer Berufsunfähigkeitszusatzversicherung. Ziel einer solchen Versicherung ist es, eine Versorgungslücke zwischen dem letzten Gehalt und der Berufsunfähigkeitrente zu schließen. Vermieden werden soll hingegen eine Überversorgung, d.h. Leistungen die unter Umständen höher sind als das letzte Gehalt. Um beurteilen zu können, ob eine solche – für die/den Versicherte/n durchaus lukrative – Überversorgung eintreten könnte, prüfen die Versicherungen, ob die Höhe der Berufsunfähigkeitszusatzrente in einem angemessenen Verhältnis zu dem jeweiligen Einkommen steht. Grundlage für eine solche Prüfung ist ein Einkommensnachweis der Antragsteller/innen.

Ein Petent hatte sich an die Aufsichtsbehörde für den Datenschutz gewandt und die Forderung eines Versicherers nach einem solchen Nachweis moniert. Seine Berufsgruppe werde auf Grund firmeninterner Weisungen nur bis zu einem Festbetrag versichert, daher sei ein Einkommensnachweis nicht erforderlich und dürfe auch nicht verlangt werden.

Laut Stellungnahme des Versicherers werden bei Anträgen auf Berufsunfähigkeitszusatzversicherungen immer Einkommensnachweise gefordert. Vorliegend habe bereits eine Zusatzversicherung über eine Rentensumme von seinerzeit 1.000,-- DM bestanden, die letzten Endes auf 3.500,-- DM aufgestockt werden sollte. Dies sei von der Versicherung abgelehnt worden. Statt dessen habe man eine Gesamtversorgung in Höhe von 3.000,-- DM angeboten. Interne Richtlinien sähen die Prüfung einer eventuellen Überversorgung vor, aus diesem Grund sei bei allen Anträgen ein Einkommensnachweis erforderlich.

Aus datenschutzrechtlicher Sicht ist die Forderung nach einem Einkommensnachweis bei Anträgen auf Berufsunfähigkeitszusatzversicherungen durchaus nachvollziehbar. Die hier vorliegende Eingabe war denn auch – wie sowohl die Stellungnahme der Versicherung als auch die weiteren Ausführungen des Petenten zeigten - eher durch die Ablehnung der Versicherung motiviert als durch datenschutzrechtliche Überlegungen. Letzten Endes ging es also vornehmlich um eine Frage der Vertragsfreiheit und um die Zulässigkeit geschäftspolitischer Entscheidungen über den Abschluss von Verträgen. Solche Fragen sind jedoch allenfalls zivilrechtlich zu klären und unterliegen nicht der Bewertung der Aufsichtsbehörde für den Datenschutz.

Der Zusammenschluss zweier Versicherungen

Die Arbeit der Aufsichtsbehörde für den Datenschutz besteht - wie eingangs erwähnt - nicht nur aus Anlasskontrollen, sondern wird auch von Beratungstätigkeit geprägt. Der Zusammenschluss zweier Versicherungsgesellschaften unter dem Dach einer einheitlichen Holding stellte hier einen Schwerpunkt dar. Beide Gesellschaften werden auch in der neuen Konzernstruktur als rechtlich selbstständige Unternehmen weitergeführt.

Aus datenschutzrechtlicher Sicht relevant war die künftige Struktur der Datenverarbeitung: Diese sollte nicht etwa analog zu der Konzernstruktur konzipiert werden, vielmehr sollte ein Austausch personenbezogener Daten zum Zwecke der Vertrags- und Leistungsbearbeitung innerhalb des Konzerns erfolgen. Da beide Unternehmen als rechtlich selbständige Unternehmen weiterhin verantwortliche Stellen bleiben, ist hierin eine Übermittlung personenbezogener Daten zu sehen.

Aus Sicht der Aufsichtsbehörde für den Datenschutz ist die Verarbeitung personenbezogener Daten von Neukunden in der neuen Konzernstruktur unproblematisch, da bei diesen die Einwilligung in den konzernweiten Datenaustausch mit dem Vertragsangebot eingeholt werden kann. Die entsprechenden Formulierungen wurden mit der Aufsichtsbehörde für den Datenschutz abgestimmt. Anders hingegen stellt sich die geplante Verarbeitung der bereits vorhandenen Kundendaten dar.

§ 4 BDSG erlaubt jegliche Datenverarbeitung nur, wenn sie durch Gesetz bzw. sonstige Rechtsvorschrift erlaubt ist oder die Betroffenen hierin einwilligen. Eine Rechtsvorschrift war hier nicht erkennbar, so dass die Übermittlung nur auf Grundlage einer Einwilligung der Betroffenen zulässig sein kann. Die Versicherung bat uns zu prüfen, ob wegen der großen Zahl der Versicherten nicht auch die Annahme einer stillschweigenden Einwilligung der Betroffenen zulässig sei.

Form und Voraussetzungen einer wirksamen Einwilligung sind in § 4a BDSG geregelt. Danach bedarf diese der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form objektiv angemessen ist. Es genügt nicht, dass eine andere Form angemessen erscheint, also auf den ersten Blick praktikabler ist. Eine objektives Kriterium kann in den besonderen Umständen der beabsichtigten Datenverarbeitung liegen, so etwa Zeitdruck, Umfang der Datenverarbeitung etc. Regelmäßig wird in solchen Fällen eine (fern-) mündliche Einwilligung ausreichen, die Datenverarbeitung zu erlauben.

Nach Auffassung der Aufsichtsbehörde für den Datenschutz kann die hier geforderte stillschweigende oder konkludente Einwilligung hingegen nur in nochmals spezielleren Konstellationen wirksam zum Tragen kommen, da bei dieser Form der Zustimmung vom Einverständnis der Betroffenen in die beabsichtigte Datenverarbeitung ausgegangen wird. Mit anderen Worten: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist in einem solchen Fall zulässig bis die Betroffenen widersprechen. Im Hinblick auf die hohe Zahl der bei den beteiligten Unternehmen Versicherten war die beabsichtigte „Widerspruchslösung“ nach Auffassung der Aufsichtsbehörde für den Datenschutz vertretbar, da die ansonsten zu erwartenden geringen Rücklaufquoten kaum zu dem Ziel einer einheitlichen Bearbeitung führen könnten.

Selbstverständlich setzt auch die stillschweigende Einwilligung eine detaillierte Information der Betroffenen voraus. Die Anforderungen an die Qualität der Kundeninformation sind dabei höher als bei einer aktiven Willenserklärung der Betroffenen: Alle „Altkundinnen“ und „-kunden“ müssen daher bereits im Vorfeld über die geplante neue Struktur der Datenverarbeitung informiert werden. Da die Betroffenen ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können, muss die Kundeninformation einen entsprechenden Hinweis enthalten.

Die Aufsichtsbehörde für den Datenschutz vertrat die Auffassung, dass es wegen der besonderen Umstände hier ausreiche, mündlich zu widersprechen. Dem Widerspruch muss stattgegeben werden und er ist den Versicherten umgehend schriftlich zu bestätigen. Diese vereinfachte Form die Datenverarbeitung zu untersagen korrespondiert als Recht der Betroffenen mit der dem Unternehmen zugestandenen Form der Einwilligungserklärung.

Soweit all diese Voraussetzungen vorliegen, ist die Datenübermittlung innerhalb des neuen Versicherungskonzerns aus datenschutzrechtlicher Sicht zulässig. Bis Redaktionsschluss war noch nicht ersichtlich, wie weit die Umsetzung der rechtlichen Anforderungen in die Praxis gediehen ist, so dass eine endgültige Bewertung durch die Aufsichtsbehörde für den Datenschutz noch aussteht.

Datenlöschung durch Aktenvernichtung

Altakten sind Datenträger und daher datenschutzgerecht zu vernichten. Krankenakten am Papiercontainer sind der Alptraum einer jeden Datenschützerin und eines jeden Datenschützers.

In der DIN 32757 sind verschiedene Sicherheitsstufen und die Umsetzungen bei der Datenträgervernichtung geregelt. Ein einfaches Zerreißen ist schon deshalb wenig sachgerecht, weil die zulässige Partikelgröße – in dem Fall die „Schnipsel"-Größe – in den meist geforderten Sicherheitsstufen S 3 und S 4 gerade mal 320 mm^2 bzw. 30 – 90 mm^2 beträgt. Zum Vergleich: Ein 21 x 29,7 cm großes DIN A 4 Blatt hat eine Oberfläche von 62370 mm^2.

Um alte Unterlagen datenschutzgerecht zu entsorgen, bieten sich mehrere Alternativen an:

- Die Nutzung von hochwertigen Aktenschreddern, die die Anforderungen der genannten DIN-Norm erfüllen. Billigangebote sind demgegenüber meist nur eine teure Alternative zum eigenhändigen Zerreißen.
- Die Beauftragung eines Unternehmens, das die datenschutzgerechte Vernichtung von Datenträgern anbietet.

Solche Unternehmen stellen ihren Auftraggebern in aller Regel verschließbare Behältnisse zur Verfügung. Der Inhalt wird bei Bedarf abgefahren und vernichtet. Altakten werden dabei geschreddert und zu Papierpresslingen verarbeitet, die wiederum als Rohstoff für die Papier- oder Kartonherstellung – manchmal auch für neue Aktenordner – dienen.

Besonders kritisch ist die Zwischenlagerung bis zum Schreddern: Diese muss in einem geschlossenen Behälter erfolgen, der selbst wiederum unzugänglich aufbewahrt sein muss. Hierzu bietet sich eine Lagerung in einem verschlossenen Raum an.

Ein weiteres Augenmerk ist auf das Personal zu legen. Alle Beschäftigten, die personenbezogene Daten erheben, verarbeiten (⇨ löschen) oder nutzen, müssen auf das Datengeheimnis verpflichtet werden (§ 5 BDSG). Dies gilt selbstverständlich auch für Aktenvernichtungsunternehmen.

Die Aufsichtsbehörde für den Datenschutz wurde durch eine Eingabe darauf hingewiesen, dass ein Containerunternehmen, das auch Aktenvernichtung anbiete, vertrauliche Unterlagen offen unter freiem Himmel lagere. Auf Grund der Qualität dieser Vorwürfe wurde eine unangemeldete Kontrolle des Unternehmens durchgeführt. Der Containerdienst bot zu diesem Zeitpunkt schon seit längerem die Vernichtung von Altakten an und war auch bei der Aufsichtsbehörde für den Datenschutz im damaligen Register nach § 32 BDSG gemeldet.

Den Kunden wurden nach Darstellung des Unternehmens abschließbare 240-Liter-Gefäße zur Verfügung gestellt, die auf Anforderung abgefahren und gleichzeitig durch leere ersetzt würden. Die weitere Verarbeitung folge dem oben beschriebenen Verfahren.

Ob dem tatsächlich immer so war, konnte die Aufsichtsbehörde für den Datenschutz nicht feststellen, zum Zeitpunkt der Kontrolle allerdings waren die gemachten Vorwürfe unbegründet. Es waren keine Anhaltspunkte ersichtlich, dass das Unternehmen bei der Vernichtung von Altakten gegen datenschutzrechtliche Vorschriften verstieß.

Im Zusammenhang mit der Kontrolle des Containerdienstes wurde noch eine Vergleichskontrolle bei einem weiteren Aktenvernichtungsunternehmen durchgeführt. Dieses Unternehmen betreibt eine Großschredderanlage, die auch von anderen Firmen

genutzt wird. Technische Mängel oder Verstöße gegen datenschutzrechtliche Vorschriften waren auch hier nicht zu verzeichnen, eher das Gegenteil war der Fall. Technische Vorkehrungen und Ablauforganisation waren nahezu mustergültig.

Ordnungswidrigkeiten und Straftaten

Die vermutete Weitergabe von Auskunftei-Daten

Auskunfteien dürfen – wie vorne erwähnt – bestimmte personenbezogene Daten im Rahmen ihrer Tätigkeit erheben, speichern und übermitteln. Die Übermittlung der Daten setzt voraus, dass die Anfrager zunächst das berechtigte Interesse an der Auskunftserteilung darlegen. In aller Regel wird es sich um Bonitätsanfragen im weitesten Sinne handeln. In jedem Fall unzulässig ist die Anfrage aus privaten Gründen, vulgo: aus Neugierde. Dem steht bereits entgegen, dass als Voraussetzung für jede Datenübermittlung durch Auskunfteien ein berechtigtes, also ein objektiv nachvollziehbares Interesse gefordert wird.

Der Staatsanwaltschaft lag folgende Strafanzeige vor: Der Anzeigende hatte vorgetragen, ein naher Verwandter seiner Verlobten habe sich unberechtigt sog. „Schufa-Daten“ über ihn verschafft und diese weitergegeben. Da eine Strafbarkeit bereits grundsätzlich verneint wurde, hat die Staatsanwaltschaft den Fall an die Aufsichtsbehörde für den Datenschutz weitergeleitet.

Vertragspartner der Schufa können nur Kredit gewährende Unternehmen im weitesten Sinne sein. Der hier angesprochene Verwandte gehört nicht zu diesem Kundenkreis. Die Schufa hatte folglich auch auf Nachfrage bestätigt, dass keine Daten an den verdächtigten Anfrager übermittelt wurden.

„Schufa-Daten“ sind zunächst Auskünfte der Schufa selbst. Der Begriff wird jedoch auch als Synonym für die Datensammlungen von Wirtschaftsauskunfteien verwandt. Die Aufsichtsbehörde hat sich daher an die im Saarland ansässigen Auskunfteien gewandt und gebeten, zu überprüfen, ob und an wen personenbezogene Daten des Petenten übermittelt worden seien. Das Ergebnis war negativ: Auch von dieser Seite hatte der Verwandte der Verlobten keine Informationen erhalten. Übrig blieb von den saarländischen „Datenquellen“ nur noch die Industrie- und Handelskammer (IHK). Die zuständigen Amtsgerichte erstellen das sog. „Schuldnerverzeichnis“. Die IHK wiederum erstellt Listen mit Auszügen aus dem Schuldnerverzeichnis und übermittelt diese Listen auf Anfrage an ihre Mitglieder. Darüber hinaus werden auch Einzelanfragen beantwortet. Auf Nachfrage hin hat sich ergeben, dass auch die IHK nicht die Datenquelle sein kann: Zwar gehört der Verdächtigte zum Mitgliederkreis der IHK, er hatte jedoch weder Listen von dort bezogen, noch wurde eine Einzelanfrage zu dem Petenten gestellt.

Im Ergebnis konnte somit noch nicht einmal festgestellt werden, ob hier überhaupt personenbezogene Daten übermittelt wurden. Zwar waren die Angaben des Petenten bei der Staatsanwaltschaft sehr detailliert, die Aufsichtsbehörde für den Datenschutz konnte jedoch keine unrechtmäßige Datenübermittlung nachweisen.

Darüber hinaus erscheint es fraglich, ob der Vorgang datenschutzrechtlich gewürdigt werden könnte. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ausschließlich zu persönlichen oder familiären Zwecken - auch wenn Neugierde das eigentliche Motiv ist - wird vom Bundesdatenschutzgesetz nicht umfasst. Dies bedeutet, dass in solchen Fällen die dortigen Vorschriften nicht greifen. Wenn die hier vermutete Erhebung personenbezogener Daten des Petenten tatsächlich allein unter diesen Aspekten erfolgt wäre, könnte dies datenschutzrechtlich kaum beanstandet werden. Der Gesetzgeber hat den rein persönlichen und familiären Bereich – auch um einer weiteren formellen Verrechtlichung der Privatsphäre entgegenzuwirken – bewusst außen vor gelassen.

Die unzulässige Videoüberwachung

Der folgende Fall ist vielleicht für Philipp Marlowe oder Sam Spade alltäglich, nicht jedoch für die Aufsichtsbehörde für den Datenschutz:

Ein Mann betritt ein Geschäft und bemerkt dabei, dass dieses aus dem gegenüberliegenden Haus mit einer Kamera überwacht wird. Die Geschäftsinhaberin informiert den Kunden darüber, dass die Videoüberwachung von Ihrem geschiedenen Mann in Auftrag gegeben worden sei. Dieser vermute, sie habe ihre eigenen Einkünfte bei der Festsetzung des Ehegattenunterhalts zu niedrig angegeben und habe deshalb ein - mittlerweile auch ihr bekanntes - Detektivbüro beauftragt, ihr Geschäft zu überwachen.

Der Kunde wandte sich an die Aufsichtsbehörde für den Datenschutz, um zu erfahren, ob diese Videoüberwachung, die ja auch ihn direkt betraf, zulässig sei. Daraufhin wurde das Detektivbüro um Stellungnahme gebeten. Hierbei stellte sich heraus, dass das Geschäft in der Tat mehrfach mit Hilfe einer Videokamera und zumindest einmal durch einen Bediensteten der Detektei überwacht worden war.

Die Videobeobachtungen wurden sowohl vor als auch nach dem In-Kraft-Treten des novellierten Bundesdatenschutzgesetzes vorgenommen. Hierdurch ergeben sich verschiedene Bewertungen ein- und desselben Sachverhaltes: Die Beobachtung öffentlich zugänglicher Räume war nach alter Rechtslage nicht geregelt. Wegen des fehlenden Dateibezugs zumindest bei der Verwendung analoger Videotechnik war das BDSG daher nicht anwendbar. Denkbar gewesen wäre in dieser Situation allenfalls ein zivilrechtlicher Unterlassungsanspruch. Das neue BDSG hingegen regelt in § 6b die Zulässigkeit der Videoüberwachung. Demnach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Hilfsmitteln 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 dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

In Frage kam hier nur die dritte Alternative, die Wahrung berechtigter Interessen für konkret festgelegte Zwecke. Berechtigte Interessen können auch wirtschaftliche Interessen sein, wirtschaftliche Interessen sowohl des Ex-Mannes als Auftraggeber als auch der Detektei. Auch an einem konkret festgelegten Zweck fehlte es nicht: die Beobachtung des Ladenlokals zur Feststellung der Kundenzahlen.

Allerdings ging aus der Darstellung der Detektive nicht hervor, ob die Videobeobachtung auch tatsächlich erforderlich war. Erforderlich heißt, dass der verfolgte (zulässige!) Zweck sonst nicht, nicht mit zumutbarem Aufwand, nicht zeitgerecht oder nicht rechtmäßig erreicht werden kann. Eine Videoüberwachung zur bloßen Arbeitserleichterung scheidet aus. Das Detektivbüro hatte selbst dargelegt, dass zumindest einmal eine sog. „personelle Observierung“ durchgeführt wurde, somit war eine Videoüberwachung nach Einschätzung der Aufsichtsbehörde für den Datenschutz nicht erforderlich, da die Angaben zur Kundenfrequenz auf eine weniger belastende Art und Weise erhoben werden konnten. Selbst wenn man dieser Auffassung nicht folgen wollte, war die Videoüberwachung wegen der fehlenden Kennzeichnung unzulässig: § 6b Abs. 2 BDSG schreibt verbindlich vor, auf eine Videoüberwachung hinzuweisen. Jede solche Maßnahme ist erkennbar zu machen, wobei insbesondere auf den Verantwortlichen hingewiesen werden muss. Wenn diese Hinweise unterbleiben, darf eine Videoüberwachung nicht erfolgen.

Die Detektei wurde auf die rechtswidrige Videoüberwachung hingewiesen und gebeten, künftig die Vorschriften des Bundesdatenschutzgesetzes zu beachten. Auf ein Bußgeldverfahren, das wegen unbefugter Datenerhebung denkbar gewesen wäre, wurde verzichtet, da die Regelung zur Videoüberwachung erst während der Tätigkeit der Detektei eingeführt wurde und daher noch nicht bekannt war. Der Vertreter der Detektei wurde in einem ausführlichen persönlichen Gespräch nochmals auf die neue Rechtslage und die Möglichkeit, sich beim Bundesverband der Detektive weiter zu informieren, hingewiesen. Der erwähnte Kunde hat allerdings selbst Strafanzeige erstattet; ob die Staatsanwaltschaft tatsächlich ein Strafverfahren eingeleitet hat, war bei Redaktionsschluss noch nicht bekannt.

.

Adressen der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich und der Landesbeauftragten für den Datenschutz [31]

Bundesland	Oberste Aufsichtsbehörde	Regional zuständige Aufsichts-behörde	Landesbeauftragte/r für Daten-schutz
Baden-Württemberg	Innenministerium Baden-Württemberg Dorotheenstraße 6 70173 Stuttgart 07 11 / 231 – 32 50 Fax: 23 1 – 32 99 poststelle@im.bwl.de http://www.innenministerium.baden-wuerttemberg.de/		Der Landesbeauftragte für den Daten-schutz in Baden-Württemberg Marienstraße 12 70178 Stuttgart 07 11 / 61 55 41 – 0 Fax: 61 55 41 – 15 poststelle@lfd.bwl.de http://www.baden-wuerttemberg.datenschutz.de
Bayern	Bayerisches Staatsministerium des Inneren Odeonsplatz 3 80539 München 0 89 / 21 92 – 25 85 Fax: 21 92 – 1 22 66 poststelle@stmi.bayern.de http://www.innenministerium.bayern.de	Regierung von Mittelfranken Promenade 27 (Schloss) 91522 Ansbach 09 81 / 53-0 Fax: 09 81 / 53-12 06 poststelle@reg-mfr.bayern.de http://www.regierung.mittelfranken.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 http://www.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 http://www.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 http://www.datenschutz-berlin.de/

[31] Die hier aufgeführten Links verweisen mit Ausnahme unserer eigenen Adresse (http://www.innen.saarland.de) auf externe Angebote. Für die Inhalte der verlinkten Seiten ist der jeweilige Anbieter verantwortlich. Die Aufsichtsbehörde für den Datenschutz übernimmt insoweit keine Haftung.

Bundesland	Oberste Aufsichtsbehörde	Regional zuständige Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Brandenburg	Innenministerium des Landes Brandenburg Henning-von-Tresckow-Straße 9-13, 14467 Potsdam 03 31 / 8 66 - 0 Fax: 03 31 / 8 66 – 23 02 http://www.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 http://www.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 http://www.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 http://www.datenschutz-bremen.de/
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg 0 40 / 4 28 41 – 20 44/45 Fax: -23 72 office@datenschutz.hamburg.de http://www.hamburg.datenschutz.de/		Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg 0 40 / 4 28 41 – 20 44/45 Fax: -23 72 office@datenschutz.hamburg.de www.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 / 9 32 09 – 13 02 http://www.hmdi.hessen.de/	Regierungspräsidium Darmstadt Luisenplatz 2 64283 Darmstadt 0 61 51 / 12 – 0 Fax: 12 – 26 50 datenschutz@rpda.hessen.de http://rpda.de	Der Hessische Datenschutzbeauftragte Uhlandstr. 4 65189 Wiesbaden 06 11 / 14 08 – 0 Fax: 06 11 / 14 08 – 9 00 poststelle@datenschutz.hessen.de http://www.datenschutz.hessen.de

Bundesland	Oberste Aufsichtsbehörde	Regional zuständige Aufsichts-behörde	Landesbeauftragte/r für Daten-schutz
Mecklenburg-Vorpommern	Innenministerium Mecklenburg-Vorpommern Arsenal am Pfaffenteich Wismarsche Straße 133 19048 Schwerin http://www.mv-regierung.de/im/		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 http://www.datenschutz.mvnet.de/
Niedersachsen	Niedersächsisches Innenministerium Lavesallee 6 30169 Hannover 05 11 / 1 20 – 0 Fax: 1 20 – 65 50 http://www.mi.niedersachsen.de/	Der Landesbeauftragte für den Daten-schutz Brühlstraße 9 30169 Hannover 05 11 / 1 20 – 45 52 Fax: 1 20 – 45 91 poststelle@lfd.niedersachsen.de http://www.lfd.niedersachsen.de	Der Landesbeauftragte für den Daten-schutz Brühlstraße 9 30169 Hannover 05 11 / 1 20 – 45 52 Fax: 1 20 – 45 91 poststelle@lfd.niedersachsen.de http://www.lfd.niedersachsen.de
Nordrhein-Westfalen	Innenministerium des Landes Nord-rhein-Westfalen Haroldstraße 5 40213 Düsseldorf 02 11 / 8 71 – 01 Fax: 8 71 – 33 55 poststelle@im.nrw.de http://www.im.nrw.de/	Die Landesbeauftragte für Datenschutz und Informationsfreiheit Reichsstraße 43 40217 Düsseldorf 02 11 / 3 84 24 – 0 Fax: 3 84 24 – 15/16 poststelle@ldi.nrw.de http://www.ldi.nrw.de/ http://www.lfd.nrw.de	Die Landesbeauftragte für Datenschutz und Informationsfreiheit Reichsstraße 43 40217 Düsseldorf 02 11 / 3 84 24 – 0 Fax: 3 84 24 – 15/16 poststelle@ldi.nrw.de http://www.ldi.nrw.de/ http://www.lfd.nrw.de
Rheinland-Pfalz	Ministerium des Innern und für Sport Schillerstraße 3 – 5 55116 Mainz 0 61 31 / 16 – 0 Fax: 33 69 http://ism.rlp.de	Aufsichts- und Dienstleistungsdirektion Trier Willy-Brandt-Platz 3 54290 Trier 06 51 – 94 94 – 0 Fax: 9 4 94 – 1 79 poststelle@add.rlp.de http://www.add.rlp.de/	Der Landesbeauftragte für den Daten-schutz Rheinland-Pfalz Deutschhausplatz 12 55116 Mainz 0 61 31 / 2 08-24 49 Fax: 2 08-24 97 poststelle@datenschutz.rlp.de http://www.datenschutz.rlp.de

Bundesland	Oberste Aufsichtsbehörde	Regional zuständige Aufsichts-behörde	Landesbeauftragte/r für Daten-schutz
Saarland	Ministerium für Inneres und Sport Franz-Josef-Röder-Straße 21 66119 Saarbrücken 06 81 / 5 01 – 00 06 81 / 9 62 – 16 30 Fax: 9 62 – 16 05 datenschutz@innen.saarland.de http://www.innen.saarland.de		Landesbeauftragter für Datenschutz Fritz-Dobisch-Straße 12 66111 Saarbrücken 06 81 / 9 47 81 – 15 Fax: 9 47 81 – 29 ldf-saar@t-online.de http://www.lfd.saarland.de/
Sachsen	Sächsische Staatsministerium des Innern Wilhelm-Buck-Straße 2 01097 Dresden 03 51 / 5 64 – 0 Fax: 5 64 – 32 79 datenschutz@smi.sachsen.de http://www.sachsen.de/de/bf/staatsregierung/ministerien/smi/index.html	Regierungspräsidium Chemnitz Altchemnitzer Straße 41 09120 Chemnitz 03 71 / 5 32 – 11 49 Fax: 5 32 – 11 59 post@rpc.sachsen.de http://www.rpc.sachsen.de/content_page_1.html Regierungspräsidium Dresden Stauffenbergallee 2 01076 Dresden 03 51 / 8 25 – 14 20 Fax: 8 25 – 91 42 datenschutz@rpdd.sachsen.de www.rp-dresden.de/ds Regierungspräsidium Leipzig Braustraße 2 04013 Leipzig 03 41 / 9 77 – 14 41 9 77 – 14 99 poststelle@rpl.sachsen.de http://www.rpl.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 http://www.datenschutz.sachsen.de

Bundesland	Oberste Aufsichtsbehörde	Regional zuständige Aufsichts-behörde	Landesbeauftragte/r für Daten-schutz
Sachsen-Anhalt	Ministerium des Landes Sachsen-Anhalt Halberstädter Straße 2 39112 Magdeburg 03 91 / 5 67 – 01 Fax: 5 67 – 54 53/ 52 90 http://www.mi.sachsen-anhalt.de/	Regierungspräsidium Halle Willy-Lohmann-Straße 7 06114 Halle 03 45 / 5 14 – 0 Fax: 5 14 1 44 poststelle@rph.mi.lsa-net.de	Der Landesbeauftragte für den Daten-schutz Sachsen-Anhalt Berliner Chaussee 9 39114 Magdeburg 03 91 7 8 18 03 – 0 Fax: 03 91 / 8 18 03-33 http://www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Da-tenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel 04 31 / 9 88 – 12 00 Fax: 9 88 – 12 23 mail@datenschutzzentrum.de http://www.datenschutzzentrum.de		Unabhängiges Landeszentrum für Da-tenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel 04 31 / 9 88 – 12 00 Fax: 9 88 – 12 23 mail@datenschutzzentrum.de http://www.datenschutzzentrum.de
Thüringen	Innenministerium des Landes Thürin-gen Steigerstraße 24 99096 Erfurt 03 61 / 3 79 – 00 Fax: 3 79 – 37 04 http://www.thueringen.de/de/tim/	Thüringer Landesverwaltungsamt Weimarplatz 4 99423 Weimar 0 36 43 / 5 87-2 58 Fax: 0 36 43 / 5 87-1 90	Der Thüringer Landesbeauftragte für den Datenschutz Johann-Sebastian-Bach-Straße 1 99096 Erfurt 03 61 / 3 77 - 9 00 03 61 / 3 77 - 19 04 poststelle@datenschutz.thueringen.de http://www.datenschutz.thueringen.de/

Bundesbeauftragter für Datenschutz	Der Bundesbeauftragte für den Datenschutz Friedrich-Ebert-Straße 1 53173 Bonn 02 28 / 8 19 95 – 0 Fax:8 19 95 – 5 50 poststelle@bfd.bund.de http://www.datenschutz.bund.de