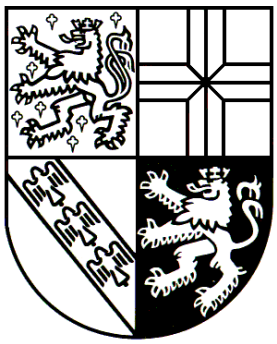

2. Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich

Berichtszeitraum

2003 / 2004

Impressum:

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

Hausanschrift:
Mainzer Straße 136
66121 Saarbrücken
Telefon: 0681 / 962 – 1630, 1631, 1634
Telefax: 0681 / 962 – 1605
E-Mail: datenschutz@innen.saarland.de
www.innen.saarland.de

Liebe Bürgerinnen und Bürger,

beim Lesen des zweiten Tätigkeitsberichts der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich wird deutlich vor Augen geführt, in wie vielen Lebensbereichen tagtäglich personenbezogene Daten erhoben, verarbeitet oder genutzt werden - sei es beim Abschluss eines Mietvertrages, einem Vereinsbeitritt, beim Einkauf oder aber bei der Teilnahme an einem Preisrätsel, überall fällt eine Fülle von Daten an. Erstaunlicherweise scheinen aber viele von uns im Umgang mit ihren Daten zunächst recht großzügig zu sein – vielleicht auch, weil sie viele Gefahren und Möglichkeiten, die mit der Preisgabe ihrer Daten verbunden sind, zunächst gar nicht erkennen.

Der Bericht gibt insoweit nicht nur einen Überblick über die bei der Aufsichtsbehörde für den Datenschutz auflaufenden Probleme vieler Bürgerinnen und Bürger, sondern bietet dem Einzelnen darüber hinaus die Möglichkeit, sich selbst für Datenschutzfragen und –probleme zu sensibilisieren. Nutzen Sie die Möglichkeiten und wenden auch Sie sich bei Fragen und Problemen im Datenschutz an die Aufsichtsbehörde für den Datenschutz beim Ministerium für Inneres, Familie, Frauen und Sport.

Ihre

Anngret Kramp-Karrenbauer

Inhaltsverzeichnis

	Seite
Häufig gestellt Fragen - FAQs :	**5**
Für wen gilt das Bundesdatenschutzgesetz?	5
Was sind nicht öffentliche Stellen?	6
Was versteht man unter „Homebanking“ und welche speziellen Risiken sind damit verbunden?	6
Welche Rechtsvorschriften sind beim Vereinsauftritt im Internet zu beachten?	9
Was bedeutet „Scoring“?	15
Sind Warndateien zulässig?	16
Unter welchen Voraussetzungen ist eine Videoüberwachung zulässig?	19
Was sind biometrische Daten und wie können oder dürfen sie erhoben, verarbeitet oder genutzt werden?	22
Welche datenschutzrechtlichen Anforderungen gelten für Kundenkarten?	25
Aus der Tätigkeit der Aufsichtsbehörde für den Datenschutz	**27**
Versicherungen	29
Ausweiskopien und Erheben von Ausweisdaten	36
Videoüberwachung und webcams	39
Kreditschutzorganisationen und Auskunfteien	42
Mobile Kommunikation – „Handys“	45
Ordnungswidrigkeiten	46
Sonstiges – Quer durch den Aktenplan	48
Zum Surfen – eine kleine Linkliste	**58**

Häufig gestellte Fragen – „FAQs“

Wie bereits im ersten Tätigkeitsbericht der Aufsichtsbehörde für den datenschutz (http://www.innen.saarland.de/medien/inhalt/mfis-publikationen-datenschutz.pdf) werden auch in diesem häufig auftauchende Fragen im Zusammenhang mit dem Thema „Datenschutz“ angesprochen. Es handelt sich wiederum um Probleme, die in unserer täglichen Arbeit entweder als pauschale Fragen oder aber im Rahmen der konkreten Fallbearbeitung an uns herangetragen wurden. Ergänzt werden die vorgenannten Themen durch solche, die im Berichtszeitraum von allgemeinem Interesse waren. Auswahl und Ausführungen vermitteln so einen Einblick in die Aufgaben und die Arbeit der Aufsichtsbehörde für den Datenschutz.

Viele der Probleme, die an uns herangetragen werden, sind von breitem Interesse und können auf diesem Weg der Öffentlichkeit näher gebracht werden. Wie bereits im ersten Tätigkeitsbericht ergeht auch hier die Bitte an Sie, mit allen möglichen Fragen zum Datenschutz an uns heranzutreten, gleichgültig ob es sich um einen konkreten Fall oder einfach nur reine Wissbegierde handelt. Wir erhalten dadurch auch eine Rückmeldung oder „feedback“ über das, was Sie an unseren Aufgaben wirklich interessiert und stellen – gerade bei den FAQs – nicht nur theoretische Diskurse an.

Für wen gilt das Bundesdatenschutzgesetz?

Diese Frage wurde und wird relativ häufig an uns gestellt und kann genau nur im jeweiligen Kontext beantwortet werden. Zum einen gilt das Gesetz für die Bundesverwaltung sowie mit sehr starken Einschränkungen für bestimmte Verwaltungstätigkeiten der Länder, falls diese keine eigenen Datenschutzgesetze erlassen haben[1]. Zum anderen gilt es dem Grundsatz nach für alle (➔) nicht öffentlichen Stellen, allerdings auch nicht ausnahmslos. Soweit sog. spezialgesetzliche Regelungen oder anerkannte Berufs- bzw. Amtsgeheimnisse existieren, gilt das Bundesdatenschutzgesetz (http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf) nach § 1 Absatz 4 nicht oder nur eingeschränkt (Subsidiarität). Dies ist beispielsweise beim „Internetrecht“ so der Fall: Das Teledienstedatenschutzgesetz (http://www.iid.de/iukdg/gesetz/tddschutzgesetz.pdf) regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Verhältnis Nutzer (= „Surfer“)/Anbieter. In diesem eng umgrenzten Bereich werden die allgemeinen Regelungen des Bundesdatenschutzgesetzes nicht angewandt.

Nicht anwendbar ist das Bundesdatenschutzgesetz auch bei einer rein persönlich oder familiär bestimmten Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Der Gesetzgeber hat bewusst darauf verzichtet, diese Lebenssphäre noch weiter zu verrechtlichen als dies ohnehin bereits der Fall ist. Eine Definition dessen, was unter eine „rein persönlichen oder familiären Zwecken dienenden Erhebung, Verarbeitung und Nutzung“ fällt, erscheint schwierig, da das denkbare Spektrum sehr weit ist. Die Aufsichtsbehörde für den Datenschutz behilft sich in solchen Fällen mit einer Negativdefinition: Bezieht sich die Datenerhebung, -verarbeitung und/oder

[1] Da jedoch alle Bundesländer Landesschutzgesetze erlassen haben, ist diese Regelung faktisch gegenstandslos.

–nutzung auf Außenstehende - insbesondere in Zusammenhang mit einer wirtschaftlichen Betätigung – kann auch ein Hinweis auf ein ursprünglich rein persönliches oder familiäres Interesse nicht zu einer Privilegierung führen, da es an der Ausschließlichkeit jener Interessen fehlt. Mit anderen Worten: Dienen Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch z. B. wirtschaftlichen Interessen, ist das Bundesdatenschutzgesetz immer anzuwenden.

Was sind nicht öffentliche Stellen?

Das Bundesdatenschutzgesetz regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Bundesverwaltung sowie durch sog. „nicht öffentliche Stellen“ (§ 1 Abs. 2 des Bundesdatenschutzgesetzes). Mit diesem sehr abstrakten Begriff sind sowohl natürliche als auch juristische Personen, Gesellschaften oder Personenvereinigungen des privaten Rechts gemeint. Hierunter fallen alle denkbaren Organisationsformen des menschlichen oder wirtschaftlichen Zusammenseins, außer der Familie: Einzelkaufleute, Selbstständige (z. B. Handwerker), freiberuflich Tätige (Ärzte, Architekten etc.), Vereine oder gar Stiftungen, Gesellschaften bürgerlichen Rechts (GbR), Offene Handelsgesellschaften (OHG), Kommanditgesellschaften (KG), Gesellschaften mit beschränkter Haftung (GmbH), Aktiengesellschaften (AGs) sowie alle zulässigen denkbaren Kombinationen dieser Organisationsformen (GmbH & Co. KG, KG aA, gGmbH). Für diese gelten – von einigen Ausnahmen abgesehen – die Regelungen des Bundesdatenschutzgesetzes für die Datenverarbeitung nicht öffentlicher Stellen[2]. Soweit im Folgenden der Begriff der „Stellen“ genannt wird, greift dies nur die Diktion des Gesetzes auf und soll der möglichst neutralen Umschreibung derjenigen dienen, die personenbezogene Daten erheben, verarbeiten und nutzen.

Was versteht man unter „Homebanking“ und welche speziellen Risiken sind damit verbunden?[3]

Der Begriff des „Homebanking“ umfasst zunächst alle denkbaren Arten der von zuhause aus durchführbaren Finanztransaktionen, so also auch das Telefonbanking. Die folgenden Ausführungen beschränken sich jedoch auf das häufigste Verfahren, die Nutzung des heimischen PCs zu Bankgeschäften, der so eine zweite Daseinsberechtigung neben der als Spielkonsole erfährt. Homebanking bietet – zumindest nach Eigenwerbung der Anbieter – eine kostengünstige, zuverlässige und kundenfreundliche Möglichkeit, Finanzgeschäfte aller Art zu tätigen. Zugleich birgt Homebanking durch geringere Investitionen in Infrastruktur und Personal langfristig erhebliche Einsparpotentiale für die Banken.

Die Möglichkeit, „Bankgeschäfte nach Feierabend“ regeln zu können, ist durchaus eine reizvolle, entfällt für die Kundinnen und Kunden doch so die obligatorische Bindung an die Öffnungszeiten von Banken und Sparkassen. Auch im Vergleich zu der

[2] Ohne dass es einer besonderen Erwähnung bedürfte, meint der Bundesgesetzgeber hier auch die Erhebung und Nutzung personenbezogener Daten.
[3] Quellen: U. a. Süddeutsche Zeitung vom 17.2.2005, Datenschutz von A – Z, Hoax-Info der TU Berlin (http://www.tu-berlin.de/www/software/hoax/idtheft.shtml) zum Thema Phishing

Alternative „Geldautomat“ bzw. „Überweisungsautomat“ bietet das Homebanking in der Tat Vorteile: Mit Ausnahme der Möglichkeit Geld abzuheben, bietet das Verfahren die gesamte Palette der Bankdienstleistungen an und zwar bis hin zur Anlageberatung. Automaten hingegen können nur mit Geld oder Kontoauszügen bzw. Überweisungen dienen.

Wie sicher ist „Homebanking“? Homebanking kann keine 100%ige Datensicherheit bieten. Dies ist eine Binsenweisheit, die sich allein schon dadurch erklärt, dass kein technisches System völlig vor Ausfällen, Manipulation oder Angriffen geschützt werden kann, von Fehlverhalten der Benutzer ganz zu schweigen. Die systemimmanente Unsicherheit wird allerdings allein nicht als Argument contra Homebanking gewertet werden können, schließlich existiert nirgendwo im Diesseits ein kriminalitätsfreier Raum. Im Umkehrschluss gilt aber auch, dass Sicherheitsmaßnahmen für sich noch kein ausschließliches Argument für die Erledigung von Bankgeschäften vom heimischen Schreibtisch aus sein können. Entscheidend wird vielmehr sein, mit welchem Aufwand welche Sicherheit erreicht werden kann und vor allem, wie benutzerfreundlich die jeweilige Technik ist.

Derzeit existieren zwei Grundtypen von Homebanking-Systemen,

- der Homebanking Computer Interface – Standard und
- die weit verbreiteten PIN/TAN-Systeme.

Der Homebanking Computer Interface-Standard, kurz HBCI genannt, stellt einen Standard zur sicheren Durchführung von Homebankinggeschäften dar, der unter Federführung des Zentralen Kreditausschusses der deutschen Kreditwirtschaft entwickelt wurde. Kennzeichnendes Element dieses Standards ist, dass er kein bestimmtes Verfahren definiert, sondern dem Ziel einer möglichst sicheren Kommunikation durch Verwendung von integrierten Schutzmechanismen wie einer ausreichend langen Verschlüsselung und digitalen Signaturen Rechnung trägt. Besonders sichere HBCI-Systeme funktionieren auf der Basis von Chipkarten, seltener mit Disketten, die mittels dort gespeicherter Programme dazu dienen, die einzelnen Transaktionen zu verschlüsseln. Voraussetzung für die besonders sicheren Chipkartenverfahren ist allerdings, dass ein entsprechendes Lesegerät zur Verfügung steht. Da solche Lesegeräte noch nicht allzu gängig sind, gelten chipkartenbasierte Systeme bisweilen als wenig benutzerfreundlich, ermöglichen sie in der Regel das Homebanking doch nur vom eigenen entsprechend ausgestatteten Rechner aus. Anders hingegen verhält es sich bei Diskettenlösungen. Da Diskettenlaufwerke immer noch recht weit verbreitet sind, sind Transaktionen von nahezu jedem internet-fähigen Rechner aus möglich. Bedacht werden muss allerdings, dass Disketten von fast jeder/jedem ohne Vorkenntnisse kopiert werden können.

PIN/TAN-Systeme basieren auf 2 kombinierten Identifikationsverfahren: Mit der PIN - der persönlichen Identifikationsnummer - weist sich der Kunde gegenüber dem Bankrechner aus. Nach erfolgter Legitimation können die Bankgeschäfte durch die TAN – Transaktionsnummern – freigegeben werden. Die TANs werden bei klassischen Systemen in einer fortlaufenden Liste angegeben und können nur jeweils einmal verwandt werden, wohingegen die PIN als virtueller Ausweis unverändert bleibt. Als zusätzliche Sicherung wird der eigentliche Kommunikationsvorgang mit der Bank kryptografisch verschlüsselt.

Von der Grundausrichtung her können beide Verfahren als relativ sicher beschrieben werden, wobei ein Restrisiko immer verbleibt. Die größte Gefahr für ein zuverlässiges Homebanking liegt im unberechtigten Zugriff durch Fremde, beispielsweise in Folge eines Angriffs mit Viren oder „Trojanischen Pferden". Daher sollten weder PINs noch TANs oder Passwörter in dem Computer gespeichert werden. Folglich sollte auch auf das bequeme automatische Einloggen beim Bankrechner verzichtet werden. Dies setzt nämlich immer voraus, dass die Anmeldedaten auf dem heimischen Rechner gespeichert sind. Unkomfortabler, aber sicherer ist es, Passwort, PIN und TAN bei jeder Sitzung manuell einzugeben.

„**Phishing**", ein Kunstwort, das zusammengesetzt ist aus den Wörtern „Password" und „Fishing" (angeln, fischen), oder auch Identity-Theft – Daten-/Identitätsklau - ist eine u.a. von Kreditkartenbetrügern häufig genutzte Methode, die immer größere Ausmaße annimmt. Mit dieser Art des virtuellen „Identitätsdiebstahls" ist das Erschleichen oder Ausspionieren von persönlichen Daten wie etwa Passwörtern, Kreditkartennummern und Kontodaten gemeint. Mit Hilfe gefälschter E-Mails, die zumeist noch Link(s) auf eine ebenfalls gefälschte Homepage enthalten, verleiten Kriminelle ihre Opfer dazu, ihnen vertrauliche Daten zu übermitteln, um so unter dem Namen der Opfer kostenpflichtige Transaktionen - meist im Internet – zu tätigen. Die ersten Phishingaktionen galten Kreditkartennummern, da diese im Internet quasi als Ersatzwährung weithin anerkannt sind. Die aktuellsten Phishing-Warnungen hingegen beziehen sich nahezu ausschließlich auf gefälschte E-Mails, die einen Link auf täuschend echt nachgebildete Originalwebsites von Banken enthielten. Die Nachrichten enthielten übereinstimmend die Aufforderung, sich via Link mit der Bank in Verbindung zu setzen und dort das Passwort/PIN und/oder eine mehrere TANs anzugeben. Teilweise werden Grafiken eingebunden, die wie Texte aussehen, aber als Ganzes mit einem Link zur Website der Betrüger versehen sind. Da HTML-fähige E-Mail-Programme (im Gegensatz zu den meisten Web-Browsern) das Link-Ziel meist nicht in einer Statuszeile anzeigen, ist die Illusion nahezu perfekt. Betroffen ist potenziell jedes Unternehmen, das online Geld bewegt. Die „Erfolgsquote" der Urheber ist zwar vergleichsweise gering, da nicht jeder Empfänger einer solchen Mail Homebanking betreibt, noch viel weniger bei der in der Nachricht genannten Bank. Die Täter gehen jedoch hierbei nach der Schrotschussmethode vor: das meiste geht zwar am Ziel vorbei, manche Kugel aber trifft doch. Zu bedenken ist auch, dass der Aufwand für solche Massenmails relativ gering und zudem die Verfolgung der Urheber oft kaum möglich ist, da sie in der Regel gefälschte oder „gekaperte" Absenderadressen benutzen.

Phishing ist jedoch entgegen eines weit verbreiteten Eindrucks nicht etwa auf Kontodaten beschränkt. Weniger spektakulär, aber durchaus gängig ist das Abschöpfen scheinbar unproblematischer Daten wie dem Geburtsdatum. Mit diesem können Täter z. B. bei Internet-Auktionen als Verkäufer unter der gestohlenen Identität auftreten und Waren verkaufen und in Rechnung stellen, selbstverständlich ohne sie zu liefern. Die/der Täuscher/in erhält so Geld oder Waren, der/dem abgeblichen Verkäufer/in, dessen Daten hier benutzt wurden, verbleiben lediglich der Ärger und u. U. die Verpflichtung, nachzuweisen, dass man selbst weder Anbieter noch Käufer war.

Kurzfristige Abhilfe kann z. B. durch konsequentes Negieren solcher E-Mails[4] geschaffen werden. Niemand käme schließlich auf die Idee, auf bloßen Zuruf hin sein

[4] In Frage kommen Filterprogramme, Wegklicken von Phishing-Mails, direktes Löschen etc.

Geld im wahrsten Sinne des Wortes aus dem Fenster zu werfen; auf E-Mails unbekannter Absender mit Kreditkartennummer und womöglich PIN zu antworten, kommt dem jedoch sehr nahe. Solange nicht wirkungsvolle Abhilfe in irgendeiner technischen Form geschaffen ist, sollte der Kontakt zur Online-Bank daher nur über den Browser, der das Ziel in der Statusleiste anzeigt, aufgenommen werden. Diese ist nicht zu verwechseln mit der Verlaufsleiste, die lediglich die eingegebene Adresse enthält. Die Statusleiste hingegen zeigt die tatsächliche u. U. abweichende Webadresse an. Weiter sollte dort nicht die in der Mail angegebene Adresse, sondern nur die bekannte verwandt werden. Sichere Zugänge sind i. Ü. an dem Kürzel „https://“ im Adressfeld erkennbar. Dieses verdeutlicht, dass der Zugang auf die gewählte Webseite über eine verschlüsselte Verbindung aufgebaut wird und so die transportierten Informationen zumindest nicht ohne weiteres gelesen werden können. Aktualisierte Firewalls und Virenscanner sollten bereits jetzt zum Standardrepertoire eines jeden internetfähigen Rechners gehören.

Weitere Sicherheitsinformationen zum Thema Online-Banking sind u. a. beim Bundesverband deutscher Banken e.V., Burgstraße 28, 10178 Berlin, Telefon: (030) 16 63-0, Fax: (030) 16 63-13 99, E-Mail: bankenverband@bdb.de, http://www.bdb.de/, erhältlich.

Welche Rechtsvorschriften sind beim Vereinsauftritt im Internet zu beachten?

Datenschutzrechtliche Aspekte der Vereinspräsentation im Internet

Das Internet ist mittlerweile zur beliebtesten Präsentationsplattform überhaupt geworden. DENIC[5] verzeichnet laut einer Pressemitteilung (http://www.denic.de/de/denic/presse/press_62.html) vom 7. Oktober 2004 zur Zeit etwa 8 Millionen „de-Domains“, die Tendenz ist weiterhin steigend. Hinzu kommen noch weitere Registrierungen unter Top-level-domains wie „.com“, „.edu“, „.org“ oder seit neuerem auch „.name-domains“.

Die Präsentation im Internet gilt demnach als zeitgemäß. Sie bietet allerdings neben dem Chic des Modernen auch handfeste Vorteile, die zunehmend von Vereinen erkannt werden. Die Internetauftritte lösen verstärkt die althergebrachten Mitteilungs-

[5] Die DENIC eG ist eine eingetragene Genossenschaft. Sie wurde am 17. Dezember 1996 gegründet und am 29. September 1997 ins Genossenschaftsregister eingetragen. Die Mitglieder (http://www.denic.de/doc/DENIC/mitglieder.shtml) der DENIC eG sind Internet Service Provider, kurz ISPs, die ihren Kunden lokale Zugänge zum Internet zur Verfügung stellen. Zu den Aufgaben der DENIC eG gehören:

- Betrieb des Primary-Nameservers für die Toplevel-Domain DE
- Bundesweit zentrale Registrierung von Domains unterhalb der Top Level Domain DE
- Administration des Internets in Zusammenarbeit mit internationalen Gremien (CENTR - http://www.centr.org/, ICANN - http://www.icann.org/, CORE - http://www.corenic.org/)
- Bereitstellung verschiedener Datenbankdienste - http://www.denic.de/DENICdb/index.html
- Bereitstellung verschiedener Informationen, insbesondere zu rechtlichen Fragen (http://www.denic.de/doc/recht/index.html) bei der Domainregistrierung und –verwaltung. (Quelle: DENIC)
-

blätter der Vereine mitsamt ihren Verteilproblemen ab oder ergänzen sie zumindest. Die weltweite Erreichbarkeit einer Homepage ist ein weiterer Vorteil. Die Mitglieder – selbstverständlich auch ehemalige - können sich von nahezu jedem Ort der Welt über „ihren“ Verein informieren, was bei der herkömmlichen Präsentation über gedruckte Mitteilungen nicht möglich wäre. Die gängige haushaltsübliche Datenverarbeitungstechnik, deren Kapazitäten wohl die der NASA bei den Apollo-Missionen in den Schatten stellen, bietet die Voraussetzungen für immer neue Arten der virtuellen Information: speicherintensive Features, Fotos, animierte Bilder und Vereinswappen, visuell aufbereitete Informationen, deren Umsetzung noch vor wenigen Jahren Profis vorbehalten war. Der vielbeschworene Umbruch in der Medienlandschaft hat nicht erst begonnen, er ist längst Realität geworden.

Schnelligkeit und Aktualität sind die Hauptvorzüge des Mediums Internet im Vergleich zu Printmedien oder auch Rundfunk und Fernsehen. Jede/r ist Ihre/sein eigene/r Redakteur/in und in der Lage Aktualisierungen fast ohne Zeitverlust aufzunehmen. Spielergebnisse können so bereits wenige Minuten nach Ende der jeweiligen Partie veröffentlicht werden. Auch unter Kostengesichtspunkten kann der Internetauftritt durchaus eine Alternative zur Papierform sein, erleichtern doch gängige Programme selbst technischen Laien die Gestaltung von Webseiten.

Einfach von der Technik her bedeutet jedoch nicht, dass dies auch für die inhaltliche Gestaltung von Internetseiten gilt. Die Pionierzeit des Internets ist vorbei und zumindest für die Anbieter im Inland existieren verbindliche Regelungen, die bei einem Internetauftritt zu beachten sind:

Zunächst ist zu klären, ob es sich um einen Mediendienst oder einen Teledienst handelt. Je nachdem ist entweder der Mediendienste-Staatsvertrag oder das Teledienstegesetz anwendbar.

Kennzeichnend für Mediendienste ist die redaktionelle Gestaltung[6] zur Meinungsbildung. Redaktionell bedeutet, an der Bildung der öffentlichen Meinung im weitesten Sinne mitzuwirken, sei es als Träger einer eigenen Meinung oder in Form der verstärkenden Wiedergabe fremder Meinungen. Zielgruppe von Mediendiensten ist die Allgemeinheit. Die bekanntesten Beispiele für Mediendienste sind die Internetausgaben von Zeitungen und Zeitschriften („SPIEGELonline“, „BILDonline“). Rechtsgrundlage für die Tätigkeit der Mediendienste ist der Mediendienste-Staatsvertrag (MdStV) (http://www.datenschutz-berlin.de/recht/de/stv/mdstv.htm).

Teledienste sind elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung bestimmt sind. Hierunter fallen Telebanking, Informationsangebote ohne redaktionelle Ausgestaltung (Nachrichtenticker, Wetterdienste, Tarifrechner), Angebote zur Nutzung des Internets (Access-Provider) sowie Warenangebote (eBay, Hood, Autoscout, FindlinG etc.). Rechtsgrundlage für die Tätigkeit von Telediensten ist das Teledienstegesetz (TDG) (http://www.datenschutz-berlin.de/recht/de/rv/tk_med/tdg_de.htm)

Die reine Information über Strukturen des Vereins und die Organbesetzung wird wohl eher einen Teledienst darstellen, da es hier meist an der redaktionellen Komponente

[6] Redaktionelle Tätigkeit ist das Auswählen, Sammeln, Bearbeiten und/oder Verfassen von Beiträgen zum Zwecke der Berichterstattung.

zur Meinungsbildung fehlt, dies gilt auch für Hinweise auf Termine oder ähnliche Angebote.

Anders hingegen verhält es sich bei Berichten über Veranstaltungen gleich welcher Art. Hier stellt das Internet nur ein anderes Medium als die klassische Zeitung oder Zeitschrift dar. Bei solchen „Artikeln" liegt eine redaktionelle Bearbeitung vor, so dass hier von einem Mediendienst ausgegangen werden kann. Internetseiten von Vereinen stellen demnach tatsächlich meist eine Mischform von Tele- und Mediendienst dar. Bedeutsam ist dies für den Bereich der Meinungsfreiheit, da das Presse-/Medienprivileg[7] eben nur für Mediendienste, nicht für Teledienste, gilt. Das Saarländische Mediengesetz (http://www.lmsaar.de/upload/download/smg.pdf) unterscheidet im Übrigen nicht zwischen klassischen Printmedien sowie Rundfunk einer- und Medienangeboten im Sinne des Mediendienste-Staatsvertrags andererseits. Dies hat zur Folge, dass der Mediendienste-Staatsvertrag auch auf ausschließlich virtuell erscheinende „Zeitungen" anzuwenden ist.

Datenschutzrechtliche Anforderungen:

Unterrichtungspflichten

Nutzer/in eines (Informations-)Angebotes ist laut Definition im jeweiligen § 3 des Mediendienste-Staatsvertrages und des Teledienstegesetzes jede natürliche oder juristische Person, die den Dienst zu beruflichen oder sonstigen Zwecken in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen. Vereinfacht ausgedrückt sind hiermit alle gemeint, die sich die jeweilige Seite anschauen, dorthin „surfen".

Wer personenbezogene Daten von Nutzerinnen und Nutzern seines Angebots erhebt, verarbeitet oder nutzt, muss die Betroffenen darüber informieren. Diese Informationspflicht besteht auch, wenn Cookies verwandt werden, die über das Ende der jeweiligen (Internet-)Sitzung hinaus gespeichert bleiben. Die Information muss erfolgen, bevor ein Cookie gesetzt wird. Viele Anbieter verwenden hierzu bereits eine Datenschutzklausel. Diese auch „privacy-policys" genannten Hinweise müssen auf den ersten Blick erkennbar (deutlicher Link), und nicht etwa „klein gedruckt" und möglichst unauffällig gestaltet sein.

Die freiwilligen Selbstbeschränkungen in den Datenschutzhinweisen bzw. „privacy policies" gehen meist über die in § 4 Abs. 1 des Teledienstedatenschutzgesetzes genannten Verpflichtungen des Anbieters hinaus, indem sie Datenschutz als integralen Teil der Geschäftspolitik und nicht bloß als gesetzliche Verpflichtung begreifen. Dies kann auch für Vereine interessant sein, da so nicht zuletzt das Vertrauen der Nutzerinnen und Nutzer in die jeweiligen Angebote gestärkt wird. Um die Besucher/innen der Seiten über die Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten, kann die vom Landesbeauftragten für Datenschutz verwandte Datenschutzklausel übernommen und angepasst werden.

Alternativ kann hierzu auch P3P (http://www.w3.org/P3P), eine Internetplattform, deren Betreiber sich das Ziel gesetzt haben, den Schutz personenbezogener Daten im

[7] Art. 5 Abs. 1 Satz 2 des Grundgesetzes: Die Pressefreiheit und die Freiheit der Berichterstattung durch Funk und Film werden gewährleistet.

Internet zu verbessern, genutzt werden. Bei der Verwendung der dort angebotenen Tools/Werkzeuge „stimmen“ die Rechner von Nutzerinnen/Nutzern und Anbieter die Erhebung, Verarbeitung und Nutzung personenbezogener Daten miteinander ab. Neuere Versionen der gängigen Browser erlauben über spezielle P3P-Agents eine individuelle Konfiguration der Daten, die man als Nutzer selbst preisgeben möchte.

Rechtsvorschrift oder Einwilligung im Anbieter/in - Nutzer/in-Verhältnis

Nach § 3 Abs. 1 TDDSG und § 17 Abs. 1 MDStV dürfen personenbezogene Daten nur dann zur Durchführung von Telediensten (Mediendiensten) erhoben, verarbeitet oder genutzt werden, wenn dies durch Gesetz/Rechtsvorschrift erlaubt ist oder die Nutzerinnen/Nutzer eingewilligt haben. Der Gesetzgeber hat die Erhebung personenbezogener Daten von Nutzerinnen und Nutzern ohne Einwilligung abschließend geregelt (s. hierzu §§ 5, 6 TDDSG bzw. § 19 MDStV). Welche Daten wie lange gespeichert werden dürfen, ist dort geregelt. Grundsätzlich gilt, dass nur die Daten erhoben werden dürfen, die erforderlich sind, um die Dienste überhaupt nutzen bzw. um kommerzielle Dienstleistungen abrechnen zu können.

Die Einwilligung ist eine Form der Zustimmung, der Einverständniserklärung. Begrifflich ist sie bereits vor der Erhebung personenbezogener Daten zu erteilen. Eine wirksame Einwilligung erfordert immer, dass die Betroffenen über die Art der erhobenen Daten sowie Verarbeitung und Nutzung informiert werden. Grundsätzlich ist eine stillschweigende Einwilligung unzulässig, so dass es nicht genügt, in allgemeinen Geschäftsbedingungen auf die Datenerhebung, -verarbeitung bzw. –nutzung hinzuweisen.

Sonderfall Pseudonym: Viele kommerzielle Diensteanbieter haben ein ausgeprägtes Interesse daran, zu erfahren, wie lange ihr Angebot von den Nutzerinnen und Nutzern in Anspruch genommen wird, welche Seiten den größten Zuspruch finden etc. Alles was im weitesten Sinne mit dem Nutzen des jeweiligen Angebotes zusammenhängt, kann von Interesse sein. Solche Daten dürfen für Werbezwecke, zur Markt- und Meinungsforschung oder um das jeweilige Angebot bedarfsgerecht zu gestalten, pseudonym genutzt werden. Der Anbieter muss hierüber sowie über die einzuräumende Widerspruchsmöglichkeit informieren. Technisch wird das Verfahren so ausgestaltet, dass personenbezogene Identifikationsmerkmale von den reinen Nutzungsdaten getrennt werden, Klarnamen also z. B. durch ein Chiffre ersetzt werden. Selbstverständlich dürfen die Erkenntnisse über das Nutzungsverhalten nicht wieder mit den Angaben zu den Nutzerinnen und Nutzern zusammengeführt werden (sog. „Re-Identifizierung“). Wer sich nicht sicher ist, ob und welche Daten ein Anbieter erhebt, verarbeitet oder speichert, kann Auskunft hierüber verlangen.

Welche Arten personenbezogener Daten kennt das Teledienste- bzw. Medienrecht und unter welchen Voraussetzungen dürfen sie verarbeitet werden?

Formell setzen sowohl TDDSG als auch MDStV der Datenerhebung, -verarbeitung und –nutzung enge Grenzen. § 3 Abs. 1 TDDSG und § 17 Abs. 1 MDStV schreiben vor, dass personenbezogene Daten von Nutzerinnen und Nutzern vom Dienstanbieter (Betreiber der Homepage) zur Durchführung von Tele-/Mediendiensten nur erhoben, verarbeitet und genutzt werden dürfen, soweit das jeweilige Gesetz oder eine andere Rechtsvorschrift es erlaubt oder eine Einwilligung der Betroffenen vorliegt.

Bei den Daten selbst wird grundsätzlich zwischen

- Bestandsdaten,
- Nutzungsdaten
  und
- Abrechnungsdaten

unterschieden (§§ 5,6 TDDSG, §19 MDStV).

Bestandsdaten sind personenbezogene Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen Nutzerinnen/Nutzern und Anbietern erforderlich sind. Sie dürfen ohne Einwilligung der Betroffenen erhoben werden.

Nutzungsdaten hingegen beziehen sich über die Bestandsdaten hinaus auf die abgerufenen Seiten und umfassen zudem Angaben über Beginn und Ende der jeweiligen Sitzung. Sie dürfen nur erhoben, verarbeitet und genutzt werden, um die Nutzung der Dienste überhaupt zu ermöglichen. Diese Daten dürfen grundsätzlich nur dann über die eigentliche Nutzungsdauer hinaus gespeichert und verarbeitet werden, wenn sie zur Abrechnung benötigt werden *(= Abrechnungsdaten*). Die Speicherungsfrist beträgt sechs Monate nach Versand der Rechnung. Wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen existieren, muss der Diensteanbieter die Daten sperren, sobald die 6-Monats-Frist abgelaufen ist.

Die Speicherung von Bestandsdaten kommt vor allem bei Providern wie T-Online, AOL etc. in Frage, die tatsächlich über einen festen Kundenstamm verfügen. Dem wird bei Vereinen in der Regel nicht so sein. Dort dürfte die Speicherung von Bestandsdaten wohl hauptsächlich bei Vereinsnewslettern bzw. bei E-Mail-Adressbüchern der Mitglieder in Betracht kommen.

Inhaltsdaten

Im Regelfall werden Vereine wohl kaum personenbezogene Daten von Nutzerinnen und Nutzern erheben und speichern. In Frage kommt allerdings die – zulässige – anonyme Speicherung und Nutzung, um die Daten zu statistischen Zwecken auszuwerten.

Problematischer gerade bei Vereinsseiten ist die Veröffentlichung personenbezogener Daten. Werden solche Daten in das Internet-Angebot eingestellt, handelt es sich datenschutzrechtlich um eine Übermittlung. Dies setzt entweder eine Rechtsvorschrift, die das Übermitteln erlaubt, oder die Einwilligung der Betroffenen voraus. Eine Rechtsvorschrift wird man in diesem Zusammenhang zumeist vergeblich suchen. Eine rechtmäßige Datenübermittlung setzt daher – zumindest im nicht redaktionellen Teil des Angebots – voraus, dass die Betroffenen bereits im Vorfeld der Veröffentlichung ihrer Daten zugestimmt haben. Wer wirksam einwilligen soll, muss zunächst über die Konsequenzen ihres/seines Tuns informiert werden (Transparenzgebot). Diese scheint auf den ersten Blick eine sehr formaljuristische Forderung zu sein, hat jedoch durchaus einen ernsten Hintergrund:

Einer der größten Vorteile des Internets ist die weltweite Verfügbarkeit, datenschutzrechtlich ist das zugleich ein riesiges Problem, da die eingestellten Daten quasi über-

all hin übertragen, überall gespeichert („download“) und überall genutzt werden können. Auch dann, wenn die Informationen nicht mehr im Vereinsangebot enthalten sind, existieren sie noch in den digitalen Galaxien fremder Datenbanken. Das Internet kennt kein Vergessen, Suchmaschinen speichern z. B. Screenshots ohne Löschfristen. Die Aufsichtsbehörde für den Datenschutz rät daher dringend, personenbezogene Daten nur dann in das Angebot aufzunehmen, wenn die Betroffenen eingewilligt haben. Bei Minderjährigen müssen die Vereine die Einwilligung der Eltern einholen[8]. Grundsätzlich ist die Einwilligung schriftlich zu erteilen, es sei denn, wegen besonderer Umstände ist eine andere Form auch angemessen. Solche Umstände sind auch bei Internetpräsentationen durchaus denkbar, allerdings sollte allein schon aus Beweissicherungsgründen nicht auf eine schriftliche Erklärung verzichtet werden.

Ausnahmen gelten für personenbezogene Daten von Funktionsträgern, da hier ein berechtigtes Interesse des Vereines oder Verbandes anerkannt werden kann und in der Regel auch keine schutzwürdigen Belange der Betroffenen entgegenstehen. Die Aufsichtsbehörden für den Datenschutz vertreten hierzu vielmehr die Auffassung, dass es häufig im Eigeninteresse der Funktionsträger liege, sich als Verantwortliche in der Öffentlichkeit zu präsentieren. Rechtsgrundlage für die Veröffentlichung personenbezogener Daten von Funktionsträgern ist § 28 Abs. 1 Nr. 2 des Bundesdatenschutzgesetzes. Aus datenschutzrechtlicher Sicht sollten allerdings ausschließlich vereinsbezogene Kontaktdaten aufgeführt werden. Soweit dennoch private Angaben zu Adressen, E-Mail-Adressen, Telefon- bzw. Faxnummer aufgeführt werden, setzt dies die Einwilligung der Betroffenen voraus. Dies kann – worauf hinzuweisen ist – jederzeit widerrufen werden.

Eine weitere Ausnahme wird für die Veröffentlichung von Spielergebnissen, Mannschaftsaufstellungen oder Ranglisten anerkannt. Da die zu Grunde liegenden Veranstaltungen meist öffentlich ausgetragen werden, handelt es sich insoweit um allgemein zugängliche Daten, deren Übermittlung sich hier an den Vorgaben des § 28 Abs. 1 Nr. 3 des Bundesdatenschutzgesetzes bemessen lassen muss. Grundsätzlich steht der Veröffentlichung solcher Daten nichts entgegen; allerdings sollte sich die Veröffentlichung auf Namen und Vereinszugehörigkeit beschränken. Wenn darüber hinaus weitere Angaben für erforderlich gehalten werden, ist eine Einwilligung der Betroffenen erforderlich. Weitere Informationen zur Verarbeitung personenbezogener Daten in Vereinen können dem Merkblatt „Datenschutz im Verein“ des baden-württembergischen Innenministeriums (http://www.innenministerium.baden-wuerttemberg.de/sixcms/media.php/1227/MB_Datenschutz_im_Verein_Febr_05.pdf) und den gleichnamigen Hinweisen der Aufsichtsbehörden für den Datenschutz Bremens, Hamburg, Niedersachsens, Nordrhein-Westfalens und Schleswig-Holsteins (http://cdl.niedersachsen.de/blob/images/C361981_L20.pdf), sowie dem 1. Tätigkeitsbericht der Bayerischen Aufsichtsbehörde für den Datenschutz (http://www.regierung.mittelfranken.bayern.de/aktuell/presse/datenschutzbericht_lang.pdf) entnommen werden.

[8] Das Datenschutzrecht knüpft zwar nicht an die Geschäftsfähigkeit an, sondern an die Einsichtsfähigkeit, die bei Kindern und Jugendlichen individuell im jeweiligen Verwendungszusammenhang zu prüfen ist. Maßstab kann hier die Regelung des Sozialgesetzbuches sein, wonach Minderjährige ab dem 15. Lebensjahr berechtigt sind, Anträge zu stellen und Sozialhilfeleistungen entgegen zu nehmen (§ 36 SGB I).

Was bedeutet „Scoring“?

„Living by numbers“ – „Leben durch bzw. unter Zahlen“. So überschreibt die Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen ein Kapitel in ihrem 17. Tätigkeitsbericht (http://www.ldi.nrw.de/pressestelle/presse_7_1_komplett.html) in dem sie sich mit dem Thema „Scoring[9]“ befasst.

Statistische Aussagen brauchen statistische Angaben oder Daten. Dieser Kernsatz gilt auch für das Scoring, bei dem jede angefragte Person einer definierten Risikoklasse zugeordnet wird. Klassische statistische Angaben sind Geschlecht, Alter, Nationalität, Wohnort, Wohngegend, Beruf, Einkommen, Personenstand, Kinderzahl und Verbindlichkeiten.

Scoring stellt für viele Kritiker den augenscheinlichsten Beweis für einen Umbruch im Kreditgeschäft dar: Beurteilt wird nicht mehr der Mensch, der einen Kredit in Form von Geld oder Waren beantragt, sondern lediglich eine aus Vergleichsparametern zusammengesetzte Schablone, die im schlimmsten Fall keinen tatsächlichen Bezug zu der/dem Betroffenen aufweist. Der Bundesgesetzgeber hat diese Gefahr, die oben nur teilweise überspitzt beschrieben ist, erkannt und in Umsetzung der EG-Datenschutzrichtlinie in § 6a des Bundesdatenschutzgesetzes ein Verbot automatisierter Einzelentscheidungen formuliert. Hieraus ergibt sich, dass Entscheidungen, die für die Betroffenen eine rechtliche Folge zeitigen oder sie erheblich beeinträchtigen können, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Der Begriff Scoring ist durch diese Vorschrift sehr genau umschrieben. Man mag dies für ein gesetzgeberisches Versehen oder geduldetes sprachliches Genie in der Verwaltung halten, jedenfalls stellt die Beschreibung „automatisierte Verfahren, die der Bewertung einzelner Persönlichkeitsmerkmale dienen“, eine gute Basis für die nähere Befassung mit Scoring dar und vermittelt zudem, was diese Verfahren ermöglichen und wo ihre (tatsächlichen und rechtlichen) Grenzen sind.

Scoring beschreibt als Oberbegriff jedes Verfahren zur Bestimmung eines statistischen Risikos. In den meisten Fällen ist der Zweck eines Scoring-Verfahrens in der Bestimmung eines Kreditausfallrisikos, mithin der Bonität der Betroffenen zu sehen. Mit anderen Worten: Ein seriöses Verfahren erlaubt eine Aussage darüber, wie hoch die Wahrscheinlichkeit ist, dass in einer Vergleichsgruppe Kredite nicht oder nicht vollständig zurückgezahlt werden. Hieraus folgt, dass – wiederum bei seriöser Nutzung des Scoring-Wertes – individuell zu prüfen ist, wie hoch das tatsächliche Risiko ist.

Weiter wird der Score-Wert erheblich davon beeinflusst, wie verlässlich die statistisch aufbereiteten Daten sind, die in die Berechnung einfließen. Handelt es sich hierbei um Angaben oder Kriterien, die individuell steuerbar sind und in direktem Zusammenhang mit dem Zahlungsverhalten oder einem sonstigen Persönlichkeitsmerkmal

[9] **Scoring** bedeutet primär das Zählen von Punkten. Im erweiterten Sinne wird es für analytisch statistische Verfahren benutzt, um aus wenigen erhobenen Daten anhand von Erfahrungswerten, die in *Score-Cards* beschrieben werden, zu Risikoeinschätzungen zu kommen. Kreditscoring wird zur Bonitätseinschätzung für die Vergabe von Ratenkrediten an private Kunden von Kreditinstituten verwendet. (Quelle: Wikipedia - http://de.wikipedia.org/wiki/Hauptseite)

stehen, ist der Scoring-Wert relativ aussagekräftig. Dieser Wert wird in Zahlen ausgedrückt, deren Bedeutung je nach verwandtem mathematischem Verfahren variiert. In aller Regel gilt jedoch, dass die Bewertung mit der Punktezahl steigt. Insofern ist auch ein Scoring-Verfahren an die allen seit der Grundschule bekannten Benotungsverfahren angelehnt.

Aus datenschutzrechtlicher Sicht ist Scoring immer dann problematisch oder gar unzulässig, wenn die Verfahren von ihrer Konzeption, also den zur Auswertung benötigten und festgelegten Datenkategorien, her intransparent sind. Dies gilt auch dann, wenn besonders sensible personenbezogene Daten in die Berechnung des Wertes einfließen. So ist die Nutzung von Angaben über die rassische / ethnische Herkunft, politische Meinungen, religiöse / philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben nur unter sehr engen Voraussetzungen zulässig. In aller Regel wird hier nur auf öffentlich zugängliche Informationen, die statistisch aufbereitet sind, zurückgegriffen werden können, um eine Vergleichsgruppe bilden zu dürfen.

Weiter ist manchem Scoring-Verfahren eigen, dass Betroffene nicht im nachhinein erfahren können, welche Werte in der Vergangenheit errechnet und übermittelt wurden. Aus datenschutzrechtlicher Sicht ist dies ein unhaltbarer und daher auch unzulässiger Vorgang, da es das Recht auf Auskunft über die eigenen Daten untergräbt. Daraus folgt, dass die Mindestanforderungen an ein zulässiges Verfahren darin bestehen, dass Betroffene erfahren können, welche Scoring-Werte an wen übermittelt wurden und welche Informationen in das Verfahren einfließen. Einzelne Gewichtungen, also der bestimmende Faktor, mit dem diese Angaben in den Score-Wert einfließen, sind hingegen aus rein datenschutzrechtlicher Sicht eher unkritisch, da es sich hier eher um ein mathematisch-statistisches Problem handelt.

Sind Warndateien zulässig?

Warndateien dienen – wie bereits die Bezeichnung zum Ausdruck bringt – dazu, die angeschlossenen Nutzerinnen und Nutzer auf bestimmte Risiken hinzuweisen. Im Gegensatz zu „herkömmlichen“ Auskunfteien und Kreditinformationssystemen wie der SCHUFA, deren Ziel es ist, einen möglichst umfassenden Überblick über die jeweiligen Kunden zu verschaffen, belässt es die Warndatei bei sog. „Negativdaten“. Das sind solche Daten bzw. Angaben, die Auskunft über nicht-vertragsgemäßes Verhalten geben, z.B. „unbestrittene“ Mahnbescheide, eidesstattliche Versicherungen, titulierte Forderungen, Haftbefehle, Gesamtfälligstellungen.

Man unterscheidet grundsätzlich zwischen zwei verschiedenen Arten von Warndateien:

- Interne und
- externe Warndateien.

Interne Warndateien – auch „Schwarze Listen“ genannt – werden innerhalb eines Unternehmens oder eines Konzerns betrieben und enthalten i. d. R. bei den eingemeldeten Personen direkt erhobene Daten in Form eigener Erkenntnisse des Unter-

nehmens. Die Datensätze können allerdings auch durch Mitteilungen von Auskunfteien oder Kreditinformationssystemen ergänzt werden.

Rechtsgrundlage für den Betrieb interner Warndateien ist § 28 Abs. 1 Nr. 2 des Bundesdatenschutzgesetzes. Danach ist das Erheben, Speichern, Verändern, Übermitteln und Nutzen personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse ist jedes von der Rechtsordnung anerkannte (legitime) Interesse, also auch ein finanzielles bzw. geschäftliches.

„Klassische" Anwärterinnen und Anwärter für die Aufnahme in einer Warndatei sind Personen, die ihren vertraglichen Verpflichtungen gegenüber dem Betreiber der internen Warndatei nicht nachgekommen sind, sei es durch strafbare/unerlaubte Geschäftspraktiken wie Diebstahl, Betrug oder Unterschlagung, oder auch dadurch, dass vereinbarte Raten o.ä. nicht bezahlt wurden. Gerade Angaben über strafbare Handlungen, die vor allem im Einzelhandel von Bedeutung sind, dürfen jedoch nur dann gespeichert werden, wenn ihre Richtigkeit von der verantwortlichen Stelle bewiesen werden kann. Andernfalls sind die entsprechenden Daten umgehend zu löschen.

Soweit personenbezogene Daten zulässig in internen Warndateien gespeichert wurden, sind sie zu löschen, sobald ihre Kenntnis für die Erfüllung des Speicherungszwecks nicht mehr erforderlich ist (§ 35 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes). Dieser Vorgabe dient die Festlegung von Regelfristen, nach deren Ablauf geprüft wird, ob eine weitere Speicherung tatsächlich erforderlich ist. Das Bundesdatenschutzgesetz sieht diese zwar nicht ausdrücklich vor, sie sind jedoch aus Sicht der Aufsichtsbehörde für den Datenschutz unerlässlich, um die Vorgabe des § 35 Abs. 2 Nr. 3 umzusetzen.

Externe Warndateien basieren ähnlich wie SCHUFA und andere Auskunfteien/Kreditinformationssysteme auf Gegenseitigkeit. Jede teilnehmende Stelle verpflichtet sich vertraglich oder per Satzung, die in Frage kommenden Informationen an die Warndatei bzw. deren Betreiber zu übermitteln. Dort werden die Daten gespeichert und aufbereitet, d.h. sie werden mit evtl. bereits vorhandenen Informationen zusammengeführt und erneut ausgewertet. So entstandene Datensätze werden dann auf Anfrage übermittelt bzw. zum Abruf bereitgehalten. Von der rechtlichen Konstruktion her sind externe Warndateien mit Auskunfteien zu vergleichen, da in beiden Varianten personenbezogene Daten Dritter, also Personen, zu denen die Betreiber der Auskunftei / Warndatei keinerlei rechtliche Beziehungen unterhalten, erhoben, gespeichert, verändert und übermittelt werden. Die Rechtsgrundlage für die Tätigkeit der externen Warndateien ist § 29 des Bundesdatenschutzgesetzes. Diese Vorschrift regelt allerdings nur, unter welchen formellen Voraussetzungen eine Warndatei überhaupt betrieben werden darf. Welche Daten gespeichert bzw. übermittelt werden dürfen, muss im konkreten Fall geprüft werden. Weiter ist zu beachten, dass Betroffene ein schutzwürdiges Interesse daran haben können, dass sowohl Speicherung wie auch die Übermittlung unterbleiben. Besonders sensible Daten[10] dürfen gar nur unter nochmals engeren Voraussetzungen überhaupt erhoben werden. Soweit sol-

[10] s. § 3 Abs. 9 des Bundesdatenschutzgesetzes: Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

che Daten Aufnahme in ein nach § 29 des Bundesdatenschutzgesetzes zu beurteilendes Auskunftei- oder Warnsystem finden sollen, ist dies nur unter den Voraussetzungen des § 28 Abs. 7 – 9 des Bundesdatenschutzgesetzes zulässig.

Die Übermittlung personenbezogener Daten aus Warndateien ist nur unter den Voraussetzungen des § 29 Abs. 2 des Bundesdatenschutzgesetzes zulässig. Ausschlaggebend ist u. a., dass in der Anfrage ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft gemacht wird. Reine Neugier wird regelmäßig nicht ausreichen; vielmehr muss es sich um ein objektiv nachvollziehbares Interesse handeln.

Sonderfall Versicherungswirtschaft:

Die Versicherungswirtschaft ist in ihrer Gesamtheit der wohl größte Betreiber von Warndateien, was sich bereits dadurch erklärt, dass dort die meisten Informationen über Risiken - Gesundheits-, Unfall-, Sach-, Lebens-, Rechtsschutzrisiken etc. - anfallen. Dementsprechend groß ist bei aller Konkurrenz untereinander das Interesse, sich über „schlechte“ Risiken gegenseitig zu informieren.

Die Versicherungsunternehmen führen Warndateien nicht etwa wie klassische externe Warndateien, sondern im Wege der Auftragsdatenverarbeitung (§ 11 des Bundesdatenschutzgesetzes). Bei dieser Konstruktion bleiben die einmeldenden Unternehmen verantwortliche Stellen, da der Auftragnehmer den Betroffenen gegenüber nicht aus eigenem Interesse und nicht als eigene Rechtspersönlichkeit auftritt. Die einmeldenden Unternehmen bleiben somit nach außen verantwortlich für eine rechtmäßige Datenverarbeitung.

Eine weitere Besonderheit der Versicherungswarndateien liegt darin, dass diese anonymisiert geführt werden. Die Datensätze, die eingemeldet werden sollen, müssen durch das jeweilige Unternehmen codiert werden und sind nicht durch den Auftragnehmer zu entschlüsseln. Da bei diesem Verfahren keine personenbezogene Daten im eigentlichen Sinne anfallen, dürfen die so gespeicherten Informationen ohne weitere Prüfung an alle angeschlossenen Unternehmen übermittelt oder von diesen abgerufen werden. Die anfragenden Unternehmen stellen eine Anfrage zu einer bestimmten Person, deren Daten nach denselben Kriterien verschlüsselt wurden wie die der bereits eingemeldeten. Ergibt sich aus dieser Anfrage ein Hinweis auf eine vermutliche Personenidentität, löst dies einen Hinweis an die anfragende Versicherung aus. Dieser wird mitgeteilt, welches andere Unternehmen Informationen zu der angefragten Person gespeichert hat. Das weitere Auskunftsverfahren vollzieht sich ausschließlich zwischen den beteiligten Versicherungen selbst. Die Versicherungswarndateien enthalten somit nur codierte Hinweise auf Identifikationsmerkmale wie Namen und Adresse.

Dieses Verfahren ist mit den Aufsichtsbehörden für den Datenschutz abgesprochen und berücksichtigt sowohl die Interessen der Betroffenen wie auch die der Versicherungsunternehmen. Die Betroffenenrechte werden dadurch gewahrt, dass dem Auftragnehmer selbst keine Zuordnung zu einer bestimmten Person möglich ist und zudem keine Hinweise darüber übermittelt und gespeichert werden, aus welchem Grund eine Meldung erfolgte. Die tatsächliche Übermittlung personenbezogener Daten erfolgt nur zwischen den direkt beteiligten Versicherungsunternehmen, denen so – auch im Interesse anderer Versicherungsnehmer – die Möglichkeit geboten wird, Schadensrisiken besser beurteilen zu können.

Zulässig ist die beschriebene Datenweitergabe immer dann, wenn die Betroffenen wirksam darin eingewilligt haben. Hierzu bedienen sich die Versicherungen derzeit noch einer Einwilligungsklausel folgenden Inhalts:

> *„Ich willige ferner ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung ergeben, an Rückversicherer zur Beurteilung des Risikos und zur Abwicklung der Rückversicherung sowie zur Beurteilung des Risikos und der Ansprüche an andere Versicherer sowie an den (XY)-Versicherungsverband zur Weitergabe dieser Daten an andere Versicherer übermittelt. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Vertrages sowie für entsprechende Prüfungen bei anderweitig beantragten (Versicherungs-)Verträgen und bei künftigen Anträgen."*

Hinweis: Die Aufsichtsbehörden für den Datenschutz haben zwischenzeitlich eine Arbeitsgruppe eingesetzt, deren Aufgabe es ist, die Einwilligungsklauseln der Versicherungen kritisch zu überprüfen und mit Blick auf die Anforderungen des Datenschutzes, insbesondere hinsichtlich einer größeren Transparenz, zu überarbeiten. Auch die o. g. Einwilligungsklausel steht auf der Agenda dieser Arbeitsgruppe.

Unter welchen Voraussetzungen ist eine Videoüberwachung zulässig?

Der Fluch der Kameras – so könnte man zumindest meinen – lastet auf Kaufhäusern, Ladenpassagen, Tankstellen, Imbissbuden, Fitnesscentern, Videotheken, kurz auf allen Orten, an denen sich Menschen aufzuhalten pflegen. In Großstädten findet man mittlerweile mehr künstliche Starenkästen als echte auf dem Land. Die anscheinende oder auch nur scheinbare Bedrohung durch Kriminalität und Vandalismus hat dazu geführt, dass Videokameras in zunehmendem Maße zu vertrauten Begleiterinnen beim Einkaufen und beim Bummel durch die Innenstädte werden. Allenfalls Umkleidekabinen, Toiletten und Sozialräume gelten derzeit noch als kamerafreie Zonen.

§ 6b des Bundesdatenschutzgesetzes regelt den Einsatz von Videotechnik zur Beobachtung öffentlich zugänglicher Räume sowohl durch private wie auch durch öffentliche Stellen. Die Begrifflichkeit ist zunächst verwirrend, da sie offen lässt, was mit öffentlich zugänglichen Räumen eigentlich gemeint ist. Weder Rechtsprechung noch Literatur kannten zum Zeitpunkt des In-Kraft-Tretens des novellierten Bundesdatenschutzgesetzes im Mai 2001 eine Definition dieses Begriffes. Auch heute existiert eine solche nicht, so dass lediglich Beispiele und das bewährte Instrument der Negativabgrenzung Hilfe zu bieten vermögen. So hat sich die Sprachregelung durchgesetzt, dass damit solche Räume gemeint sind, die von jedermann ohne besondere Zulassungsbeschränkungen betreten werden können. Verkaufsräume fallen unter diese Definition ebenso wie Ladenpassagen oder die anderen eingangs aufgeführten Örtlichkeiten. Nicht erfasst von der gesetzlichen Regelung sind öffentliche Wege, Straßen und Plätze, die nach erfolgter Widmung aufgrund eines öffentlich rechtlichen Rechtsaktes allein dieser Sphäre zuzuordnen und als solche der Verfügung privater Stellen weitestgehend entzogen sind.

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

Private Stellen dürfen öffentlich zugängliche Räume dann mit Videokameras überwachen, wenn dies

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

erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (§ 6 b Abs. 1 Nr. 2, 3 des Bundesdatenschutzgesetzes). Nach Absatz 2 der Vorschrift sind sowohl der Umstand der Beobachtung als auch die verantwortliche Stelle durch geeignete Maßnahmen kenntlich zu machen. Das deutsche Institut für Normung e. V. (DIN) hat zwischenzeitlich ein entsprechendes Piktogramm erstellt.

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

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

Gerade dies ist bei der Videoüberwachung nicht der Fall. Gegenstand des Einsatzes von Überwachungstechnik ist üblicherweise nicht der Mensch, sondern der Raum, der überwacht werden soll. Bei der reinen Beobachtung verhindert allein schon die Flüchtigkeit des Augenblicks eine „Erhebung“ personenbezogener Daten. Dieser Vorgang ist bei der Videoüberwachung von der Speicherung in Form der Aufzeichnung von Bildern nicht zu trennen. Auch dann fehlt es immer noch an dem bestimmenden Merkmal der althergebrachten Datenverarbeitung: Genau genommen wird ein Bild erst dann zu einem personenbezogenen Datum, wenn ein solcher Bezug tatsächlich existiert oder zumindest mit vertretbarem Aufwand hergestellt werden kann. Erfolgt jedoch eine solche Identifizierung, müssen die Betroffenen, wie bei jeder anderen Ausprägung der automatischen Datenverarbeitung, benachrichtigt werden.[11]

Unverzichtbar ist ein Hinweis auf die Maßnahme selbst sowie auf die verantwortliche Stelle, dies ergibt sich aus § 6b Absatz 2 des Bundesdatenschutzgesetzes. Nach dem Volkszählungsurteil (http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm) ist es grundsätzlich jeder/jedem selbst über-

[11] Selbstverständlich muss ein/e erkannte/r Ladendieb/in nicht durch die/den Inhaber/in darüber informiert werden, dass sie/er während der Tat gefilmt wurde.....

lassen, was sie/er von sich preisgeben möchte. Voraussetzung hierfür ist Transparenz, also schlechthin das Wissen darum, ob und wie personenbezogene Daten erhoben, verarbeitet und genutzt werden. So bedingt auch die Entscheidung, ob man sich der Beobachtung durch Videokameras aussetzt, das Wissen hierum. Der vielfach verfolgte Abschreckungszweck wird im Übrigen auch nur erreicht, wenn den Störern bewusst wird, dass sie beobachtet und mitsamt ihren Taten aufgezeichnet werden. Die Aufsichtsbehörde für den Datenschutz vertritt daher die Auffassung, dass geeignete Hinweise eine Grundvoraussetzung für eine zulässige Videoüberwachung sind. Ohne die geforderten Hinweise und ohne die Möglichkeit, die verantwortliche Stelle zu erkennen, ist eine Videoüberwachung unzulässig, auch wenn ansonsten die gesetzlichen Voraussetzungen erfüllt sind.

Es ist ein weit verbreiteter Irrtum, die Vorschrift des § 6b habe die pandemische Verbreitung von Videokameras an allen möglichen denkbaren Orten erst ermöglicht. Vor In-Kraft-Treten dieser gesetzlichen Regelung war die Videoüberwachung im nicht öffentlichen Bereich lediglich ungeregelt und konnte nur dann datenschutzrechtlich gewürdigt werden, wenn die erhobenen Bilder/Daten (digital) aufgezeichnet und in automatisierten Dateien gespeichert wurden.

Ein weiteres Vorurteil, das sich auch im öffentlichen Bereich zunehmend findet, ist jenes, dass eine Erlaubnisvorschrift ausreiche, um eine Videoüberwachung einrichten zu können. Allein die Tatsache, dass Erlaubnisvorschriften wie § 6b BDSG existieren, rechtfertigt es noch nicht, öffentlich zugängliche Räume nach Gutdünken mit Videotechnik zu überwachen. Eine solche Auffassung verkennt, dass die gesetzlich geregelten Voraussetzungen auch erfüllt sein müssen: Für nicht öffentliche Stellen gilt, dass die Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein muss. Gerade dieses Kriterium der Erforderlichkeit wird regelmäßig nur unzulänglich erfüllt. Dem Wortlaut nach muss die Videoüberwachung notwendig sein, um einen bestimmten Zweck zu erfüllen. Dies erfordert, auch bei einem weit gefassten Zweck wie Wahrung des Hausrechts, eine Prognose und eine tragfähige, nachvollziehbare Begründung. Der Begriff der Erforderlichkeit leitet sich nämlich ab aus dem hier auch für private Stellen geltenden Verhältnismäßigkeitsgrundsatz. Danach muss vor jedem Eingriff in die Rechtssphäre anderer geprüft werden, ob nicht ein weniger belastendes Mittel ebenso zielführend eingesetzt werden könnte. Die Videoüberwachung ist demnach nur dann erforderlich, wenn die Aufgabe oder der Zweck anders nicht, nicht vollständig, nicht rechtmäßig oder nicht mit vertretbarem Aufwand erreicht werden kann. Dies ist die Grundüberlegung, die vor jedem Einsatz von Videotechnik stehen muss. In diesem Zusammenhang taucht vielfach der Hinweis auf, dass ein verstärkter Einsatz von Wachpersonal vielfach die Videoüberwachung ersetzen könnte. Eine solche Auffassung verkennt allerdings, dass denkbare Alternativen auch unter Kostengesichtspunkten zumutbar sein müssen.

Die Überwachung muss – wenn sie nicht ausschließlich der Wahrung des Hausrechts dient - zudem berechtigten Interessen für konkret festgelegte Zwecke dienen. „Berechtigt“ sind alle von der Rechtsordnung anerkannten Interessen, gleich ob sie ideeller, finanzieller, öffentlicher oder privater Natur sind. Die Vorschrift bietet insofern ein recht großes Spektrum denkbarer Voraussetzungen für eine rechtmäßige Videoüberwachung. Das berechtigte Interesse stellt jedoch nur die erste Stufe der sog. „Tatbestandsvoraussetzungen“ dar, da die Zwecke oder der Zweck der Überwachung konkret festgelegt werden müssen. Dies provoziert die Frage, ob der Zweck

schriftlich fixiert werden sollte. Aus rein pragmatischen Überlegungen heraus ist das zu bejahen, da „Festlegung“ in diesem Zusammenhang bedeutet, dass sie nicht ohne Weiteres geändert werden kann. Zuzugeben ist, dass auch hier auf den Einzelfall abgestellt werden muss[12]. Bei der Anwendung der Vorschrift wird oft übersehen, dass hier tatsächlich ein konkreter Zweck, also ein ganz bestimmter, tatsächlicher Zweck verfolgt werden muss. Ist dieser Zweck nachhaltig erfüllt, muss sie eingestellt werden.

Sonderfall: Videoüberwachung am Arbeitsplatz

Grundsätzlich gilt das allgemeine Datenschutzrecht auch im Arbeitsverhältnis. Da § 6b des Bundesdatenschutzgesetzes jedoch nur die Videoüberwachung öffentlich zugänglicher Räume regelt, muss im Arbeitsverhältnis differenziert werden: Wird die Arbeitsleistung in einem öffentlich zugänglichen Raum (Ladenlokal o.ä.) erbracht, gilt § 6b uneingeschränkt. Ist Publikumsverkehr ausgeschlossen, richtet sich die Rechtmäßigkeit entweder nach § 28 des Bundesdatenschutzgesetzes oder dem Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG). Im Ergebnis ist in beiden Fallkonstellationen (öffentlich zugängliche/unzugängliche Räume) die Videobeobachtung von Arbeitnehmerinnen und Arbeitnehmern nur unter sehr engen Voraussetzungen zulässig:

- Grundsätzlich muss auch die Überwachung von Arbeitnehmern offen erfolgen.

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

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

Was sind biometrische Daten und wie können oder dürfen sie erhoben, verarbeitet oder genutzt werden?

Die Biometrie (auch Biometrik; gr. Bio = Leben und Metron = Maß) beschäftigt sich mit der Vermessung quantitativer Merkmale von Lebewesen. Hierzu werden statistische Verfahren angewendet. Oft sind zur Bearbeitung große Datenmengen erforderlich, die erst mit speziellen Techniken der Informationstechnologie beherrschbar werden.

Die "klassische Biometrie" beschäftigt sich mit der Anwendung statistischer Methoden in Human- und Veterinärmedizin, in Land- und Forstwirtschaft, in der Biologie, sowie in verwandten Wissenschaftsgebieten. Der Begriff Biometrie wird daher oft als Synonym für Biostatistik verwendet.

[12] s, hierzu: Duhr, Naujok, Peter, Seiffert, Neues Datenschutzrecht in der Wirtschaft, DUD 2002, S. 5 (28)

Die "neuere Biometrie" beschäftigt sich insbesondere mit Merkmalen von Menschen. Aus einzelnen oder einer Kombination von biometrischen Daten wird auf eine Person geschlossen. Diese kann sich authentifizieren (aus einem definierten Personenkreis), etwa gegenüber Zugangsbeschränkungen, oder sie wird identifiziert (aus einem undefinierten Personenkreis). In der Biometrie spricht man auch vom Vergleich one-to-one (Verifizierung), bzw. vom Vergleich one-to-many (Identifizierung).(Quelle: Wikipedia).

Iris, Kopfdurchmesser, Augenform, Gesichtsgeometrie, Oberkörper, Armlänge, Fingerabdrücke, Anordnung der Finger, Unterkörper, Beinlänge, Fußform, Schuhgröße, Größenverhältnisse der Körperglieder zueinander, alles das sind biometrische Daten ebenso wie Stimme, Unterschrift oder die DNS (= DNA) als genetischer Fingerabdruck. Der Staatssicherheitsdienst der ehemaligen DDR soll gar Auswertungs- und Zuordnungsversuche mit Körpergerüchen durchgeführt haben.

Das bekannte Beispiel der Fingerabdrücke verdeutlicht, wozu biometrische Daten dienen können, nämlich der (Wieder-)Erkennung einer bestimmten Person. Voraussetzung für die Wiedererkennung ist, dass die zu überprüfenden Daten bereits erhoben und gespeichert worden sind („Referenzdatensatz“). Prinzipiell erfolgt ein Abgleich neu gewonnener Daten mit den Referenzdaten. In den Grundzügen ist dieses Verfahren seit den ersten daktyloskopischen Vergleichen zu Beginn des 19. Jahrhunderts unverändert geblieben. Für die Ausgestaltung des Verfahrens selbst gilt dies natürlich nicht: Bereits seit den 60er Jahren können Fingerabdrücke automatisiert verarbeitet und identifiziert werden[13].

Die Codierung und Decodierung biometrischer Daten verläuft unabhängig davon, welche Einzeldaten (Fingerabdrücke, Iris, Gesichtsform etc.) erfasst werden sollen, immer nach demselben Muster:

1. Erheben und Speichern der Daten, z.B. durch Filmaufnahme, Irisfotografie, Fingerabdruck,
2. Berechnung eines Datensatzes („Template“[14]), der die bestimmenden Merkmale des jeweiligen biometrischen Datums in Zahlen ausdrückt,
3. Speicherung dieses Datensatzes.

Da die Codierung identischer „Rohdaten“ zumindest theoretisch zu identischen Datensätzen führt, erlauben diese Verfahren einen relativ schnell durchzuführenden Vergleich neuer Daten mit den Referenzdaten. Um Messfehler zu vermeiden, arbeiten alle Verfahren zur Verarbeitung biometrischer Daten mit definierten Toleranzen. Der Grund hierfür liegt darin, dass auch identische biometrische Daten einer Person nicht immer zu ein und denselben Datensatzberechnungen führen, so z.B. bei ungenauer Gesichtserkennung, Verletzung von Fingern etc.. Um in solchen Fällen dennoch eine biometrie-gestützte Identifizierung/Verifizierung zu ermöglichen, muss ein Schwellenwert definiert werden, ab dem eine Übereinstimmung oder Zurückweisung erfolgt.

[13] s. hierzu auch: „Kleine Historie der Daktyloskopie“, Quelle: Bundeskriminalamt - http://www.bka.de/pressemitteilungen/hintergrund/hintergrund1.html

[14] = (elektronische) Schablone

Ein weiterer biometrischen Verfahren immanenter Unsicherheitsfaktor liegt in der Möglichkeit der Täuschung durch Fälschen scheinbarer biometrischer Daten. Ein klassisches Beispiel hierfür ist der Gummifinger: Mittels eines genauen Abbildes eines echten Fingers und der zugehörigen Fingerabdrücke können einfache biometrische Kontrollverfahren getäuscht werden, da sie lediglich die Papillarleisten abscannen und mit den gespeicherten Datensätzen vergleichen. Seriöse Verfahren zur Verarbeitung biometrischer Daten greifen daher zusätzlich auf Methoden zur Lebenderkennung zurück, d.h. , es wird ein Test durchgeführt, ob der Fingerabdruck überhaupt durch eine lebende natürliche Person und eben nicht etwa durch einen Gummifinger erfolgte. Parameter für eine Lebenderkennung können z.B. Hautwiderstand oder Körpertemperatur sein.

Biometrische Verfahren können grundsätzlich in allen Bereichen angewandt werden, in denen eine sichere Identifizierung/Verifizierung erforderlich ist. Klassisches Beispiel ist die Strafverfolgung, aber auch im nicht hoheitlichen Bereich, also in der Privatwirtschaft oder im reinen Privatbereich ist der Einsatz denkbar und zum Teil auch Realität:

- Zutrittssicherungen,
- elektronische Signatur,
- Definition pseudonymer Benutzergruppen usw.

Biometrische Verfahren lösen zudem eines der ältesten Probleme der Menschheit: „Wie greife ich einem nackten Mann in die Tasche?“ [15]. Ganz einfach indem dieser eine Einzugsermächtigung/Einwilligung in ein Lastschriftverfahren gibt und zusätzlich ein biometrisches Datum, vorzugsweise Iris oder Fingerabdruck, erhoben und gespeichert wird. Möchte eine registrierte Person eine Forderung durch Abbuchung vom Konto begleichen, bestätigt sie diese durch einen erneuten Fingerabdruck oder Irisabgleich. Die so erfassten biometrischen Daten werden mit den hinterlegten verglichen und bei Übereinstimmung erfolgt die Zahlung.

Datenschutzrechtlich ist die Verarbeitung biometrischer Daten immer dann zulässig, wenn sie durch Gesetz oder eine sonstige Rechtsvorschrift erlaubt wird. Dies ist vor allem im öffentlichen Bereich der Fall, so z. B. zu Zwecken der Strafverfolgung (genetischer Fingerabdruck). Besteht eine solche gesetzliche Eingriffsgrundlage nicht, dürfen biometrische Daten nur mit Einwilligung der Betroffenen erhoben werden. Eine wirksame Einwilligung setzt nach der Vorschrift des § 4 a Abs. 1 und Abs. 3 des Bundesdatenschutzgesetzes voraus, dass die Betroffenen ausführlich über die Verarbeitungszwecke und eventuelle Risiken informiert werden sowie die Einwilligung freiwillig abgeben. Soweit diese Voraussetzungen erfüllt sind und die durch die Information der Betroffenen dokumentierte Beschränkung hinsichtlich der Nutzung gespeicherter biometrischer Daten beachtet wird, begegnet die Verarbeitung solcher Daten keinen grundsätzlichen Bedenken. Etwas anderes gilt allenfalls für sog. „genetische Fingerabdrücke“ deren Sensibilität im Vergleich zu „herkömmlichen“ biometrischen Daten außerordentlich hoch einzustufen ist. Hier werden nochmals höhere Anforderungen sowohl an die grundsätzliche Zulässigkeit als auch konkret an die Einwilligung zu stellen sein.

[15] Ein anderes weit verbreitetes Problem ist ebenfalls auf biometrischen Weg bereits gelöst: der verlorene Schlüssel. Selbstverständlich kann das Aufschließen einer Tür ebenfalls biometrisch gesteuert werden.

Eines der Hauptrisiken im Zusammenhang mit biometrischen Daten liegt darin, dass die meisten der derzeit verfolgten Ansätze auf eine berührungslose bzw. unbemerkte Erhebung solcher Daten abzielen. Hinzu kommt, dass im Prinzip jedes eindeutig zuordenbare biometrische Merkmal zumindest theoretisch ein personenbezogenes Datum darstellen kann, das mit Informationen aus unterschiedlichen Quellen zusammengeführt wird. Sichere Verfahren zur Identifizierung/Authentifizierung sind nach Kenntnis der Aufsichtsbehörde derzeit nur unter aktiver Mithilfe der Betroffenen darstellbar, da die derzeit am Markt befindlichen Verfahren, wie die zum Videoabgleich, eine (noch) zu hohe Fehlerquote aufweisen.

Welche datenschutzrechtlichen Anforderungen gelten für Kundenkarten?

„Haben Sie schon unsere Karte?“, lautet die mittlerweile gängigste Fragen an den Kassen der großen Warenhäuser. Kundenkarten, die den Kundinnen und Kunden über Preisnachlässe beim Einkauf hinaus vielfältige Erlebnismöglichkeiten bieten sollen, sind heute so weit verbreitet, dass es weder den Käuferinnen und Käufern, noch den Verbraucher- und Datenschützern gelingt, eine seriöse Schätzung über Zahl und genaue Funktionsweise der verschiedenen Systeme abzugeben. Der genaue Oberbegriff für all diese lautet „Kundenbindungssysteme“. „Eine Karte, sie zu knechten, sie alle zu finden, ins Kaufhaus zu treiben und ewig zu binden“ wie Verschwörungstheoretiker in Anlehnung an den Herrn der Ringe und dessen düstere Absichten meinen könnten.

Ganz so ist dem nicht: Nach dem Wegfall des Rabattgesetzes wurden unterschiedliche Modelle von Rabattsystemen entwickelt, so dass sich neben den unternehmens- und branchenübergreifenden Systemen der großen Anbieter Payback und HappyDigits auch eine Vielzahl von Firmen-, Konzern-, Branchen- und sonstigen Kartensystemen am Markt etabliert haben. Voraussetzung für die Teilnahme an einem Rabattprogramm ist, dass die Kundinnen und Kunden einen Vertrag mit dem Karten emittierenden Unternehmen schließen. Einigendes Merkmal aller Kundenbindungsprogramme ist weiter, dass die Teilnahme an ihnen mit der Preisgabe personenbezogener Daten verbunden ist:

Zunächst werden die Stamm- oder Basisdaten erhoben. Hierunter versteht man Angaben, die für die sichere Identifizierung erforderlich sind, wie z. B. Name, Vornamen, Adresse und Geburtsdatum. Auch weitere Informationen wie z. B. Anrede oder E-Mail-Adresse, aber auch zu Familienstand, Anzahl der Kinder, Wohn- und Einkommensverhältnissen sind als Stammdaten denkbar, die im Rahmen der Vertragserfüllung meist auf freiwilliger Basis erhoben werden.

Für alle Kartensysteme gilt, dass bei einem Einkauf oder der Bezahlung einer Dienstleistung sog. „rabattrelevante Daten“ erhoben und gespeichert werden. Diese Nutzungsdaten umfassen die Ware oder Dienstleistung selbst, den Preis, Rabattbetrag sowie Ort und Datum. Bei unternehmensübergreifenden Systemen, die partnerschaftlich organisiert sind, werden die erhobenen Daten gemeinsam mit der Kundennummer an den jeweiligen Systemanbieter übermittelt. Dieser führt die so erhaltenen Daten mit dem bereits vorhandenen Datensatz zusammen. Bei Unternehmenskarten,

die nur jeweils in einem Unternehmen oder einer Unternehmensgruppe[16] eingesetzt werden, findet datenschutzrechtlich keine Übermittlung statt, da die erhobenen personenbezogenen Daten im Unternehmen verbleiben.

Allen Systemen ist immanent, dass die so erhaltenen Daten über Data-warehouse-/Data-mining-Programme[17] genutzt werden können, um Kunden- oder Zielgruppenprofile zu bilden. So scheint es sich geradezu anzubieten, die Angaben für Werbezwecke zu nutzen, da die jeweiligen Kundenvorlieben und –neigungen direkt aus dem Kaufverhalten ableitbar sind. In dieser Vorstellung des „gläsernen Kunden" bündeln sich die begründeten Vorbehalte von Daten- und Verbraucherschützern gegen Rabattsysteme, die über den eigentlichen Rabattbetrag und den einmeldenden Partner (=Verkäufer) hinaus personenbezogene Daten erheben, speichern und nutzen. Ginge es nur darum, den Kundinnen und Kunden einen Vorteil zu bieten, wären diese Zusatzinformationen nicht erforderlich.

Aus datenschutzrechtlicher Sicht sind daher Kundenbindungssysteme, die eine weiter gehende Nutzung personenbezogener Daten ermöglichen, nur dann zulässig, wenn die Betroffenen über die Erhebung und Nutzung ihrer personenbezogenen Daten ausführlich informiert und hiermit einverstanden sind. Wünschenswert ist insbesondere im Zusammenhang mit Werbe- und Marktforschungsaktivitäten eine ausdrückliche schriftliche Einwilligung in die Nutzung der Daten. Aus Sicht der Aufsichtsbehörde für den Datenschutz ist es zudem nicht hinnehmbar, wenn die Teilnahme am Rabattprogramm davon abhängig gemacht wird, dass die Kundinnen und Kunden zuvor in die Nutzung ihrer personenbezogenen Daten zu Werbezwecken eingewilligt haben. Seriöse Unternehmen verzichten daher auf solche Vorbedingungen.

---

[16] Vorreiter war hier der Bekleidungsfachhandel.

[17] Ein **Data-Warehouse** (deutsch *Daten-Waren-Lager*) ist eine zentrale Datensammlung (meist eine Datenmbank - http://de.wikipedia.org/wiki/Datenbank), deren Inhalt sich aus Daten unterschiedlicher Datenquellen zusammensetzt. Die Daten werden von den Datenquellen in das Data-Warehouse kopiert und dort vor allem für die Analyse und zur betriebswirtschaftlichen Entscheidungshilfe in Unternehmen langfristig gespeichert. Der Begriff stammt aus dem Informationsmanagement in der Betriebswirtschaft. (...) Im Data-Warehouse werden die gespeicherten Informationen mit speziellen Programmen, sog. „Tools" bzw. Extraktionstools analysiert, und für neue Verknüpfungen aufbereitet. Data-Warehouse-Programme sind in der Regel so konzipiert, dass Auswertungszwecke nicht vorgegeben sind. Das Data-Warehouse stellt so auch einen neuen Ansatz zur Ordnung des vielfältigen Datenmaterials dar.
Data-Mining bedeutet nicht anderes als „Daten-Bergbau". Spezielle Programme ermöglichen das Auffinden neuer Verbindungen der im Ware-House vorhandenen Daten. Herkömmliche Auswertungsprogramme sind von den Vorgaben des Anwenders, Programmierers oder Anwendungsbereiches her auf bestimmte Ergebnistypen festgelegt, wohingegen Mining-Programme ergebnisoffen konzipiert sind, d. h. sie stellen automatisiert zunächst alle scheinbaren Ähnlichkeiten in den vorhandenen Datensätzen in einen Zusammenhang und überprüfen diesen darauf, ob eine Art Gesetzmäßigkeit besteht, also ein ursächlicher Zusammenhang. Erkannte gemeinsame Ursachen und Wirkungen werden analysiert, beschrieben und angezeigt.
Quelle: U. a. Wikipedia, Weichert, Data-Warehouse und Data-Mining, in: Bäumler, Breinlinger, Schrader „Datenschutz von A – Z", Luchterhand 1999

Aus der Tätigkeit der Aufsichtsbehörde für den Datenschutz

Der Berichtszeitraum 2003/2004 wies keine besonderen Schwerpunkte im Tätigkeitsfeld „Anlasskontrolle“ auf. Anfragen und Prüfungen betrafen das gesamte Aufgabenspektrum, wobei anteilig der Bereich „Versicherungen“ am häufigsten nachgefragt wurde. Die Aufsichtsbehörden für den Datenschutz in den anderen Bundesländern dürften ähnliche Erfahrungen gemacht haben. Dies sollte allerdings nicht als Hinweis auf eine besondere datenschutzrechtliche Delinquenz der Versicherungsunternehmen gewertet werden, sondern erklärt sich vielmehr als Reflex auf die schiere Menge personenbezogener Daten, die von dort erhoben, verarbeitet und genutzt werden.

Augenfällig hingegen waren die Anfragen zur Bestellung betrieblicher Datenschutzbeauftragter. Die Aufsichtsbehörde für den Datenschutz hatte bereits im 2003 erschienenen 1. Tätigkeitsbericht die Voraussetzungen genannt, unter denen ein/e betriebliche/r Datenschutzbeauftragte/r bestellt werden muss. Grundsätzlich muss jeder, der personenbezogene Daten nicht ausschließlich für persönliche oder familiäre Zwecke erhebt, verarbeitet oder nutzt, eine/n betriebliche/n Datenschutzbeauftragte/n benennen. Eine Ausnahme ist dann zulässig, wenn höchstens 4 Personen mit dieser Tätigkeit befasst sind. Diese Regelung findet sich als § 4f im novellierten Bundesdatenschutzgesetz, das am 23. Mai 2001 in Kraft getreten ist.

Eine andere Vorschrift dieses Gesetzes schuf im Zusammenhang mit der Pflicht, betriebliche Datenschutzbeauftragte zu bestellen, einige Verwirrung und bot dem einen oder anderen mehr oder minder seriösen Beratungs- und Schulungsunternehmen ein neues Tätigkeitsfeld: Nach § 45 des neuen Bundesdatenschutzgesetzes waren laufende Erhebungen, Verarbeitungen und Nutzungen, also solche, die beim In-Kraft-Treten bereits angewandt wurden, binnen drei Jahren der aktuellen Rechtslage anzupassen. Diese Vorschrift wurde vielfach so interpretiert, dass spätestens bis zum 22. Mai 2004 betriebliche Datenschutzbeauftragte zu benennen seien. Die hier vorliegenden - meist telefonischen – Anfragen sprechen eine sehr eigene und beredte Sprache: Offenbar wurden häufig vor allem kleinere und mittelgroße Unternehmen von externen Beratern und Seminaranbietern auf ein bestehendes Manko und den bevorstehenden Fristablauf hingewiesen, verbunden mit dem Bemerken, dass die Aufsichtsbehörde für den Datenschutz im Falle der Nichtbestellung eine/r/s Datenschutzbeauftragten ein Bußgeld bis zu einer Höhe von 25.000 € verhängen könne.

Kaum eine Interpretation dieser Vorschriften könnte falscher sein: § 45 regelt eindeutig, dass **Verfahren**, mit denen personenbezogene Daten erhoben, verarbeitet und/oder genutzt werden, spätestens nach 3 Jahren anpasst sein müssen. Die Kommentarmeinung[18] führt hierzu aus, „... (dass) die Regelung daher beispielsweise auf automatisierte Informationssysteme anzuwenden (ist), in denen ein Datenbestand geführt wird, der hinsichtlich der Qualität der Daten oder der Zulässigkeit ihrer Verarbeitung nicht den Anforderungen der Novellierung entspricht...“. Keine Rede davon, dass hier organisatorische Maßnahmen wie die Bestellung eine/r/s Datenschutzbeauftragten gemeint sein könnten. Jedoch nicht nur in dieser Hinsicht geht die Panikmache fehl:

[18] Damman in Simitis (Hrsg.) u. a., Kommentar zum Bundesdatenschutzgesetz, Baden-Baden 2003[5], § 45 RN 2

Die Verpflichtung, betriebliche Datenschutzbeauftragte zu bestellen, besteht nicht erst seit Ablauf der „Schonfrist“ in § 45 des Bundesdatenschutzgesetzes. Sie wurde auch nicht erst im Jahr 2001 mit der Novellierung des Bundesdatenschutzgesetzes eingeführt, sondern sie besteht für nicht öffentliche Stellen bereits seit In-Kraft-Treten des ersten Bundesdatenschutzgesetzes im Jahre 1977. In § 28 dieses Gesetzes ist die Vorgabe enthalten, wonach Unternehmen, die mindestens 5 Mitarbeiter ständig mit der automatischen (!) Verarbeitung personenbezogener Daten beschäftigen, einen betrieblichen Datenschutzbeauftragten schriftlich bestellen müssen. Gleiches galt, soweit in der Regel mindestens 20 Mitarbeiter mit konventioneller (nicht automatisierter) Datenverarbeitung beschäftigt wurden. Das Bundesdatenschutzgesetz von 1991 griff diese Vorschrift auf und normierte in § 36 eine entsprechende Verpflichtung. Insoweit enthält § 4f Absatz 1 des neuen Bundesdatenschutzgesetzes keine wirklich neuen Vorgaben, lediglich die „Hausnummer“ wurde insofern geändert. Auch das Quorum ist in der Realität unverändert geblieben: Forderten die Gesetze 1977 und 1991 noch eine Mindestmitarbeiterzahl von 5 um die Verpflichtung einzutreten zu lassen, spricht das Bundesdatenschutzgesetz 2001 von einer Befreiung von eben dieser Vorgabe, wenn höchstens 4 Mitarbeiter mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten befasst sind. Wenn personenbezogene Daten nicht automatisiert erhoben, verarbeitet oder genutzt werden, muss ein/e betriebliche/r Datenschutzbeauftragte/r dann bestellt werden, wenn damit in der Regel mindestens 20 Personen beschäftigt sind. Die entsprechende Vorgabe ist in § 4f Abs. 1 Satz 3 des Bundesdatenschutzgesetzes zu finden.

Danach sind die beschriebenen „Hinweise“ auf bestimmte gesetzliche Verpflichtungen, verbunden mit dem Angebot, die Voraussetzungen zu prüfen und ggf. betriebliche Datenschutzbeauftragte zu schulen, mit Vorsicht zu genießen:

Zum einen verrät die hier wiedergegebene Argumentation eine profunde Nichtkenntnis der tatsächlichen Rechtslage oder doch zumindest ein Ignorieren der rechtlichen Gegebenheiten. Zum anderen ist es schon per se unseriös, als privates Unternehmen mit Bußgeldern zu drohen. Die Aufsichtsbehörde für den Datenschutz rät daher allen betroffenen Unternehmen, solche Angebote einer besonders strengen Qualitätsprüfung zu unterziehen. Im Berichtszeitraum wurde daher auf Anfrage einer Kammer als Dienstleisterin für saarländische Unternehmen angedacht, ein gemeinsames qualifiziertes Fortbildungsangebot zu begleiten. Dieses gemeinsame Vorhaben konnte jedoch bis Redaktionsschluss noch nicht in die Tat umgesetzt werden.

Ausgewählte Fälle

Versicherungen

Der Zusammenschluss zweier Versicherungen

Der im ersten Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz beschriebene Zusammenschluss zweier Versicherungen war Gegenstand einer Anfrage, die sich sehr kritisch mit den datenschutzrechtlichen Aspekten dieser Verbindung befasste. Die zuständigen Aufsichtsbehörden für den Datenschutz in Bayern und im Saarland hatten das gesamte Verfahren schon frühzeitig begleitet und auf die datenschutzrechtlichen Probleme hingewiesen. Aus datenschutzrechtlicher Sicht war die damals geplante und mittlerweile umgesetzte Struktur der Datenverarbeitung bedeutsam: Künftig sollten personenbezogene Daten der Kundinnen und Kunden innerhalb des Konzerns zum Zwecke der Vertrags- und Leistungsbearbeitung ausgetauscht werden. Da beide Unternehmen als rechtlich selbstständige Unternehmen weiterhin verantwortliche Stellen blieben, war hierin eine Übermittlung personenbezogener Daten zu sehen, die nicht vom ursprünglichen Versicherungsvertrag gedeckt war.

§ 4 des Bundesdatenschutzgesetzes erlaubt jegliche Datenverarbeitung, also auch die Übermittlung, nur, wenn sie durch Gesetz bzw. sonstige Rechtsvorschrift erlaubt ist oder die Betroffenen hierin eingewilligt haben. Da es keine Rechtsgrundlage für die geplante neue Struktur der Datenverarbeitung gab, setzte die Übermittlung in Form des Datenaustauschs voraus, dass die Betroffenen darin einwilligten. Die beiden beteiligten Versicherungen baten uns zu prüfen, ob es wegen der großen Zahl der Versicherten nicht auch zulässig sein könnte, eine stillschweigende Einwilligung der Betroffenen anzunehmen.

Form und Voraussetzungen einer wirksamen Einwilligung sind in § 4a des Bundesdatenschutzgesetzes geregelt. Danach muss die Einwilligung schriftlich erfolgen, soweit nicht wegen besonderer Umstände eine andere Form objektiv angemessen ist. Nach Auffassung der Aufsichtsbehörden für den Datenschutz kann die hier geforderte stillschweigende oder konkludente Einwilligung nur in sehr speziellen Konstellationen wirksam zum Tragen kommen, da bei dieser Form der Zustimmung grundsätzlich 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 Versicherten war die beabsichtigte „Widerspruchslösung“ für den vorhandenen Versichertenbestand nach Auffassung der Aufsichtsbehörden für den Datenschutz vertretbar. Ansonsten wäre angesichts der zu erwartenden geringen Rücklaufquoten das angestrebte Ziel einer neu organisierten Datenverarbeitung im Konzern kaum realisierbar gewesen. Das Interesse der beteiligten Versicherungsunternehmen, personenbezogene Daten einheitlich zu verarbeiten, ist aus Sicht der Aufsichtsbehörden für den Datenschutz durchaus berechtigt, zumal hierdurch den Betroffenen auch keine Nachteile entstehen. Die Situation bei Neu-

kunden hingegen ist insofern datenschutzrechtlich unproblematisch, als bei diesen ohnehin eine Einwilligung in die Datenverarbeitung eingeholt wird.

In der Folge wurden die Versicherten beider Unternehmen über die neue Struktur der Datenverarbeitung sowie die hierfür erforderliche neue Einwilligungsklausel informiert und auf die Möglichkeit des Widerspruchs hingewiesen. Hiergegen wandte sich der Petent mit dem Hinweis, die Einwilligungsklausel diene vor allem dazu, den Betroffenen weitere Finanzdienstleistungen des nunmehr größeren Versicherungskonzerns anbieten zu können und zudem sei auf seinen Widerspruch nicht reagiert worden.

Dieser Auffassung konnte die Aufsichtsbehörde für den Datenschutz nicht folgen, da sich für Versicherungsnehmer, die in die Beratung und Betreuung in sonstige Finanzdienstleistungen eingewilligt haben, nichts änderte. Die entsprechende Einwilligungsklausel („Allfinanzklausel“) wird bereits seit 1997 verwandt. Wurde die Klausel hingegen seinerzeit gestrichen, war dies auch bei der Neuorganisation der Datenverarbeitung zu beachten, da sich die erbetene konkludente Einwilligung nach unserer Auffassung nur auf die geänderten Vertragsbestandteile beziehen konnte. Im Falle älterer Verträge ohne Einwilligungsklausel könnte sich das Unternehmen zwar unter Umständen auf § 28 Abs. 4 des Bundesdatenschutzgesetzes stützen, wodurch im Ergebnis die Nutzung rechtmäßig erhobener personenbezogener Daten für Werbezwecke immer dann zulässig wäre, wenn Betroffene dem nicht widersprechen. Dies würde jedoch sowohl der Absprache mit der Aufsichtsbehörde für den Datenschutz wie auch der vorgetragenen Absicht des Versicherungsunternehmens widersprechen.

Anders verhielt es sich im Hinblick auf die zu Recht monierte Reaktion der Versicherung. Die Aufsichtsbehörde für den Datenschutz hatte im Vorfeld des Zusammenschlusses bereits darauf verwiesen, dass jeglicher Widerspruch gegen eine Datenübermittlung schriftlich zu bestätigen sei; das wurde hier unterlassen. Das Versicherungsunternehmen wurde auf dieses Defizit hingewiesen und angemahnt, künftig entsprechend der Vorgaben der Aufsichtsbehörde für den Datenschutz zu verfahren.

Ein Gutachten in falschen Händen – Scheidung 1.0

Das häufigste Ende der zivilrechtlichen Ehe ist immer noch der Tod [§ 1482 des Bürgerlichen Gesetzbuches - http://dejure.org/gesetze/BGB (BGB)], direkt gefolgt von der Scheidung (§ 1564 BGB), was insofern nicht weiter verwunderlich ist, als lediglich zwei Möglichkeiten zur formellen Beendigung derselben bestehen. Scheidungen sind oft mit Auseinandersetzungen um Geld und Unterhalt verbunden und tun weh, wie der Volksmund weiß. So auch in einem Fall, der die Aufsichtsbehörde für den Datenschutz beschäftigte:

Ein Ehepaar hatte bei einem saarländischem Versicherungsunternehmen gesamtschuldnerisch ein Darlehen aufgenommen, um so den Kauf einer Immobilie zu finanzieren. Alleineigentümer war der Ehemann. Der Darlehensvertrag ermächtigte die Versicherung, ein Wertgutachten anfertigen zu lassen, das in deren Eigentum verbleiben sollte. Nach der Trennung der Eheleute wurde der Ehefrau eine Ausfertigung des Gutachtens überlassen, die dieses offenbar im Scheidungsverfahren verwandte.

Hiergegen richtete sich die Eingabe des Ehemannes, der eine Rechtsgrundlage für die Übermittlung seiner personenbezogenen Daten (hier: Immobilienvermögen) verneinte. Nach Prüfung des Sachverhaltes konnte die Aufsichtsbehörde für den Datenschutz keinen Verstoß gegen datenschutzrechtliche Bestimmungen feststellen, da sich beide Eheleute durch Anerkennung der Allgemeinen Darlehensbedingungen unwiderruflich untereinander und gegenseitig zu Zustellungsbevollmächtigten hinsichtlich aller Erklärungen und Handlungen der Gläubigerin bestellt hatten. Dem war nach unseren Feststellungen nichts hinzuzufügen. Zudem stellte die Ermächtigung an die Versicherung, ein Wertgutachten zu erstellen, einen Auftrag dar. Aus diesem lässt sich ein zivilrechtlicher Anspruch der Ehefrau auf Vorlage des Gutachtens ableiten, da nach § 667 des BGB Beauftragte verpflichtet sind, alles zur Geschäftsbesorgung Erlangte dem Auftraggeber herauszugeben. Dies statuiert selbstverständlich auch einen Herausgabeanspruch der Auftraggeberin.

Letztlich wäre dem eigentlichen Anliegen des Petenten, zu verhindern, dass seine Ex-Gattin den Grundstückswert erfährt, ohnehin kein Glück beschieden gewesen, da das Familiengericht die Vorlage der Urkunde hätte anordnen können: Hätte die Ehefrau im Scheidungsverfahren auf das Immobilienvermögen hingewiesen, wäre der Richter verpflichtet gewesen, die Unterlagen zu verlangen, um den tatsächlichen Zugewinn ermitteln zu können.

Auskunftsanspruch mitversicherter Familienangehöriger – Scheidung 2.0

Wie bereits gezeigt und ohnehin immer wieder zu erfahren, sind gütliche Trennungen nicht unbedingt die Regel. Wie weit die Auseinandersetzungen gehen können, zeigt der folgende Fall:

Eine von Ihrem Ehemann getrennt lebende Frau wandte sich an die Aufsichtsbehörde für den Datenschutz, weil sie befürchtete, ihr (Ex-)Ehemann habe die für sie und das gemeinsame Kind abgeschlossenen privaten Krankenversicherungsverträge gekündigt. Von ihm selbst erhielte sie keine Information hierüber und von der Krankenversicherung sei eine Auskunft unter Hinweis auf datenschutzrechtliche Vorschriften verweigert worden.

Der datenschutzrechtliche Auskunftsanspruch ist ein höchst persönlicher und umfasst allenfalls noch unter elterlicher Sorge stehende Kinder, denen die Einsichtsfähigkeit fehlt, sowie Personen, die unter Betreuung stehen. Ein solcher Anspruch erstreckt sich also keinesfalls auf Versicherungsverträge des Ehegatten. Bei dieser puristischen Betrachtungsweise war das Versicherungsunternehmen sogar verpflichtet, die Auskünfte zu verweigern. Übersehen wurde dort jedoch, dass es der Petentin nicht darum ging, Informationen über ihren Ehemann, sondern über sich selbst zu erhalten. Gegenstand der Anfrage war weder die Vertragsausgestaltung noch der Rechnungsschuldner, sondern lediglich die mit „ja“ bzw. „nein“ zu beantwortende Frage, ob sie selbst und ihr Kind noch versichert seien. Ein solcher Auskunftsanspruch ist in § 34 Abs. 1 des Bundesdatenschutzgesetzes statuiert. Danach konnte die Petentin Auskunft über die zu ihrer Person gespeicherten Daten verlangen, so dass sich die Versicherung auch nicht auf die sie vermeintlich betreffende Schweigepflicht nach § 203 des Strafgesetzbuches (http://bundesrecht.juris.de/bundesrecht/stgb/gesamt.pdf) berufen durfte. Die Vor-

schrift stellt die Übermittlung personenbezogener Daten durch Mitglieder bestimmter Berufsgruppen unter Strafe. Am bekanntesten ist sicherlich das Arztgeheimnis, doch auch andere Gruppen fallen hierunter, so auch Mitarbeiter/innen von Krankenversicherungen. Ein Verstoß gegen die Schweigepflicht ist jedoch nicht gegenüber der/dem betroffenen Anfrager/in denkbar. § 203 StGB bezieht sich nun mal auf ein Geheimnis, also Angaben, die sich auf Dritte beziehen, die nicht mit der anfragenden Person identisch sind.

Das Versicherungsunternehmen schloss sich im Ergebnis unserer Auffassung an und erteilte der Petentin die gewünschten Auskünfte. Zudem wurde sie darüber informiert, dass nach § 178n Abs. 2 des Versicherungsvertragsgesetzes Krankenversicherungspolicen mitversicherter Personen nur dann gekündigt werden dürfen, wenn der Versicherungsnehmer vorher nachweisen kann, dass die Betroffenen hiervon Kenntnis erlangt haben. Diese eher unbekannte Vorschrift dient nach Auffassung der Aufsichtsbehörde für den Datenschutz zwar dem Schutz der Betroffenen; gerade in Situationen wie der beschriebenen vermag sie jedoch das positive Wissen nicht zu ersetzen.

Postmortaler Datenschutz

De mortuis nil nisi bene – über die Toten rede nur Gutes, sie können sich nämlich nicht wehren. Tote können sich nicht nur nicht mehr wehren, sie können überhaupt keine höchst persönlichen Rechte mehr geltend machen, dies betrifft auch das Recht auf informationelle Selbstbestimmung. Folglich gelten datenschutzrechtliche Vorschriften grundsätzlich auch nur für Lebende (s.a. 1. Tätigkeitsbericht, „Was muss bei der Ahnenforschung beachtet werden?“). Vor diesem Hintergrund sollte man meinen, dass die Aufsichtsbehörde für den Datenschutz sich eigentlich nicht mit den personenbezogenen Daten Verstorbener zu beschäftigen habe, dennoch erreichte uns hierzu eine interessante Eingabe einer gesetzlichen Krankenkasse:

Ein saarländisches Versicherungsunternehmen bat diese gesetzliche Krankenkasse um die Übermittlung von Krankheits- und Behandlungsdaten einer mittlerweile Verstorbenen, die bei der Versicherung einen Lebensversicherungsvertrag abgeschlossen hatte. Ursächlich für die Anfrage war eine interne Anweisung, nach der bei bestimmten Fallgruppen eine Leistungsprüfung zu erfolgen hat. Diese Fallgruppen werden definiert über die Art der Erkrankung und das Datum des Vertragsabschlusses. Versicherungen prüfen regelmäßig den Umfang ihrer Leistungsverpflichtung, insbesondere darauf, ob Todesursache nicht eine im Antrag verschwiegene Krankheit sein könnte.

Üblicherweise sind hiermit keine größeren Probleme verbunden, da in solchen Fällen regelmäßig für einen Zeitraum von bis zu 5 Jahren nach Antragstellung auf die Einwilligung der Versicherten bei Vertragsabschluss zurückgegriffen werden kann. Aufgrund einer solchen Einwilligung darf die Versicherung Ärzte und Angehörige anderer Heilberufe um Auskunft zu den Antragstellern bitten, um mit Hilfe von deren Informationen die Vertragsrisiken zu beurteilen. Zurzeit ist aus datenschutzrechtlicher Sicht gerade im Falle von Lebensversicherungen gegen diese Praxis nichts einzuwenden. Interessant war die Anfrage vor allem wegen der unterschiedlichen in Frage kommenden Rechtssphären: Die Datenerhebung durch die (private) Lebensversicherung erfordert im vorliegenden Fall keine Rechtsgrundlage, da keine personenbezo-

genen Daten erhoben werden. Anders hingegen verhält es sich bei der gesetzlichen Krankenkasse. Die Erhebung, Verarbeitung und Nutzung sog. „Sozialdaten“[19] Verstorbener ist nach den Vorschriften des Sozialgesetzbuches (http://www.bmgs.bund.de/download/gesetze_web/gesetze.htm - SGB) faktisch den gleichen Bedingungen unterworfen wie dies bei Daten Lebender der Fall ist. Folglich sind die unterschiedlichen Erfordernisse und rechtlichen Zwänge, denen die hier beteiligten Versicherungsunternehmen unterworfen sind, nicht ohne weiteres kompatibel.

Der Datenschutzbeauftragte der gesetzlichen Krankenkasse bat uns, Art und Umfang des Auskunftsanspruches der hier ansässigen Versicherung zu prüfen, sowie als Vermittler bei der Konzeption eines Verfahrens zu helfen, das in solchen Fällen die Belange aller Beteiligten ausreichend berücksichtigt.

Das Interesse des saarländischen Versicherungsunternehmens, zu prüfen, ob tatsächlich eine Leistungsverpflichtung vorlag, konnte nachvollzogen werden. Da es sich bei den Krankheitsdaten der Verstorbenen nicht um personenbezogene Daten handelte, bedurfte es keiner Prüfung datenschutzrechtlicher Vorschriften zur Erhebung personenbezogener Daten. Die in diesem Zusammenhang ebenfalls gestellte Frage, ob das Grundrecht auf informationelle Selbstbestimmung auf den Erben übergeht, musste hier nicht geprüft werden[20]. Das Versicherungsunternehmen war daher aus Sicht der Aufsichtsbehörde für den Datenschutz berechtigt, die Daten anzufragen. Damit korrespondierte jedoch keine Verpflichtung der gesetzlichen Krankenkasse, eben jene Daten auch zu übermitteln. Dieser war es allenfalls erlaubt, die erbetenen Daten zu übermitteln, verpflichtet war sie dazu nicht. § 35 Abs. 5 Satz 2 SGB X erlaubt zwar die Nutzung personenbezogener Daten Verstorbener auch dann, wenn ihre schutzwürdigen Interessen oder die ihrer Angehörigen dadurch nicht beeinträchtigt werden können. Gerade das war jedoch aus der Anfrage nicht ersichtlich, so dass der Datenschutzbeauftragte der gesetzlichen Krankenkasse sich außer Stande sah, dem Begehren nachzugeben.

Letztlich war die Diskussion um die Datenübermittlung also lediglich auf die nicht ausreichend transparente Anfrage des saarländischen Versicherungsunternehmens zurückzuführen. Dort erklärte man sich daher auch bereit, Anfragen künftig so zu formulieren, dass sich die Anfragegründe nicht erst infolge der Tätigkeit der Aufsichtsbehörde für den Datenschutz erschließen.

Wer speichert welche personenbezogenen Daten wo, wie lange, warum und wozu?

Die Überschrift bringt eine Grundfrage zum Ausdruck, die allen Aufsichtsbehörden für den Datenschutz immer wieder gestellt wird und die nur mit Hilfe einer der beliebtesten juristischen Formulierungen beantwortet werden kann: „Es kommt darauf an!“. Es kommt in der Tat darauf an, wer die Daten erhebt, verarbeitet und nutzt, ebenso wie auf die Arten der personenbezogen Daten. Es ist für die Beurteilung erheblich, wo

[19] § 67 Abs. 1 SGB X definiert personenbezogene Daten, die von Sozialleistungsträgern zur Erfüllung ihrer Aufgaben erhoben, verarbeitet oder genutzt werden, als Sozialdaten.
[20] Grundsätzlich stellen die allgemeinen Persönlichkeitsrechte höchst persönliche dar, die nicht übertragbar sind, auch nicht im Erbfall. Eine Ausnahme gilt allenfalls für den über den Tod hinausreichenden kommerzialisierbaren Teil des allgemeinen Persönlichkeitsrechts, so z. B. Fotos Prominenter.

die personenbezogenen Daten gespeichert sind, in der EU oder in einem unsicheren Drittland. Es existiert zudem keine allgemein gültige Speicherfrist[21]. Der Erhebungsgrund ist nur individuell feststellbar ebenso wie der Zweck der weiteren Verarbeitung und Nutzung.

Im Spannungsfeld wiederum zwischen gesetzlicher und privater Krankenversicherung angesiedelt war die Frage, welche Kasse welche Daten auf welcher Grundlage speichern dürfe. Zu Grunde lag die Vermutung, dass

- unterschiedliche Rechtsgrundlagen in verschiedenen rechtlichen Ausprägungen existierten, und
- dass beide Formen der Krankenversicherungen auch qualitativ unterschiedlich personenbezogene Daten erheben, verarbeiten und nutzen.

Dem ist tatsächlich so. Die Rechtsgrundlagen für beide Versicherungsformen sind – wie bereits beschrieben – unterschiedlich. Die gesetzliche Krankenversicherung ist im Sozialgesetzbuch V (SGB V) öffentlich-rechtlich geregelt, die private hingegen im Versicherungsvertragsgesetz in Verbindung mit dem privatrechtlichen Versicherungsvertrag.

Die Datenerhebung folgt dem Erforderlichkeitsgrundsatz. Demnach ist sie nur zulässig, wenn die Kenntnis der personenbezogenen Daten für die Aufgabenerfüllung erforderlich ist. Im Falle von Versicherungen ist dies vor allem für Zwecke der Abrechung denkbar. Die gesetzliche Krankenversicherung ist so organisiert, dass sich die Krankenkassen zur Abrechnung mit den Behandlungsträgern der Kassenärztlichen Vereinigungen bedienen. Nach der Vorschrift des § 285 Abs. I SGB V überweisen die Träger der gesetzlichen Krankenversicherung den Vereinigungen eine Gesamtsumme, deren Höhe sich nach der Anzahl der jeweiligen Versicherten im jeweiligen Bezirk richtet. Diese Summe ist Basis für die Abrechnung der Kassenärztlichen Vereinigung mit den Behandlungsträgern. Die Abrechnung mit der Krankenkasse wiederum erfolgt grundsätzlich fallbezogen, lediglich bei bestimmten Leistungen regelt § 295 Abs. 2 SGB V, dass personenbezogene Daten der Patientinnen und Patienten an die gesetzliche Krankenkasse zu übermitteln sind.

Anders verhält es sich bei der privaten Krankenversicherung. Privat Krankenversicherte gehen einen zivilrechtlichen Behandlungsvertrag ein, der auch die Verpflichtung umfasst, die erbrachten Leistungen zu bezahlen. Grundlage ist ein ausführlicher Leistungsnachweis in Form einer Rechnung der/des jeweils Behandelnden an die/den Versicherte/n. Diese/r wiederum kann unter Vorlage der Rechnung Kostenersatz im Rahmen des jeweils vertraglich Vereinbarten verlangen.

Übermittlung personenbezogener Daten an ein Versicherungsunternehmen

Versicherungen erheben in unterschiedlichen Zusammenhängen personenbezogene Daten der Versicherten wie auch der Antragsteller. Umfang und Arten der zu erhe-

[21] Zu den wenigen fest vorgegebenen Fristen zählen die Speicherfristen nach dem Handelsgesetzbuch (in der Regel 10 Jahre), bei Auskunfteien (Relevanzprüfung nach 4 Kalenderjahren) sowie den ärztlichen Berufsordnungen (10 Jahre nach Abschluss der Behandlung).

benden personenbezogenen Daten richten sich nach dem Verarbeitungszusammenhang, vornehmlich bestimmt durch das jeweils zu versichernde Risiko (Leben, Gesundheit, KFZ, Haus, Haftpflicht, Rechtsschutz etc.). Gemeinsames Element aller genannten Fälle ist, dass das Versicherungsunternehmen aktiv die benötigten Daten erhebt. Anders in einem der Aufsichtsbehörde für den Datenschutz zur rechtlichen Beurteilung vorgelegten Fall:

Ein Autofahrer, der infolge einer Unachtsamkeit einen Unfall mit Sachbeschädigung verursacht hatte, musste erfahren, dass die Geschädigte sich direkt mit seiner Versicherung in Verbindung gesetzt und diese über den Vorfall informiert hatte. Der Versicherungsnehmer bat unter Hinweis darauf, dass die Schadensersatzpflicht zunächst ihn und eben nicht die Versicherung treffe, um eine datenschutzrechtliche Beurteilung der Datenübermittlung.

Grundsätzlich ist der Auffassung des Betroffenen zuzustimmen. In § 823 des BGB ist die Ersatzpflicht der Schädigerin/des Schädigers geregelt. Danach ist sie/er dem Grunde nach selbst verpflichtet, einen von ihr/ihm verursachten Schaden zu regulieren. Vereinfacht ausgedrückt: Jede/r haftet zunächst selbst für den Schaden, den er oder sie verursacht hat. Dies geht einher mit der Geltendmachung von Ersatzansprüchen der/des Geschädigten gegenüber der/dem Schädiger/in. Auch das Versicherungsvertragsrecht folgt nahezu durchgängig dieser bewährten Festlegung. Eine Ausnahme ist allerdings im Pflichtversicherungsrecht zu finden: Nach § 1 des Pflichtversicherungsgesetzes (http://dejure.org/gesetze/PflVG) ist der Halter eines Kraftfahrzeuges verpflichtet, für sich, den Eigentümer und den Fahrer eine Haftpflichtversicherung abzuschließen. Nach § 3 Nr. 1 dieses Gesetzes kann ein/e Dritte/r (Geschädigte/r) im Rahmen der Leistungspflicht ihren/seinen Anspruch auf Schadensersatz auch gegenüber der Versicherung geltend machen. Dies setzt selbstverständlich auch die Übermittlung personenbezogener Daten an die Versicherung voraus. Nach Nummer 2 der Vorschrift haften dann Versicherer und Versicherungsnehmer/in als Gesamtschuldner.

Grundsätzlich ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann erlaubt, wenn eine Rechtsvorschrift dies erlaubt bzw. anordnet oder die Betroffenen darin eingewilligt haben (§ 4 Abs. 1 des Bundesdatenschutzgesetzes). Rechtsgrundlage für die Datenübermittlung war hier § 3 des Pflichtversicherungsgesetzes. Danach war die Übermittlung im Ergebnis zulässig.

Reiserücktrittsversicherung

Urlaub ist die schönste Zeit des Jahres und wenn diese doch einmal durch Krankheit getrübt werden sollte, möchte man wenigstens finanzielle Belastungen vermeiden. Dazu dient eine Reiseversicherung, genauer: eine Reiserücktrittskostenversicherung. Entgegen einer vielfach verbreiteten Auffassung stellen Versicherungen keine organisatorische Sonderform von Banken oder Sparkassen dar. Ihre Zweckbestimmung ist es nicht, eingezahlte Risikoprämien an die Versicherungsnehmer/innen zurückzuzahlen, sondern bestimmte Fährnisse des Lebens auszugleichen. Demzufolge sind die Versicherungen auch gehalten und berechtigt, die tatsächliche Leistungspflicht zu prüfen. In diesem Zusammenhang dürfen auch personenbezogene Daten erhoben werden, soweit dies der Vertragserfüllung dient. Dass dies auch kommuniziert und so transparent gemacht werden muss, ist leider noch nicht bei allen Versicherungen zu

einer allgemeinen Erkenntnis geworden, wie die Aufsichtsbehörde für den Datenschutz feststellen musste.

Ein Versicherungsunternehmen forderte von den Betroffenen, welche die Leistungen der Reiserücktrittskostenversicherung in Anspruch nehmen wollten, umfangreiche Angaben, die nebst anderem auch den Beruf und ärztliche Atteste mit Diagnosen und Behandlungsdaten betrafen. Hiermit waren die Betroffenen nicht einverstanden, da ihrer Meinung nach eine Bestätigung des Krankenhauses über die Dauer der stationären Behandlung ausreichen müsste. Auf Nachfrage teilte uns das Versicherungsunternehmen mit, dass sie im Rahmen einer solchen Versicherung nach den „Allgemeinen Versicherungsbedingungen“ und dem Versicherungsvertragsgesetz berechtigt sei, die Ursachen einer Reisestornierung zu erfahren. Eine Leistungspflicht bestehe nach den vertraglichen Vereinbarungen insbesondere bei schwerer Unfallverletzung, unerwarteter schwerer Erkrankung oder nicht abzusehender Verschlechterung des bekannten Gesundheitszustandes. Dies alles sei aus der Verweildauer im Krankenhaus nicht zu erkennen.

Die „Allgemeinen Versicherungsbedingungen“ sind als „Allgemeine Geschäftsbedingungen“ Bestandteil des Versicherungsvertrages. Aus datenschutzrechtlicher Sicht waren sie nicht zu beanstanden, zumal sie die Rechte der Betroffenen im konkreten Fall nur so weit einschränkten, wie es für die Vertragserfüllung unbedingt erforderlich war.

Die ebenfalls erfragten Angaben zum Beruf hingegen waren nicht erforderlich. Die Versicherung hat dies anerkannt und zugesagt, die Formulare zu ändern. Was das Kommunikationsproblem anbetrifft, so hatte man dies ebenfalls wohl bereits erkannt und den Betroffenen zugesagt, deren Kritik künftig ernst zu nehmen.

Ausweiskopien und Erheben von Ausweisdaten

„Kopieren geht über studieren“. In vielen Bereichen des täglichen Lebens ist dies zu einer Maxime der Arbeitserleichterung geworden. Eine weitere allgemein gültige Feststellung ist die, dass sich die Verifizierung des nicht persönlich bekannten Menschen mittels Personalausweises bewährt und so auch Eingang in das Geschäftsleben gefunden hat.

Immer häufiger muss allerdings festgestellt werden, dass in Kombination des Bewährten auch Personalausweise kopiert werden. Mit Blick auf eine eventuell notwendige Beweissicherung kann dies durchaus nachvollziehbar sein, doch es stellt sich die Frage, ob es tatsächlich erforderlich ist, alle dort aufgeführten Daten[22] zu erhe-

[22] Nach § 1 Abs. 2, 3 des Personalausweisgesetzes (http://bundesrecht.juris.de/bundesrecht/persauswg) sind dies Familienname und ggf. Geburtsname, Vornamen, Doktorgrad, Ordensname/Künstlername, Tag und Ort der Geburt, Größe, Farbe der Augen gegenwärtige Anschrift, Staatsangehörigkeit, sowie in der Zone für das automatische Lesen: die Abkürzung "IDD" für "Identitätskarte der Bundesrepublik Deutschland", der Familienname, der oder die Vornamen, die Seriennummer des Personalausweises, die sich aus der Behördenkennzahl der Personalausweisbehörde und einer fortlaufend zu vergebenden Ausweisnummer zusammensetzt, die Abkürzung "D" für die Eigenschaft als Deutscher, der Tag der Geburt, die Gültigkeitsdauer des Personalausweises, die Prüfziffern und Leerstellen.

ben. Mit Sicherheit kann man dies zumindest für die Ausweisnummer hinterfragen, auch eingedenk dessen, dass es sich bei jener um ein eindeutig zurechenbares Merkmal handelt, welches auf die/den Inhaber/in, die zuständige Ausweisbehörde etc. verweist.

In der Bank

Eine langjährige Kundin einer damals noch rechtlich selbstständigen Tochtergesellschaft einer Deutschen Großbank hatte sich an die Aufsichtsbehörde für den Datenschutz gewandt und darauf hingewiesen, dass ihr Personalausweis gegen ihren Willen von Bankmitarbeiter/innen kopiert worden sei. Anlass war eine erforderlich gewordene Überprüfung der bei der Bank gespeicherten Kundendaten.

Soweit solche Relevanzprüfungen zu erhebender oder bereits gespeicherter personenbezogener Daten nach den Vorgaben der Abgabenordnung oder des Geldwäschegesetzes erfolgen, ist selbstverständlich nichts dagegen einzuwenden, dass auch Personalausweise *kontrolliert* werden. Anders verhält es sich, wenn Ausweispapiere gegen den Willen der Betroffenen *kopiert* werden. Keine der genannten Vorschriften enthält eine Verpflichtung zu einer solchen Vorgehensweise, das Geldwäschegesetz lässt beispielsweise den Banken die Wahlfreiheit, eine Ausweiskopie zu verlangen oder die (erforderlichen) Daten aufzuzeichnen.

Lt. Stellungnahme der Bank konnte der konkrete Vorgang von dort nicht nachvollzogen werden[23] und zudem wurde darauf verwiesen, dass die Legitimationsprüfung nach den bankinternen Arbeitsanweisungen grundsätzlich die Kopie des vorgelegten Ausweises vorsehe, in begründeten Fällen – Ablehnung der Betroffenen – jedoch auch die Möglichkeit offen stehe, die Angaben zu notieren.

Nach Auffassung der Aufsichtsbehörde für den Datenschutz ist dieses Vorgehen dann nicht zu beanstanden, wenn die Kundinnen und Kunden eingewilligt haben. Dies setzt zumindest eine Nachfrage voraus, da es der freien Entscheidung der Betroffenen obliegt, das Kopieren der Ausweispapiere zu gestatten. Der Schilderung der Bank war hier allerdings zu entnehmen, dass die Mitarbeiterinnen und Mitarbeiter das Ablichten als Regelfall ansehen, was erfahrungsgemäß zu Missverständnissen zwischen diesen und den Kundinnen und Kunden führen kann. Die Aufsichtsbehörde für den Datenschutz hat hierzu gegenüber der Bank die Auffassung vertreten, dass ein handschriftliches Notieren der für die Kontrolle erforderlichen Daten aus den Ausweispapieren als vollwertige Alternative zum Kopieren derselben empfohlen werden sollte.

Auf mehrfache Bitte mitzuteilen, wie künftig verfahren werden sollte, hat die Bank nicht reagiert, sondern lediglich darauf verwiesen, dass sich in Folge der zwischenzeitlich stattgefundenen Verschmelzung mit der Muttergesellschaft nunmehr die datenschutzrechtliche Kontrollzuständigkeit auf die für dieses Unternehmen zuständige

---

[23] Hierzu ist anzumerken, dass die Aufsichtsbehörde für den Datenschutz grundsätzlich auf eine Namensnennung verzichtet, wenn aus der Eingabe ersichtlich ist, dass der vermutete Verstoß auf organisatorischen o. ä. Fehlern beruht. Dem war hier so gewesen. Die Vorgabe, Personalausweise zu kopieren, war für die handelnden Mitarbeiter/innen eine ständige Übung, deren Beurteilung nicht der Mitteilung des Namens der Petentin bedurfte.

Aufsichtsbehörde für den Datenschutz übergegangen sei. Daher musste der Vorgang zur endgültigen Beurteilung dorthin abgegeben werden.

Beim Einkauf

Eine denkbare Alternative zum Kopieren stellt demnach das Notieren der erforderlichen Angaben dar. Allerdings sind auch hierbei bestimmte rechtliche Vorgaben zu beachten wie z. B. die Information der Betroffenen.

Durch einen Kunden wurde die Aufsichtsbehörde für den Datenschutz darauf hingewiesen, dass in einem Supermarkt bei Zahlung im Lastschriftverfahren u. a. die Personalausweisnummer kontrolliert und notiert werde. Um Stellungnahme gebeten, teilte die Marktleitung mit, dass bei Rechnungen, die einen Betrag von 50 € überschritten, die Kunden um eine freiwillige Vorlage der Personalausweises zur Kontrolle und Notierung des Namens und Ausweisnummer gebeten würden. Alternativ bestünde die Möglichkeit der Barzahlung.

Grundsätzlich liegt es in der freien Entscheidung des Unternehmens, ob – wie hier – das Lastschriftverfahren als Zahlungsmöglichkeit überhaupt angeboten wird. Im Vergleich zu anderen Varianten des unbaren Zahlungsverkehrs stellt dieses Verfahren prinzipbedingt ein sehr unsicheres Verfahren dar, da weder eine Mindestdeckung existiert, noch das Verfahren selbst eine Verifizierung der/des Kundin/Kunden erlaubt. Die Kontrolle der Ausweispapiere liegt daher als bedingter Schutz vor Zahlungsausfällen auch aus datenschutzrechtlicher Sicht im berechtigten Interesses der Gewerbetreibenden. Allerdings erfordert das anschließende Notieren der Ausweisnummer eine Information der Kundinnen und Kunden über die Verwendung der Daten; dies kann auch durch Aushang erfolgen. Die Einwilligung in die Datenerhebung muss grundsätzlich schriftlich erfolgen, hierfür bietet sich der eigentliche Lastschriftbeleg an. Nach Zahlungseingang sind die Notizen zu vernichten.

Grundsätzlich besteht bei allen unbaren Zahlungsformen prinzipbedingt das Problem der Authentifizierung, auf die es vor allem im Falle von Zahlungsausfällen eben ankommt. Um dem zu begegnen, wurden mehrere Verfahren entwickelt, die sowohl datenschutzrechtlichen Anforderungen wie auch den Interessen des Handels und der Banken gerecht werden. So erfordert das PIN-basierte EC-Cash-Verfahren[24] keine weitere Erhebung personenbezogener Daten, da die Zahlungsbestätigung unmittelbar beim Bezahlvorgang erfolgt und die weitere Abwicklung lediglich das Verhältnis Kundin/Kunde und Bank betrifft.

[24] **Electronic Cash** (kurz: *EC-Cash, ec-cash*) ist eines von vier Zahlungsverfahren zum bargeldlosen und kartengestützten Bezahlen von Waren und Dienstleistungen mit der EC-Scheckkarte oder Bankkundenkarte. Die drei anderen Zahlungsverfahren sind Geldkarte, POZ und ELV. Electronic Cash wird mit einer PIN (Persönliche Identifikationsnummer) beim Bezahlvorgang über sogenannte EFT-POS-Terminals (Electronic-Fund-Transfer-Terminals, Elektronische-Wert-Übertragungs-Terminals) abgewickelt. Die Bezeichnung EC stammt ursprünglich von Eurocheque, einem europaweiten, einheitlichen Scheckzahlungssystem in Verbindung mit einer Bankgarantie. Heute wird EC als Abkürzung für Electronic Cash genutzt. Ähnliche Systeme sind „maestro“ und „Visa Electron“ (Quelle: wikipedia).

Bei der Anzeigenaufnahme

Wie im vorstehenden Fall geschildert, lehnt die Aufsichtsbehörde für den Datenschutz weder das Kopieren von Personalausweisen noch das Notieren der dort enthaltenen Angaben in jedem Fall ab, es muss allerdings feststehen, zu welchem Zweck die Daten so erhoben werden und zudem eine Einwilligung der Betroffenen vorliegen. Zahlungsausfälle sind ein triftiger Grund für eine solche Datenerhebung; die Bereitschaft, vorab in bar zu zahlen, müsste demgegenüber das Kopieren von Personalausweisen obsolet machen. Weit gefehlt, wie ein Petent erfahren musste, der in einem Lokalblatt eine Todesanzeige aufgeben und im Voraus bar bezahlen wollte. Von ihm wurde die Vorlage des Personalausweises gefordert, um diesen zu kopieren. Als Erklärung wurde angegeben, dies sei nötig, um den Auftraggeber nachträglich identifizieren zu können, falls in böswilliger Absicht eine falsche Anzeige aufgegeben worden sei.

Nun liegt es in der Natur der Sache, dass anonym oder unter falschen Angaben aufgegebene Anzeigen auch falsche Angaben enthalten, gar einen lebenden Menschen für vermeintlich tot erklären können. Dies alles ist den Anzeigenredaktionen nicht fremd, wie der Aufsichtsbehörde für den Datenschutz glaubhaft versichert wurde. Daher wurde durchaus ein berechtigtes Interesse an einer sicheren Verifizierung der Auftraggeber anerkannt, allerdings nur für einen relativ kurzen Zeitraum von 2 Monaten, der ausreichen müsste, um solche Vorfälle im Nachhinein noch zuordnen zu können. Eine Kopie des Ausweises ist wie in anderen Fällen auch nur mit Einwilligung des Betroffenen zulässig.

Videoüberwachung und webcams

Wie bereits in den FAQs ausgeführt, nimmt die Videoüberwachung des öffentlichen Lebens immer weiter zu. In dem Zusammenhang vermag es kaum zu beruhigen, dass die weit überwiegende Mehrheit der Videokameras von privaten Stellen betrieben wird. Die in diesem Kapitel geschilderten Fälle stellen nur einen Bruchteil der Anfragen zu dem Komplex „Video“ dar, da die meisten Fälle telefonisch an die Aufsichtsbehörde für den Datenschutz herangetragen wurden. Gerade diese Anfragen bezogen sich mehrheitlich auf die allgemeinen Zulässigkeitsvoraussetzungen, wobei zwei Schwerpunkte auszumachen waren:

- Die gewollte oder ungewollte Überwachung von Nachbargrundstücken sowie
- die Videoüberwachung im Arbeitsumfeld.

Ersteres unterfällt nicht der Regelung des § 6b des Bundesdatenschutzgesetzes, da dort lediglich die Überwachung öffentlich zugänglicher Räume geregelt wird. Private umgrenzte Grundstücke fallen eben nicht hierunter, so dass Rechtsschutz hier im Wege der Zivilklage gesucht werden muss. Die Aufsichtsbehörde für den Datenschutz kann daher in solchen Fällen die Parteien nur auf die Rechtsprechung der Zivilgerichte verweisen und darauf hinwirken, wenn schon nicht die Rechte der Nachbarn, so doch die einschlägigen Urteile zu beachten.

Anfragen zur Videoüberwachung am Arbeitsplatz wurden durchweg anonymisiert oder verbunden mit dem Wunsch, noch nicht tätig zu werden, an die Aufsichtsbehörde für den Datenschutz herangetragen. Daher konnten in diesem Zusammenhang lediglich allgemeine Hinweise zur Mitwirkungspflicht des Betriebsrates und zur Unterscheidung zwischen öffentlich zugänglichen Räumen, z. B. Ladenlokalen, und anderweitigen Räumlichkeiten (Sozialräume beispielsweise) gegeben werden.

Die Überwachung eines Betriebsgeländes

Aufgrund einer Eingabe hatte die Aufsichtsbehörde für den Datenschutz Gelegenheit, die Funktionalitäten einer modernen Videoüberwachungsanlage kennen zu lernen. Konkret bezog sich die Eingabe auf die Überwachung eines Betriebsgeländes mit Videokameras, von denen mindestens eine so schwenkbar sei, dass vom Beobachtungsbereich auch die benachbarten Gärten umfasst würden.

Vor Ort konnte dann festgestellt werden, dass die Angaben zumindest subjektiv zutrafen: Tatsächlich waren insgesamt 8 Kameras zur Überwachung des gesamten Betriebsgeländes installiert, von denen eine als Schwenkkamera zur Überwachung der Einfahrt ausgelegt war. Die Justierung dieser Kamera wurde anhand von 4 festgelegten Referenzpunkten vorgenommen, von denen einer außerhalb des Betriebsgrundstückes lag. Diese Referenzpunkte stellen die Begrenzung des weitesten denkbaren Schwenkbereichs dar und sollten, so die Erläuterungen des installierenden Unternehmens, von dem Betreiber gar nicht angewählt werden können, da hierfür ein Zugang mittels Konfigurationspasswort erforderlich wäre. Jenes wiederum sollte dem eigentlichen Betreiber, also dem Besitzer des Betriebsgeländes, nicht bekannt sein.

Aufzeichnungen waren nur innerhalb des Betriebsgeländes möglich. Zu diesem Zweck wurde der gesamte denkbare Aufnahmebereich softwaregesteuert in ein virtuelles Raster zerlegt, anhand dessen der Aufnahmebereich definiert wurde. So sollte sichergestellt werden, dass tatsächlich nur Vorgänge auf dem Betriebsgelände aufgezeichnet werden können. Nach den Feststellungen der Aufsichtsbehörde für den Datenschutz ist es bei ordnungsgemäßem Funktionieren der Anlage in der Tat nicht möglich, die Nachbargrundstücke zu überwachen und Aufzeichnungen herzustellen.

Ursächlich für die Installation der Videoanlage waren Versicherungsauflagen, was aus Sicht der Aufsichtsbehörde für den Datenschutz eine solche Maßnahme dem Grunde nach rechtfertigte. Das Bundesdatenschutzgesetz regelt in § 6b unter anderem, dass die Beobachtung öffentlich zugänglicher Räume mit Videotechnik auch zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig sei. Da unter den Begriff des berechtigten Interesses jedes von der Rechtsordnung anerkannte fällt, sei es privat oder öffentlich, ideell oder finanziell, war das Interesse am Schutz des Eigentums durchaus als berechtigtes anzuerkennen. Auch der Zweck war nachvollziehbar und allein schon durch die Versicherungsauflagen festgelegt, nämlich Abschreckung und nachträgliche Beweissicherung, so dass nach einer Anpassung der Kamerakonfiguration ein rechtmäßiger Zustand hergestellt war. Schutzwürdige Interessen der Betroffenen waren objektiv nicht tangiert, wenngleich das subjektive Gefühl des „Beobachtet-Werdens“ nachempfunden werden konnte.

Kamera und Kantine

Manche Kamera dient Zwecken, die sich auf den ersten Blick nicht erschließen, so auch im Falle einer Kamera, die im Treppenaufgang zu einer Kantine angebracht war.

Seitens der Geschäftsleitung wurde auf Anfrage mitgeteilt, die Videobeobachtung diene dem Koch dazu, sich einen Überblick über die Zahl der unmittelbar (zu er-) wartenden Gäste zu verschaffen. Da die Treppe weder von der Essenausgabe noch von der Küche aus einsehbar war und ist, konnte diese Begründung durchaus nachvollzogen werden. Nach § 6b Abs. 1 Nr. 3 des Bundesdatenschutzgesetzes ist die Videobeobachtung unter anderem dann zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das „berechtigte Interesse“ ist ein unbestimmter Rechtsbegriff, der von den Gerichten inhaltlich voll überprüfbar ist. Die Spannbreite umfasst jedes von der Rechtsordnung geschützte objektive Interesse (s.a. „Die Überwachung eines Betriebsgeländes“, letzter Absatz). Dieses geforderte objektiv nachvollziehbare Interesse zu einem konkret festgelegten Zweck dürfte durch die Notwendigkeit, ausreichend viele Essen zeitgerecht zuzubereiten, gegeben sein, da Voraussetzung hierfür eine annähernd genaue Kenntnis der Zahl Wartender ist.

Problematisch erschien hingegen die Erforderlichkeit der Kamerainstallation. Erforderlich bedeutet, dass der mit der Videobeobachtung verfolgte Zweck (hier: die bedarfsgerechte Essenzubereitung) nicht, nicht vollständig, nicht zeitgerecht oder nicht rechtmäßig erreicht werden kann. Die Beobachtung der Wartenden, um so dem Küchenleiter einen Anhaltspunkt zu verschaffen, wie viele Essen noch zuzubereiten sind, wäre u. U. auch anderweitig denkbar.

Letzten Endes konnte diese Frage jedoch offen bleiben, da in Anbetracht der technischen Voraussetzungen eine Identifizierung der Wartenden angesichts der optischen Qualität der Kamera kaum möglich war. Daher war die durchgeführte reine Beobachtung ohne Aufzeichnung angesichts des vergleichsweise geringen Eingriffs in die Rechtsposition der Betroffenen noch zulässig.

Wie in den ➔FAQ bereits angesprochen, erfordert jede Videoüberwachung öffentlich zugänglicher Räume einen Hinweis auf die Maßnahme selbst sowie auf die verantwortliche Stelle. Entsprechende Schilder sollten an den äußeren Glaseingangstüren zum Gebäude angebracht werden und mittels Piktogramm auf die Kameras und den Trägerverein als verantwortliche Stelle hinweisen. Dies wurde auch zugesagt.

Die webcam als Stauwarner

Straßenbauarbeiten bewirken Verkehrsbehinderungen und Staus. Diese unausweichliche Kausalfolge bringt zudem Ärger und Zeitverzögerungen mit sich. Der Gewerbeverband einer saarländischen Gemeinde wollte dem mittels einer webcam zumindest etwas entgegenwirken. Beabsichtigt war, durch die Live-Bilder über die aktuelle Stausituation zu informieren, so dass jede/r Interessierte sich im wahrsten Sinne des Wortes ein „Bild“ über die Verkehrssituation verschaffen konnte.

Die Kamera selbst sollte fest installiert werden und weder schwenk- noch drehbar sein, zudem sollte die Grundeinstellung (Zoom) nur vom Gewerbeverband selbst verändert werden können.

Zulässig war die Maßnahme nach Auffassung der Aufsichtsbehörde für den Datenschutz nur dann, wenn die bereits beschriebenen Voraussetzungen des § 6b des Bundesdatenschutzgesetzes erfüllt waren. Dem war hier so; da zudem weder Personen noch Autokennzeichen erkennbar waren, wurde dem Gewerbeverband auf Nachfrage bestätigt, dass der Betrieb der webcam aus datenschutzrechtlicher Sicht unbedenklich sei.

Kreditschutzorganisationen/Auskunfteien

Kreditschutzorganisationen/Auskunfteien sammeln personenbezogene Daten, um diese auf Anfrage zu übermitteln. Geregelt ist deren Tätigkeit in § 29 des Bundesdatenschutzgesetzes. Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient, ist zulässig, wenn

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

Die Daten dürfen dann übermittelt werden, wenn der Anfrager ein berechtigtes Interesse an den Daten nachweisen kann. Ein solches liegt grundsätzlich bei jedem von der Rechtsordnung gedeckten finanziellen oder ideellen, öffentlichen oder privaten Interesse vor. Weiter darf kein Grund zur Annahme bestehen, dass Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

Der Nachweis dieses Interesses erfolgt zumeist über standardisierte Anfragen wie beispielsweise „Bonitätsprüfung“ oder Fragen zu Bürgschaften, Kreditkarten, Girokonten, Warenkrediten, Krediten, Hypotheken oder bestehenden Grundschulden. Seit der Novellierung des Bundesdatenschutzgesetzes können Betroffene durch die Vorschrift des § 34 Absatz 2 Auskunft über Herkunft und Empfänger der Daten verlangen, soweit hierdurch nicht Geschäftsgeheimnisse verletzt werden. Die Aufsichtsbehörden für den Datenschutz vertreten in diesem Zusammenhang die Auffassung, dass bei Datenübermittlungen an Unternehmen folgender Branchen stets die Auskunftsempfänger bekannt zu geben sind:

- Banken,
- Factoringgesellschaften,
- konzernangehörige Gesellschaften,
- Leasinggesellschaften,
- Telekommunikationsunternehmen,

- Versicherungen und
- Versandhandel.

Diese Liste basiert auf einem Vorschlag des Verbandes der Handelsauskunfteien (VdH), der von den Aufsichtsbehörden für den Datenschutz angenommen wurde. Anzumerken ist, dass bei anderen Datenempfängern eine Einzelfallentscheidung erforderlich ist.

Datenübermittlung an ein Risk-Management-Unternehmen

In wirtschaftlich schwierigen Zeiten wächst das Kreditausfallrisiko, diese Feststellung aus dem ersten Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz gilt leider immer noch. Banken sind aufgrund der ➔Basel-II-Vorgaben gehalten, das Risiko bei Unternehmenskrediten bereits vorab zu bewerten und in die Entscheidung einfließen zu lassen. Der Schutz vor solchen Verlusten wird als berechtigtes Interesse auch von den Aufsichtsbehörden für den Datenschutz anerkannt.

Größere Konzerne verfügen oft über eigene Tochterunternehmen, deren einzige Aufgabe Risikobewertungen sind. Die hierfür notwendigen Informationen stammen sowohl von anderen Konzernunternehmen wie auch aus öffentlich zugänglichen Registern wie dem Schuldnerverzeichnis oder von Auskunfteien. So auch hier:

Ein Petent hatte sich an die Aufsichtsbehörde für den Datenschutz gewandt, weil eine im Saarland ansässige Auskunftei seine personenbezogenen Daten übermittelt hatte, ohne ihn darüber zu informieren, wer der Empfänger war. Weiter ging es darum zu erfahren, ob Angaben, die seiner privaten Homepage entnommen waren, von der Auskunftei genutzt werden durften, um ihn anzurufen.

Datenempfänger war ein solches Risk-Management-Unternehmen, das im Rahmen einer Bonitätsprüfung Informationen über den Petenten erhob. Es handelte sich somit um ein Unternehmen, bei dem selbst der VdH davon ausgeht, dass kein überwiegendes Interesse an der Wahrung eines Geschäftsgeheimnisses besteht, so dass der Adressat bekannt gegeben werden musste. Dies ist auch erfolgt.

Die der Homepage entnommenen Daten durften genutzt werden, da es sich um solche handelte, die aus allgemein zugänglichen Quellen stammten und zudem noch vom Petenten selbst veröffentlicht wurden. Ein überwiegendes schutzwürdiges Interesse konnte daher nicht von vornherein unterstellt werden. Es war wohl auch nicht weiter schwierig, die monierten Informationen zu erheben, da eine Google-Suche mehrere Treffer erbrachte, die allesamt direkte Informationen über den Petenten enthielten.

Auch in einem weiteren Fall wurde die Auskunftei, der übrigens nach glaubhafter Darstellung die VdH-Liste nicht bekannt war, darauf hingewiesen, dass schutzwürdige Geschäftsinteressen nicht bestünden und mithin die erbetene Auskunft zu erteilen war.

Eine Einzelfallentscheidung

Der „Löwenanteil“ des Auskunfteigeschäfts besteht aus Datenübermittlungen an die genannten Branchen, so dass nach Auffassung der Aufsichtsbehörde für den Datenschutz eher selten ein Interesse an der Wahrung von Geschäftsgeheimnissen geltend gemacht werden kann. In einem besonderen Fall jedoch schien dem so zu sein. Eine hiesige Auskunftei hatte erstmalig personenbezogene Daten eines Betroffenen übermittelt und diesen entsprechend der Vorgabe des § 33 Abs. 1 Satz 2 des Bundesdatenschutzgesetzes informiert. Die Frage des Betroffenen nach dem Auskunftsempfänger blieb mit Verweis auf das Geschäftsgeheimnis unbeantwortet. Die Prüfung durch die Aufsichtsbehörde für den Datenschutz ergab, dass Datenempfänger eine Rechtsanwaltskanzlei war. Bei dieser handelte es sich also nicht um ein Unternehmen, bei dem ein besonderes Geschäftsgeheimnis schon pauschal zu verneinen war. Da der Betroffene jedoch nach aller Lebenserfahrung mit dieser in irgendeiner Form in Berührung kommen musste, wurde ein Geheimhaltungsinteresse der Auskunftei verneint.

Die aussagekräftige Information

Informationen von Auskunfteien sollen es den Empfänger/innen ermöglichen, sich ein Bild über die Betroffenen zu verschaffen, das wiederum eine Einschätzung über deren Verhalten in verschiedenen Situationen des Wirtschaftslebens ermöglicht. Manche Informationen, die in den Datensätzen von Auskunfteien enthalten sind, stechen ins Auge wie ein schwarzer Fleck auf einem weißen Hemd und prägen so das Bild der Betroffenen. Dies können lokal oder regional bekannte Adressen wie die einer Heilanstalt oder der Justizvollzugsanstalt sein, übel beleumundete Straßen, Geschäftspartner oder auch nur im schlimmsten Sinne prägnante Namen.

Ein Petent wandte sich an die Aufsichtsbehörde für den Datenschutz mit der Bitte zu prüfen, ob zwei hier ansässige Auskunfteien Informationen über abgewiesene Insolvenzverfahren und die Voranschriften, darunter nebst anderen die der Justizvollzugsanstalt, speichern dürften.

Die Prüfung und datenschutzrechtliche Bewertung ergab, dass die Adressen in der Tat zu löschen waren. Zwar wird man solchen Angaben in der Regel keine besondere Sensibilität im Sinne des § 3 Abs. 9 des Bundesdatenschutzgesetzes zugestehen können, doch auch für sie gilt, das sie aufgrund der Vorschrift des § 35 Absatz 2 Nr. 4 dieses Gesetzes nach 4 Jahren gelöscht werden müssen, wenn eine Prüfung ergibt, dass sie nicht mehr erforderlich sind.

Anders verhielt es sich jedoch bei den Angaben zum Insolvenzverfahren. Der Petent verwies in diesem Zusammenhang auf eine Löschfrist von drei Jahren. Einträge über eidesstattliche Versicherungen und Haftbefehle werden nach den Vorgaben der Zivilprozessordnung (http://dejure.org/gesetze/ZPO) nach drei Jahren aus dem Schuldnerverzeichnis gelöscht. Diese Vorschriften gelten nach den Vorgaben der Insolvenzordnung (http://dejure.org/gesetze/InsO) (§ 26 Abs. 2) für die Abweisung von Insolvenzverfahren entsprechend. Allerdings beträgt die Löschungsfrist bei diesen Verfahren fünf Jahre. Zum Zeitpunkt der Eingabe war daher die Speicherung noch rechtmäßig.

Mobile Kommunikation – „Handys“

Organizer, Video- oder Fotokamera, UKW-Radio, Walkman, Spielekonsole, mobiler Computer (Handheld), Textverarbeitungsmaschine, Datenspeicher, E-Mail-Client, Kurzstreckenfunkgerät, GPS-Empfänger, Nervensäge oder einfach nur Mobiltelefon mit einigen Zusatzfunktionen. Handys sind aus der Gesellschaft einfach nicht mehr wegzudenken, was sich allein schon dadurch belegen lässt, dass bereits 2003 die Zahl der Mobilfunkanschlüsse in Deutschland bei rd. 79 pro 100 Einwohner/innen lag, die der Festnetzanschlüsse hingegen nur bei etwa 66[25].

Da in Mobiltelefonen eben auch personenbezogene Daten gespeichert werden, war für die Aufsichtsbehörde für den Datenschutz absehbar, dass auch in diesem Bereich früher oder später Fragen auftauchen würden. Die meisten Anfragen wurden auch hier telefonisch gestellt und bezogen sich in der Regel auf das Vertragsverhältnis zwischen Nutzer/in und Netzanbieter oder Provider. Grundsätzlich liegt zwar die Kontrollkompetenz für Telekommunikationsunternehmen beim Bundesbeauftragten für Datenschutz (http://www.bfd.bund.de/), Anfragen zum Datenumfang oder zur Schufa-Klausel in Mobilfunkverträgen können jedoch auch hier erörtert werden.

Schriftliche Eingaben/Anfragen per E-Mail erreichten uns tatsächlich nur wenige, genauer, lediglich zwei. Diese bezogen sich beide auf das interne Telefonbuch der Mobiltelefone. Grundsätzlich werden Telefonnummern samt zugehöriger Namen menügesteuert auf der SIM-Karte des Gerätes gespeichert. Bei einem Gerätewechsel sind so die Daten direkt wieder präsent, ohne sie neu eingeben oder sonst übertragen zu müssen. Anders verhält es sich bei Informationen die im internen Telefonbuch gespeichert sind. Diese bleiben auch bei einem SIM-Kartenwechsel dort erhalten.

Bei einem eventuellen Verkauf des Gerätes oder einer sonstigen Weitergabe müssen diese Daten zuvor gelöscht werden, da die Rechtslage hier vergleichbar der beim Verkauf gebrauchter Computer oder Festplatten ist. Gleiches gilt natürlich auch für Daten, die im Organizer des Gerätes oder an sonstiger Stelle gespeichert sind.

Was für die private Weitergabe gilt, muss erst recht für den gewerblichen Umgang gelten. Ein Elektrofachmarkt bot seinen Kundinn/en für die Dauer von Reparaturen Leihgeräte an, bedacht wurde jedoch nicht, dass der Speicher spätestens vor der Ausleihe an den nächsten Kunden kontrolliert und gelöscht werden sollte.

Die Petentin jedenfalls staunte wohl nicht schlecht, als sie von einem Unbekannten angerufen wurde, der ihr mitteilte, die Telefonnummer sei in einem Leih-Handy gespeichert. Auf Ihre Rückfrage bei dem Elektrofachmarkt wurde ihr zudem wohl noch mitgeteilt, man sei nicht verpflichtet, die Telefonbücher von Leihgeräten zu prüfen, dies sei vielmehr Sache der Kunden selbst. Künftig wolle man jedoch versuchen, hierauf zu achten. Auf Intervention der Aufsichtsbehörde für den Datenschutz sind die Mitarbeiter künftig gehalten, die Speicher bei Rückgabe der Leihgeräte zu prüfen.

Aus datenschutzrechtlicher Sicht war dem wenig hinzuzufügen. Zwar handelte es sich um eine unberechtigte Weitergabe personenbezogener Daten, es dürfte jedoch

[25] Quelle: eurostat (http://epp.eurostat.cec.eu.int/pls/portal/docs/PAGE/PGP_PRD_CAT_PREREL/PGE_CAT_PREREL_YEAR_2005/PGE_CAT_PREREL_YEAR_2005_MONTH_02/4-07022005-DE-AP.PDF)

schwer fallen, den Verursacher festzustellen: Der letzte Leihkunde oder das Personal, womöglich gar der neue Kunde?

Ordnungswidrigkeiten

Wahlwerbung

Bestimmte Berufsgruppen genießen in der Bevölkerung ein besonderes Vertrauen. Pfarrer als Verpflichtete des ältesten aller bekannten Verschwiegenheitsgebote zählen hierzu, Ärzte ebenso wie Notare[26]. Der Gesetzgeber hat die Brisanz der ihnen bekannten Informationen – Daten – schon früh erkannt und den Bruch der Schweigepflichten unter Strafe gestellt. Berufsordnungen und auch das Bundesdatenschutzgesetz lassen Erhebung, Verarbeitung und Nutzung solch sensibler Daten konsequent nur unter sehr engen Bedingungen zu. Die Aufsichtsbehörde für den Datenschutz jedenfalls stellt schon seit Jahren immer wieder fest, dass kaum Eingaben gerade in diesen Bereichen vorliegen. Aber auch hier gilt leider, dass es Ausnahmen gibt, die die Regel bestätigen:

Ein Angehöriger einer zur besonderen Verschwiegenheit verpflichteten Berufsgruppe hatte im Vorfeld der Wahlen im Jahr 2004 seine Kundendatei genutzt, um allgemeine Wahlinformationen zu versenden und auch auf seine eigene Kandidatur hinzuweisen. Dies war eine Vorgehensweise, die zu einer für ihn offenbar völlig unvorhergesehenen Reaktion der Betroffenen führte. Sie wandten sich nämlich an die Aufsichtsbehörde für den Datenschutz um die Zulässigkeit der Wahlwerbung zu hinterfragen. Wie sich in diesem Zusammenhang noch herausstellte, gehörten einige der Betroffenen nicht zum Kunden-/Mandanten-/Patientenkreis des Verantwortlichen, sondern waren bei der Geschäftsübergabe durch den Vorgänger quasi zum jetzigen Inhaber gewechselt.

Mithin waren hier zwei verschiedene Komplexe datenschutzrechtlich zu würdigen:

Zum einen die Geschäftsübergabe durch den Vorgänger, der zudem noch bestätigt haben soll, dass die Übergabe datenschutzrechtlich nicht zu beanstanden war, und zum anderen die Nutzung personenbezogener Daten zu Wahlwerbezwecken.

Grundsätzlich – so die Auffassung der Aufsichtsbehörde für den Datenschutz war die Übergabe der Kundenkartei dem Veräußerer und nicht dem Erwerber anzulasten, da die hierfür einschlägige Berufsordnung sehr dezidierte Vorgaben enthält, die nach unseren Feststellungen zumindest nicht in jedem Fall eingehalten wurden.

Anders hingegen die Nutzung personenbezogener Daten zu Wahlwerbezwecken. Der Gesetzgeber hat die Erhebung, Verarbeitung und Nutzung solcher Daten in § 28 Abs. 6ff des Bundesdatenschutzgesetzes einer strengen Zweckbindung unterworfen, die nur in gesetzlich bestimmten Ausnahmen durchbrochen werden darf. Keine der

[26] Wie schon im ersten Tätigkeitsbericht ausgeführt, gilt das nicht für das Bankgeheimnis. Es existiert auch kein den Ärzten vergleichbares Standesrecht. Dies mag mit der Vertreibung der Geldverleiher und –wechsler aus dem Tempel von Jerusalem durch Jesus Christus in Zusammenhang stehen, jedenfalls haben Banker/innen keinen eigenen Stand und wenn, dann nur einen schweren.

im Gesetz selbst genannten Ausnahmen traf hier zu. Diese Auffassung wurde auch von der für den Verantwortlichen zuständigen Berufskammer geteilt, die nach Kenntnis der Aufsichtsbehörde für den Datenschutz die Einleitung eines berufsgerichtlichen Verfahrens gegen diesen beantragte.

Gelegenheit macht Diebe

Eines der Hauptthemen mit denen sich Datenschutzinstitutionen in den letzten Jahren beschäftigten, war die Zulässigkeit von Bonitätsanfragen im Mietverhältnis. Unbestritten ist das berechtigte Interesse der Vermieter, einschätzen zu können, ob ihre Mieter überhaupt willens und in der Lage sind, ihre vertraglichen Verpflichtungen zu erfüllen. Dies legt auf den ersten Blick die Übertragung des im Kreditwesen bewährten Modells der Auskunfteien bzw. der Schufa nahe.

Ein Bankmitarbeiter wollte offenbar die Entscheidung darüber, in welchem Umfang solche Institutionen personenbezogene Daten an Vermieter übermitteln dürfen, nicht abwarten und nutzte die ihm dienstlich gebotene Möglichkeit zu einer Anfrage bei der Schufa. Da diese keine Informationen an Privatpersonen übermittelt, auch wenn sie Bankbedienstete sind, musste zunächst ein Anfragegrund konstruiert werden.

Dieser scheinbare Nachweis eines berechtigten Interesses war es schließlich, der die Betroffenen zu einer Anfrage bei der Aufsichtsbehörde für den Datenschutz veranlasste: Eine Eigenauskunft belegte, dass die Bank eine Schufa-Auskunft über sie erhalten hatte. Sie vermuteten, dass dies im Zusammenhang mit einer Mietanfrage zu sehen sei, denn der Vermieter war bei der anfragenden Bank beschäftigt. Die Nachforschungen der Aufsichtsbehörde für den Datenschutz ergaben, dass dies zutraf. Der Bankmitarbeiter gab auch zu, die Anfrage bei der Schufa veranlasst zu haben. Als Begründung führte er an, die Betroffenen seien mit diesem Verfahren einverstanden gewesen, so dass die Abfrage rechtmäßig wäre.

Dem war hier jedoch nicht so. Zwar hatten die Betroffenen im Rahmen eines Vorgesprächs mit dem Vermieter Namen, Adresse, Bankverbindung etc. handschriftlich notiert. Dies kann jedoch nicht als gültige Einwilligung im Sinne des § 4a Absatz 1 des Bundesdatenschutzgesetzes gewertet werden. Zudem konnte er nicht nachweisen, dass er die Betroffenen über die Schufa-Anfrage informiert habe. Dass er die Formvoraussetzungen für eine rechtswirksame Einwilligung nicht kannte, war nach Auffassung der Aufsichtsbehörde für den Datenschutz nicht anzunehmen.

Sowohl die Übermittlung personenbezogener Daten an die Schufa als auch der Datenabruf von dort setzt zwingend die Information der Betroffenen wie auch deren Einwilligung in die Schufa-Klausel voraus. Dass ausgerechnet ein Bankmitarbeiter dies nicht wissen sollte, widerspricht jeder Lebenserfahrung. Die dort geforderte Einwilligung muss schriftlich erteilt werden, da hier eine andere Form zu Gunsten der Betroffenen wie auch aus Gründen der Beweissicherung ausgeschlossen ist. Daher musste das sog. „Schriftformerfordernis“ dem Vermieter aus seiner beruflichen Tätigkeit bekannt sein.

Selbst wenn sein Interesse an der Auskunft subjektiv nachvollziehbar gewesen wäre, konnte er sich wegen der Täuschungshandlung nicht auf eine Rechtsgrundlage berufen. Nach § 28 Absatz 1 Nr. 1 des Bundesdatenschutzgesetzes ist die Erhebung

personenbezogener Daten auch zulässig, soweit dies der Erfüllung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses dient. In diesem Rahmen bedarf es keiner Einwilligung der Betroffenen. Allerdings ist es auch nicht zulässig, Falschangaben zu machen, um die begehrten Informationen zu erhalten. § 29 Absatz 2 des Bundesdatenschutzgesetzes fordert den Nachweis eines berechtigten Interesses. Dies setzt selbstverständlich voraus, dass sowohl der tatsächliche Abfragende wie auch das tatsächliche Motiv für die Anfrage angegeben werden. Falsche Angaben können diese Bedingungen nicht erfüllen.

Nach § 43 Absatz 2 Nr. 4 des Bundesdatenschutzgesetzes handelt ordnungswidrig, wer sich durch unrichtige Angaben die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, erschleicht. Eine solche Ordnungswidrigkeit kann mit einer Geldbuße bis zu einer Höhe von 250.000 € geahndet werden. Da dieser Tatbestand erfüllt war, wurde ein Bußgeld gegen den Bankmitarbeiter verhängt. Die Rechtsauffassung der Aufsichtsbehörde für den Datenschutz wurde im Ergebnis auch vom zuständigen Amtsgericht geteilt.

Sonstiges - Quer durch den Aktenplan

Grundrecht auf informationelle Selbstbestimmung vs. Pressefreiheit

Die Freiheit der Berichterstattung, ja die Freiheit der Medien und ihrer gesamten redaktionellen Tätigkeit stellt eines des höchsten Güter in einem demokratischen Staat dar - ein Recht also, das eigentlich schon von seiner Bestimmung her, der Bekanntmachung von Informationen, mit dem Grundrecht auf informationelle Selbstbestimmung kollidieren kann. Die für das Presserecht zuständigen Landesgesetzgeber haben für diese Konstellation eine Grundsatzfestlegung getroffen, wonach auf Unternehmen und Hilfsunternehmen der Presse das Bundesdatenschutzgesetz nur sehr eingeschränkt anwendbar ist. Insbesondere die rechtliche Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung wird nicht beschnitten. Diese Grundentscheidung pro Pressefreiheit kann, wie der nachfolgend geschilderte Fall zeigt, zu datenschutzrechtlich unbefriedigenden Ergebnissen führen:

Die Redaktion eines lokalen Mitteilungsblatt veröffentlichte einen Brief an ein Ortsratsmitglied und nannte die vollen Namen aller Unterzeichner/innen. Die Aufsichtsbehörde für den Datenschutz wurde gebeten, diesen Vorgang datenschutzrechtlich zu würdigen. Ergebnis der Prüfung war, dass die Veröffentlichung der personenbezogenen Daten nicht erforderlich war, jedoch nicht beanstandet werden konnte:

Die Erhebung, -verarbeitung und -nutzung personenbezogener Daten durch Presseunternehmen bemisst sich an der Regelung des § 41 Abs. 1 des Bundesdatenschutzgesetzes. Dieser Vorgabe folgend sieht das Saarländische Mediengesetz vor, dass für die genannten Unternehmen nur die §§ 5, 9 und 38a des Bundesdatenschutzgesetzes sowie eine hierauf bezogene Schadensersatzregelung nach § 7 des Bundesdatenschutzgesetzes gelten. Die Veröffentlichung personenbezogener Daten ist daher der Bewertung durch die Aufsichtsbehörde für den Datenschutz entzogen. Dies gilt selbst dann, wenn sie objektiv nicht erforderlich war oder gegen den Pressekodex (http://www.presserat.de/pressekodex.html) verstößt. Die darin manifestierte

Selbstbindung verpflichtet die Presseunternehmen unter anderem dazu, das Privatleben zu achten und zu prüfen, ob durch eine Veröffentlichung Persönlichkeitsrechte Dritter verletzt werden. Die Presse hat danach auf die Einhaltung des Rechts auf informationelle Selbstbestimmung zu achten und den redaktionellen Datenschutz zu gewährleisten. Der Pressekodex ist freilich nur für die Unternehmen bindend, die ihn anerkennen und sich so dieser Selbstverpflichtung unterwerfen. Zudem ist eine Verletzung des Grundrechts auf informationelle Selbstbestimmung, wie bereits erwähnt, nicht von den Aufsichtsbehörden für den Datenschutz zu überprüfen, sondern muss im Wege der Zivilklage oder beim Presserat (http://www.presserat.de/) geltend gemacht werden.

Datenschutz bei Telediensten

Nach einer hier vorliegenden Eingabe wurden im Forum bzw. den angebotenen Foren einer im Saarland betriebenen Webseite sowohl die IP-Adressen als auch die sog. Header-Informationen[27] der Diskussionsteilnehmer veröffentlicht. Eine Überprüfung der Webseite ergab, dass dies zwar mittlerweile geändert wurde, jedoch noch mehr im Argen lag:

Der eigentliche Betreiber der Seite konnte nur über DENIC (➔FAQ, Vereine) ermittelt werden, da das durch § 6 des Teledienstegesetzes vorgeschriebene Impressum fehlte. Die beanstandeten Informationen über die Forenteilnehmer/innen waren zwar nicht mehr aufgeführt, es war jedoch nicht ersichtlich, wer diese Angaben überhaupt erhob, noch wo und wie lange sie gespeichert wurden.

Auf die Anfrage beim Betreiber wurde die Aufsichtsbehörde für den Datenschutz darauf hingewiesen, dass aus dessen Sicht das Teledienstegesetz nicht einschlägig sei, da es sich um eine private Webseite handele. Weiter werde das Forum von einem externen Anbieter betrieben und liege daher auf dessen Server, so dass dieser Betreiber Ansprechpartner sei.

Dieser Rechtsauffassung musste widersprochen werden. Zum einen entbindet der Hinweis auf eine privat betriebene Webseite nicht von der Verpflichtung ein Impressum aufzunehmen. Voraussetzung hierfür ist lediglich, dass eine gewisse Nachhaltigkeit oder Regelmäßigkeit vorliegt. Auf eine Gewinnerzielung hingegen kommt es nicht an. Eine andere Auslegung wäre auch widersinnig, da Hintergrund des § 6 des Teledienstegesetzes der Transparenzgedanke ist. Durch diese Vorschrift wie auch durch die Korrespondenzvorschrift des § 10 im Mediendienste-Staatsvertrag soll sichergestellt werden, dass jede/r Nutzer/in sich über die Betreiber der Domain informieren kann, ohne auf Registrardatenbanken zugreifen zu müssen. Unzutreffend war auch, dass ausschließlich der (externe) Forumanbieter für dessen Inhalt verantwortlich sei. Der Link auf diese Seite enthielt keine Hinweise auf einen Anbieterwechsel, das beanstandete Forum selbst war und ist optisch in die verweisende Seite eingebettet. Auch ändert sich im Adressfeld nicht der Domainname, vielmehr wird dort nur

[27] Internet-Protokoll-Adresse, die jedem Rechner, der das world-wide-web nutzt, zumindest für die Dauer der Sitzung (dynamische IP) oder gar fest zugeordnet wird (statische IP). Über die Zuordnung zu einem bestimmten Rechner kann auch ein Personenbezug hergestellt werden. Header-Informationen, die von jedem Mail-Programm über bestimmte Programmschritte einfach dargestellt werden können, enthalten quasi die Wegbeschreibung und nähere Angaben zum Mail-Versender, oftmals auch dessen Namen.

eine neues Angebot unter der Hauptseite angezeigt. Lediglich aus der Statusleiste wird im Verlauf der Anwahl ersichtlich, dass es sich um ein Fremdangebot handelt. Wird dieser Fremdanbieter als Auftragsdatenverarbeiter im Rahmen eines entsprechenden Vertragsverhältnisses für den Domainbetreiber tätig, muss letzterer sich dessen Verhalten grundsätzlich als eigenes anrechnen lassen.

BASEL-II und Scoringverfahren

„Basel-II“ bezeichnet die Gesamtheit der Eigenkapitalvorschriften, die vom Basler Ausschuss für Bankenaufsicht in den letzten Jahren vorgeschlagen wurden. Die Regeln werden offiziell in der Europäischen Union Ende 2006 in Kraft treten, finden aber bereits heute in der täglichen Praxis Anwendung (Quelle: wikipedia, Basel II). Es handelt sich um Vereinbarungen, die klare Regeln für die Kreditvergabe definieren. Diese Bestimmungen sind für alle Kreditinstitute verbindlich und Ihre Einhaltung wird von der nationalen Bankenaufsicht kontrolliert; in der Bundesrepublik ist dies das Bundesamt für Finanzdienstleistungsaufsicht (http://www.bafin.de/) in Bonn. Die Basel-II-Vorgaben zielen auf ein verbessertes Risikomanagement bei der Kreditvergabe dergestalt ab, dass eine fundierte Prognose des kreditorischen Risikos sowohl in die grundsätzliche Entscheidung über eine Kreditvergabe wie auch in die individuell zu vereinbarenden Konditionen einzufließen hat. Zu diesem Zweck wird ein Rating, eine Einschätzung der ökonomischen Risiken nach standardisierten Regeln, vorgenommen. Das Ergebnis wird oft in einem ➔Scoringwert wiedergegeben.

Im Rahmen einer Eingabe wurde die Aufsichtsbehörde für den Datenschutz mit der Frage konfrontiert, welche personenbezogenen Daten in diesem Zusammenhang verarbeitet würden.

Zunächst einmal gilt, dass Unternehmen nicht durch das Bundesdatenschutzgesetz geschützt sind, da der Begriff der personenbezogenen Daten ausschließlich natürliche Personen, Menschen, meint. Weiter sind die Basel-II-Vorgaben nur auf Unternehmen anzuwenden, so dass auf den ersten Blick die Aufsichtsbehörde für den Datenschutz überhaupt nicht hätte tätig werden können. Wie so oft jedoch stellte sich die tatsächliche Situation etwas anders dar, als es eine rein an den Buchstaben des Gesetzes orientierte Auslegung vermuten ließe: der Petent stellte sich als Einzelkaufmann vor, dessen Hausbank ihn um verschiedene rating-relevante Angaben bat. Zwar genießen Einzelkaufleute in ihrer unternehmerischen Tätigkeit nicht den Schutz des Bundesdatenschutzgesetzes, da sie insoweit rein juristischen Personen gleichgestellt sind. Gerade im Verhältnis zu Banken jedoch ist eine solche trennscharfe Unterscheidung nicht immer möglich. Jedenfalls bediente sich die Hausbank des Petenten eines Auftragsdatenverarbeiters, um die individuellen Scorewerte ihrer Kunden berechnen zu lassen. Auf dessen Frage hin, welche personenbezogenen Daten dort verarbeitet und genutzt würden, wurde er an den Auftragnehmer verwiesen, da diesem die Einzelheiten bekannt seien.

Der bundesweit tätige Auftragnehmer teilte wiederum mit, dass die personenbezogenen Daten, die für das Scoringverfahren verwandt würden, sich auf solche beschränkten, die entweder in direktem Zusammenhang mit dem Vertragsverhältnis zwischen Kunden und Bank stünden oder die eine Bewertung des Geschäftsführers - und zwar nur im Zusammenhang mir dessen beruflicher Tätigkeit - zuließen.

Aus datenschutzrechtlicher Sicht war dies nicht zu beanstanden. Das Verfahren, dessen sich der Auftragnehmer zur Berechung bedient, beruht auf einer wissenschaftlich anerkannten mathematisch-statistischen Methode zur Prognose von Risikowahrscheinlichkeiten, so dass auch in dieser Hinsicht kein Anlass zu Beanstandung gegeben war.

Anders hingegen war das Verhalten der Hausbank zu bewerten, die hier eine besondere Auffassung, wie das Gebot der Transparenz im Datenumgang umzusetzen sei, vertrat: Zum einen muss dem Kreditinstitut selbstverständlich bekannt sein, welche Kundendaten an den Auftragnehmer weitergegeben werden; hierzu hätte es nur eines Blickes in den Vertrag bedurft. Zum anderen wurde der Aufsichtsbehörde für den Datenschutz direkt von dem Bundesverband, dem die Hausbank angehört, mitgeteilt, dass von dort eine eigene Informationsbroschüre erstellt und herausgegeben wurde, die betroffene Kunden über das Ratingverfahren informieren soll. Diese Broschüre müsste demnach bei allen Mitgliedsbanken bekannt sein, nur war dem in unserem Fall nicht so. Die Aufsichtsbehörde für den Datenschutz hätte gerne das Kreditinstitut auf seine Verpflichtungen in dieser Hinsicht verwiesen, der Petent wollte jedoch weder Ross und Reiter noch den Namen der Bank nennen.

Datenerhebung bei der Ausgabe von „Gelben Säcken“

In der öffentlichen Wahrnehmung ist ein scheinbares Paradoxon festzustellen, was die Preisgabe personenbezogener Daten angeht: Immer mehr Menschen sind anscheinend bereit, auch ihre Privat- oder Intimsphäre einer mehr oder minder breiten Öffentlichkeit zu offenbaren. Die oft eher peinlichen Geständnisse der Leitfiguren des Medienzeitalters scheinen hier eine animierende Wirkung zu zeitigen, die nicht nur in Sendungen wie „Big Brother“ ihren sichtbaren Ausdruck findet. Warum dem so ist, darüber kann allenfalls philosophiert werden, jedenfalls muss es letztlich jedem erwachsenen Menschen selbst überlassen bleiben, sich zum vermeintlichen Idol einer wie auch immer definierten Ziel- oder Fangruppe zu machen.

Gleichzeitig ist jedoch eine stärkere Sensibilisierung festzustellen, wenn personenbezogene Daten von anderer Seite nachgefragt werden, also das Moment der Selbstbestimmung fehlt. Viele Menschen weigern sich, die einfache Erklärung, „das müsse eben so sein...“ zu akzeptieren und ihre personenbezogenen Daten ohne weiteren Hinweis auf deren Verwendung preiszugeben, wie auch der folgende Fall zeigt:

Bei der Ausgabe von „Gelben Säcken“ des Dualen Systems Deutschland wurden in der Ausgabestelle Namen und Anschriften der Empfänger erhoben und handschriftlich in einer Liste erfasst. Als Begründung wurde angegeben, dies solle sicherstellen, dass nur Bewohner/innen des jeweiligen Ortsteils dort Rollen mit Gelben Säcken erhalten können. Offenbar sollte so wohl dem sozialschädlichen Treiben einer speziellen Unterart des Jägers und Sammlers, nämlich des Gemeinen saarländischen Gelbsack-Sammlers, Einhalt geboten werden.

Die Nachfrage der Aufsichtsbehörde für den Datenschutz bei dem Unternehmen, das mit der Ausgabe und dem Einsammeln der Gelben Säcke beauftragt war, führte zu einer sehr viel einfacheren Erklärung: Grundlage für die Abrechnung mit den Ausgabestellen ist die Zahl der ausgegeben Gelben Säcke. Um einen Missbrauch zu verhindern, bestätigen die Bürger/innen den Empfang der jeweiligen Rollen in einer Lis-

te. Diese Namenlisten werden nicht gespeichert oder anderweitig genutzt, sondern dienen lediglich der Abrechnung und werden halbjährlich im Aktenschredder vernichtet. Aus datenschutzrechtlicher Sicht ist dies unbedenklich, zumal das Unternehmen selbst ausgeführt hat, dass es den Betroffenen selbst überlassen bleibt, ob sie nur die Namen oder die komplette Anschrift in die Liste eintragen. Bliebe nur noch, dies den Betroffenen genau so mitzuteilen und zumindest bei Nachfragen auf die Verwendung ihrer personenbezogenen Daten hinzuweisen.

Zulässigkeit eines Mietspiegels

Mietspiegel dienen dazu, die durchschnittliche Miethöhe vergleichbarer Wohnungen zu ermitteln. Wie für jede brauchbare statistische Erhebung unabdingbar, kommt es auch hierbei auf eine möglichst breite Datenbasis an. Zu diesem Zweck werden bei Vermietern Angaben zu Baujahr, Nutzungsart, Allgemeinzustand der Wohnung/des Hauses, durchgeführte Modernisierungsarbeiten, Kostenträger für Reparaturen, Lage der Wohnung, Größe, Ausstattung und Miethöhe derselben erfragt. Ebenfalls erhoben wird die Adresse.

Auf die Anfrage eines betroffenen Mieters, ob die Übermittlung dieser Daten an Dritte (=Herausgeber des Mietspiegels) zur Erstellung eines Mietspiegels rechtmäßig sei, hat die Aufsichtsbehörde für den Datenschutz die Auffassung vertreten, dass dem dann so sei, wenn die Betroffenen darin eingewilligt haben.

Die Erstellung und Aktualisierung eines Mitspiegels setzt die Übermittlung personenbezogener Daten der Mieterinnen und Mieter an ein hiermit beauftragtes Unternehmen voraus. Näheres hierzu ist in den Paragraphen 558c,d,e des BGB geregelt. Dort ist jedoch nichts zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten gesagt.

Das Bundesdatenschutzgesetz regelt wie alle anderen datenschutzrechtlichen Vorschriften den Umgang mit persönlichen, genauer: personenbezogenen Daten. Diese sind Anknüpfungspunkt aller Gebots- und Verbotsregelungen. Personenbezogene Angaben werden definiert als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Gemeint sind hier alle denkbaren Informationen, die einer Person zugeordnet werden können. Die Informationen, die in einen Mietspiegel einfließen, stellen zunächst keine personenbezogenen Daten dar, da sie sich ausschließlich auf die Wohnung beziehen (Wohnungsgröße, Lage, Baujahr, Ausstattung, Miethöhe etc.). Es war nicht beabsichtigt, die Namen der Bewohnerinnen und Bewohner an den Mietspiegel weiterzugeben. Allerdings kann aus der Adresse und der genauen Lage der Wohnung im Gebäude auf diese geschlossen werden. So besteht zumindest bei dem Unternehmen, das den Mietspiegel erstellt, die Möglichkeit, auf die einzelnen Bewohner/innen zu schließen. Anzumerken ist allerdings, dass der Mietspiegel selbst keine Rückschlüsse auf einzelne Personen zulässt, da dieses allen zugängliche Register weder Adressen noch sonstige Mieterdaten enthält.

Da für die Übermittlung personenbeziehbarer Daten im Zusammenhang mit der Erstellung eines Mietspiegels keine Rechtsgrundlage existiert, ist sie nur mit Zustimmung der betroffenen Mieterinnen und Mieter zulässig. § 4a des Bundesdatenschutzgesetzes nennt die Voraussetzungen für eine wirksame Einwilligung: So sind

die Betroffenen über den Zweck der Erhebung, Verarbeitung und Nutzung zu unterrichten (hier: „Mietspiegel“) sowie über mögliche Datenempfänger.

Alle diese Voraussetzungen waren hier erfüllt, so dass eine gegebene Einwilligung auch wirksam wäre.

Der Schutz vermuteter Anlegerinteressen

Wie bereits im ersten Tätigkeitsbericht am Beispiel einer Überwachung durch Detektive geschildert, bewegt sich die Aufsichtsbehörde für den Datenschutz nicht nur auf dem von trockenen Paragraphen bedeckten Boden des Amtsstubenlebens, sondern wird bisweilen auch in Bereichen tätig, die zumindest von außen betrachtet eine gewisse Spannung versprechen. Datenschutz bei vermutetem Anlegerbetrug stand diesmal auf der Agenda und zwar nicht im Zusammenhang mit der Datenerhebung, -verarbeitung und -nutzung durch das verdächtigte Unternehmen. Vielmehr bezog sich die Eingabe darauf, ob eine Selbsthilfegemeinschaft einen der mutmaßlichen Anleger anschreiben durfte.

Jener hatte sich über die Aufsichtsbehörde für den Datenschutz seines Bundeslandes an uns gewandt und darüber beschwert, dass er von einer Selbsthilfegemeinschaft für Anlagegeschädigte mit Sitz im Saarland angeschrieben worden sei und bat darum, diesen Vorgang datenschutzrechtlich zu bewerten. Der Betroffene vermutete offenbar, seine personenbezogenen Daten seien durch den Fonds-Anbieter weitergegeben worden.

Bei der hier ansässigen Selbsthilfegemeinschaft handelt es sich um eine „Aktionsgemeinschaft“, die lt. eigener Erklärung von betroffenen Anlegern initiiert und mit deren Organisation ein hierin erfahrenes Unternehmen betraut wurde. Bei letzterem handelte es sich um eine Privatdetektei, die sich nach eigener Darstellung vor allem auf Wirtschaftkriminalität spezialisiert hat. Ein besonderes Augenmerk lege man auf die Untersuchung von Anlagebetrügereien und dem Angebot professioneller Hilfe für die Betroffenen. Nach Auskunft der Verbraucherzentrale lagen dort sowohl über die „Aktionsgemeinschaft“ wie auch deren Organisator keine Erkenntnisse vor, was insofern positiv zu bewerten war, als dort in aller Regel vor allem gegen Verbraucherinteressen handelnde Unternehmen bekannt sind.

Da weder die „Aktionsgemeinschaft“ noch die sie tragende Auskunftei aus rein altruistischen Motiven handeln, ist beiden sehr daran gelegen, über den ursprünglichen Kreis der Auftraggeber hinaus weitere Betroffene als Kunden zu gewinnen. Diesem Ziel diente auch der an den Petenten gerichtete Brief. Datenschutzrechtlich ist diese Spielart der Direktwerbung in der Regel dann unbedenklich, wenn die verwandten Adressen rechtmäßig erhoben wurden und nicht ersichtlich ist, dass dem schutzwürdige Interessen der Betroffenen entgegen stehen könnten. Die Aufgabe der Aufsichtsbehörde für den Datenschutz bestand hier also darin, die Herkunft der personenbezogenen Daten des Petenten zu klären und zu bewerten, was sich in der Folge komplizierter als üblich darstellte: Wie die Detektei in den Besitz der Adressen gelangte, konnte von dort selbst nicht erklärt werden, da man die für die Briefaktion verwandten Angaben anonym erhalten habe. Mit der Erfahrung der Aufsichtsbehörde für den Datenschutz auf dem Gebiet der Datenerhebung ist diese Vorstellung allerdings nur schwer vereinbar, was Anlass zu einer weiteren Nachfrage bot. Der Ge-

schäftsführer der Detektei gestand zu, dass dies in der Tat für Außenstehende nur schwer nachvollziehbar sei, in seinem speziellen – sehr verschwiegenen - Arbeitsbereich jedoch nicht so selten wäre. In aller Regel handele es sich bei diesen anonymen Hinweisen um CD-ROMs bzw. Disketten, die nicht mit einer Absenderangabe versehen seien. Nach einem Relevanzabgleich mit vorhandenen Unterlagen, z. B. bereits vorhandenem Adressmaterial, würden die so gewonnenen Erkenntnisse für Werbeaktionen genutzt.

Ob dem tatsächlich so war, ließ sich im Nachhinein nicht mehr feststellen, jedenfalls konnte die Aufsichtsbehörde für den Datenschutz die Angaben nicht widerlegen. Da der Petent zudem Strafanzeige erstattet hatte, musste es bei dieser Feststellung bleiben, allein schon, um dem Votum des Gerichts nicht vorzugreifen.

Datenschutz im Arbeitsverhältnis

Der beim Arbeitgeber geführte Stammdatensatz einer/s jeden Beschäftigten umfasst im Regelfall eine Vielzahl von Datenkategorien. Zu nennen wären Namen, Vornamen, Alter, Familienstand, Anzahl der Kinder, Zugehörigkeit zu einer Religionsgemeinschaft, Qualifikation, Art der Beschäftigung, Tarifgruppe, Steuerklasse, Urlaubsanspruch, krankheitsbedingte Fehlzeiten, arbeitsrechtlich relevante Vorgänge, Bankverbindungen, Lohnpfändungen und anderes mehr. Rechtsgrundlage für die Verarbeitung all dieser Daten ist – soweit die Angaben nicht direkt vom Arbeitgeber stammen oder spezialgesetzlich vorgegeben sind - in der Regel § 28 Absatz 1 Nr. 1 des Bundesdatenschutzgesetzes. Danach ist das Erheben, Speichern, Verändern, Übermitteln und Nutzen für die Erfüllung eigener Geschäftszwecke dann zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient. Anders als bei anderen Verarbeitungssituationen kommt es hierbei nicht darauf an, dass die Kenntnis der Daten erforderlich ist, es reicht vielmehr aus, wenn sie dem Vertragszweck dienlich ist oder nützen kann.

Dennoch ist trotz dieser relativ weit reichenden Gestattung stets auch das Interesse der Betroffenen zu wahren, wie den Prozessvertretern eines Arbeitsgebers mitgeteilt wurde.

Hintergrund der Anfrage war die Äußerung eines Arbeitsrichters im Gütetermin, er halte die Einholung von Informationen über Arbeitnehmer bei Auskunfteien für unzulässig. Die beauftragten Rechtsanwälte wollten nunmehr von der Aufsichtsbehörde für den Datenschutz erfahren, ob diese Auffassung geteilt werde. Da die Aufsichtsbehörde für den Datenschutz dann auf ein eigenes Votum zu verzichten hat, wenn die zu Grunde liegende Frage bereits gerichtshängig ist, beschränkten sich die Ausführungen auf generelle Erläuterungen der allgemein wichtigen und interessierenden Frage, wieviel Datenschutz im Arbeitsverhältnis nötig und zulässig sei, insbesondere dann, wenn externe Datenerhebungen beabsichtigt sind.

Die in Rede stehenden Auskünfte über die Mitarbeiter sollten bei Wirtschaftsauskunfteien eingeholt werden. Deren Tätigkeit ist in § 29 des Bundesdatenschutzgesetzes geregelt und wird dort als geschäftsmäßiges Erheben, Speichern oder Verändern zum Zwecke der Übermittlung definiert. Einschlägig für die Beurteilung der Übermittlung ist § 29 Absatz 2 des Bundesdatenschutzgesetzes. Demnach ist sie dann zu-

lässig, wenn der Dritte dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis dargelegt hat und kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat[28].

Problematisch in derartigen Fällen ist meist der Nachweis des berechtigten Interesses an der Auskunftserteilung (➔Kreditschutzorganisationen/Auskunfteien). Anerkannt werden kann es als Begründung für eine Datenübermittlung nur dann, wenn der dem Datenschutzrecht immanente Grundsatz der Erforderlichkeit beachtet wird, das heißt, wenn die Kenntnis der personenbezogenen Daten für die Aufgabenerfüllung oder die Geschäftszwecke der anfragenden Stelle erforderlich ist. Letzteres Merkmal liegt dann vor, wenn die gestellte Aufgabe anders nicht, nicht vollständig, nicht zeitgerecht oder nicht rechtmäßig erfüllt werden könnte; Neugierde reicht mithin nicht aus, eine Erforderlichkeit zu begründen. Das Erforderlichkeitsgebot ist so nichts weiter als die Übertragung des Verfassungsgrundsatzes der Verhältnismäßigkeit in das Datenschutzrecht. Anerkannt als berechtigtes Interesse ist beispielsweise die Bonität der Geschäftspartner, insbesondere dann, wenn ein kreditorisches Risiko begründet wird.

Unzulässig hingegen sind nach Auffassung der Aufsichtsbehörde für den Datenschutz Anfragen und Datenübermittlungen zu Personalentscheidungen. Soweit hiermit nicht inzident ein höheres kreditorisches Risiko verbunden ist, wird nicht zu belegen sein, wodurch die Erforderlichkeit dieser Daten für die anfragende Stelle begründet sein wird. Dieser Überlegung folgend enthalten die Schufa-Verträge ein eindeutiges Anfrage- und Übermittlungsverbot in Personalangelegenheiten.

Eine andere Auslegung würde dazu führen, dass künftig bei jeder Personalentscheidung umfassende Bonitätsprüfungen unabhängig vom jeweiligen Arbeitsbereich zulässig wären. Soweit für eine Beschäftigung in bestimmten Bereichen eine weitergehende Prüfung tatsächlich erforderlich sein sollte, wäre nach Auffassung der Aufsichtsbehörde für den Datenschutz zunächst zu prüfen, ob nicht auch ein polizeiliches Führungszeugnis ausreicht.

Nebenkosten

Energielieferungsverträge können im Mietverhältnis entweder mit Vermieter/innen oder Mieter/innen selbst abgeschlossen werden. Im vorliegenden Fall allerdings lag ein besonderes Vertragsverhältnis vor: Der Grundvertrag wurde zwischen den Vermietern und dem Energieunternehmen abgeschlossen, die Mieter/innen wurden durch einen weiteren Vertrag zu Rechnungsschuldnern. Dieser Vertragstypus sah wiederum zwei Varianten vor:

- eine gesamtschuldnerische Haftung des Vermieters und des Mieters als Standardvertragsvariante, oder
- die ausschließliche Haftung der Mietparteien.

Bei einer gesamtschuldnerischen Haftung wäre das Energieunternehmen ohne weiteres berechtigt, die Vermieter über ausbleibende Zahlungen zu informieren. Dies

[28] Selbstverständlich wäre die Übermittlung datenschutzrechtlich auch dann zulässig, wenn der Betroffene darin eingewilligt hätte.

ergäbe sich – sofern nicht ohnehin geregelt – allein schon aus den vertraglichen Nebenpflichten und der Sorgfaltpflicht eines ordentlichen Geschäftsmannes. Anders hingegen bei der 2. Variante: In Ermangelung der Möglichkeit auf die Vermieter zurückzugreifen, besteht für deren Information keine Rechtfertigung.

Diese Vertragsausgestaltung lag in einem an die Aufsichtsbehörde für den Datenschutz herangetragenen Fall vor. Ein Mieter kam über einen Zeitraum von mehreren Monaten seinen vertraglichen Zahlungspflichten nicht nach. Darauf hin informierte das Energieunternehmen zeitgleich mit der ersten Mahnung an ihn seinen Vermieter. Der Mieter bat um eine datenschutzrechtliche Bewertung dieser Datenübermittlung.

Festgestellt wurde schließlich im Ergebnis, dass im vorgetragenen Fall abweichend vom üblichen Vorgehen eine gesamtschuldnerische Haftung ausgeschlossen war. Daher hatte der Vermieter kein eigenes Interesse an der Information über ausbleibende Zahlungen. Die Zusatzvereinbarungen zum Vertrag sahen ausdrücklich vor, den Mieter im Falle von Zahlungsverweigerung oder Zahlungsrückständen in Anspruch zu nehmen. Weiter gestattete die vertragliche Regelung, die Energieversorgung wegen ausbleibender Zahlungen zu unterbrechen. Für diesen Fall war eine Information der Vermieter vorgesehen, um ihm so die Möglichkeit zu geben, möglichen Schäden an den Versorgungsleitungen vorzubeugen.

Im konkreten Fall lag entgegen der Auffassung des Energieunternehmens eine solche Konstellation nicht vor. Dort war man zudem der Auffassung, ausbleibende Zahlungen berechtigten aufgrund des Vertrages zwischen Vermieter und Unternehmen zur Information über Zahlungsausfälle. Dies wäre jedoch eine grundsätzlich unzulässige Vertragsauslegung zu Lasten Dritter (Mieter), da allein durch die dem Mieter zuzurechnende Nichtzahlung keine Rechte des Vermieters tangiert wurden. Anders verhielte es sich, wenn der Mieter in die Übermittlung eingewilligt hätte oder eine Versorgungssperre angedroht worden wäre. In beiden Fällen wäre eine Information des Vermieters zulässig und auch angezeigt.

Ein Hausverbot und seine Folgen

Ausfluss des Hausrechts ist unter anderem die Berechtigung, Hausverbote auszusprechen. Hausverbote sind in der Regel gerichtlich kaum zu überprüfen, insbesondere, wenn sie sich auf nicht öffentlich zugängliche Räume wie z. B. Mietshäuser beziehen und die Adressaten zudem nicht zu Bewohnern zählen.

Ein Petent hatte sich an die Aufsichtsbehörde für den Datenschutz gewandt und dargelegt, ein Betreiber mehrerer großer Wohnobjekte habe seine personenbezogenen Daten an das Landeskriminalamt (LKA) übermittelt und ihm auf deren Anraten hin Hausverbot erteilt.

Hintergrund des vom Vermieter verhängten Hausverbotes waren wiederholte tätliche Auseinandersetzungen, in die auch der Petent verwickelt gewesen sein soll. Im Saarland ist beim LKA eine Beratungsstelle für polizeiliche Kriminalprävention und Opferschutz eingerichtet, deren Aufgabe auch darin besteht, mit Betroffenen Strategien zu erarbeiten, wie solche Situationen im Vorfeld bereits vermieden werden können. Im vorliegenden Fall hatte sich der Vermieter an diese Beratungsstelle gewandt und von dort den Rat erhalten, den Betroffenen Hausverbot zu erteilen. Personenbezogene

Daten wurden im Rahmen dieser Anfrage nicht übermittelt, wie auch vom LKA bestätigt wurde.

Aus datenschutzrechtlicher Sicht war dies völlig unbedenklich, die Auseinandersetzungen, die den Vermieter letztlich Rat beim LKA suchen ließen, hätten im Übrigen auch eine Mitteilung personenbezogener Daten an die Beratungsstelle rechtfertigen können.

Zum Surfen – eine kleine Linkliste[29]

Aufsichtsbehörden und Landesbeauftragte

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

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

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

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

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

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

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

Hessen:
http://www.hmdi.hessen.de
http://www.rpda.de/dezernate/datenschutz/index.htm

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

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

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

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

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

Sachsen:
http://www.sachsen.de/de/bf/staatsregierung/ministerien/smi/
http://www.rpc.sachsen.de
http://www.rp-dresden.de
http://www.rpl.sachsen.de

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

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

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

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

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

Saarland, Landesbeauftragter für Datenschutz:
http://www.lfd.saarland.de

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

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

Der Sächsische Datenschutzbeauftragte:
http://www.datenschutz.sachsen.de

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

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

Sonstige Behörden:

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

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

Datenschutzseite der EU - deutschsprachiges Informationsportal der EU mit ausführlichen Informationen über die Entwicklung des Datenschutzes auf europäischer Ebene:
http://europa.eu.int/comm/internal_market/privacy/index_de.htm

Sonstige

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

Datenschutzsuchmaschine, betrieben vom virtuellen Datenschutzbüro
http://www.datenschutz.de/suchen

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

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

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

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

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

GDD Datenschutz-Kurz-Check - Datenschutzkurzcheckliste für Unternehmen
http://www.gdd.de/kurzcheck/start.htm

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

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

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

COMPUTAS,S- ervice und Konferenzen
http://www.computas.de

Privacy.net - Englischsprachiges Verbraucherinformationsportal
http://www.privacy.net

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

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

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

allgemeiner-datenschutz.de - privates Portal zum Thema „Sicheres Internet“
http://www.allgemeiner-datenschutz.de

david-datenschutz.de - private Seite mit Informationen zum Datenschutz in der Arbeitswelt
http://www.david-datenschutz.de

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

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

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

Schufa
http://www.schufa.de

SPAM, Viren, Dialer, Hoaxes etc.

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

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

Dialerinformationen der Regulierungsbehörde für Telekommunikation und Post
http://www.regtp.de/aktuelles/pm/02878/index.html

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

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

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

BSI für Bürger - Direktlink zu Vireninformationen

http://www.bsi-fuer-buerger.de/viren/

SPAM - englischsprachige Informationsseite über SPAM
http://www.spam.com

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

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

Beschwerdestelle der Wettbewerbszentrale
www.wettbewerbszentrale.de

Hoax-Informationen der TU Berlin
http://www.hoax-info.de

Datenbanken auf die im Bericht verwiesen wird:

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

Bundesministerium für Forschung und Bildung - Vorschriften zur Informations- und Kommunikationstechnologie
http://www.iid.de

Bundesministerium für Gesundheit und Soziales – Gesetze zur sozialen Sicherheit
http://www.bmgs.bund.de/download/gesetze_web/gesetze.htm

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

Saar-Daten-Bank – Frisierte Gesetze (ab 1. Januar 2006 kostenpflichtig)
http://www.sadaba.de

Landesmedienanstalt Saarland
http://www.lmsaar.de

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

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