SACHSEN-ANHALT

Landesverwaltungsamt

# Fünfter Tätigkeitsbericht

der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt

Berichtszeitraum 01.06.2009 - 30.09.2011

## Inhaltsverzeichnis

# 1 Einführung

## 1.1 Das (Grund)Recht auf informationelle Selbstbestimmung

Im sog. Volkszählungsurteil erkannte das Bundesverfassungsgericht am 15. Dezember 1983 (BVerfGE 65, 1) vor dem Hintergrund der „heutigen und künftigen Bedingungen der automatischen Datenverarbeitung“ ein „Recht der informationellen Selbstbestimmung“ an. Dieses wurde aus dem in Artikel 1 und 2 des Grundgesetzes (GG) verankerten allgemeinen Persönlichkeitsrecht hergeleitet:

*„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“* (Art. 1 Abs. 1 GG)

*„Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßig Ordnung oder das Sittengesetz verstößt.“* (Art. 2 Abs. 1 GG)

Das abgeleitete Grundrecht **gewährleistet dem Einzelnen die Befugnis**:

- grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und
- zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.

Darüber hinaus wurde bereits zum damaligen Zeitpunkt erkannt, dass sich das Recht auf informationelle Selbstbestimmung in seiner Ausprägung den aktuellen Gegebenheiten anpassen muss. Auch nach dem Volkszählungsurteil hat das Bundesverfassungsgericht den Schutz der Privatsphäre immer wieder gestärkt. Von besonderer Bedeutung ist das Urteil des Ersten Senats des Bundesverfassungsgerichts („Online-Durchsuchungs-Urteil“) vom 27. Februar 2008 (Az. 1 BvR 370/07, 1 BvR 595/07). Angesichts fortschreitender technischer Möglichkeiten wurde die Rechtsprechung zum Schutz des Persönlichkeitsrechts dahingehend fortentwickelt, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.

Jeder muss wissen können, wer, was, wann und bei welcher Gelegenheit über die eigene Person weiß. Dies bedeutet nicht, dass jeglicher Umgang mit personenbezogenen Daten nur möglich ist, wenn sich die betroffene Person damit einverstanden erklärt hat. Sowohl in Bezug auf das Volkszählungsurteil als auch durch die aktuelle Rechtsprechung wurde aner-

kannt, dass Einschränkungen rechtmäßig sind. Etwaige Einschränkungen unterliegen allerdings strengen Anforderungen. Zunächst sind Einschränkungen des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse auf Grund eines Gesetzes zulässig. Eine gesetzliche Grundlage muss die Voraussetzungen für die Einschränkungen und deren Umfang eindeutig regeln und der Grundsatz der Verhältnismäßigkeit ist zu beachten. Verhältnismäßigkeit im weiteren Sinn verlangt von jeder Maßnahme, die in Grundrechte eingreift, dass sie einen legitimen öffentlichen Zweck verfolgt und überdies geeignet, erforderlich und verhältnismäßig im engeren Sinn (auch „angemessen“ genannt) ist. Jeglicher Umgang mit personenbezogenen Daten muss daher einer Zweckbindung unterliegen, sich an dem präzise bestimmten Verwendungszweck orientieren und ist auf das für diesen Zweck erforderliche Mindestmaß zu beschränken.

Das Grundrecht auf informationelle Selbstbestimmung wird vor allem durch das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Länder konkretisiert. Daneben finden sich in zahlreichen Bundes- und Landesgesetzen, wie z. B. dem Telekommunikationsgesetz, den Sozialgesetzbüchern oder den Landespolizeigesetzen datenschutzrechtliche Regelungen. Ob das BDSG oder die Datenschutzgesetze der Länder Anwendung finden, richtet sich danach, ob eine öffentliche oder nicht-öffentliche Stelle mit personenbezogenen Daten umgeht (erhebt, verarbeitet – speichert, verändert, übermittelt, sperrt, löscht – oder nutzt).

Vorrangiges Ziel des Datenschutzes ist es, eine Gefährdung des Persönlichkeitsrechts des Einzelnen von vornherein durch Verwendungsregeln für personenbezogene Daten und durch die Gestaltung des Einsatzes der Informationstechnik zu verhindern.

### 1.2 Grundbegriffe im Datenschutz

**Personenbezogene Daten** sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer **bestimmten** oder **bestimmbaren** Person.
Bestimmt ist eine Person, wenn sich Angaben auf eine konkret benannte Person beziehen, wie z. B. die Aussage, dass eine namentlich bezeichnete Person des öffentlichen Lebens ein Kind erwartet.
Personenbezogene Daten liegen aber auch vor, wenn sich die Daten auf eine bestimmbare Person beziehen. Für die Bestimmbarkeit ist es erforderlich, dass aus den Angaben – etwa der Adresse – ein Bezug zu einer bestimmten Person hergestellt werden kann. Stets muss eine konkrete Person direkt oder indirekt identifiziert werden können. Es kann genügen, dass der direkte Personenbezug erst nach mehreren Zwischenschritten hergestellt werden kann.

Dabei sind nicht ausschließlich die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle entscheidend. Folglich ist die Bestimmbarkeit weit auszulegen und es kommt auf die jeweilige Stelle an, die mit den Daten umgeht.
Bei den Daten muss es sich weiterhin um Einzelangaben über persönliche oder sachliche Verhältnisse handeln. Tatsachen werden ebenso erfasst wie Werturteile. Persönliche Verhältnisse sind z. B. Angaben über die finanziellen, beruflichen, wirtschaftlichen oder gesundheitlichen Verhältnisse. Als sachliche Verhältnisse werden dagegen z. B. Angaben zu einem Kfz, zu einem von einer Person geführten Betrieb oder über eine Wohnung, ein Haus oder ein Grundstück, das eine Person bewohnt oder besitzt, erfasst.

In Verfahren der Aufsichtsbehörde steht regelmäßig nicht in Rede, dass ein Umgang mit personenbezogenen Daten erfolgt. Die vorstehenden Ausführungen sollen verdeutlichen, dass ein Umgang mit personenbezogenen Daten häufiger - als es auf den ersten Blick erscheint - stattfindet und insoweit die datenschutzrechtlichen Bestimmungen einschlägig sind.

Die Unterscheidung zwischen **öffentlichen und nicht-öffentlichen Stellen** ist maßgebend für den Anwendungsbereich datenschutzrechtlicher Bestimmungen - Bundesdatenschutzgesetz oder Datenschutzgesetz der Länder -.
*Öffentliche Stellen* sind Behörden des Bundes oder der Länder, aber auch die Organe der Rechtspflege und andere öffentlich organisierte Einrichtungen ungeachtet ihrer Rechtsform. Darüber hinaus zählen auch nicht-öffentliche Stellen zu den *öffentlichen* Stellen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (§ 2 Abs. 1 – 3 und Abs. 4 Satz 2 BDSG).
*Nicht-öffentliche* Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, sofern sie nicht als öffentliche Stelle anzusehen sind. Beispielhaft zu nennen sind Banken, Versicherungen, Industrie- und Dienstleistungsunternehmen sowie sonstige Gesellschaften, aber auch freiberuflich Tätige, wie etwa Ärzte, Rechtsanwälte und Architekten. Für Stellen der Religionsgesellschaften gilt regelmäßig kirchliches Datenschutzrecht.

Der **Datenverarbeitung und Auftragsdatenverarbeitung** kommt in der modernen, durch mehrgliedrige Unternehmenskooperationen und –strukturen geprägten Wirtschaftswelt eine wichtige Bedeutung zu. Das Instrument der Auftragsdatenverarbeitung eröffnet die Möglichkeit, unter bestimmten Voraussetzungen dritte Stellen in die Datenverarbeitung einzubeziehen, ohne dass die dafür erforderliche Weitergabe eine Datenübermittlung im Rechtssinne ist. Die Verantwortung für den gesamten Umgang mit den personenbezogenen Daten obliegt dem Auftraggeber. Dazu muss ein Auftragsverhältnis bestehen.

Dies ist nach § 11 BDSG dann der Fall, wenn die beauftragte Stelle nur eine Hilfs- und Unterstützungsfunktion hat und in diesem Rahmen in völliger Abhängigkeit von den Vorgaben der verantwortlichen Stelle handelt, eben wie eine ausgelagerte Abteilung. Die den Auftrag erteilende Stelle bestimmt also weiterhin allein über die Erhebung, Verarbeitung oder Nutzung personenbezogenen Daten und behält die uneingeschränkte Verfügungsgewalt und somit das alleinige und umfassende Weisungsrecht.

Für das Vorliegen eines Auftragsverhältnisses sprechen:
- Fehlen einer eigenen Entscheidungsbefugnis zur Durchführung der Verarbeitungsschritte,
- Beschränkung der Erhebung, Verarbeitung und Nutzung der Daten, die der Auftraggeber zur Verfügung stellt oder
- Fehlen einer Vertretung nach außen.

Ein solches Verhältnis liegt beispielsweise vor, wenn ein externes Rechenzentrum die Lohn- und Gehaltsabrechnung für andere Unternehmen führt oder ein Call-Center die Hotlinetätigkeiten eines Unternehmens übernimmt. Auftragsdatenverarbeitungen sind regelmäßig auch die Werbeadressenverarbeitung, die Datenträgerentsorgung oder die reine Datenerfassung, sei es zur Sicherheitsspeicherung oder im Rahmen der Archivierung.

Handelt es sich bei der in Auftrag gegebenen Arbeit nicht um reine weisungsgebundene Hilfstätigkeiten, liegt eine sog. Funktionsübertragung vor und damit keine Auftragsdatenverarbeitung: z. B. bei der Rekrutierung von Mitarbeitern, sowie bei Unternehmens- oder Steuerberatung. Diese Aufgaben gehen über Hilfstätigkeiten bei der Datenverarbeitung hinaus. Zudem hat die eingeschaltete Stelle einen gewissen Entscheidungsspielraum beim Umgang mit personenbezogenen Daten. Auch Tätigkeiten, die im Kern nicht den Umgang mit personenbezogenen Daten betreffen, wie beispielsweise bei Transportleistungen von Post- oder Kurierkunden, Reinigungsdienstleistungen oder dem Handwerkereinsatz im Unternehmen bedingen keine Auftragsdatenverarbeitung i. S. des § 11 BDSG. Lässt sich bei den entsprechenden Dienstleistern die Möglichkeit zur Kenntnisnahme von personenbezogenen Daten nicht verhindern, ist dies nur ein unvermeidliches „Beiwerk“.

Die eindeutige Identifikation von Auftragsdatenverarbeitung oder Funktionsübertragung ist häufig schwierig und nur für den konkreten Einzelfall bestimmbar. Die Aufsichtsbehörde kann hierbei im Rahmen ihres Beratungsangebotes unterstützen.

## 1.3 Aufgaben einer Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hat die Aufgabe, die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz zu überwachen. Dies geschieht sich im Wesentlichen über

- die Bearbeitung von Anfragen (Beratung) und Beschwerden (Prüfung der Datenschutzkonformität der aufgezeigten Verfahrensweisen),
- die Durchführung von Kontrollen,
- die Beanstandung von Datenschutzverstößen, ggf. Durchführung von Bußgeldverfahren,
- die Anordnung zur Beseitigung von Sicherheitsmängeln,
- die Führung des öffentlichen Registers der meldepflichtigen Unternehmen, vor allem Auskunfteien, Adresshändler sowie Markt- und Meinungsforschungsinstitute und
- die bundesweite Zusammenarbeit mit anderen Aufsichtsbehörden in Datenschutzfragen.

Besonderen Wert legt die Aufsichtsbehörde auf die seit Mitte 2006 gesetzlich normierte Aufgabe, die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse zu beraten und zu unterstützen (§ 38 Abs. 1 Satz 2 BDSG). In einem konstruktiven Dialog wird auf die Belange potentieller Betroffener geachtet. Auf diesem Weg können die datenschutzrechtlichen Vorschriften sachgerecht ausgelegt und praktikable Lösungen entwickelt werden.

Das Tätigwerden der Aufsichtsbehörde liegt in deren pflichtgemäßem Ermessen. Für Prüfungshandlungen ist weder ein bestimmter Anlass noch ein Verdacht notwendig. Zulässig sind sowohl anlassbezogene als auch anlassunabhängige Prüfungen. Anlässe können z. B. sein: eine Eingabe eines Betroffenen, Anzeigen von Dritten (Interessenverband, Konkurrenzunternehmen, beteiligter Dritter), Informationen von Behörden, eine Berichterstattung in den Medien. Anfragen und Eingaben von Bürgerinnen und Bürgern, die telefonisch und schriftlich (gern auch per E-Mail) an die Aufsichtsbehörde herangetragen werden, machen den Hauptteil der Arbeit aus. Viele Fragen lassen sich nicht sofort beantworten, sondern erfordern eine Aufklärung des Sachverhalts. Hierzu wendet sich die Aufsichtsbehörde an die verantwortliche Stelle und bittet um eine Stellungnahme sowie ggf. um Ausführungen zu konkreten Einzelfragen. Die Mitarbeiter der Aufsichtsbehörde haben das Recht, die Geschäftsräume zu betreten und alle mit der Datenverarbeitung in Zusammenhang stehenden Unterlagen einzusehen. Oft ist erst nach umfassenden Ermittlungen eine datenschutzrechtliche Bewertung der geschilderten Fälle möglich. Die abschließende Bewertung wird dem

Petenten mitgeteilt. Von Bedeutung für die Betroffenen ist, dass ihm selbst durch die Tätigkeit der Aufsichtsbehörde grundsätzlich keine Kosten entstehen.

### 1.4 Der Beauftragte für den Datenschutz (DSB) und seine Aufgaben

Der betriebliche Datenschutzbeauftragte dient der Selbstkontrolle der verantwortlichen Stelle, für die er bestellt ist. Er wirkt mit seinen spezifischen Fachkenntnissen auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hin. Wird der Beauftragte für den Datenschutz bereits frühzeitig im Verfahren einbezogen, kann er dafür sorgen, dass datenschutzrechtliche Vorgaben beachtet und umgesetzt werden. Auch kann er notwendige technische und organisatorische Maßnahmen veranlassen, um Persönlichkeitsrechtsverletzungen zu verhindern.

Wann eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht, ergibt sich aus § 4f Abs. 1 BDSG. Nicht-öffentliche Stellen haben einen DSB zu bestellen, wenn sie in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen haben nicht-öffentliche Stellen einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn sie automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten.

Gemäß § 4f Abs. 2 S. 1 BDSG darf zum Beauftragten für den Datenschutz nur bestellt werden, wer die erforderliche Fachkunde und Zuverlässigkeit - zum Zeitpunkt der Bestellung - besitzt. Der Betroffene muss über das notwendige Wissen verfügen, um die gesetzlich vorgesehenen Aufgaben eines Datenschutzbeauftragten - auch unter Beachtung des für die verantwortliche Stelle typischen Geschäftsbetriebes - zu erfüllen. Dies ist möglich, wenn juristische Kenntnisse (gesetzliche Regelungen des Datenschutzes - BDSG, spezielles Datenschutzrecht des jeweiligen Firmenbereichs) vorhanden sind und ein möglichst umfassender Einblick in die Unternehmensstruktur und Organisation der verantwortlichen Stelle besteht. Daneben sind betriebswirtschaftliches Wissen und Erfahrung sowie Kenntnisse im Bereich der Datenverarbeitung/Informationsverarbeitung ebenfalls von Belang.

Der DSB muss auch persönlich zuverlässig sein. Das Erfordernis der Zuverlässigkeit soll verhindern, dass ein für andere Tätigkeiten nicht qualifizierter Mitarbeiter auf die Position des Datenschutzbeauftragten „abgeschoben“ wird. Es soll aber auch dazu führen, dass der Datenschutzbeauftragte seine Aufgaben unabhängig ausübt. Daher sind auch etwaige Interessenkollisionen auszuschließen; der Kontrolleur darf nicht sich selbst kontrollieren.

Die Mindestanforderungen an die Fachkunde und Zuverlässigkeit eines DSB hat der Düsseldorfer Kreis am 24./25. November 2010 in einem Beschluss zusammengefasst, der weiterführende Informationen gibt. Der Beschluss ist abrufbar auf:
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.html?nn=409242

Die wichtigsten Aufgaben des DSB sind in § 4g BDSG benannt. Es handelt sich jedoch nicht um eine abschließende Aufzählung. Die Hauptaufgabe des Datenschutzbeauftragten liegt in der Kontrolle der praktischen Umsetzung des Datenschutzrechts. Um seiner Kontrollaufgabe nachkommen zu können, ist er in bestehende und künftige Geschäftsprozesse umfassend einzubeziehen.

Weitere ausdrücklich benannte Aufgabe des Beauftragten für den Datenschutz ist die Kontrolle der Datenverarbeitungsprogramme (§ 4g Abs. 1 S. 4 Nr. 1 BDSG). Es ist die ordnungsgemäße ***Anwendung der Datenverarbeitungsprogramme zu überwachen***, wenn mit deren Hilfe personenbezogene Daten verarbeitet werden sollen. Aus diesem Grund ist der Datenschutzbeauftragte auch vor der Einführung neuer Programme so rechtzeitig zu beteiligen, dass etwaige Einwendungen beachtet werden können. Die in § 4g Abs. 1 S. 4 Nr. 2 BDSG vorgesehene ***Fortbildungsaufgabe*** hat das Ziel, unter den Beschäftigten ein Datenschutzbewusstsein zu wecken. Weiterhin obliegt dem Beauftragten für den Datenschutz die Durchführung der vorherigen Kontrolle risikoreicher Datenverarbeitung, die sog. ***Vorabkontrolle*** (§ 4d Abs. 5 und 6 BDSG).

Eine Vorabkontrolle **ist** dann **vorgesehen**, wenn eine automatisierte Verarbeitung unter Betrachtung des konkreten Falls „besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist“. Beispielhaft – nicht abschließend – nennt das Gesetz zwei Fallgestaltungen, in denen „besondere Risiken“ vorliegen und eine Vorabkontrolle durchzuführen ist:

- bei der Verarbeitung personenbezogener Daten besonderer Art i. S. des § 3 Abs. 9 BDSG und
- bei Verfahren, die dazu dienen, die Persönlichkeit des Betroffenen zu bewerten, einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Keine Vorabkontrolle ist erforderlich, wenn einer der nachfolgenden drei Ausnahmebestände erfüllt ist:

- Vorliegen einer gesetzlichen Verpflichtung zum Umgang mit den Daten (z. B. im Rahmen des Bundesseuchengesetzes oder die andauernde Speicherung aufgrund bestimmter gesetzlicher Aufbewahrungsfristen (z. B. Röntgenverordnung) **oder**
- Vorliegen einer Einwilligung des Betroffenen **oder**
- die Erhebung, Verarbeitung oder Nutzung ist für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich.

**ZU BEACHTEN:**
Die Durchführung einer Vorabkontrolle obliegt immer dem Beauftragten für den Datenschutz. Besteht eine solche Pflicht, resultiert daraus auch stets die Verpflichtung, einen Datenschutzbeauftragten zu bestellen.
Ist eine Vorabkontrolle durch das Gesetz vorgeschrieben, ist deren Durchführung eine weitere Voraussetzung für die Zulässigkeit der Datenverarbeitung. Wurde eine notwendige Vorabkontrolle nicht durchgeführt, ist die Datenverarbeitung rechtswidrig. Das Votum des Datenschutzbeauftragten ist für die verantwortliche Stelle nicht bindend.
Im Rahmen der Vorabkontrolle prüft der Datenschutzbeauftragte sowohl die rechtliche Zulässigkeit der beabsichtigten Verarbeitung als auch, ob die vorgesehenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik ausreichend und angemessen sind. Er kann hierzu eine Risikoanalyse durchführen und ein Sicherheitskonzept erstellen.

Eine ebenfalls konkret benannte Tätigkeit des DSB ist die Führung des **sog. Verfahrensverzeichnisses**. Dem DSB ist für die Führung des Verfahrensverzeichnisses von der verantwortlichen Stelle eine Übersicht über die in § 4e Abs. 1 BDSG genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Es handelt sich um folgende Angaben:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

- Regelfristen für die Löschung der Daten,
- eine geplante Datenübermittlung in Drittstaaten.

Die Angaben sind mit Ausnahme der Beurteilung der angemessenen Sicherheitsmaßnahmen nach § 4e S. 1 Nr. 9 BDSG jedem Interessierten in geeigneter Weise verfügbar zu machen. Dies trägt zur Transparenz der Datenverarbeitung bei.

**ZU BEACHTEN:**
Hat die verantwortliche Stelle keinen Datenschutzbeauftragten bestellt oder besteht auf Grund von § 4d Abs. 3 BDSG keine Meldepflicht gegenüber der Aufsichtsbehörde, so ist der Leiter der verantwortlichen Stelle selbst verpflichtet, die vorgenannten Angaben zur Verfügung zu stellen. Er muss sogar die Erfüllung sämtlicher in § 4g Abs. 1 und 2 BDSG normierter Aufgaben des Beauftragten für den Datenschutz in anderer Weise sicher stellen.

Sowohl der Widerruf der Bestellung eines Beauftragten für den Datenschutz als auch eine Kündigung des Arbeitsverhältnisses von intern bestellten betrieblichen Datenschutzbeauftragten ist nur aus wichtigem Grund i. S. des § 626 BGB zulässig (§ 4f Abs. 3 S. 4 und 5 BDSG, sog. besonderer Kündigungsschutz). Ein wichtiger Grund kann sowohl bei amts- als auch arbeitvertragsbezogenen Gründen vorliegen und zwar immer dann, wenn die verantwortliche Stelle zur Kündigung ohne Einhaltung von Fristen berechtigt wäre. Rein wirtschaftliche oder organisatorische Gründe können eine fristlose Kündigung allerdings nur in extremen Ausnahmefällen rechtfertigen. Dies wurde aktuell durch Urteil des Bundesarbeitsgerichtes vom 23.03.2011 – 10 AZR 562/09 – festgestellt. Danach stellt die organisatorische Entscheidung, zukünftig einen externen Datenschutzbeauftragten bestellen zu wollen, keinen wichtigen Grund zur Kündigung eines internen Datenschutzbeauftragten dar.

### 1.5 Die Zielstellung eines Tätigkeitsberichtes

Seit Mai 2001 sind die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nach § 38 Abs. 1 S. 7 BDSG verpflichtet, regelmäßig, spätestens alle zwei Jahre, über ihre Tätigkeit zu berichten. Mit dem Tätigkeitsbericht, der sich auf den Berichtszeitraum **vom 01.06.2009 bis 30.09.2011** bezieht, soll neben wesentlichen Entwicklungen im Datenschutz schwerpunktmäßig über die Aktivitäten und Prüfungen der Aufsichtsbehörde für den Datenschutz Aufschluss gegeben werden.

Der Tätigkeitsbericht ist Teil der Öffentlichkeitsarbeit. Damit wird dem Bürger die Einschätzung erleichtert, ob der Umgang einer nicht-öffentlichen Stelle mit seinen personenbezogenen Daten gerechtfertigt ist und wie er bei einem unzulässigen Umgang mit seinen Daten

vorgehen kann. Auch verantwortliche Stellen oder andere mit dem Datenschutz befasste Gremien, z. B. Betriebsräte, können die Ausführungen im Tätigkeitsbericht insbesondere dazu nutzen, um datenschutzgerechte Lösungen in Standardfällen zu finden, z. B. beim geplanten Einsatz einer Videoüberwachungsanlage oder der Erstellung eines Bewerberfragebogens.

Der Tätigkeitsbericht ist dementsprechend nicht allein Rechenschaftsbericht, sondern informiert Interessierte und betroffene Bürger über aktuelle datenschutzrechtliche Themen und ihre Rechte.

### 1.6 Zusammenarbeit mit anderen Aufsichtsbehörden

Die Aufsichtsbehörde stellt immer wieder fest, dass es für Betroffene – insbesondere auf Grund gegebener Unternehmensstrukturen – im Einzelfall schwierig ist, die örtlich zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zu erkennen. Die Zuständigkeit richtet sich grundsätzlich nach dem Ort der Datenverarbeitung bzw. dem Sitz der verantwortlichen Stelle. Wendet sich ein Betroffener an die für seinen Wohnort zuständige, aber im Einzelfall örtlich nicht zuständige Aufsichtsbehörde, erteilt diese allgemeine Auskünfte. Sind Sachverhaltsermittlungen notwendig, werden dem Betroffenen die Kontaktdaten der zuständigen Aufsichtsbehörde genannt oder mit seinem Einverständnis die Anfrage an die zuständige Aufsichtsbehörde weitergeleitet.

Die Aufsichtsbehörden stimmen sich bei bundesweit auftretenden Fragestellungen in ihrer Vorgehensweise ab, in diesem Berichtszeitraum hinsichtlich der Videoüberwachung in Einkaufszentren oder zu Google Street View.

Die einheitliche Auslegung des Bundesdatenschutzgesetzes koordinieren die Aufsichtsbehörden im sog. „Düsseldorfer Kreis“. Die wichtigsten Ergebnisse werden in Arbeitspapieren oder Beschlüssen veröffentlicht. Die seit November 2006 vom Düsseldorfer Kreis gefassten Beschlüsse sind auf der Website des Bundesbeauftragten für den Datenschutz (http://www.bfdi.bund.de, Pfad: „Datenschutz/Entschließungen/Düsseldorfer Kreis“) und die Informationsfreiheit veröffentlicht.

Beschlüsse des Düsseldorfer Kreises im Berichtszeitraum:

- 05.05.2011: Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

- 05.05.2011: Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen
- 05.05.2011: Datenschutzgerechte Smartphone-Nutzung ermöglichen
- 12.04.2011: Datenschutz-Kodex der BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert
- 25.11.2010: Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste
- 25.11.2010: Mindestanforderungen an die Fachkunde und Unabhängigkeit der Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 BDSG
- 25.11.2010: Minderjährige in sozialen Netzwerken wirksam schützen
- 25.11.2010: Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen
- 29.04.2010: Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe-Harbor- Abkommen durch das Daten exportierende Unternehmen
- 27.11.2009: Gesetzesänderungen bei der Datenverwendung für Werbezwecke
- 27.11.2009: Keine Internetveröffentlichung sportgerichtlicher Entscheidungen
- 27.11.2009: Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten
- 22.10.2009: Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Daneben werden in den Arbeitsgruppen des Düsseldorfer Kreises – Kreditwirtschaft, Auskunfteien/SCHUFA, Versicherungswirtschaft, Internationaler Datenverkehr, Telekommunikation/Tele- und Mediendienste sowie Beschäftigtendatenschutz – grundsätzliche Rechtsfragen erörtert und ggf. gemeinsame Handlungsweisen abgestimmt.

# 2 Das Bundesdatenschutzgesetz (BDSG)

Bei dem Bundesdatenschutzgesetz handelt es sich um ein Schutzgesetz. Es stellt zum Schutz natürlicher Personen Regeln für den Umgang mit personenbezogenen Daten auf. Insoweit hat das Gesetz auch eine verbraucherschützende Funktion. Zugleich dient das BDSG der Regulierung des Wettbewerbs. Das BDSG ist anwendbar, soweit nicht bereichsspezifische Eingriffsbefugnisse mit Rechtsnormcharakter vorliegen.

Das **sog. Verbot mit Erlaubnisvorbehalt** - normiert in § 4 Abs. 1 BDSG - **ist die Grundregel** für jeglichen Umgang mit personenbezogenen Daten. **Dies bedeutet, dass grundsätzlich verboten ist, was nicht ausdrücklich (durch ein Gesetz oder durch eine Einwilligung des Einzelnen) erlaubt ist.** Das Gesetz verpflichtet daher die Datenverarbeiter, die rechtlichen „Spielregeln" der Datenverarbeitung zu beachten (materiell rechtliche Anforderungen) und die Bürger über den Umgang mit ihren Daten zu informieren (formell gesetzliche Vorgaben).

Soll die Einwilligung des Einzelnen Grundlage für eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sein, **ist zu beachten** (siehe § 4a BDSG):

- Die Einwilligung muss freiwillig erklärt worden sein. Zweifel an der Freiwilligkeit der Einwilligung können gegeben sein, wenn ein Abhängigkeitsverhältnis (Arbeitgeber - Arbeitnehmer) vorliegt oder wenn die verantwortliche Stelle eine beherrschende Stellung (Monopolstellung) hat.
- Die Einwilligung bedarf grundsätzlich der Schriftform. Davon darf nur abgewichten werden, wenn wegen besonderer Umstände eine andere Form angemessen ist.
- Der Betroffene ist vor Erteilung einer Einwilligung über die Tragweite seiner Einwilligung aufzuklären (insbesondere über den Verarbeitungszweck und die verantwortliche Stelle).
- Der Betroffene ist darüber zu informieren, was geschieht, wenn er keine Einwilligung erteilt, soweit dies nach den Umständen des Einzelfalls erforderlich ist oder wenn er dies verlangt.

## 2.1 Grundsätze des Datenschutzrechts

Wesentlicher Garant für die informationelle Selbstbestimmung ist, dass personenbezogene Daten der **Zweckbindung** unterliegen. Grundsätzlich dürfen personenbezogene Daten nur zu den Zwecken verarbeitet werden, für die sie erhoben bzw. gespeichert worden sind.

Die Zwecke, für die Daten verarbeitet oder genutzt werden sollen, sind bereits bei der Erhebung konkret festzulegen (§ 28 Abs. 1 S. 2 BDSG). Eine „konkrete“ Festlegung hat zum Inhalt, welcher Zweck hinter dem für die Verarbeitung erforderlichen Interesse steht. Dieser Zweck ist entsprechend § 4e S. 1 Nr. 4 BDSG zu dokumentieren.

Es gibt Ausnahmen vom Grundsatz der Zweckbindung. So kommt eine Verwendung für andere Zwecke in Betracht:

- zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten,
- wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften,
- zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten und
- zu wissenschaftlichen Zwecken.

Bei diesen Ausnahmetatbeständen muss eine Interessenabwägung zwischen dem geänderten Zweck und den entgegenstehenden schutzwürdigen Interessen des Betroffenen unter dem Maßstab der Erforderlichkeit vorgenommen werden.

Ein weiterer gesetzlich ausdrücklich geregelter Grundsatz ist der **Grundsatz der Datenvermeidung und Datensparsamkeit** (§ 3a S. 1 BDSG). Schon bei der Gestaltung der eingesetzten technischen Systeme und Verfahren soll die Erhebung und Verwendung personenbezogener Daten soweit wie möglich begrenzt, ggf. ganz vermieden werden. Eine Vermeidung des Umgangs mit personenbezogenen Daten ist möglich, wenn das angestrebte Ziel auch ohne die Verarbeitung personenbezogener Daten erreichbar ist. Dem Grundsatz kann insbesondere durch die Anonymisierung oder Pseudonymisierung Rechnung getragen werden (§ 3a S. 2 BDSG).

**Begriffserläuterungen:**
*Anonymisieren* ist gemäß § 3 Abs. 6 BDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Daten, die Verhältnisse einer Person betreffen, sind dann anonym, wenn die Wahrscheinlichkeit, sie einer Person zuordnen zu können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet (Roßnagel/Scholz, MMR 2000, 721 (724)).

*Pseudonymisieren* ist laut § 3 Abs. 6a BDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Anonymisierung oder Pseudonymisierung sind grundsätzlich dann möglich, wenn in ein Verfahren zwar personenbezogene Daten einfließen, aber abstrakte Ergebnisse erzielt werden sollen (z. B. in der Forschung, bei der Planung, bei der Organisationskontrolle und bei der Qualitätssicherung).

Der Grundsatz der Datenvermeidung und -sparsamkeit kann optimal verwirklicht werden, wenn bei einem System oder Verfahren überhaupt keine personenbezogenen Daten anfallen. Ist dies nicht zu verhindern, spielt auch die frühestmögliche Datenlöschung eine wichtige Rolle.

Zu den grundlegenden Prinzipien des Datenschutzes gehört auch die **Transparenz der Datenverarbeitung**. Sie ist ein wesentlicher Akzeptanzfaktor für den Umgang mit personenbezogenen Daten und hat zum Ziel, den Betroffenen ausreichend über den Umfang des Umgangs mit seinen Daten zu informieren. Hierzu statuiert § 4 Abs. 2 Satz 1 BDSG den **Grundsatz der Direkterhebung** von Daten beim Betroffenen. Damit einher geht die Verpflichtung zur Information über Art und Verwendungszwecke der beabsichtigten Datenverarbeitung. Werden personenbezogene Daten beim Betroffenen erhoben, dann **hat** ihn die verantwortliche Stelle über

- ihre Identität,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorien von Empfängern, soweit der Betroffene mit einer Übermittlung an diese nicht rechnen muss,

**zu unterrichten**.

Eine weitere Grundregel ist, dass die Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die ***technischen und organisatorischen Maßnahmen*** treffen müssen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Dies gilt insbesondere für die in der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen – Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle incl. Schutz vor unbefugten Zugriffen, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungsgebot zur Zweckbindung. Welche Maßnahmen im Hinblick auf die Datensicherheit zu treffen sind, hängt sowohl von der Art der Daten ab, als auch

von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen der Verarbeitung.

## 2.2 Änderungen des Bundesdatenschutzgesetzes

Durch die zum 1. September 2009, 1. April 2010 sowie 11. Juni 2010 in Kraft getretenen Novellen zum BDSG kam es zu einer Reihe von Rechtsänderungen. Im Einzelnen:

- Präzisierung der Definition der Grundsätze der Datenvermeidung und -sparsamkeit, § 3a BDSG,
- Stärkung der betrieblichen Datenschutzbeauftragten, § 4f BDSG,
- Regelungen für die Übermittlung personenbezogener Daten an Auskunfteien, § 28a BDSG, einschließlich Regelungen für die Heranziehung personenbezogener Daten für die Bonitätsbewertung, §§ 6, 28a Abs. 2 S. 4, 28 Abs. 3 BDSG,
- Regelungen für den Einsatz des Scoreverfahrens im Rahmen von Vertragsverhältnissen, § 28b BDSG,
- verstärkte Informationspflichten bzw. -rechte:
  - automatisierte Einzelfallentscheidungen: der Betroffene muss umfassender informiert werden; bei beeinträchtigenden Entscheidungen muss der Betroffene auf Verlangen auch über die wesentlichen Gründe aufgeklärt werden (§ 6a BDSG).
  - der Verbraucher muss über eine Bonitätsauskunft einer Auskunftei informiert werden, wenn ein Verbraucherdarlehensvertrag auf dieser Grundlage abgelehnt wurde (§ 29 Abs. 7 BDSG).
  - Auskunfteien müssen einmal im Jahr auf Antrag kostenlos Auskunft zu den bei ihnen gespeicherten personenbezogenen Daten geben (§ 34 Abs. 8 BDSG).
  - Scoringverfahren: Der Betroffene hat einen Anspruch darauf, dass ihm das Zustandekommen seines Scorewertes einzelfallbezogenen und nachvollziehbar erläutert wird (§§ 28b, 34 BDSG).
  - Informationspflicht bei Datenschutzpannen (§ 42a BDSG),
- verschärfte Anforderungen bei der Auftragsdatenverarbeitung, § 11 BDSG,
- Beschränkungen bei postalischer Werbung und Adresshandel, § 28 Abs. 3 BDSG - Grundsatz: Einholung einer Einwilligung des Betroffenen unter dem Vorbehalt gesetzlich normierter Ausnahmen,
- Verbot der Bindung des Vertragsabschlusses an die Einwilligung in die Datenverarbeitung zu Werbezwecken, § 28 Abs. 3b BDSG,

- Privilegierung der Markt- und Meinungsforschung bei der Nutzung von Adressdaten, § 30a BDSG: Ein Datenumgang ist grundsätzlich auch ohne Einwilligung des Betroffenen möglich,
- Norm zum Arbeitnehmerdatenschutz, § 32 BDSG,
- verbesserte Sanktionsbefugnisse: Erweiterung der Bußgeldtatbestände, Erhöhung der Bußgelder, § 43 BDSG
- Anordnungsbefugnisse für Aufsichtsbehörde bei materiell-rechtlichen Verstößen, § 38 Abs. 5 BDSG.

Bereits der 4. Tätigkeitsbericht enthält Ausführungen zu den Themen Datenverarbeitung zum Zwecke der Werbung, Arbeitnehmerdatenschutz, Automatisierte Einzelentscheidung, Einmeldung von Daten bei einer Auskunftei, Scoring, Auskunftsrecht der Betroffenen. Der Bericht ist abrufbar unter:
http://www.sachsen-anhalt.de/fileadmin/Elementbibliothek/LVwA-Bibliothek/Download/Publikationen/2010_datenschutzbericht.pdf

Zu ausgewählten Regelungen wird Folgendes erläutert:

- **Arbeitnehmerdatenschutz**

Ein eigenständiges Gesetz zum Datenschutz im Beschäftigungsverhältnis wurde zunächst nicht erlassen. Stattdessen wurde ein neuer Paragraph in das Bundesdatenschutzgesetz eingefügt - § 32 BDSG Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses -. Die Vorschrift trat am 01.09.2009 in Kraft.

§ 32 BDSG regelt den Umgang mit Beschäftigtendaten und ist eine Reaktion auf die in der Vergangenheit festgestellten Defizite insbesondere beim Umgang mit Mitarbeiterdaten im Rahmen der Korruptionsbekämpfung in Unternehmen. § 32 BDSG kodifiziert weitgehend zum Arbeitnehmerdatenschutz ergangene Rechtsprechung und verdrängt im Beschäftigungsverhältnis grundsätzlich die allgemeinen Regelungen der §§ 28 Abs. 1 S. 1 Nr. 1 und 28 Abs. 1 S. 2 BDSG.

Nach § 32 Abs. 1 S. 1 BDSG darf mit personenbezogenen Daten eines Beschäftigten nur umgegangen werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung erforderlich ist. Die Vorschrift regelt den Umgang mit Daten zur Bewerberauswahl, zu Leistungs- und Verhaltenskontrollen,

zu Abmahnungen und Kündigungen, aber auch zur Verhinderung von Straftaten und sonstigen Verstößen mit Bezug zum Beschäftigtenverhältnis.
Enge Voraussetzungen zum Umgang mit Daten legt § 32 Abs. 1 S. 2 BDSG fest, wenn es um die Aufdeckung von Straftaten durch Beschäftigte geht. Insbesondere ist eine spezifische Abwägung erforderlich, in der die typische Schwere des Eingriffs in das Persönlichkeitsrecht und in Bezug auf Straftaten der Verdachtsgrad sowie die Schwere der vermuteten Straftat einzubeziehen sind.

Da die Neuregelungen zum Arbeitnehmerdatenschutz nicht als ausreichend erachtet werden, besteht weiterer Novellierungsbedarf. Gegenwärtig befindet sich ein Gesetzentwurf der Bundesregierung für ein Gesetz zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230) in der parlamentarischen Beratung. Eine öffentliche Anhörung fand am 23. Mai 2011 statt.

- **Informationspflichten bei Sicherheitslecks und Datenpannen (§ 42a BDSG)**

Der neue § 42a BDSG begründete zum 01.09.2009 bei bestimmten schwerwiegenden Datenschutzvorfällen eine Informationspflicht der verantwortlichen Stelle gegenüber der Aufsichtsbehörde sowie den Betroffenen. Letztere sollen Kenntnis davon erlangen, wenn mit ihren personenbezogenen Daten „etwas schiefgelaufen ist“. So erhalten sie die Möglichkeit, auch selbst Schutzmaßnahmen zu ergreifen und etwaige Rechte, z. B. Schadenersatzansprüche, geltend zu machen.

Vertiefte Informationen zu § 42a BDSG sind abrufbar auf der Homepage des Berliner Beauftragten für Datenschutz und Informationsfreiheit:
http://www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg.
Die dortigen Darstellungen liegen nachfolgenden Ausführungen zu Grunde:

Sobald eine verantwortliche Stelle erfährt, dass Daten abhanden gekommen sind, muss sie zunächst **feststellen, welche Datenarten betroffen sind**. Eine Pflicht zur Information nach § 42a S. 1 BDSG besteht nur, wenn es sich um folgende Datenarten handelt:
- besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG,
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen **oder**
- personenbezogene Daten zu Bank- oder Kreditkartenkonten.

Die Pflicht zur Mitteilung setzt weiterhin voraus, dass die Daten **unrechtmäßig übermittelt** oder Dritten auf **sonstige Weise unrechtmäßig zur Kenntnis** gelangt sind. Es genügt, wenn offensichtlich ist, dass Dritte Kenntnis erlangt haben oder anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon auszugehen ist. **Unrechtmäßig ist** die Übermittlung oder sonstige Kenntniserlangung dann, wenn sie ohne Rechtsgrund erfolgt.
Schließlich muss die verantwortliche Stelle eine Prognoseentscheidung treffen, ob **schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen**. Es müssen mögliche Folgen identifiziert werden und diese anhand der drohenden Belastung für die Betroffenen und der Wahrscheinlichkeit des Schadenseintritts bewertet werden. Dafür sind mögliche Verwendungsszenarien zu entwickeln und daraufhin zu untersuchen, welche Auswirkungen, materieller wie immaterieller Art (z. B. finanzielle Schäden oder soziale Nachteile wie Identitätsbetrug) möglich erscheinen.

Es empfiehlt sich im jeweiligen Fall die Prüfung der Voraussetzungen des § 42a S. 1 BDSG nachvollziehbar zu dokumentieren. Bei Zweifelsfragen sollte die Aufsichtsbehörde kontaktiert werden.

Die Benachrichtigung hat unverzüglich zu erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden (z. B. Sicherheitslücken in der eingesetzten Software geschlossen werden) oder nicht unverzüglich erfolgt sind. Mit der Benachrichtigung gegenüber der Aufsichtsbehörde müssen folgende Fragen beantwortet werden:
- Wann sind die Daten abhanden gekommen bzw. wann wurde dies von der verantwortlichen Stelle festgestellt?
- Welche Daten sind betroffen und wie wurden diese unrechtmäßig übermittelt bzw. wie sind diese Daten unrechtmäßig zur Kenntnis anderer gelangt?
- Welche nachteiligen Folgen der unrechtmäßigen Kenntniserlangung sind möglich?
- Welche Maßnahmen wurden von der verantwortlichen Stelle ergriffen?
- Sind die Betroffenen bereits benachrichtigt worden und was wurde diesen empfohlen?

Die Unterrichtung der Betroffenen dient dazu, transparent und verständlich zu machen, was (unter Nennung der konkret betroffenen Daten) passiert ist, welche Gefahren drohen und welche Maßnahmen konkret ergriffen werden können.

Um dies gewährleisten zu können, muss die unternehmensinterne Organisation so konzipiert werden, dass entsprechende Vorfälle – gleich aus welchem internen Bereich – der Unternehmens/Betriebsleitung bzw. dem Vorstand unverzüglich zur Kenntnis gelangen. Dies setzt eine Information aller Mitarbeiter über die Meldepflicht voraus. Gleichzeitig empfiehlt sich die

Regelung der Meldewege und eine regelmäßige Überprüfung in Bezug auf deren Wirksamkeit. Verstöße gegen die Meldepflicht können mit Bußgeld geahndet werden.

- **Auftragsdatenverarbeitung**

Hintergrund der ergänzenden Regelung sind die sog. Datenschutzskandale der Vergangenheit. Mehrfach kam es zu unkontrolliertem und unbefugtem Umgang mit personenbezogenen Daten durch Callcenter und andere Auftragnehmer. Der jetzige § 11 BDSG nimmt Auftraggeber schärfer in die Pflicht. Bei der Auftragsdatenverarbeitung sind folgende wesentliche Punkte zu beachten (Neuerungen hervorgehoben):

- Der Auftraggeber ist für die Einhaltung des Datenschutzes verantwortlich.
- Der Auftraggeber muss den Auftragnehmer sorgfältig auswählen.
- Der Auftrag ist schriftlich unter Regelung der **konkretisierten Vertragsinhalte** zu erteilen.
- Die getroffenen Datensicherungsmaßnahmen müssen **vor Beginn der Datenverarbeitung getroffen und beschrieben** werden.
- Vor Beginn der Datenverarbeitung muss sich der Auftraggeber beim Auftragnehmer von den getroffenen technischen und organisatorischen Maßnahmen überzeugen. Ein Verstoß gegen diese Verpflichtung ist **bußgeldbewehrt (§ 43 Abs. 1 Nr. 2b 2. Hs BDSG)**.
  **Zur Erfüllung der Verpflichtung genügt es nicht**, wenn ein Auftraggeber allein schriftliche Erklärungen des Auftragnehmers, z. B. ein Sicherheitskonzept, entgegen nimmt ohne dass die konkrete Umsetzung überprüft wird.
- Der Auftraggeber hat sich regelmäßig von der **Einhaltung der Datensicherheitsmaßnahmen zu überzeugen und dies zu dokumentierten.** Aus der Dokumentation sollte zumindest der Zeitpunkt der Überprüfung, die geprüften Aspekte, die konkreten Prüfmechanismen und das Ergebnis der Prüfung hervorgehen. Eine gesetzliche Normierung der zeitlichen Intervalle erfolgte nicht. Diese sollten sich zweckmäßigerweise am Umfang der Auftragsdatenverarbeitung, des Gefährdungspotentiales für die Betroffenen, der Innovationsgeschwindigkeit und der Sensibilität der verarbeiteten personenbezogenen Daten orientieren.
- Die Berechtigung zur Schaffung von Unterauftragsverhältnissen muss geregelt sein.
- Datenschutzverstöße müssen gemeldet werden.
- Ansprechpartner müssen benannt sein.

Altverträge nach § 11 BDSG, die nicht den inhaltlichen Anforderungen des erweiterten § 11 Abs. 2 S. 2 BDSG entsprechen, sind unverzüglich anzupassen.

- **Einmeldung von Daten bei einer Auskunftei**

Erstmalig hat der Gesetzgeber in § 28a BDSG in einem konkreten Katalog festgelegt, unter welchen Voraussetzungen Daten über eine Forderung bei einer Auskunftei eingemeldet werden dürfen. Personenbezogene Daten über eine Forderung dürfen an Auskunfteien nur übermittelt werden, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und es sich um eine Forderung nachstehender Art handelt:

- Forderung, die durch rechtskräftiges oder vorläufig vollstreckbares Urteil festgestellt worden ist;
- Forderungen im Rahmen von Insolvenzverfahren;
- ausdrücklich vom Betroffenen anerkannte Forderungen;
- nicht titulierte Forderungen,
  die mindestens zweimal schriftlich gemahnt und nicht bestritten worden sind, wobei auf die Einmeldung hingewiesen worden sein muss, oder
  welche die verantwortliche Stelle zur fristlosen Kündigung berechtigen, wenn vorher über die Einmeldung bei einer Auskunftei informiert wurde.

Neben den vorgenannten sog. Negativdaten dürfen Auskunfteien von Banken und anderen Kreditinstituten auch sog. Positivdaten erhalten. Dies gilt für Informationen über die Begründung, die ordnungsgemäße Durchführung und die Beendigung des Vertragsverhältnisses über ein Bankgeschäft (z. B. Girokontenverträge, laufende Kredite, beantragte Hypotheken). Es bedarf hierfür nicht mehr der Einwilligung des Betroffenen (sog. SCHUFA-Klausel). Die Regelung wurde getroffen, weil geforderte Einwilligungserklärungen faktisch nicht freiwillig waren. Ohne Einwilligungserklärung kam es nicht zum Vertragsabschluss.

Da kein Kreditrisiko besteht, dürfen zu einem Girokonto auf Guthabenbasis keine Angaben zum Bestehen, Ablauf, zur Dauer oder Beendigung des Giroverhältnisses an eine Auskunftei eingemeldet werden. Hier ist die Einmeldung von Daten gesetzlich nicht erlaubt.

- **Scoring**

Bei Scoring-Verfahren wird für bestimmte Merkmale ein Wert, der sog. Scorewert, errechnet. Dieser Wert drückt die statistische Wahrscheinlichkeit aus, mit welcher ein bestimmtes Ereignis eintritt oder ein bestimmtes Verhalten zukünftig erfolgt. Dem Betroffenen wird dieser Wert in einem Entscheidungsverfahren, z. B. im Rahmen einer Kreditvergabeentscheidung, mit entsprechenden Konsequenzen zugerechnet.

§ 28b BDSG regelt Scoring-Verfahren erstmals gesetzlich. Welche Merkmale beim Scoring genutzt werden dürfen, wird nur bedingt normiert. Es kommt auf eine Interessenabwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Belangen der Betroffenen an. Folgende Bedingungen müssen beachtet werden:

- Zur Ermittlung des Scorewertes dürfen nur wissenschaftlich anerkannte mathematisch-statistische Verfahren eingesetzt werden. Jede Stelle, die Scorewerte berechnet, muss der zuständigen Datenschutzaufsichtsbehörde darlegen können, dass die verwendeten Daten und die angewandte Methode tatsächlich geeignet ist, eine Prognose über das zu beurteilende Verhalten des Betroffenen anzustellen. Dies ist der Aufsichtsbehörde bei entsprechender Kontrolle nachzuweisen und somit bereits im Vorfeld zu dokumentieren.
- Die ausschließliche Nutzung von Anschriftendaten zur Ermittlung eines Scorewertes ist unzulässig. Die Bonität eines Betroffenen darf also nicht allein davon abhängig gemacht werden, in welcher Wohngegend dieser lebt.

Scoringverfahren müssen für den Betroffenen transparent sein. Der Scorewert muss daher im Rahmen eines entsprechenden Auskunftsersuchens verständlich, einzelfallbezogen und nachvollziehbar erklärt werden. Dies ermöglicht Betroffenen beurteilen zu können, ob bei der Scorewertermittlung die richtigen Daten zu Grunde liegen und ob etwaige Besonderheiten bei der Bewertung ausreichend berücksichtigt wurden. Der Betroffene hat allerdings keinen Anspruch, dass ihm das mathematische Berechnungsverfahren im Detail erläutert wird.

- **Werbung und Adresshandel**

Bei Werbemaßnahmen sind sowohl Vorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG) als auch datenschutzrechtliche Vorgaben einzuhalten. Für Werbung via Telefon, Telefax, E-Mail und SMS-Werbung setzt das UWG enge Grenzen. Nachfolgend werden die Änderungen durch die Novellierung des BDSG zum 01.09.2009 erläutert.

Das sog. Listenprivileg erlaubte bis zur Novellierung, dass bestimmte personenbezogene Daten, wie Name, Anschrift und Geburtsjahr von Betroffenen, die einer bestimmten Personengruppe angehören und listenmäßig zusammengefasst sind, für eigene oder fremde Werbezwecke verarbeitet und übermittelt werden durften, **ohne dafür die Einwilligung des Betroffenen** einzuholen. Dies ermöglichte zum einen die Briefwerbung für eigene Kunden, zum anderen den Handel mit Daten. Es bestand lediglich die Verpflichtung, spätestens zum Zeitpunkt der Ansprache für die Zwecke der Werbung über das Werbewiderspruchsrecht zu informieren. Mit dem Werbewiderspruchsrecht (im Detail siehe 2.3 – Die Rechte der Betroffenen nach dem BDSG) kann sich der Beworbene gegen weitere Werbung aussprechen.

*Listendaten* umfassen nur folgende Daten:
- Angaben zu Personengruppen (sog. Gruppenmerkmal wie z. B. Autofahrer, Hobbygärtner),
- Beruf,
- Branchen- oder Geschäftsbezeichnung,
- Name und Anschrift,
- Titel, akademischer Grad und
- Geburtsjahr (nicht: Geburtsdatum!)

Weitere Daten wie z. B. E-Mail-Adresse, Telefonnummer, Daten über das Zahlungsverhalten stellen keine Listendaten dar.

Mit der Änderung des BDSG zum 01.09.2009 wurde zum **Grundsatz**, dass personenbezogene Daten für persönlich adressierte Werbung **nur mit Einwilligung** des Betroffenen möglich ist. Von diesem Grundsatz gibt es jedoch zahlreiche Ausnahmen, z. B.:
- Ohne Einwilligung dürfen Unternehmen ihre eigenen Kunden bewerben. Hierfür dürfen nur die sog. Listendaten genutzt werden. Diese wurden entweder beim Betroffenen selbst erhoben oder aus allgemein zugänglichen Quellen.
- Ohne Einwilligung kann Werbung versandt werden, wenn der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weitergeben hat. Es muss die Herkunft und die Weitergabe der Adressdaten dokumentiert werden und sich bereits aus der Werbung ergeben, wer die Daten erstmalig weitergegeben hat.

Alle gesetzlich normierten Ausnahmen stehen unter dem grundsätzlichen Vorbehalt, dass
- der Werbung unter Nutzung der Adressdaten (nicht E-Mail oder Telefonnummer) keine schutzwürdigen Interessen entgegenstehen.
- Werbewidersprüche, die strikt zu beachten sind, nicht bestehen.
- der Betroffene bereits bei Vertragsabschluss und bei jeder werblichen Ansprache auf sein Widerspruchsrecht und die verantwortliche Stelle hinzuweisen ist.

Der sog. Handel mit Adressen, d. h. die Übermittlung von Listendaten zu beliebigen Werbezwecken, ist zulässig sofern, die „Lieferkette“ (d. h. von wem wurden welche Daten bezogen) dokumentiert ist und die erhebende Stelle (die ursprüngliche Datenquelle) eindeutig aus der Werbung hervorgeht (§ 28 Abs. 3 S. 4 BDSG).
Die übermittelnde Stelle (der Adressverkäufer) und auch der Empfänger (der Adresskäufer) müssen ab dem 01.04.2010 die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren speichern (§ 34 Abs. 1a BDSG). Diese Verpflichtung trifft den Erstempfänger und jeden weiteren Empfänger. Sind die Daten über mehrere Unternehmen weitergegeben worden, ist immer das Unternehmen anzugeben, welches die Daten erstmalig erhoben hat.

- **Ausblick**

Das Bundesdatenschutzgesetz basiert nicht allein auf nationalem Recht. Vielmehr ist der Rahmen durch EU-Recht vorgegeben. Die EU-Kommission hat ein Gesamtkonzept zur Neuregelung des Datenschutzes innerhalb der EU vorgelegt.

Zum einen geht es darum, dem veränderten Rechtsrahmen, der mit dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) geschaffen wurde, Rechnung zu tragen. Nach Art. 16 Abs. 2 AEUV erlassen das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Bedeutsam ist, dass die bisherige Säulenstruktur aufgegeben wurde. Die im Rahmen der früheren 3. Säule (Polizeiliche und justizielle Zusammenarbeit in Strafsachen) erlassenen Rahmenbeschlüsse treten nach einer Übergangsbestimmung von fünf Jahren nach dem Inkrafttreten des Vertrages von Lissabon außer Kraft und sind bis dahin durch Richtlinien bzw. Verordnungen abzulösen.

Zum anderen geht es um darum, das europäische Datenschutzrecht, das mit der EG-Datenschutzrichtlinie von 1995 geschaffen wurde, den veränderten Bedingungen, die sich aus der rasanten technologischen Entwicklung und der Globalisierung der Datenverarbeitung ergeben, anzupassen.

Die EU-Kommission wird nach der Absichtserklärung vom 04.11.2010 (Az. IP/10/1462) in diesem Jahr neue klare und konsequente Datenschutzbestimmungen vorschlagen, um folgende Kernziele zu erreichen:

- Stärkung der Rechte des Einzelnen: Sammlung und Nutzung personenbezogener Daten sollen auf das erforderliche Mindestmaß beschränkt werden und jeder soll klar und transparent darüber informiert werden, wie, warum, von wem und wie lange seine Daten verwendet werden.
- Stärkung der Binnenmarktdimension durch Verringerung des bürokratischen Aufwands für Unternehmen und die Gewährleistung gleicher Rahmenbedingungen.
- Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit der Polizei- und Strafjustizbehörden, damit personenbezogene Daten Einzelner auch an dieser Stelle geschützt werden.

- Gewährleistung eines hohen Schutzniveaus bei außerhalb der EU übermittelten Daten durch die Verbesserung und Erleichterung von Verfahren für den internationalen Datentransfer.
- Verbesserte Durchsetzung der Vorschriften durch die Stärkung und weitere Harmonisierung der Aufgaben und Befugnisse der Datenschutzbehörden, um den freien Datenverkehr im EU-Binnenmarkt zu gewährleisten.

### 2.3 Die Rechte der Betroffenen nach dem Bundesdatenschutzgesetz

Der Einzelne kann kaum noch überblicken, wer, was, bei welcher Gelegenheit, über ihn weiß und welcher Umgang mit seinen Daten erfolgt oder beabsichtigt ist. Umso wichtiger ist es, Transparenz beim Umgang mit personenbezogenen Daten herzustellen. Dieser Zielrichtung dienen auch die in den §§ 33 – 35 BDSG normierten Rechte für die Betroffenen. Diese Rechte versetzen Betroffene in die Lage, Korrektur-, Löschungs- oder ggf. Schadenersatzansprüche gegenüber der verantwortlichen Stelle geltend zu machen.

**Begriffserläuterungen:**
*Verantwortliche Stelle* ist die Stelle, die personenbezogene Daten für sich erhebt, speichert, übermittelt, verarbeitet, nutzt oder dies durch andere im Auftrag vornehmen lässt.

§ 33 BDSG normiert eine **Verpflichtung zur individuellen Benachrichtigung der Betroffenen**, wenn eine verantwortliche Stelle Daten von einem Betroffenen verarbeitet, die sie nicht direkt bei ihm erhoben hat. Der Zeitpunkt der Benachrichtigung ist unterschiedlich. Die Benachrichtigung muss umfassen:

- die Angabe der verantwortlichen Stelle (Name und Anschrift),
- die Tatsache, dass erstmals Daten über die zu benachrichtigende Person gespeichert oder übermittelt werden,
- die Art der Daten,
- die Zweckbestimmung der Erhebung bei Verarbeitung oder Nutzung sowie
- die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung an diese rechnen muss.

In bestimmten gesetzlich geregelten Fällen besteht keine Pflicht zur Benachrichtigung. Beispielsweise, wenn eine überwiegende Geheimhaltungspflicht besteht, die Unterrichtung einen unverhältnismäßigen Aufwand erfordert oder der Betroffene auf andere Weise Kenntnis von der Speicherung oder Übermittlung erlangt hat.

Der Betroffene kann mit einem an eine verantwortliche Stelle gerichteten Auskunftsersuchen (§ 34 Abs. 1 BDSG) selbst in Erfahrung bringen:

- welche Daten zu seiner Person gespeichert sind,
- die Herkunft dieser Daten,
- den Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
- den Zweck der Speicherung.

Hat ein Scoring stattgefunden, kann der Betroffene gemäß § 34 Abs. 2 BDSG nunmehr auch Auskunft erhalten über:

- die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,
- die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und
- das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte, einzelfallbezogen und nachvollziehbar.

Das Recht auf Auskunft hat jeder, unabhängig von Alter, Wohnsitz und Nationalität. Eine Auskunft ist grundsätzlich unentgeltlich. Von Stellen, die die Daten geschäftsmäßig zum Zwecke der Übermittlung speichern, so z. B. von Kreditschutzorganisationen (SCHUFA) und Handels- und Wirtschaftsauskunfteien, kann **einmal im Kalenderjahr kostenlos** Auskunft begehrt werden.
Die Auskunftserteilung kann in Ausnahmefällen bei Geschäftsgeheimnissen (§ 34 Abs. 1 S. 3, Abs. 3 S. 2 BDSG) und ansonsten nur in den Fällen abgelehnt werden, in denen keine Benachrichtigungspflicht besteht (Einzelheiten in § 34 Abs. 7 i. V. m. § 33 Abs. 2 S. 1 Nr. 2, 3 und 5-7 BDSG).

**Wie erhalten Sie Auskunft?**

- Es empfiehlt sich, die Auskunft schriftlich anzufordern. Formelle Vorgaben bestehen jedoch nicht. Im Ausnahmefall kann eine Kopie eines Personalausweisdokumentes zur Legitimation notwendig sein. Auf dieser Kopie sollten bis auf Name, Anschrift, Geburtsdatum und ggf. Gültigkeitsdauer des Dokuments alle weiteren Daten geschwärzt werden. Weitere Daten sind zur Identifikation nicht erforderlich. Soweit der Auskunftsanspruch in einem zeitlichen Zusammenhang zu einer vorherigen Benachrichtigung nach § 33 BDSG geltend gemacht wird (bis zu vier Wochen nach der Benachrichtigung) oder eine Auskunftei keine Bonitäts- oder sonstigen Inhaltsdaten gespeichert hat, erscheint die Bitte um Vorlage einer Ausweiskopie keinesfalls berechtigt.

- Bei persönlicher Vorsprache wird eine sofortige Auskunft oft nicht sofort möglich sein. Hier reicht die Einsichtsgewährung in ein Personaldokument zur Ansicht stets aus, um sich als Betroffener zu legitimieren. Eine telefonische Auskunft wird in der Regel nicht erteilt, da die Identifikationsmöglichkeiten fehlen.

- Beschreiben Sie möglichst genau, worüber Sie Auskunft wünschen.

- Wird Ihnen keine Auskunft erteilt oder haben Sie Zweifel, ob die Auskunft korrekt erteilt bzw. eine Auskunftsverweigerung oder -beschränkung nicht hinreichend erläutert wurde, können Sie sich an die zuständige Aufsichtsbehörde wenden.

Zu erwähnen bleibt, dass jedermann ein **Recht auf Einsicht in das sog. Verfahrensverzeichnis für jedermann** bei der verantwortlichen Stelle hat. Dabei handelt es sich um eine Übersicht über die automatisierten Verarbeitungen. Darin sind insbesondere die von dem Unternehmen verwendeten Verfahren verzeichnet und festgehalten, zu welchem Zweck bzw. zur Erfüllung welcher Aufgabe die Verfahren angewendet werden. Außerdem sind dem Verfahrensverzeichnis die verarbeiteten Datenarten, die Personengruppen, über die Daten gespeichert werden sowie Kategorien von Empfängern denen die Daten übermittelt werden, zu entnehmen. Das Verzeichnis enthält allerdings keine Angaben über die konkret gespeicherten Datensätze einer Person. Es ergibt sich auch nicht, ob überhaupt und wenn ja, welche Daten über eine bestimmte oder eine andere Stelle gespeichert sind.

Stellt ein Betroffener fest, dass unrichtige Daten über ihn bei der verantwortlichen Stelle gespeichert werden, besitzt er ein **Berichtigungsrecht** (§ 35 Abs. 1 BDSG).

**Begriffsbestimmung:**
**Unrichtig** sind Daten, wenn falsche Angaben, zum anderen aber auch unvollständige Angaben vorliegen und dadurch ein unzutreffender Eindruck entsteht. Unrichtig können grundsätzlich nur Tatsachenangaben, nicht aber Werturteile sein, es sei denn, sie sind einem (prozessualen) Beweis zugänglich.

Die Berichtigungspflicht besteht auch, wenn die Daten später unrichtig werden, es sei denn, es soll ein zu einem bestimmten Zeitpunkt bestehender, zutreffender Sachverhalt beschrieben werden. Die verantwortliche Stelle ist zur Berichtigung verpflichtet, wenn sie von der Unrichtigkeit Kenntnis erlangt, unabhängig auf welche Art und Weise dies geschieht (Information durch den Betroffenen selbst oder auf andere Weise). Der Betroffene muss grundsätzlich die Unrichtigkeit der Daten beweisen. Eine Verpflichtung zur Angabe der korrekten Daten besteht indes nicht.

Personenbezogene Daten sind i. d. R. zu **löschen** (§ 35 Abs. 2, 3 und 4 BDSG), wenn sie nicht mehr gebraucht werden oder die verantwortliche Stelle sie gar nicht hätte erheben dürfen. Gegebenenfalls tritt an die Stelle einer Löschung eine Sperrung, wenn

- besondere Gründe einer fälligen Löschung entgegenstehen, z. B. gesetzliche, satzungsmäßige sowie vertragliche Aufbewahrungsfristen, schutzwürdige Interessen des Betroffenen,
- wegen der Art der Speicherung eine Löschung nur mit unverhältnismäßigem Aufwand möglich ist, aber auch
- wenn der Betroffene ihre Richtigkeit bestreitet und sich weder deren Richtigkeit noch Unrichtigkeit feststellen lässt.

Gesperrte Daten dürfen grundsätzlich nicht mehr übermittelt oder genutzt werden. Ausnahmen gelten bei einer Verarbeitung oder Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegende Gründe. Die Tatsache der Sperrung darf nicht übermittelt werden.

Weiterhin besitzt jeder Betroffene ein **Recht auf Widerspruch**. Dieses Recht ist hinsichtlich der zur eigenen Person gespeicherten Daten begründet, wenn die schutzwürdigen Interessen des Betroffenen wegen einer besonderen persönlichen Situation das Interesse der privaten Stelle an der Datenverarbeitung überwiegen. Ein **besonderes** Widerspruchsrecht steht Betroffenen gegen die Verarbeitung oder Nutzung personenbezogener Daten zum Zwecke der Werbung und der Markt- oder Meinungsforschung zu (§ 28 Abs. 4 Satz 1 BDSG). Im Rahmen des **Werbewiderspruchsrechtes** besteht das Recht, der Zusendung persönlich adressierter Werbung zu widersprechen. Auf dieses Recht ist hinzuweisen, sobald Betroffene erstmals für entsprechende Zwecke angesprochen werden. In einem diesbezüglichen Werbeschreiben sollte vermerkt sein, wo und wie der Widerspruch eingelegt werden kann. Ggf. empfiehlt sich auch der Hinweise, das eine nach § 4a BDSG erteilte Einwilligung **jederzeit** widerrufen werden kann.

**Hinweis:**
Das aus dem genutzten Widerspruchsrecht resultierende Nutzungsverbot kann auch bereits bei der erstmaligen Bekanntgabe der persönlichen Daten gegenüber dem Geschäfts- oder Vertragspartner ausgesprochen werden. Bereits auf Antrags- bzw. Vertragsformularen kann der Widerspruch vermerkt werden oder es können entsprechende Passagen in den Unterlagen gestrichen werden. Der Widerspruch kann auch bei den Stellen eingelegt werden, denen die Daten übermittelt worden sind.

Für den Widerspruch, der keiner Begründung bedarf, und für den grundsätzlich keine Form vorgeschrieben ist (die Schriftform wird dennoch empfohlen), bietet sich folgende Formulierung an:
*„Ich widerspreche der Nutzung oder Übermittlung meiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung (§ 28 Abs. 4 BDSG).“*

Die Betroffenen haben jederzeit das **Recht, sich an die Kontrollinstitutionen für den Datenschutz zu wenden**, wenn sie der Auffassung sind, bei der Erhebung, Verarbeitung oder Nutzung ihrer persönlichen Daten in ihren Rechten verletzt worden zu sein.

Zudem gibt es das **Recht auf Schadenersatz (§ 7 BDSG)**. Dies bedeutet, dass eine verantwortliche Stelle einem Betroffenen, dem durch eine unzulässige oder unrichtige Datenverarbeitung ein Schaden zugefügt wurde, zum Ersatz des Schadens verpflichtet ist.

# 3 Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt

## 3.1 Allgemeines zur Aufsichtstätigkeit

### 3.1.1 Bisheriger Ansprechpartner

Das Landesverwaltungsamt war im Berichtszeitraum vom 01.06.2009 bis zum 30.09.2011 in Sachsen-Anhalt die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Mit Urteil vom 09.03.2010 hat der Europäische Gerichtshof (EuGH) festgestellt, dass die Bundesrepublik Deutschland Art. 28 Abs. 1 der „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ falsch umgesetzt hat, weil in den Ländern die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich staatlicher Aufsicht unterstellt waren und damit nicht wie gefordert, ihre Aufgaben „in völliger Unabhängigkeit“ ausübten. In Umsetzung dieses Urteils wurde auch in Sachsen-Anhalt die Datenschutzaufsicht neu strukturiert. Wie - das erfahren Sie unter Punkt 6.

Die örtliche Zuständigkeit der Aufsichtsbehörde für den nicht-öffentlichen Bereich bestimmt sich nach § 3 des Verwaltungsverfahrensgesetzes (VwVfG).

Eine besondere Zuständigkeit gibt es für Telekommunikationsunternehmen. Bei Sachverhalten, in denen im Zusammenhang mit der Erbringung von Telekommunikationsdiensten Daten erhoben, verarbeitet und genutzt werden, obliegt die Kontrollzuständigkeit dem Bundesbeauftragten für den Datenschutz (§ 115 Abs. 4 des Telekommunikationsgesetzes (TKG)).

Im Rahmen des bisherigen Internetauftrittes des Landesverwaltungsamtes wurden u. a. die Tätigkeitsberichte veröffentlicht. Diese können nach wie vor unter http://www.sachsen-anhalt.de/index.php?id=14693 eingesehen werden.

### 3.1.2 Tätigkeitsschwerpunkte

Schwerpunkt der Tätigkeit der Aufsichtsbehörde war auch in den Jahren 2009 bis 2011 die Bearbeitung von Beschwerden betroffener Bürger. Das Landesverwaltungsamt stellte für den aktuellen Berichtszeitraum einen sich fortsetzenden starken Anstieg (vom Jahr 2009 bis zum Jahr 2010 um 78 %) der Beschwerden von Betroffenen fest. Die Fallzahlen sind dem unter 3.2 abgedruckten Überblick über die Tätigkeit der Aufsichtsbehörde im Detail zu entnehmen.

Die meisten Verfahren konnten im schriftlichen Verfahren mit den verantwortlichen Stellen geklärt werden. Im Bereich der Videoüberwachung fanden zudem Vorortkontrollen statt. Sowohl die Ausrichtung der zu überprüfenden Anlagen als auch deren technische Details konnten im schriftlichen Verfahren nicht hinreichend aufgeklärt werden. Unterstützung erhielt die Aufsichtsbehörde in diesem Zusammenhang ggf. auch durch vor Ort ansässige Ordnungsbehörden.

### 3.1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten

Zusätzlich zu den förmlichen Beschwerden hatte die Aufsichtsbehörde vermehrt telefonische Anfragen und Beratungswünsche von Bürgern und Unternehmen zu verzeichnen. Da im Datenschutzrecht regelmäßig ein Abwägungsprozess zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen notwendig ist, können im Rahmen einer telefonischen Beratung die Bestimmungen des Datenschutzrechts häufig nur allgemein erläutert und eine summarische Beurteilung der Rechtslage vorgenommen werden. Bei einem tiefergehenden Beratungsbedarf bzw. der Bitte um Prüfung der Zulässigkeit einer Verfahrensweise, bat die Aufsichtsbehörde um schriftliche Sachverhaltsschilderung (auch per E-Mail). Von den telefonischen Anfragen wurden ca. 2/3 einer detaillierten Prüfung im schriftlichen Verfahren unterzogen.

Im Rahmen ihrer personellen und zeitlichen Möglichkeiten nahm die Aufsichtsbehörde an den von der Gesellschaft für Datenschutz und Datensicherung e.V. organisierten Sitzungen der Erfahrungsaustausch-Kreise der betrieblichen Datenschutzbeauftragten teil. In diesem sogenannten ERFA-Kreis werden aktuelle Datenschutz- und Datensicherheitsfragen erörtert. Bei Bedarf präsentierte die Aufsichtsbehörde bestimmte Themen ausführlich.

Im Berichtszeitraum hielten die Mitarbeiter der Aufsichtsbehörde wiederholt Vorträge zu verschiedenen Themen, wie „Datenschutz im Mittelstand“, „Datenschutz und ärztliche Schweigepflicht“, „Datenschutz im Krankenhaus“, „Datenschutz in der Wohnungswirtschaft“ oder „Datenschutz bei Familienhebammen“.

Um das Bewusstsein für den Datenschutz bereits im jugendlichen Alter zu fördern, beteiligte sich die Aufsichtsbehörde mit eigenen Beiträgen an dem Schulprojekt „Sozialkunde- und Rechtskundeunterricht in Sekundarschulen und Gymnasien“ des Landesverwaltungsamtes. Unter dem Thema „Datenschutz und Internet“ wurde in das Datenschutzrecht eingeführt, die Tätigkeit der Aufsichtsbehörde dargestellt und an Beispielen aufgezeigt, welche Gefahren

bei einem zu freizügigen Umgang mit den eigenen Daten bestehen und welche Gegenmaßnahmen ergriffen werden können.

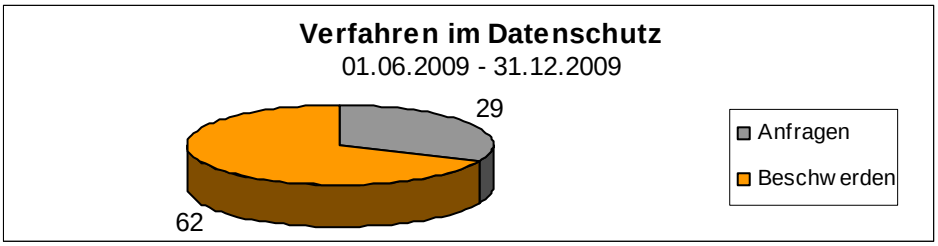
### 3.1.4 Ordnungswidrigkeitenverfahren

Nach § 43 des BDSG sind zahlreiche Verstöße gegen dieses Gesetz bußgeldbewehrt. Die Aufsichtsbehörde für den Datenschutz des Landes Sachsen-Anhalt machte nach pflichtgemäßem Ermessen von der Möglichkeit Gebrauch, ein Bußgeld zu verhängen. Bei Bußgeldbewehrtheit eines Verstoßes wurde im pflichtgemäßen Ermessen auch geprüft, ob eine Verwarnung, ggf. mit Verwarngeld, welches maximal 35,00 EUR beträgt, ausreichend ist.
Die notwendigen Sachverhaltsnachermittlungen bei materiell rechtlichen Verstößen (Bußgeldverfahren i. S. des § 43 Abs. 2 BDSG) gestalten sich häufig schwierig. Auf Grund komplexer Unternehmensstrukturen ist eine namentliche Ermittlung der konkret für einen Verstoß verantwortlichen Person nur bedingt möglich. In diesem Zusammenhang ist auch zu untersuchen, ob ein Organisationsverschulden der verantwortlichen Stelle vorliegt und ob der Verstoß ggf. einer juristischen Person zugerechnet werden kann.
Für die Aufsichtsbehörde steht die Durchführung von Bußgeldverfahren jedoch nicht im Vordergrund. Die Aufsichtsbehörde hat mehr Interesse daran, durch Aufklärung und Beratung das datenschutzgerechte Verhalten der verantwortlichen Stellen zukünftig sicherzustellen, als Verstöße in der Vergangenheit zu ahnden.

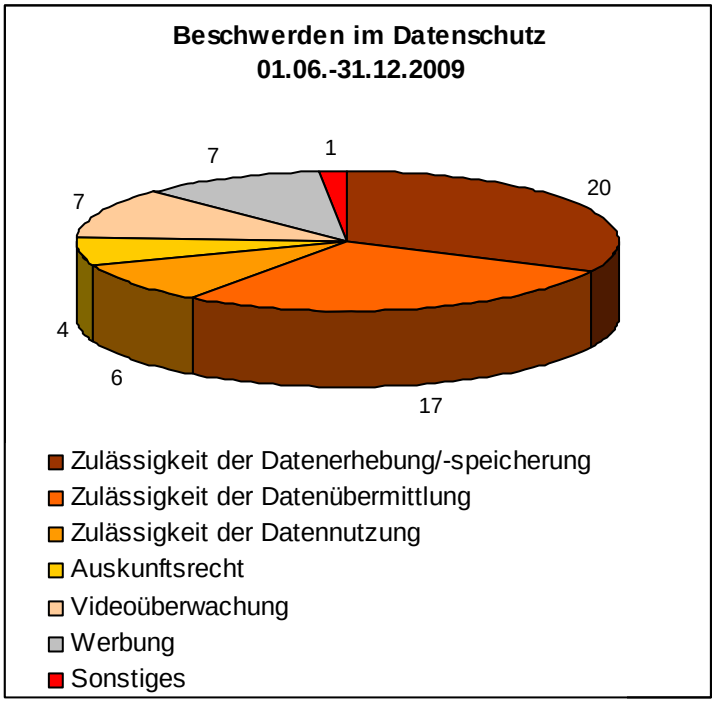
## 3.2 Zahlenmäßiger Überblick über die Tätigkeit der Aufsichtsbehörde

**Zeitraum vom 01.06.2009 – 31.12.2009**

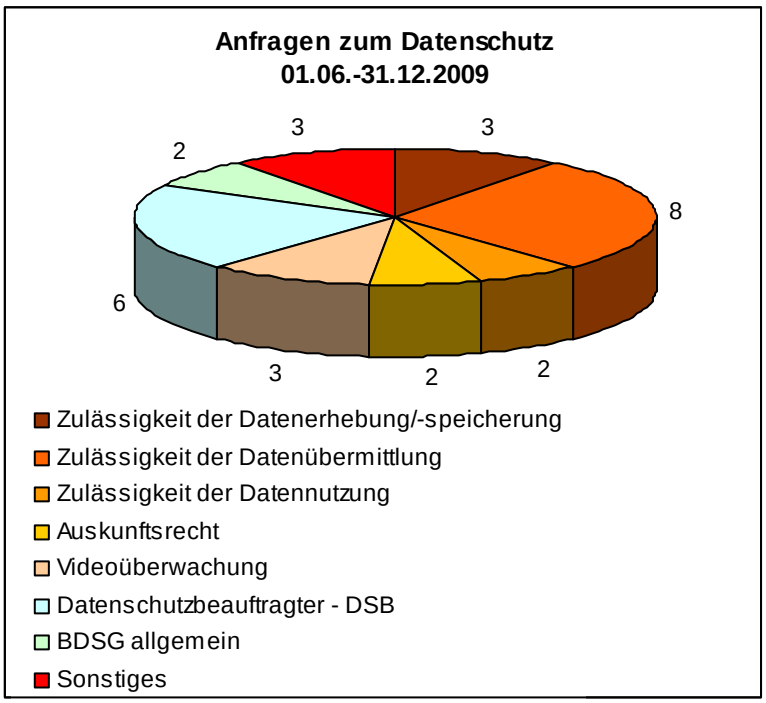
| Verfahren im Datenschutz **- Überblick -** 01.06.2009 - 31.12.2009 | |
|---|---|
| Anfragen | 29 |
| Beschwerden | 62 |



| Beschwerden im Datenschutz - Überblick 01.06.-31.12.2009 | |
|---|---|
| Zulässigkeit der Datenerhebung/-speicherung | 20 |
| Zulässigkeit der Datenübermittlung | 17 |
| Zulässigkeit der Datennutzung | 6 |
| Auskunftsrecht | 4 |
| Videoüberwachung | 7 |
| Werbung | 7 |
| Sonstiges | 1 |

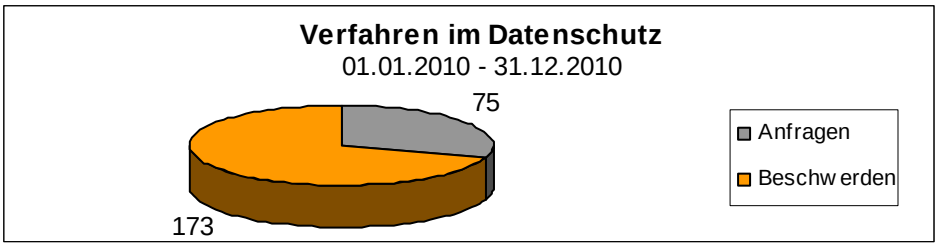



| Anfragen im Datenschutz - Überblick 01.06.-31.12.2009 | |
|---|---|
| Zulässigkeit der Datenerhebung/-speicherung | 3 |
| Zulässigkeit der Datenübermittlung | 8 |
| Zulässigkeit der Datennutzung | 2 |
| Auskunftsrecht | 2 |
| Videoüberwachung | 3 |
| Datenschutzbeauftragter - DSB | 6 |
| BDSG allgemein | 2 |
| Sonstiges | 3 |

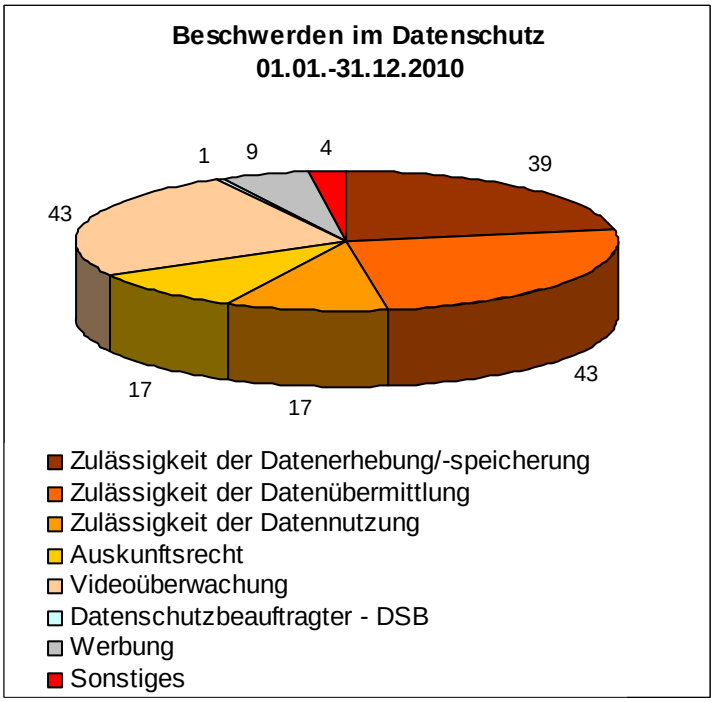


## Zeitraum vom 01.01.2010 – 31.12.2010

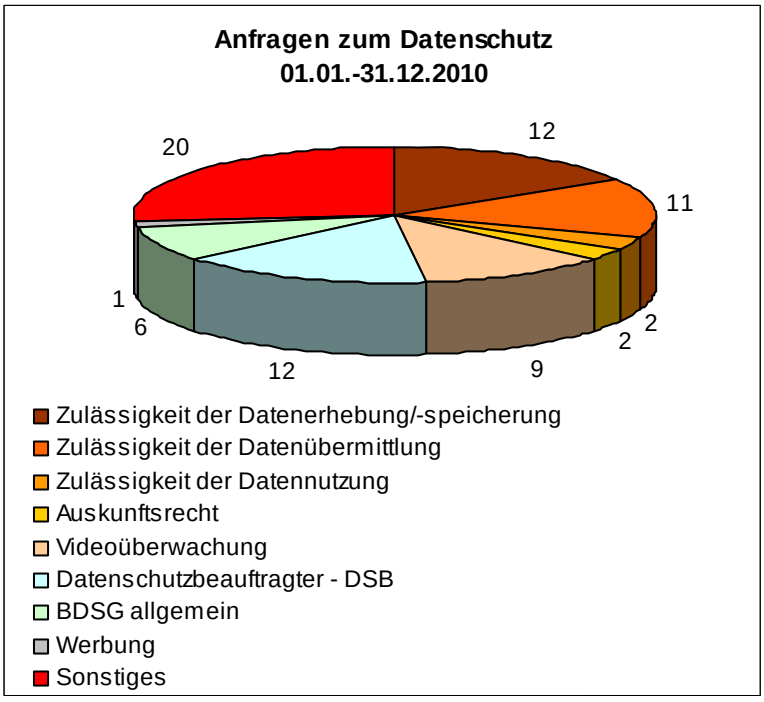
| Verfahren im Datenschutz – **Überblick** – 01.01.2010 - 31.12.2010 | |
|---|---|
| Anfragen | 75 |
| Beschwerden | 173 |




| **Beschwerden im Datenschutz - Überblick 01.01.-31.12.2010** | |
|---|---|
| Zulässigkeit der Datenerhebung/-speicherung | 39 |
| Zulässigkeit der Datenübermittlung | 43 |
| Zulässigkeit der Datennutzung | 17 |
| Auskunftsrecht | 17 |
| Videoüberwachung | 43 |
| Datenschutzbeauftragter - DSB | 1 |
| Werbung | 9 |
| Sonstiges | 4 |

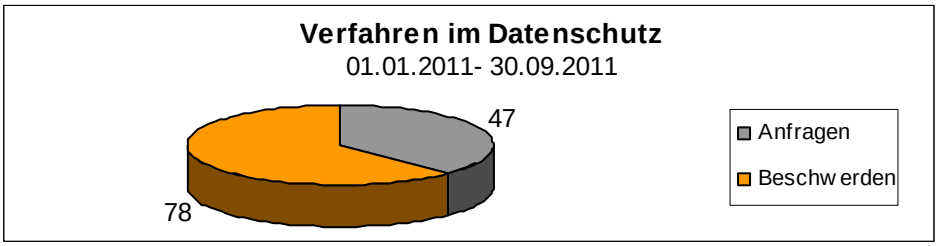



| **Anfragen im Datenschutz - Überblick 01.01.-31.12.2010** | |
|---|---|
| Zulässigkeit der Datenerhebung/-speicherung | 12 |
| Zulässigkeit der Datenübermittlung | 11 |
| Zulässigkeit der Datennutzung | 2 |
| Auskunftsrecht | 2 |
| Videoüberwachung | 9 |
| Datenschutzbeauftragter - DSB | 12 |
| BDSG allgemein | 6 |
| Werbung | 1 |
| Sonstiges | 20 |

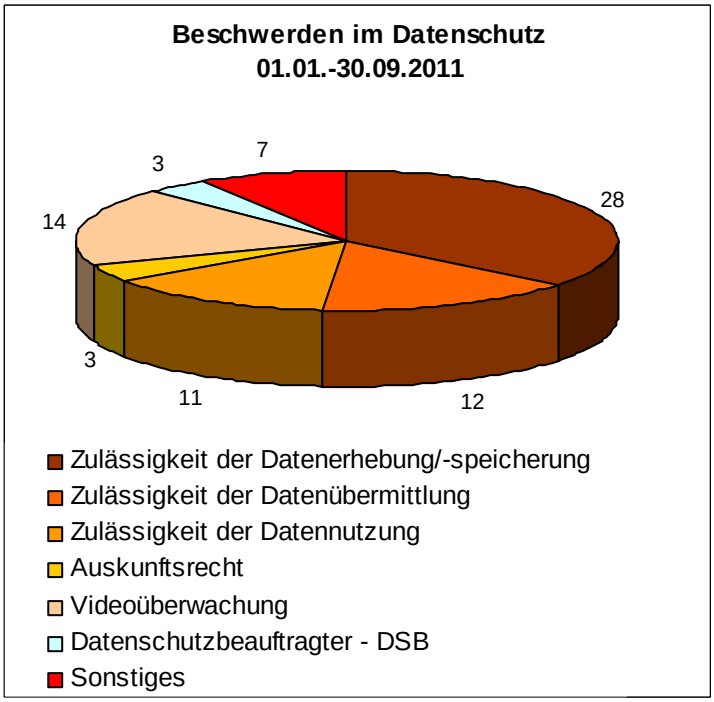


## Zeitraum vom 01.01.2011 – 30.09.2011

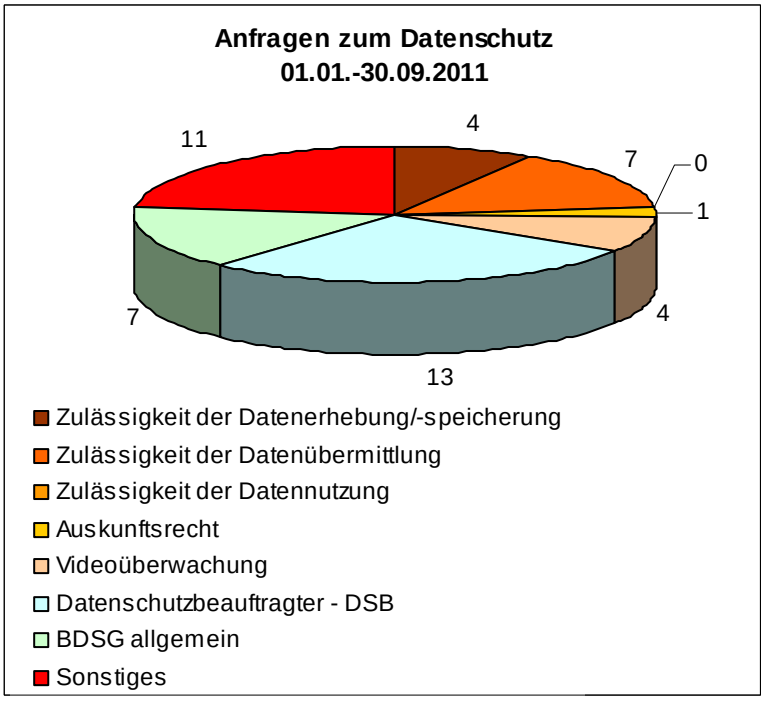
| Verfahren im Datenschutz **- Überblick -** 01.01.2011 - 30.09.2011 | |
|---|---|
| Anfragen | 47 |
| Beschwerden | 78 |




| **Beschwerden im Datenschutz - Überblick 01.01.-30.09.2011** | |
|---|---|
| Zulässigkeit der Daten-erhebung/-speicherung | 28 |
| Zulässigkeit der Daten-übermittlung | 12 |
| Zulässigkeit der Daten-nutzung | 11 |
| Auskunftsrecht | 3 |
| Videoüberwachung | 14 |
| Datenschutzbeauftragter - DSB | 3 |
| Sonstiges | 7 |




| **Anfragen im Datenschutz - Überblick 01.01.-30.09.2011** | |
|---|---|
| Zulässigkeit der Daten-erhebung/-speicherung | 4 |
| Zulässigkeit der Daten-übermittlung | 7 |
| Zulässigkeit der Daten-nutzung | 0 |
| Auskunftsrecht | 1 |
| Videoüberwachung | 4 |
| Datenschutzbeauftragter - DSB | 13 |
| BDSG allgemein | 7 |
| Sonstiges | 11 |



# 4 Beispiele aus Anfragen und Beschwerden

## 4.1 Von Beratungsinteresse – ausgewählte Anfragen

### 4.1.1 Betriebs-/Dienstvereinbarungen

Eine Betriebsvereinbarung ist ein Vertrag zwischen Arbeitgeber und Betriebsrat. Dieser begründet nicht nur kollektive Rechte und Pflichten der Betriebsparteien, sondern grundsätzlich auch verbindliche Normen für alle Arbeitnehmer eines Betriebes. Derartige Verträge werden aus unterschiedlichen Anlässen geschlossen, so z. B. zur Einführung und Nutzung eines Zeiterfassungssystems, zur Nutzung von Informations- und Kommunikationstechnik im Betrieb, wie im aktuellen Berichtszeitraum zum ELENA Verfahren und zum betrieblichen Eingliederungsmanagement.

Die Betriebsräte sind besonders gefordert, wenn Betriebsvereinbarungen als Rechtsgrundlage für einen zulässigen Umgang mit personenbezogenen Daten des Personals herangezogen werden sollen. Dies ist nur möglich, wenn die Betriebsvereinbarungen nicht gegen – höherrangige – Gesetze verstoßen.

Der Abschluss einer Betriebs-/Dienstvereinbarung ist für die Rechtmäßigkeit der Personaldatenverarbeitung von Bedeutung. Zum einen ist eine ohne Beachtung der Beteiligungsrechte durchgeführte Verarbeitung auch dem betroffenen Mitarbeiter gegenüber unzulässig. Zum anderen stellt eine abgeschlossene Vereinbarung eine vorrangige Erlaubnis-, Zweckbindungs- oder auch Verbotsregelung zum Umgang mit Personaldaten i. S. des § 4 Abs. 1 BDSG dar. Dies allerdings mit der Einschränkung, dass durch Betriebs-/ Dienstvereinbarungen keine Verarbeitung von Personaldaten abweichend vom BDSG zum Nachteil der Arbeitnehmer zugelassen wird.

Die Zulässigkeit von Personaldatenverarbeitung als Gegenstand einer Betriebs-/Dienstvereinbarung ist nach § 32 BDSG – Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses – zu prüfen. Zu näheren allgemeinen Ausführungen zu Betriebsvereinbarungen – Zielen, Inhalten, Anwendungsbereichen – wird auf den 4. Tätigkeitsbericht verwiesen. Im Folgenden wird über konkrete Beratungsfälle berichtet.

**In einem Fall** wurde ein Entwurf einer Betriebsvereinbarung „Übermittlung von Daten im elektronischen Entgeltnachweis (ELENA)“ zur Prüfung übersandt. Grundsätzlich verfügen Betriebsräte bezogen auf ELENA nur über begrenzte Handlungsmöglichkeiten. Nach § 80

Abs. 1 Nr. 1 des Betriebsverfassungsgesetzes (BetrVG) können diese beispielsweise vom Arbeitgeber umfassende Informationen über das Verfahren und die Struktur der übermittelten Daten verlangen. Kein direktes Mitbestimmungsrecht dagegen besteht bezüglich der Daten, die Arbeitgeber zwingend an ELENA übermitteln müssen. Welche Daten dies sind, ist für die zu meldenden Personen in den §§ 4 bis 6 der Verordnung zur Übermittlung der Daten im Verfahren zur Erstellung und Verarbeitung des elektronischen Entgeltnachweises (ELENA-Datensatzverordnung – ELENA-DV) geregelt. Die Ausgestaltung der Datensätze, die die Arbeitgeber übermitteln müssen, wird allerdings durch § 28b des 4. Sozialgesetzbuches (SGB IV) konkretisiert. Gesetzlich vorgesehene Stellen bekamen auf dieser Grundlage den Auftrag, gemeinsame Grundsätze für die Erstattung von Meldungen im Rahmen des ELENA-Verfahrens zu erarbeiten. Zu den ursprünglichen Festlegungen gab es als Reaktion auf Proteste der Gewerkschaften bereits Änderungen bei der Erfassung im Bereich der Fehlzeiten und von Informationen über rechtmäßige oder unrechtmäßige Streiks und Aussperrungen. Die datenschutzrechtliche Literatur wandte sich insbesondere gegen Detailangaben, z. B. hinsichtlich einer Verpflichtung zur Übermittlung näherer Angaben zur Kündigung – wie dem Kündigungsgrund.

Vor diesem Hintergrund empfahl die Aufsichtsbehörde in Betriebsvereinbarungen auf eine Reduzierung oder mindestens Standardisierung der Einträge in Freitextfeldern hinzuwirken. Entsprechende Vereinbarungen können darauf zielen, in Freitextfeldern nur festgelegte Stichworte einzutragen. Zudem legte die Aufsichtsbehörde dem Betriebsrat dar, dass es zweckmäßig ist, die Beschäftigten in einem transparenten Verfahren über die Daten zu informieren, die an ELENA übermittelt werden. Die Aufsichtsbehörde erachtete es nicht als notwendig, dass jeder Mitarbeiter vom Arbeitgeber monatlich informiert wird, welche Daten in dem jeweiligen Monat übermittelt wurden. Vielmehr sollte die Art der Daten, die regelmäßig übermittelt werden, transparent in einem Informationsblatt dargestellt werden. Für darüber hinausgehende Daten wurde eine Vereinbarung empfohlen, diese Daten nicht nur ELENA mitzuteilen, sondern auch den betroffenen Beschäftigten. Im Ergebnis legte die Aufsichtsbehörde die Verifizierung des vorgelegten Entwurfs zur BV ELENA Version 30.04.2010 nahe. Den Betroffenen sollte das gesetzlich vorgesehene Verfahren transparent dargestellt werden. Die verantwortliche Stelle sollte herausarbeiten, welche konkreten Daten für die Erstellung der benannten Bescheinigungen notwendig sind, sofern diese Daten nicht bereits durch die ELENA-DV zur Übermittlung vorgegeben sind.

**AKTUELL**

Gemeinsame Pressemitteilung des Bundesministeriums für Wirtschaft und Technologie und des Bundesministeriums für Arbeit und Soziales vom 18. Juli 2011:
„Das Bundesministerium für Wirtschaft und Technologie und das Bundesministerium für Arbeit und Soziales haben sich nach eingehender Überprüfung des ELENA-Verfahrens darauf verständigt, das Verfahren schnellstmöglich einzustellen.
Grund ist die fehlende Verbreitung der qualifizierten elektronischen Signatur. … Die Bundesregierung wird dafür Sorge tragen, dass die bisher gespeicherten Daten unverzüglich gelöscht und die Arbeitgeber von den bestehenden elektronischen Meldepflichten entlastet werden. Das Bundesministerium für Wirtschaft und Technologie wird in Kürze einen entsprechenden Gesetzentwurf vorlegen. […]“

**Der Aufsichtsbehörde** wurde auch ein Entwurf einer Konzernbetriebsvereinbarung über die Einführung und Durchführung eines Betrieblichen Eingliederungsmanagements (BEM) mit der Bitte um Unterstützung aus datenschutzrechtlicher Sicht übersandt. Grundlage für das Betriebliche Eingliederungsmanagement ist § 84 Abs. 2 SGB IX. Diese Vorschrift begründet eine Initiativpflicht des Arbeitgebers – unter Einbeziehung der zuständigen Interessenvertretung i. S. des § 93 SGB IX und ggf. der Schwerbehindertenvertretung, aber unter Zustimmung und Beteiligung der betroffenen Personen – zur Hilfestellung bei krankheitsbedingten betrieblichen Komplikationen. Die Einführung eines BEM ist somit als gesetzlicher Auftrag vorgegeben und eine Betriebsvereinbarung sollte sich allein auf die Durchführung und nicht auf die Einführung des BEM beziehen.

Zu dem vorgelegten Entwurf gab die Aufsichtsbehörde folgende Empfehlungen:

- Wegen der gesetzlichen Regelungen wurde empfohlen, in der vorgesehenen Präambel den Gesetzeswortlaut hervorzuheben.
  Ausweislich einer aktuellen Entscheidung des Bundesarbeitsgerichtes (BAG, Urteil vom 10.12.2009 – 2 AZR 400/08) stellt das BEM einen rechtlich regulierten Suchprozess dar, zu dem der Arbeitgeber verpflichtet ist und mit dem individuell angepasste Lösungen zur Vermeidung zukünftiger Arbeitsunfähigkeiten ermittelt werden sollen. Konkret ist der Sinn und Zweck des BEM nach der Intention des Gesetzgebers:

1. Die Rückkehr arbeitsunfähiger Beschäftigter in den Betrieb zu erleichtern (Rehabilitation),
2. deren Integration zu verbessern und die vorzeitige Beendigung von Beschäftigungsverhältnissen zu vermeiden (Prävention).

- Die in der vorgelegten Vereinbarung definierten Ziele (Erhalt und Förderung der Arbeitsfähigkeit und Gesundheit, Vermeidung von Behinderungen und chronischer Erkrankungen) sind auch Ziele im Rahmen des dem BEM übergeordneten Gesundheitsmanagements,

das alle Beschäftigten betrifft. Das BEM erstreckt sich hingegen nur auf ArbeitnehmerInnen, die innerhalb der letzten 12 Monate länger als 6 Wochen ununterbrochen oder wiederholt arbeitsunfähig waren. Die Aufsichtsbehörde beurteilte, dass der Geltungsbereich des BEM (§ 1 der vorgelegten Betriebsvereinbarung) dem anzupassen war. Auch ließ sich der Ausschluss leitender Angestellter nicht durch § 5 Abs. 3 BetrVG rechtfertigen.

- Die Aufsichtsbehörde empfahl Ziele und Begriffsbestimmungen in der Betriebsvereinbarung nicht vermischt zu regeln und die Begriffsbestimmungen in einer gesonderten Rubrik aufzuführen. Hier wurde die Definition empfohlen, wann Arbeitsunfähigkeit vorliegt. Dies ist unzweifelhaft dann der Fall, wenn eine Arbeitsunfähigkeitsbescheinigung vorgelegt wird. Soweit jedoch die Möglichkeit besteht, ohne entsprechende Bescheinigung für einen kurzen Zeitraum entschuldigt vom Arbeitsplatz fernzubleiben, sei dies ebenfalls im Rahmen der Ermittlung der Tage der Arbeitsunfähigkeit einzubeziehen und anzugeben.
- Die Aufsichtsbehörde empfahl Verfahrensregelungen, die den Prozess nachvollziehbar werden lassen. Diese sollten schrittweise in der Betriebsvereinbarung dargestellt werden, da sich dadurch auch die zu beteiligenden/zuständigen Stellen ergeben. Ausführungen zur Zusammensetzung, Aufgaben etc. der zuständigen Stellen wurde in einem weiteren Paragraphen für zweckmäßig erachtet.

  Verfahrensregelungen sollten folgende Punkte behandeln:
  - die Art und Weise der Einleitung des Verfahrens (z. B. Personalabteilung wertet die krankheitsbedingten Fehlzeiten eines Arbeitnehmers aus und macht diesen darauf aufmerksam, dass das BEM zur Anwendung kommt und daher ein Ansprechpartner für das BEM Kontakt mit ihm aufnehmen wird),
  - die Bestimmung besonderer Ansprechpartner für den Arbeitnehmer (BEM Beauftragte, Integrationsteam…),
  - die Einschaltung der betrieblichen Vertretungen,
  - die Konkretisierung der Verfahrensrechte der Betroffenen und der Betriebsvertretungen,
  - die Rolle des Betriebs- oder Werksarztes,
  - die Bestimmung von Korrespondenzpartnern für Servicestellen, Rehabilitationsämter und Integrationsamt (siehe §§ 22 ff, 102 Abs. 2 S. 7, 109 ff SGB IX),
  - die Mitwirkung der Betroffenen. Diesen ist die Teilnahme am BEM nach § 84 Abs. 2 SGB IX freigestellt. *Eine mögliche Formulierung könnte wie folgt lauten*: „Die Mitarbeit der betroffenen Beschäftigten ist freiwillig, jedoch ist die aktive Mitarbeit des Betroffenen Voraussetzung für ein gelungenes BEM. In diesem Zusammenhang wird ein Verfahren geschaffen, in dem sich die Betroffenen sicher werden sollen, dass die notwendige Offenheit, über eigene Erkrankungen zu sprechen, keine negativen Folgen haben wird. Die Entscheidung der Betroffenen für oder gegen die Mitarbeit kann zudem jeder-

zeit geändert werden. Eine fehlende Bereitschaft oder Zustimmung zum Eingliederungsmanagement darf zu keinen daraus resultierenden arbeitsrechtlichen Folgen führen, erleichtert allerdings den Kündigungsprozess für den Arbeitgeber aus krankheitsbedingten Gründen“ (in Anlehnung an: *Prof. Dr. Wolfhard Kohte*, Anmerkung zu BAG 2. Senat, Urteil vom 10.12.2009 – 2 AZR 400/08, jurisPR-ArbR 21/2010 Anm. 1 und *Gerd Nickel*, Betriebliches Eingliederungsmanagement – Praktische Tipps zu seiner Umsetzung, AiB 2009, S. 423 (427)),

- Ende des BEM (z.B. mit vollwertiger Wiedereingliederung und abschließendem Eingliederungsgespräch)

- Schließlich empfahl die Aufsichtsbehörde im Rahmen des BEM-Verfahrens ein separates BEM-Datenblatt anzulegen, in dem Name, Vorname, Alter, Bereich, Vollzeit/Teilzeit, Schwerbehinderung, Ausbildung/Qualifikation, derzeitige Tätigkeit im Unternehmen sowie Verlaufsdaten des eigentlichen BEM-Prozesses (BEM-Erstkontakt, BEM-Klärungsgespräch, BEM-Maßnahmenangebot etc.) erfasst werden. Das Gespräch mit dem Betroffenen sollte wiederum folgende Aspekte beinhalten:
  - eine Arbeitsplatzanalyse,
  - die Hinzuziehung von weiteren Experten,
  - die Information externer Stellen,
  - die gemeinsame Lösungssuche,
  - die Lösungsauswahl
  - Planungen zur Umsetzung der Lösungen.
- Die Betriebsvereinbarung muss für alle vorgesehenen Beteiligten (z. B. BEM-Beauftragte(r), Integrationsteam) Ausführungen zur Zusammensetzung (z. B. je 2 Vertreter des Arbeitgebers und des Betriebsrates), zur Hinzuziehung weiterer Fachleute bei Beratungsbedarf, zur Entscheidungsfindung, zur Möglichkeit der Einbeziehung der Einigungsstelle und zum Tätigwerden (regelmäßige Sitzung oder Einberufung durch Arbeitgeber) beinhalten. Die Aufgaben der Verfahrensbeteiligten, z. B. die Beurteilung der gesundheitlichen Gefährdung und die Eingliederungsplanung sind klar zu definieren. Es wurde darauf hingewiesen, dass der Eingliederungsplan die operative Grundlage des BEM ist. Der Eingliederungsplan definiert Zielsetzung, Verlauf und Qualität der erforderlichen individuellen Integrations-, Rehabilitations- und Präventionsmaßnahmen. Die Maßnahmen müssen für die Betroffenen erforderlich, bedarfsgerecht durchführbar und freiwillig sein.
- Die Aufsichtsbehörde regte an, konkreter darzustellen, dass medizinisch-diagnostische Daten der ärztlichen Schweigepflicht und den datenschutzrechtlichen Bestimmungen unterliegen. Um zu verhindern, dass vorhandene Arbeitsunfähigkeitsdaten oder andere Angaben über den Gesundheitszustand und die Arbeitsunfähigkeit womöglich zu einer nega-

tiven Prognose der zukünftigen Arbeitsfähigkeit verwendet werden dürfen, empfahl die Aufsichtsbehörde eine gesonderte Regelung.

- Abschließend regte die Aufsichtsbehörde an klarzustellen, dass die BEM-Akte gesondert von der Personalakte geführt wird.

### 4.1.2 Datenerhebung – Mieterfragebögen, Personalfragebögen & Co.

Der Einsatz von **sog. Mieterfragebögen** vor Abschluss von Mietverträgen ist gängige Praxis. Soweit nur die Daten erhoben werden, die für die berechtigten Belange des Vermieters erforderlich sind, ist gegen eine solche Verfahrensweise nichts einzuwenden. Die Befugnis hierzu ergibt sich aus § 28 Abs. 1 S. 1 Nr. 1 und ggf. Nr. 2 BDSG. Die Erhebung weiterer, für die Entscheidung über den Vertragsabschluss nicht erforderlicher Daten, sieht die Aufsichtsbehörde als bedenklich an. Der Grundsatz der Datensparsamkeit steht dem entgegen. Es ist davon auszugehen, dass Einwilligungserklärungen keine Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten begründen können, denn es erscheint äußert zweifelhaft, ob eine Einwilligung als freiwillig angesehen werden kann, wenn der Mietinteressent im Falle der Verweigerung der Einwilligung keine Chance auf Anmietung des Wohnraumes hat.

**Ein Wohnungsunternehmen** nutzte das Beratungsangebot der Aufsichtsbehörde und übersandte das genutzte Formblatt zur Selbstauskunft und den Fragebogen für Wohnungsinteressenten zur Prüfung.

Ein berechtigtes Interesse eines Wohnungsunternehmens an einer Prüfung der Mietinteressenten ergibt sich aus dem finanziellen Risiko des Vermieters, dass der Vermieter dem Mieter eine Wohnung zur Verfügung stellt, selbst wenn der Mieter die Miete ggf. nicht zahlt.
Einzelne im Vordruck enthaltene Fragen wurden auf ihre Zulässigkeit geprüft. Dabei wurde der Grundsatz beachtet, dass sich das Fragerecht des Vermieters auf solche Fragen beschränkt, die sich ausschließlich auf das Mietverhältnis beziehen und den Mieter nicht zwingen, seine Lebensweise und Lebensumstände nach Belieben des Vermieters zu offenbaren.

Nach objektiven Kriterien sind folgende Fragen zulässig:

- Anzahl und Alter der zum Hausstand gehörenden Personen;
- Einkommensverhältnisse und berufliche Stellung der Personen, die aus dem Mietvertrag zu Zahlungen verpflichtet werden können (Rückschlüsse auf die Bonität);
- Frage nach Privatinsolvenz oder eidesstattlicher Versicherung;
- Tierhaltung.

Entsprechende Fragen in der vorgelegten Selbstauskunft wurden daher als zulässig erachtet.

Kritisch dagegen ist die Frage nach der Staatsangehörigkeit. Die Frage ist vor dem Hintergrund des Allgemeinen Gleichbehandlungsgesetzes (AGG) unzulässig. Nach § 19 Abs. 1 Nr. 1 AGG ist eine Ungleichbehandlung aufgrund der ethnischen Herkunft bei der Begründung von zivilrechtlichen Schuldverhältnissen unzulässig. Eine Ungleichbehandlung erscheint nur zulässig, wenn diese im Interesse der Schaffung sozial stabiler Wohnstrukturen geboten ist. Daher wird es nicht als zulässig angesehen, von jedem Mietinteressenten für jegliches Mietobjekt die Staatsangehörigkeit zu erfragen. Nur wenn ein Vermieter ein anerkennenswertes Interesse daran hat, mit einer solchen Frage einer etwaigen „Ghettosierung“ eines Mietobjektes entgegenzuwirken, kann die Frage ausnahmsweise berechtigt sein.

Die Frage nach Mietzinsrückständen in den letzten 3 Jahren wurde als zu pauschal angesehen. Mietzinsrückstände kann es auch geben, wenn Zahlungen zulässig zurückbehalten wurden oder ein Rechtstreit anhängig ist. Es dürften nur harte Negativmerkmale erfragt werden, d. h. solche zu denen bereits gerichtliche Entscheidungen vorliegen.

Auch die Frage des Unternehmens nach bestehenden (Ab)zahlungsverpflichtungen ist nicht zulässig. Ein Vergleich zwischen Einkommen und einzelnen Verpflichtungen gibt keinen dezidierten Aufschluss, ob die verbleibende Bonität des Mieters genügt, um die geschuldete Miete zu zahlen. Soweit die Selbstauskunft hierüber Auskunft geben soll, können allein Gesamtzahlungsverpflichtungen erfragt werden, nicht jedoch einzelne Zahlungsverpflichtungen. Weiterhin dürfen Fragen nach bestehenden Pfändungen nicht zu sämtlichen möglichen Verpflichtungen gestellt werden. Dies kann nur in Bezug auf den Mietzins von Relevanz sein, da zu anderen möglichen gepfändeten Beträgen kein statistisch nachweisbarer Zusammenhang zur Bonität des Mieters besteht.

Die Frage zur Kündigung vorhergehender Mietverhältnisse ist nicht in jedem Fall unzulässig. Die konkrete Fragestellung des Wohnungsunternehmens „Ist Ihr derzeitiges Mietverhältnis oder das des als Vertragspartner vorgesehenen Mitmieters vom Vermieter gekündigt worden bzw. steht eine solche Kündigung bevor? Falls ja, aus welchem Grund?“ erschien jedoch zu pauschal und damit nicht zulässig. Für das neue Mietverhältnis ist es ohne Relevanz, ob der bisherige Vermieter das Mietverhältnis z. B. wegen Eigenbedarfs gekündigt hat. Zweifelhaft ist auch, ob eine verhaltensbedingte Kündigung anzugeben ist, da es in derartigen Verhältnissen vorkommen kann, dass Mieter sich wegen der angespannten Situation gegen eine

etwaige unberechtigte Kündigung nicht zur Wehr setzen. Zulässig ist dagegen die Frage, ob das bisherige Mietverhältnis wegen ausstehender Mietzahlungen gekündigt wurde, da diese Frage einen unmittelbaren Bezug zur Zahlungsfähigkeit und -willigkeit des Mieters hat. Dies gilt allerdings nur dann, wenn Forderungen des bisherigen Vermieters unbestritten oder rechtskräftig festgestellt sind. Die im vorliegenden Fall gestellte Frage zum gerichtlichen Räumungsverfahren war unter diesen Prämissen ebenfalls zu undifferenziert. Es sind nur solche Verfahren wegen ausstehender Mietzahlung von Belang, nicht jedoch z. B. wegen Eigenbedarfskündigung.

**Im Zusammenhang** mit der Personalauswahl wenden Unternehmen häufig standardisierte Fragebögen an. Das Interesse, sich vollständige und miteinander vergleichbare Informationen über die Bewerber zu beschaffen, ist berechtigt. Jedoch ist nicht jede damit verbundene Datenerhebung zulässig. Im Bewerberverfahren wird zwar vielfach davon ausgegangen, dass die Datenerhebung auf Basis einer Einwilligung zulässig ist. Damit eine Einwilligung allerdings wirksam ist, muss sie den Anforderungen des § 4a BDSG genügen. Welche Anforderungen dies im Detail sind, sind dem Abschnitt 2. – Das Bundesdatenschutzgesetz (BDSG) – zu entnehmen. Diese Erfordernisse werden mit der Aufforderung, einen Fragebogen auszufüllen i. d. R. jedoch nicht entsprechend berücksichtigt. Aufgrund des bestehenden Abhängigkeitsverhältnisses ist es ohnehin fraglich, ob eine Einwilligung eines Bewerbers überhaupt freiwillig und damit wirksam sein kann.
Als Rechtsgrundlage für die Datenerhebung kommt insoweit allein § 28 Abs. 1 Nr. 1 bzw. 2 BDSG in Betracht.
Unabhängig von den vorgenannten Aspekten ist eine Einwilligung entsprechend § 134 BGB unwirksam, wenn sie den Zugriff auf Daten ermöglichen soll, die den Interessenten kraft zwingenden Rechts verschlossen bleiben müssen. Hier findet sich auch die Informationserhebung in Bezug auf Bewerber, denn die Grenzen des arbeitgeberseitigen Fragerechts dürfen auch nicht mit Zustimmung des Bewerbers überschritten werden. Dies bedeutet, dass ein Arbeitgeber bei Bewerbern nur Informationen abfragen darf, an deren Kenntnis er ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat (vgl. BAG, Urteil vom 20.02.1986, Az.: 2 AZR 244/85, NZA 1986, 739).

Die Aufsichtsbehörde teilte **dem Betriebsrat** eines Unternehmens zum genutzten Einstellungsbogen Folgendes mit:

- Angaben zum Familienstand und zur Zahl der Kinder spielen in der Phase der Personalauswahl noch keine Rolle. Mithin besteht kein berechtigtes Interesse an dieser Datenerhebung. Erst nach der Einstellung, wenn die gegenseitigen Pflichten aus einem Arbeitsver-

hältnis abgewickelt werden (Lohnzahlung, Abführung Sozialversicherungsbeiträge), werden diese Daten benötigt, etwa zum Zwecke des Lohnsteuerabzugs.

- Fragen nach der Schwerbehinderung sind im Auswahlverfahren nur zulässig, wenn das Fehlen einer solchen Behinderung wesentliche und entscheidende berufliche Anforderung für die Tätigkeit ist. Bei einer Schwerbehinderung > 50 % ist typischerweise mit maßgeblichen Auswirkungen zu rechnen, daher kann auch gefragt werden, ob eine solche gravierende Schwerbehinderung vorliegt.

  Nach der Einstellung besteht für einen Arbeitnehmer die Pflicht, eine Schwerbehinderung zu offenbaren.
- Fragen nach der Vermögensbildung, Renten und Lohnpfändungen/-abtretungen betreffen die Vermögensverhältnisse eines Bewerbers. Derartige Fragen sind allenfalls bei leitenden Angestellten und bei Positionen, die ein besonderes Vertrauensverhältnis erfordern, zulässig. Soweit nach der Einstellung vermögenswirksame Leistungen in Anspruch genommen werden können, wäre die Erhebung weiterer Daten erforderlich. Angaben zur Lohnpfändung/-abtretung sind bei der Zahlbarmachung des Arbeitsentgelts relevant.
- Die konkrete Frage nach Nebenbeschäftigungen „Bestehen noch weitere Arbeitsverhältnisse neben der Beschäftigung, wenn ja, bitte Anschriften der anderen Arbeitgeber angeben“ ist unzulässig. Aus der Fragestellung sollen allgemein Nebentätigkeiten, die keinen Bezug zum konkreten Arbeitsplatz haben, in Erfahrung gebracht werden. Eine solche Frage ist allenfalls zulässig, wenn es darum geht, Konkurrenztätigkeiten herauszufinden bzw. um die ordnungsgemäße Leistungserbringung gewährleisten zu können.
- Bei Fragen nach einer Vorbeschäftigung ist der Hintergrund der Frage relevant. Geht es um die Frage, wo ein Bewerber seine Berufserfahrung gesammelt hat, ist diese grundsätzlich nicht zu beanstanden. Insbesondere kann die Tätigkeit bei dem vormaligen Arbeitgeber häufig Rückschlüsse auf die Qualität der Ausbildung etc. ermöglichen. **Dies führt allerdings nicht dazu, dass der potentielle Arbeitgeber berechtigt ist, den vorherigen Arbeitgeber näher zum Bewerber zu interviewen.**

Über die vorgenannten Aspekte hinaus ist bei der Erhebung von Bewerberdaten Folgendes zu beachten:

- **Fragen nach der Staatsangehörigkeit** als solche sind unzulässig. Es kann allein gefragt werden, ob ein befristetes oder unbefristetes Aufenthaltsrecht besteht.
- Sofern **Fragen nach körperlichen Beeinträchtigungen** auf konkrete tätigkeitsrelevante Beeinträchtigungen beschränkt werden, ist dies nach § 32 Abs. 1 Satz 1 i. V. m. § 28 Abs. 6 Nr. 3 BDSG zulässig.

- Die **Frage nach Vorstrafen** ist nur dann zulässig, wenn und soweit die Art der Tätigkeit dies erfordert. Es sollte daher von vornherein eine entsprechende Einschränkung und Verdeutlichung der einschlägigen und tätigkeitsrelevanten Vorstrafen erfolgen. Beispielsweise kann bei einem Berufskraftfahrer nach Vorstrafen wegen Trunkenheit am Steuer gefragt werden.
- Soweit **Fragen zum Lohn bzw. Gehalt** beim letzten Arbeitgeber keinen Einfluss auf das Bewerberverfahren haben, z. B. wenn alle Beschäftigten im Unternehmen in Abhängigkeit von der konkreten Tätigkeit gleich bezahlt werden, sind diese unzulässig.
- **Fragen nach anderen Bewerbungsverfahren** sind unzulässig.
- Im Zusammenhang mit **Bewerbungen als Franchisenehmer** sind **Fragen nach den wirtschaftlichen Verhältnissen** zulässig. Diese müssen sich an den für Franchisegeber relevanten Informationen orientieren. Ausreichend dürften Angaben zum Gesamtvermögen, d. h. zu den frei verfügbaren, gebundenen bzw. als Sicherheit zur Verfügung stehenden finanziellen Mitteln, zu den Gesamtverbindlichkeiten und dem insgesamt bestehenden Nettovermögen sein.

### 4.1.3 Datenschutzrechtliche Einwilligungserklärung

Der datenschutzrechtlichen Einwilligungserklärung kommt insbesondere dann eine wichtige Bedeutung zu, wenn Daten wie E-Mail-Adressen und Telefonnummern verwendet werden sollen.

Ein Unternehmen mit hohen Ansprüchen an die Belange des Datenschutzes zu Gunsten der eigenen Kunden, hatte sich bereits umfassend mit den Anforderungen an wirksame Einwilligungserklärungen i. S. des § 4a BDSG beschäftigt und bat die Aufsichtsbehörde um Mitteilung, ob die aktuell verwendete datenschutzrechtliche Einwilligungserklärung gesetzeskonform sei.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der neue § 28 Abs. 3a BDSG bedingt, dass eine Einwilligung in die Verarbeitung oder Nutzung personenbezogener Daten zu Werbezwecken vom Betroffenen schriftlich zu bestätigen ist, wenn die Einwilligung in anderer Form eingeholt wurde.

Da das Unternehmen die Erklärungen schriftlich einholte, galt dies lediglich als Hinweis. Auch die übrigen aus § 4a BDSG ersichtlichen Anforderungen an eine Einwilligungserklärung wurden als grundlegend erfüllt angesehen.

> ***§ 4a BDSG – Einwilligung***
> *Abs. 1: Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.*

Eine Einwilligungserklärung darf niemals einen pauschalen Charakter haben, sondern muss erkennen lassen, welche Daten zu welchem Zweck verarbeitet werden. Es ist wichtig, dass Betroffene selbst entscheiden können, auf welche Art und Weise (telefonisch, schriftlich, per E-Mail) eine Kontaktaufnahme mit ihnen erfolgen darf.

Will ein Unternehmen zu verschiedenen Zwecken (Werbung, Kundenbetreuung, persönliche Kundeninformation und Zufriedenheitsbefragungen usw.) Kontakt zu Betroffenen aufnehmen, sollte der Betroffene die Möglichkeit erhalten, seine Einwilligungserklärung entsprechend differenziert abzugeben.

Im vorliegenden Fall differenzierte das Unternehmen nach den Zwecken: Werbung, Kundenbetreuung, persönliche Kundeninformation und Zufriedenheitsbefragung. Der Betroffene konnte jedoch nicht entscheiden, zu welchem dieser Zwecke er eine Kontaktaufnahme wünscht und zu welchen nicht. Auch muss der Einwilligende Einfluss darauf nehmen können, welche Daten konkret zu welchen Zwecken genutzt werden dürfen, z. B. Name, Kontaktdaten (E-Mail, Handy oder Festnetz etc.), Hobby und Beruf für Zwecke der Werbung, jedoch nur Name, Kontaktdaten und technische Daten des Fahrzeuges zur Kundenbetreuung.

Aus diesem Grund teilte die Aufsichtsbehörde dem Unternehmen mit, dass die Möglichkeiten des „Ankreuzens“ erweitert werden müssen. Zudem wurde als Verbesserungsvorschlag unterbreitet, das Wort „willige ich ein“ im Text hervorzuheben. Schließlich empfahl die Aufsichtsbehörde am Ende der Einwilligungserklärung den Hinweis, dass die Versagung der Einwilligung keine negativen Auswirkungen für den Betroffenen hat und dass eine einmal erteilte Einwilligungserklärung jederzeit widerrufen werden kann.

Unabhängig von der Prüfung der Einwilligungserklärung wurde der Aufsichtsbehörde aus den Erläuterungen zur Datenschutzerklärung ersichtlich, dass das Unternehmen im Einzelfall Ausweiskopien fertigt. Es wurde darauf hingewiesen, dass dies datenschutzrechtlich bedenklich ist, da die Vorlage des Ausweises zur Identifikation und das Notieren der erforderlichen Daten (weder Lichtbild, Größe noch Augenfarbe und Personalausweisnummer dürften für die Interessen des Unternehmens von Belang sein) genügt (ausführliche Erläuterungen unter Punkt 4.2.).

**Im Zusammenhang** mit der Vortragstätigkeit der Aufsichtsbehörde im Bereich der Arbeitsvermittlung wurde um die Prüfung der verwendeten Einwilligungserklärung zur Erhebung, Verarbeitung und Nutzung von Personaldaten gebeten. Unter Berücksichtigung der datenschutzrechtlichen Vorgaben an die Tätigkeit der privaten Arbeitsvermittlung in §§ 292 ff. SGB III informierte die Aufsichtsbehörde zunächst inhaltlich detailliert zu den formellen Anforderungen an eine wirksame Einwilligungserklärung i. S. des § 4a BDSG. Weiterhin wurde darauf hingewiesen, dass neben den formellen Erfordernissen auch inhaltliche Schranken zu beachten sind. Eine Einwilligung ist entsprechend § 134 BGB auch unwirksam, wenn sie den Zugriff auf Daten ermöglichen soll, die den Interessenten kraft zwingenden Rechts verschlossen bleiben müssen. Für die Arbeitsvermittlung bedeutet dies, dass die Grenzen des arbeitgeberseitigen Fragerechts beachtlich sind und eine Umgehung nicht über die Zwischenschaltung eines Arbeitsvermittlers oder durch Einholung von Einwilligungserklärungen möglich erscheint. Einzelheiten der Grenzen des Fragerechtes wurden nicht erläutert.

Die Aufsichtsbehörde wies auch darauf hin, dass eine Einwilligungserklärung inhaltlich angemessen sein muss (siehe § 307 Abs. 1 BGB). Nur wenn sich die Einwilligungserklärung auf einen genau umschriebenen Verarbeitungsvorgang bezieht, kann der Betroffene die Tragweite seiner Erklärung überschauen. Eine hinreichend bestimmte Einwilligung muss somit klar zu erkennen geben, unter welchen Bedingungen sich der Betroffene mit der Verarbeitung welcher Daten einverstanden erklärt hat. Weder Blankoeinwilligungen noch pauschal gehaltene Erklärungen sind mit § 4a Abs. 1 BDSG vereinbar.

Im Ergebnis schlug die Aufsichtsbehörde dem Verein folgende Einwilligungserklärung vor:

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt unter Beachtung des § 298 SGB III und des Bundesdatenschutzgesetzes (BDSG), speziell des § 4a BDSG.

Um in Ihrem Interesse einen Kontakt mit Arbeitgebern zur Begründung von Arbeitsverhältnissen herstellen können, werden die aus dem Personalfragebogen ersichtlich werdenden Daten *(Anmerkung: soweit die Grenzen des arbeitgeberseitigen Fragerechts beachtet werden)* benötigt.

Ich willige ein, dass die vorgenannten Daten des Personalfragebogens für die erstmalige Vermittlungstätigkeit erhoben, verarbeitet und genutzt werden dürfen.
Da sich aus dem Personalfragebogen auch besondere personenbezogene Daten ergeben, bezieht sich meine Einwilligung ausdrücklich auch auf folgende Daten: … *(Anmerkung: an dieser Stelle müssen die besonderen personenbezogenen Daten – Definition siehe § 3 Abs. 9 BDSG - aufgeführt werden)*

Ich willige ferner ein, dass die vorgenannten Daten gespeichert bleiben, um weitere Vermittlungsangebote zu erhalten oder zu einem späteren Zeitpunkt wieder in die aktive Suche aufgenommen zu werden und für diesen Zweck verarbeitet und genutzt werden dürfen.
Dies gilt auch für die nachfolgenden besondere personenbezogenen Daten: …

Im Zusammenhang mit dem Bedarf an späteren Vermittlungstätigkeiten stimme ich zu, dass auch die durch mich zur Verfügung gestellten Unterlagen über den Abschluss der Vermittlungstätigkeit hinaus beim Vermittler verbleiben können.

*(Anmerkung: Grundsätzlich sind die dem Vermittler überlassenen Unterlagen - Bewerbungsunterlagen und Nachweise - nach Abschluss der Vermittlungstätigkeit gem. § 298 Abs. 2 S. 1 SGB III zurückzugeben. Maßgebender Zeitpunkt ist der Tag, an dem für den Vermittler feststeht, dass er keine weiteren Vermittlungstätigkeiten ergreifen will oder er Gewissheit darüber hat, dass ein Arbeitsvertrag geschlossen worden ist. Von § 298 Abs. 2 S. 1 SGB III kann der Betroffene allerdings gem. § 298 Abs. 2 S. 4 SGB III schriftlich Abweichungen gestatten. Möchte der Vermittler statt der Rückgabe lediglich die Abholung und die Rücksendung via frankierten Rückumschlag vorsehen, müsste diese Abweichung ebenfalls transparent geregelt werden. Z.B. Ich stimme zu, dass die eingereichten Unterlagen – die ich nicht im Original einreicht – bei Nichtabholung aufgrund der zahlreichen zurückzugebenden Unterlagen nach einem Jahr in nicht wieder herstellbarer Art und Weise vernichtet werden. Diese Zustimmung müsste separat eingeholt werden, andernfalls verstieße eine Vernichtung der Unterlagen wie in der 2. Erklärung ersichtlich gegen § 298 Abs. 2 SGB III. Ebenso transparent müsste die Zustimmung zur Archivierung und Vernichtung wie in der 3. Erklärung vorgesehen eingeholt werden.*
*Alle übrigen Unterlagen des Vermittlers – somit auch eigene Personalfrageböen – sind den Geschäftsunterlagen zuzurechnen und drei Jahre lang aufzubewahren. Eine Zustimmung bedarf es in diesem Zusammenhang somit grundsätzlich nicht. Diese Frist beginnt mit dem Tag, der auf den Tag folgt, an dem der Vermittler die Unterlagen nach Satz 1 zurückgegeben hat. Danach sind die Unterlagen und Daten gem. § 298 Abs. 2*
*S. 4 SGB III zu löschen. Da von dieser Vorschrift Abweichungen getroffen werden können, kann die Verpflichtung zur Löschung durch entsprechende Erklärung des Betroffenen herausgeschoben werden.)*

Ferner willige ich ein, dass meine Kontaktdaten – Name, Anschrift, Telefonnummer, E-Mail-Adresse (Daten, die nicht genutzt werden sollen, bitte streichen) für Zwecke der Eigenwerbung genutzt werden dürfen.

---------- ----------
Ort, Datum Unterschrift (AG)

Die hier erteilten Einwilligungen können jederzeit mit Wirkung für die Zukunft widerrufen werden. Vermittlungstätigkeiten können ohne personenbezogene Daten jedoch nicht wahrgenommen werden. Die Zulässigkeit des Umganges mit personenbezogenen Daten berührt das grundsätzliche Vertragsverhältnis jedoch nicht.“

### 4.1.4 „Smart Meter“ – „intelligente“ Messeinrichtungen für die Messung gelieferter Energie

Eine Möglichkeit den bewussten Umgang mit Energie – gleich ob Strom, Gas oder weiteren Versorgungssparten – zu fördern, sind die sog. „Smart Meter“. Unter dem Begriff werden intelligente Zähler für die Messung des Verbrauchs verschiedener Energieversorgungssparten verstanden. Bislang ist diese Zählertechnik in den Bereichen Strom und Gas am Weitesten verbreitet. Sie ermöglicht dem Anschlussinhaber den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit zu erkennen. Mit dem bisher für elektrische Energie in Privathaushalten eingesetzten „Ferraris-Zähler“ wird allein der Gesamtverbrauch an Energie zum Ablesezeitpunkt wiedergegeben.

Seit dem 01. Januar 2010 sind grundsätzlich „intelligente“ Zähler in Neubauten und bei Renovierungen von Gebäuden zur Verbesserung der Gesamtenergieeffizienz verpflichtend einzubauen (§ 21b Abs. 3 a des Energiewirtschaftsgesetzes (EnWG)). Damit diese Zähler verbreitet zum Einsatz kommen, wurden Energieversorgungsunternehmen gemäß § 40 EnWG verpflichtet, mit Ablauf des Jahres 2010 Verbrauchern Stromtarife anzubieten, die Anreize zur Einsparung oder Steuerung des Energieverbrauches setzen. Dies sind lastvariable und tageszeitabhängige Tarife (z. B. Nutzung bestimmter energieverbrauchender Geräte über Nacht).

Vorteile für den Endverbraucher sind, dass die innovative Technik in Echtzeit arbeitet, die Verbräuche für den Benutzer optisch aufgearbeitet werden und in Zeiten geringer Auslastung des Netzes die verbrauchte Energie preisgünstiger abgerechnet werden kann. Der Endverbraucher kann sich hierauf in seinem Energieverbrauchsverhalten einstellen. Weitere Vorteile sind, dass durch das Ablesen per Funk keine „lästigen“ Vorortttermine erfolgen müssen oder im Falle eines Umzuges eine stichtagsgenaue Abrechnung problemlos möglich ist.

Smart Metering hat aber auch Nachteile und Gefahren für den Endverbraucher. Die Messdaten liefern interessante Informationen über den Konsumenten. So sind Rückschlüsse auf den Tagesablauf eines Haushaltes möglich. Auch die Datensicherheit kann gefährdet sein, wenn ein intelligenter Zähler den Verbrauch per Funk, per Stromnetz oder über das Internet weiterleitet.
Folgender Überblick verdeutlicht das technische Potenzial intelligenter Zähler:

- Intelligente Zähler messen (im datenschutzrechtlichen Sinne erheben) sowohl abrechnungsrelevante als auch steuerungsrelevante Daten. Abrechnungsrelevante Daten sind die Informationen, die Auskunft über die entnommene Energiemenge (kWh) geben. Steue-

rungsrelevante Daten enthalten zusätzliche Informationen darüber, wann in welcher Menge Energie durch den Abnehmer verbraucht wird. Die Energie- und Ressourcenverbrauchsdaten geben Auskunft über die Lebensweise und –verhältnisse der Verbraucher. Hierbei kann es sich um personenbezogene Daten i. S. des § 3 Abs. 1 BDSG handeln.

- Die steuerungsrelevanten Messdaten sind erforderlich, um ein individuelles Lastprofil, d. h. den zeitlichen Verlauf der abgenommenen Energieleistungen über einen bestimmten Zeitraum zu erstellen. Die Ablesung erfolgt in der Regel in 15minütigen Zeitintervallen, also etwa 35.000 Messzeitpunkten im Jahr. Technisch realisierbar wäre allerdings auch die sekundengenaue Erfassung der Verbrauchszahlen. Dann wäre selbst die Identifizierung einzelner Geräte und deren spezifischer Energieverbrauch einfach ermittelbar.
- Charakteristisch für intelligente Zähler ist das kontaktlose Auslesen der gespeicherten Daten und die Übermittlung der Messdaten via Internet, Funkverbindung etc.. Die Verbrauchsinformationen werden somit (entgegen dem Grundsatz der Direkterhebung) ohne Mitwirkung oder gar Kenntnis der Betroffenen erhoben.

Im Zusammenhang mit digitalen Zählern sind die bisherigen Rechtsnormen in Bezug auf die angesprochenen Risiken für die Privatsphäre der Betroffenen nur unzureichend. Da aber auch eine effiziente Energiedistribution und –nutzung nicht zu datenschutzrechtlichen Beeinträchtigungen führen darf, wurde auf der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. November 2010 Folgendes gefordert:

- Es muss eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen geschaffen werden. In dieser müssen die schutzwürdigen Interessen der Betroffenen Berücksichtigung finden und die erhobenen Daten einer strikten Zweckbindung unterworfen werden. Auch ist für Transparenz zu sorgen.
- Der Grundsatz der Datenvermeidung ist gebührend zu berücksichtigen. Es ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden.
- Für den Einsatz der Technik sind technische und organisatorische Maßnahmen nach dem aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Derartiges ist durch verbindliche Standards festzuschreiben.

Die vollständige Entschließung zum Thema „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauches“ ist abrufbar:
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/80DSK_DatenschutzBeiDerDigitalenMessung.pdf?__blob=publicationFile

Inzwischen hat der Bundesrat dem Entwurf eines Gesetzes zur Neuregelung energiewirtschaftlicher Vorschriften (BR-Drs. 343/11) zugestimmt. Zukünftig wird es durch den neu eingeführten § 21g EnWG eine konkrete Rechtsgrundlage für den Datenumgang durch Messstellenbetreiber, Netzbetreiber und Lieferanten geben. In § 21g Abs. 1 EnWG sind die zum Datenumgang berechtigten Zwecke normiert. Mithin ist eine enge Zweckbindung für die sensiblen Verbrauchsdaten vorgesehen. Daneben werden verbindliche Standards für die Datensicherheit festgelegt. Weitere Stellen können nur über Einwilligungserklärungen i. S. des § 4a BDSG zu einem Umgang mit personenbezogenen Daten ermächtigt werden.

Bisher hat die Aufsichtsbehörde Beratungen durchgeführt, in denen die Belange aller Beteiligten berücksichtigt werden. Ziel der Aufsichtsbehörde ist der datenschutzkonforme Einsatz der Technik.

**Konkret hat das** Landesverwaltungsamt bereits zwei Unternehmen beraten, die Pilotprojekte zum Smart Metering durchführen. In beiden Projekten ist die Teilnahme der Verbraucher freiwillig. Die Energieunternehmen und die Teilnehmer sollen Erfahrungen im Umgang mit der neuen Technik gewinnen.
Die Unternehmen haben bei ihren Pilotprojekten datenschutzrechtliche Belange im Blick. Die Unterstützung durch die Aufsichtsbehörde war insbesondere auf die Transparenz der Verfahren für die Betroffenen gerichtet.
Der erste Umgang mit personenbezogenen Daten beginnt für das Unternehmen mit der Auswahl der Personen/Parteien, denen angeboten wird, an dem Projekt teilzunehmen. Während ein Unternehmen auf den eigenen Kundenbestand zurückgriff, rief das andere Unternehmen interessierte Bürger durch die Presse zur Teilnahme auf.
Die konkrete Auswahl der „Teilnehmer“ erfolgte anhand von Kriterien, die für die Auswahl einer repräsentativen Gesamtheit geeignet sind. Da die vorhandenen Datensätze nach diesen Kriterien gefiltert werden, findet eine Nutzung personenbezogener Daten statt. Erfolgt dies nicht auf Basis vorab eingeholter Einwilligungen, kann die Nutzung allein auf der Grundlage des § 28 BDSG, speziell § 28 Abs. 1 Nr. 2 BDSG zulässig sein. Diese Norm ist geprägt durch eine Abwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen unter dem Maßstab der Erforderlichkeit.

Die Aufsichtsbehörde empfahl den Unternehmen, die Auswahlkriterien in einem unternehmensinternen Konzept entsprechend zu begründen. Dabei ist der Zweck der Datennutzung und wie viele Personen insgesamt angeschrieben werden, um im Hinblick auf eine bestimmte Rücklaufquote die benötigte Anzahl an „Energiespar-Pionieren“ zu finden, festzuhalten. Sollten sich mehr Interessenten als benötigt zurückmelden, empfahl die Aufsichtsbehörde weiterhin bereits festzulegen, nach welchen Kriterien oder Verfahren (Zufallsprinzip – Los) entschieden wird, wer an dem Projekt teilnehmen kann.

Der Datenumgang, der bei diesen Projekten im Mittelpunkt steht, beginnt mit der **Datenerhebung** unter Nutzung der neu eingebauten Technik. Bei der Erhebung abrechnungsrelevanter Daten handelt es sich um die Angabe zu den aus dem Netz entnommenen Energiemengen über einen bestimmten Abrechnungszeitraum durch den Messstellenbetreiber über Smart Meter. Dies ist auf der Grundlage eines entsprechenden Vertrages zwischen dem Betreiber und dem Betroffenen gemäß § 28 Abs. 1 S. 1 Nr. 1 BDSG grundsätzlich zulässig. Ein solcher Vertrag sollte Grundlage beider Projekte werden.
In Bezug auf das Smart Metering sind in einem solchen Vertrag die Abrechnungszeiträume, die Art der zu erhebenden Daten und die Messzeitpunkte sowie die Form der Dokumentation der erhobenen Daten festzulegen. Die Aufsichtsbehörde wies in beiden Verfahren darauf hin, dass den Betroffenen zwingend transparent gemacht werden muss, dass eine Auslesung der Verbrauchswerte alle 15 Minuten, ohne Mitwirkung der Betroffenen erfolgt. Die Aufsichtsbehörde empfahl die Unterschiede zur herkömmlichen elektromechanischen Technik darzustellen und auf potentielle Gefahren hinzuweisen. In einem der Projekte wurde der weitere Umgang mit den erhobenen Daten für die Projektteilnehmer ausreichend deutlich. Entsprechend erteilte die Aufsichtsbehörde hinsichtlich der vorgelegten Unterlagen lediglich einzelne Hinweise.

Beim anderen Projekt wurde der weitere Umgang mit personenbezogenen Daten anhand der eingereichten Unterlagen nicht hinreichend deutlich, insbesondere hinsichtlich der Einbindung einer Vielzahl von Forschungspartnern. Im Detail waren der Zweck der Beteiligung und inwieweit dafür Daten der Betroffenen weitergegeben werden sollten, nicht hinreichend klar.

Vor diesem Hintergrund teilte die Aufsichtsbehörde dem Unternehmen zunächst mit, dass jede Weitergabe an einen Forschungspartner für sich genommen zulässig sein muss und dies grundsätzlich allein auf der Grundlage eingeholter Einwilligungen (§ 4 Abs.1 i. V. m. § 4a BDSG) möglich sein kann.

Den Unterlagen bzw. der darin enthaltenen Formulierung, „die Betroffenen sich mit der Teilnahme am Feldtest damit einverstanden erklären, dass … weitergegeben werden“ entnahm die Aufsichtsbehörde, dass Einwilligungen eingeholt werden sollen. Die Aufsichtsbehörde äußerte allerdings Zweifel, dass allein die Teilnahme am Feldtest als wirksame Einwilligung i. S. des § 4a BDSG verstanden werden kann. Die Aufsichtsbehörde wies darauf hin, dass in jedem Fall deutlich gemacht werden muss, welche Forschungspartner welche Daten zu welchem Zweck erhalten. Netzbetreiber dürfen beispielsweise grundsätzlich nur die Daten erhalten, die für den Betrieb des Netzes und die Erstellung der Abrechnung für die Netznutzung unbedingt nötig sind.

Soweit die Erstellung der Netzentgeltabrechnung ohne personenbeziehbare Daten möglich ist, erachtet die Aufsichtsbehörde die Übermittlung von Einzeldatensätzen, in personenbezogener oder in pseudonymisierter Form, datenschutzrechtlich auf der Grundlage des § 28 Abs. 1 Nr. 2 bzw. Abs. 3 Nr. 1 BDSG als unzulässig. Über die Übermittlung und den Zweck der jeweiligen Übermittlung wäre der Anschlussnutzer und somit auch der Projektteilnehmer in jedem Fall zu informieren. Dies ist nur nicht der Fall, wenn eine bestimmte, konkret geregelte Vorgehensweise auf Basis wirksamer Einwilligungserklärungen zulässig ist.

Entsprechend verhält es sich bei der Datenübermittlung vom Messstellenbetreiber an den Energielieferanten. Weiterhin sind grundsätzlich nur die Daten zu übermitteln, die im Rahmen des Energieliefervertrages erforderlich sind. Hat ein Kunde keinen zeitabhängigen- oder lastvariablen Tarif gewählt, bedeutet dies, dass grundsätzlich nur aggregierte Verbrauchsdaten übermittelt werden dürften. Etwas anderes gilt nur, wenn eine den Anforderungen des § 4a BDSG genügende Einwilligung vorliegt. Da im vorliegenden Fall allein eine pauschale Erklärung hinsichtlich des Datenflusses zwischen Messstellenbetreiber und Energielieferanten vorlag, beurteilte die Aufsichtsbehörde, dass die Anforderungen des § 4a BDSG nicht erfüllt werden können.

Im Ergebnis der Beratung bot die Aufsichtsbehörde an, ein Muster einer erarbeiteten Einwilligungserklärung unter den datenschutzrechtlichen Gesichtspunkten erneut zu prüfen. Dieses Angebot nahm das Unternehmen an.

**Checkliste für den datenschutzkonformen Einsatz „intelligenter“ Zähler**

Datensparsamkeit

- Datenverarbeitung im Energieinformationsnetz ist so zu gestalten, dass sie ohne oder mit möglichst wenig personenbezogenen Daten durchgeführt werden kann. Soweit Personenbezug nicht zu vermeiden ist, sind Datenverarbeitungsprozesse und -systeme so zu gestalten, dass die Verarbeitung personenbezogener Daten zeitlich möglichst kurz ist. Werden personenbezogenen Daten nicht mehr benötigt, sind diese zu löschen bzw. zu anonymisieren oder zu pseudonymisieren.

- Der Messturnus ist zeitlich so groß wie möglich zu wählen, damit der Rückschluss auf die individuelle Lebensweise des Verbrauchers so gering wie möglich ist.

Zweckbindung

- Es muss ausgeschlossen werden, dass personenbezogene Daten für weitere Zwecke, als diejenigen, für die sie erhoben worden sind, verwendet werden. Dies setzt eine klare Struktur und Abgrenzung bezogen auf die Funktionen und Beteiligten voraus. Erfüllt ein Unternehmen mehrere Funktionen, muss es die getrennte Verarbeitung und -speicherung der Daten gewährleisten.
- Es muss gewährleistet werden, dass Datenübermittlungen nur erfolgen, soweit dies durch eine Erlaubnisnorm oder die Einwilligung des Betroffenen gedeckt ist.

Erforderlichkeit

- Die eingesetzte Technik darf keine Standardeinstellungen aufweisen, die automatisch zu nicht erforderlichen Datenerhebungen führen. Auch müssen die verschiedenen Messfunktionen einzeln und ohne großen Aufwand konfigurierbar sein. Z.B. ist es nicht erforderlich, den Energieverbrauchszeitraum zu erheben, wenn ein Kunde keinen tages- oder lastvariablen Tarif in Anspruch nimmt.
- Personenbezogene Verbrauchsdaten sind grundsätzlich nur bis zur Abrechnung notwendig und im Anschluss daran zu löschen.

Transparenz

- Damit ein Betroffener ausreichend Kenntnis über den Umgang mit seinen personenbezogenen Daten hat, müssen personenbezogene Daten grundsätzlich direkt bei ihm erhoben werden (Grundsatz der Direkterhebung - § 4 Abs. 2 S. 1 BDSG).
- Für tageszeit- oder lastvariable Tarife würde dies aufgrund der Verbrauchsmessungen in kurzen Zeitintervallen zu einem unverhältnismäßigen Aufwand führen, sodass der Ausnahmetatbestand des § 4 Abs. 2 Nr. 2b BDSG greift. D.h. die schutzwürdigen Interessen des Anschlussnehmers, der nicht an dem Ablesevorgang beteiligt wird, müssen dadurch gewahrt werden, dass er sowohl über die Möglichkeit des automatischen Auslesens als auch über die erstellten Lastprofile in regelmäßigen Abständen informiert wird bzw. entsprechende Einsichtnahmemöglichkeiten in die erfassten Verbrauchsdaten erhält.
- Soweit ein umfassender Umgang mit personenbezogenen Daten erfolgen soll, sind hierzu Verwendungsszenarien zu erarbeiten. Es muss ersichtlich werden, welche Daten durch welche verantwortliche Stelle zu welchem Zweck erhoben, verarbeitet oder genutzt werden dürfen.

Datensicherheit

- Es sind Vorgaben zur Datensicherheit mit den Schutzzielen Integrität, Bestreitbarkeit, Verfügbarkeit und Vertraulichkeit der Daten zu treffen.

- Der Zugriff Dritter auf die Verbrauchs- und Abrechnungsdaten muss über implementierte Authentisierungs- und Zugriffsschutzmechanismen verhindert werden.
- Es müssen Maßnahmen ergriffen werden, dass Unbefugte die Daten nicht unbemerkt verändern oder entfernen können.
- Mit Verschlüsselungsverfahren muss sichergestellt werden, dass Unbefugte Kenntnis von den Daten erlangen können.
- Übermittlungsprotokolle (entsprechend Nr. 4 der Anlage 1 zu § 9 BDSG) machen nachvollziehbar, zu welchem Zeitpunkt welche Stelle über welche Daten verfügte.

Kontrolle

- Eine externe und interne Kontrolle der Datenverarbeitungsvorgänge muss möglich sein.

### 4.1.5 Datenschutz im Verein

In jedem Verein findet regelmäßig Umgang mit personenbezogenen Daten statt. Daher müssen auch im Rahmen der Vereinsarbeit Bestimmungen des Datenschutzes beachtet werden.

Jeglicher Umgang (Erhebung, Verarbeitung und Nutzung) mit personenbezogenen Daten untersteht auch im Verein dem sog. Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG. Sobald in einem Verein mit personenbezogenen Daten umgegangen wird, sind die drei grundsätzlichen Zulässigkeitsalternativen des § 4 BDSG (Einwilligung, Spezialgesetz, BDSG selbst) zu prüfen. Ein Spezialgesetz, das einem Verein einen bestimmten Umgang mit personenbezogenen Daten vorschreibt oder erlaubt, ist grundsätzlich nicht gegeben. Die Zulässigkeit eines Umgangs mit personenbezogenen Daten kann sich aus einer Einwilligung des Betroffenen i. S. des § 4a BDSG ergeben. Dabei ist zu beachten, dass eine Einwilligung jederzeit widerrufen werden kann (ausführlich unter Punkt 2. - Das Bundesdatenschutzgesetz -).
Ist keine der vorgenannten beiden Alternativen einschlägig, kann sich die Zulässigkeit der Datenerhebung, -verarbeitung, und -nutzung allein aus dem Bundesdatenschutzgesetz selbst, § 28 BDSG, insbesondere den §§ 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG, ergeben. Danach dürfen Mitgliederdaten im Rahmen des Vereinszwecks erhoben, verarbeitet oder genutzt werden. Es ist maßgeblich auf den in der Satzung festgelegten Vereinszweck abzustellen. Auf der Grundlage des § 28 Abs. 1 S. 1 Nr. 1 BDSG dürfen nur die Mitgliederdaten erhoben, verarbeitet und genutzt werden, wenn sie für die Vereinsmitgliedschaft unbedingt erforderlich sind (insbesondere Name, Anschrift, Geburtsdatum, Sportart) oder geeignet sind, den Vereinszweck zu fördern (z. B. besondere Fähigkeiten, Funktion im Verein). Darüber hinaus dürfen Mitgliederdaten, bei denen kein ausreichender Sachzusammenhang zum Verein besteht, sowie Daten von Nichtmitgliedern nur erhoben, verarbeitet oder genutzt wer-

den, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 S. 1 Nr. 2 BDSG). Bei dieser Zulässigkeitsalternative ist eine Abwägung zwischen den Interessen des Vereines und den schutzwürdigen Belangen der Betroffenen – wobei grundsätzlich per se keinem Interesse der Vorzug zu geben ist - unter dem Maßstab der Erforderlichkeit vorzunehmen.

Erläuterungen zu weitergehenden Problemstellungen:

*Übermittlung von Mitgliederdaten an andere Vereinsmitglieder:*
Mitglieder des Vereines können nur im Einzelfall Daten anderer Mitglieder erfragen und erhalten. Die Zulässigkeit der Datenübermittlung beurteilt sich danach, ob das auskunftsersuchende Vereinsmitglied ein berechtigtes Interesse an der Kenntnis der Daten hat und ob bei pauschaler Abwägung keine schutzwürdigen Interessen der betroffenen Mitglieder der Datenübermittlung entgegenstehen können. Bei der Beurteilung kommt es auf die Umstände des konkreten Falles an. Ist z. B. bekannt, dass ein Vereinsmitglied Wert darauf legt, seine Daten möglichst nur einem kleinen Kreis zugänglich zu machen, ist dies zu berücksichtigen. Hat eine Person bereits früher Einwände gegen eine Datenübermittlung geltend gemacht, so sollte im Zweifel nachgefragt werden, ob das Mitglied mit einer Übermittlung konkreter Daten einverstanden ist. Zudem muss die Erforderlichkeit stets gegeben sein. Werden Daten von Vereinsmitgliedern erbeten, um z. B. eine Fahrgemeinschaft bilden zu können, sind weder Angaben zum Geburtsdatum noch zur Bankverbindung erforderlich. Selbst die postalische Anschrift wäre entbehrlich, wenn zur Kontaktaufnahme die Angabe der Telefonnummer oder die E-Mail-Adresse ausreicht.

*Mitteilungen in Aushängen*
In vielen Vereinen ist es gängige Praxis, personenbezogene Informationen am „Schwarzen Brett“ auszuhängen oder in Vereinsblättern bekannt zu geben. Dies ist unproblematisch, solange die Angaben in engem Zusammenhang mit dem Verein stehen (in einem Sportverein z. B. die Bekanntgabe von Spielaufstellungen, Turniersiegern o. ä.), wenn die Bekanntgabe nicht über Name und Geburtsjahr/Altersklasse hinausgeht. Bei der Veröffentlichung von Vereinsjubiläen von Mitgliedern oder dem Beitritt neuer Mitglieder empfiehlt es sich, die Mitglieder generell oder im Einzelfall über die Bekanntmachung zu informieren und Gelegenheit zu geben, Einwände vorzubringen. Datenschutzrechtlich problematisch ist stets die Mitteilung von Daten aus dem persönlichen Lebensbereich der Mitglieder, beispielsweise Eheschließungen, Abschluss von Schul- oder Berufsausbildungen, Adressdaten etc.. Hierfür ist grundsätzlich die Einwilligung der betroffenen Mitglieder erforderlich.

*Veröffentlichung im Internet*

Mit Veröffentlichungen im Internet findet eine Datenübermittlung statt. Die personenbezogenen Daten sind grundsätzlich weltweit abrufbar, sodass sorgfältig zu überlegen ist, welche personenbezogenen Informationen zur Veröffentlichung im Internet wirklich notwendig sind. Es empfiehlt sich eine differenzierte Betrachtungsweise. Dem Schutz des Betroffenen kann es dienen, dass an Stelle der privaten Adresse eine Kontaktadresse angegeben wird und die Angabe der privaten Telefon-, Telefax- und Mobilfunk-Nummer sowie der privaten E-Mail-Adresse freiwillig ist.

In jedem Fall sind die potentiell Betroffenen über die Veröffentlichung im Internet zu informieren, da eine solche Veröffentlichung mit erheblich mehr Risiken verbunden ist. Will der Verein auch Informationen über seine Mitglieder (Aktive oder Inaktive) im Internet veröffentlichen, ist die vorherige Einwilligung der Betroffenen erforderlich.

Datenschutzrechtliche Aspekte spielen auch bei der reinen Verwaltung von Mitgliederdaten eine Rolle. Vereine sollten Regelungen für die ordnungsgemäße Datenverarbeitung treffen und diese in die Vereinssatzung aufnehmen. Es sollte konkret festgelegt werden, welche Daten zu welchem Zweck, in welcher Form, von wem erhoben, verarbeitet oder genutzt werden dürfen. Geregelt werden sollte auch, welche Mitgliederdaten wie lange gespeichert werden und wann Daten ausgeschiedener Mitglieder gelöscht werden. Es ist auch festzulegen, dass Daten, die nicht mehr benötigt werden, so entsorgt werden, dass Dritte keine Kenntnis von den Mitgliederdaten erlangen können, insbesondere dürfen Mitglieder- oder Spendenlisten nicht unzerkleinert in Müllcontainer geworfen werden. Zudem sollten die mit der Verarbeitung der Mitgliederdaten betrauten Personen schriftlich auf die Wahrung des Datengeheimnisses (§ 5 BDSG) verpflichtet werden.

### 4.1.6 Optisch-elektronische Einrichtungen (Videoüberwachung)

Auch zum Thema „Videoüberwachung“ gab es im Berichtszeitraum immer wieder Beratungsanfragen.

Da die Aufsichtsbehörde auf Aufklärung und Beratung setzt, ist es möglich, konkret getroffene bzw. zu treffende Maßnahmen zur Prüfung mitzuteilen.

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

*Abs. 1: Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, soweit sie*

*1. zur Aufgabenerfüllung öffentlicher*

Im Laufe der Beratung konnte regelmäßig geklärt werden, wie dem Gebot der Datenvermeidung und -sparsamkeit (§ 3a BDSG) und dem Grundsatz der frühestmöglichen Datenlöschung (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG) Folge geleistet werden kann.

*Stellen,*

2. *zur Wahrnehmung des Hausrechts oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*

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

Zum Tatbestand des § 6b Abs. 1 Nr. 3 BDSG ist Folgendes auszuführen:

*1.) Berechtigte Interessen:*

*Berechtigte Interessen der verantwortlichen Stelle* i. S. des § 6b BDSG können sowohl wirtschaftlicher als auch ideeller Natur sein. Diese müssen allerdings objektiv begründbar sein. Im Schutz des Eigentums ist regelmäßig ein berechtigtes Interesse zu sehen. Der Zweck der Videoüberwachung und damit das berechtigte Interesse an der Überwachung ist vor Beginn der Überwachung konkret festzulegen. Dies soll zum einen die Nachprüfung des berechtigten Interesses erleichtern, aber auch Aufschluss darüber geben, dass die verantwortliche Stelle nicht leichtfertig mit der Thematik „Überwachung mit optisch-elektronischen Einrichtungen“ umgegangen ist.

*2.) Erforderlichkeit der Videoüberwachung:*

Die *Erforderlichkeit* der Videoüberwachung ist grundsätzlich zu verneinen, wenn es mildere, ebenfalls geeignete Mittel gibt, oder der angestrebte Überwachungszweck so nicht erreicht werden kann. Dies wäre beispielsweise der Fall, wenn die Videoüberwachung mangels ausreichender Beleuchtung im Dunkeln keine nutzbaren Aufzeichnungen erzeugen würde. Gegenstand der Erforderlichkeitsprüfung ist sowohl die Tatsache der Anbringung der technischen Einrichtung als auch die konkrete Ausrichtung der Beobachtung und die technischen Möglichkeiten der optisch-elektronischen Einrichtung (z. B. Beweglichkeit der Kamera, Zoommöglichkeiten etc.).

*3.) Abwägung:*

Sind sowohl ein berechtigtes Interesse der verantwortlichen Stelle als auch die Erforderlichkeit des Einsatzes der Überwachungseinrichtung zur Erreichung dieses Interesses zu bejahen, ist in einem letzten Schritt zu prüfen, ob Anhaltspunkte bestehen, dass *schutzwürdige Interessen der Betroffenen dem berechtigten Interesse der verantwortlichen Stelle überwiegen*. Dabei sind Betroffene nicht nur die Personen, deren Identität bestimmt werden kann, sondern auch die, die mit zusätzlichen Informationen bestimmbar sind. Derartige schutzwür-

dige Interessen müssen sich auf belegbare Tatsachen beziehen und überwiegen, z. B. wenn die Intimsphäre eines Betroffenen beobachtet werden soll.

Auch bei einem überwiegenden berechtigten Interesse werden personenbezogene Daten erhoben und dadurch das allgemeine Persönlichkeitsrecht, d. h. das Recht auf Anonymität und Selbstbestimmung des Einzelnen, eingeschränkt. Werden jedoch die Belange des Datenschutzes beachtet und wird dies hinreichend dokumentiert, kann die Beeinträchtigung des Persönlichkeitsrechtes so gering wie nötig gehalten werden. Als umfassende Dokumentationsmöglichkeit bietet sich die Erarbeitung eines sog. Videoüberwachungskonzeptes an. In diesem kann festgelegt werden, wie die Videoüberwachung und die Datenerhebung erfolgt und zu welchem Zweck und wie die Daten überhaupt erfasst und verarbeitet werden. In einem Videoüberwachungskonzept sollten alle die Überwachung betreffenden Regelungen und Konfigurationen festgehalten werden, mindestens aber folgende Angaben:

- allgemeine Objektbeschreibung;
- die konkret festgelegten Zwecke (die Gründe) der Beobachtung;
- Festlegung des erforderlichen Rahmens für die Beobachtung und für die Aufzeichnung. Eine Erforderlichkeit ist nur dann gegeben, wenn es kein milderes und ebenfalls geeignetes Mittel gibt, mit dem der gleiche Zweck erreicht werden kann. In diesem Kontext ist stets die Möglichkeit einer Kameraattrappe zu prüfen, da das Vorhandensein und die Kenntnis einer vermeintlichen Videobeobachtung genügen könnten, dass das Verhalten an Gefahrenstellen angepasst wird. Dabei wird eine Kameraattrappe wie eine funktionierende Kamera behandelt.
- Detaillierte Beschreibung, was überwacht wird unter Angabe der Kameraposition, Überwachungsbereich, Art der Kamera etc. ;
- Angaben zur eingesetzten Technik/Software (Videosensortechnik, Zonenmaskierung etc.);
- Festlegungen zur Bildqualität;
- Festlegungen zur Datenspeicherung und zum Datenzugriff;
- Beschreibung der Maßnahmen zur Kenntlichmachung des Umstandes der Beobachtung und der verantwortlichen Stelle (§ 6b Abs. 2 BDSG);
- Löschfristen, verifiziert nach Vorgängen, in denen keine Vorfälle auftreten und solchen, für die die Kamera installiert werden soll (§ 6b Abs. 5 BDSG);
- Hinweis für welche Zwecke die Daten verarbeitet und genutzt werden sollen (§ 6b Abs. 3 BDSG) – Festlegungen zur Datenauslagerung/Datenweitergabe;
- Beschreibung der Betroffenenrechte (§ 6b Abs. 4, §§ 33 bis 35 BDSG).

### 4.1.7 Verkehrstelematik

**Ein Unternehmen** bat die Aufsichtsbehörde zu dem Thema Verkehrstelematik um Beratung. Verkehrstelematik umschreibt alles, was mit Fahrzeugen, ihren Insassen, dem Versand und Empfang, der Bearbeitung und Darstellung von Daten in einem Fahrzeug zu tun hat.

In der heutigen Zeit werden Fahrzeuge mit immer komplexeren und leistungsfähigeren elektronischen Systemen und Datenspeichern ausgerüstet. Sowohl deren Existenz und Funktionsweise als auch die Möglichkeit der Erhebung personenbezogener Daten sind bekannt. Daten des technischen Motormanagements haben zunächst keinen Personenbezug. Kommen allerdings verhaltensbedingte Informationen, wie z. B. Angaben zur (Quer-) Beschleunigung, Fahrzeugposition sowie zum Bremsverhalten hinzu, ergibt sich ein Personenbezug. Auch die bei der Wartung abrufbaren Daten können Aufschluss geben über das Fahrverhalten des Fahrzeugfahrers und können unter Umständen zu einem Nutzungs- oder auch Fahrerprofil zusammengeführt werden.

Da bei einer weiteren Verknüpfung mit Lokalisierungsdaten ein „gläserner Autofahrer“ entstehen könnte, ist die Nutzung dieser Daten durch Werkstätten zur Erfüllung von Wartungs- und Reparaturaufträgen nur zulässig, wenn vor der Auftragserteilung durch schriftliche Hinweise in der Betriebsanleitung, im Kaufvertrag des Fahrzeuges oder im Wartungs- oder Reparaturvertrag nachvollziehbar darüber informiert wird, welche Informationen sich aus den Fahrzeugdatenspeichern ergeben. Dies genügt allerdings nur, wenn Halter und Fahrer eine Person sind. Andernfalls muss ggf. zusätzlich eine Information des Fahrers sichergestellt werden. Von einer nachvollziehbaren Information ist nicht auszugehen, wenn allein pauschale Hinweise zum Fahrzeugspeicher allgemein – Unterstützung des Serviceprozesses, zur Reparatur etc. – gegeben werden, auf die personenbezogene Profilbildung jedoch nicht hingewiesen wird.

Seit einigen Jahren wird darüber diskutiert, Telematikanwendungen im Versicherungswesen zu nutzen. Diese sollen Versicherungsunternehmen Möglichkeiten geben, Zusatznutzen für Autofahrer zu generieren.

Im Fall „Copilot“ soll eine sog. Blackbox laufend die Fahrzeugbewegung, hier die Längs- und Querbeschleunigungen, per Sensoren erfassen. Wird hierbei eine Überschreitung von Grenzwerten festgestellt, die nur durch einen Unfall verursacht worden sein kann, wird automatisch die aktuelle Fahrzeugposition per GPS bestimmt und ein Notruf abgesetzt. Im

Falle eines Kfz-Diebstahles kann auch eine Fahrzeugortung durch die Polizeidienststelle veranlasst werden.

Bei der Installation einer Blackbox in ein Kfz können Fahrzeugdaten - Fahrzeugposition laut GPS und Beschleunigungsdaten - des Fahrzeuges erhoben und gespeichert werden. Zudem können etwaige Reaktionen auf Basis von parametrierbaren Schwellenwerten, z. B. g-Kräfte in Fahrtrichtung und 90 Grad quer zur Fahrtrichtung, automatisch ausgelöst werden. Dieser Prozess ist datenschutzrechtlich relevant, da die vorgenannten Daten zumindest personenbeziehbar sind. Es kann – ggf. mit Zusatzwissen – ein Bezug auf eine konkrete Person hergestellt werden, da Kraftfahrzeuge nur von einem bestimmten Personenkreis genutzt werden. Entsprechend musste die Erhebung, Verarbeitung und Nutzung auf Grundlage des sog. Verbotes mit Erlaubnisvorbehalt - § 4 Abs. 1 BDSG – zulässig sein.

Die Aufsichtsbehörde hatte grundsätzlich keine Bedenken gegen die Zulässigkeit des vorgestellten Gesamtverfahrens. Da es jedoch bei der Umsetzung maßgeblich auf die Beachtung verschiedener Datenschutzanforderungen ankommt, wurde auf folgende Anforderungen bei der Weiterentwicklung des Projektes **hingewiesen**:

- Es darf keine totale Überwachung geben.
- Es muss eine Bestimmung über die Erhebungs-/Auswertungszeitpunkte geben. Die Schwellenwerte sind entsprechend zu setzen. Es muss eine maximale Anzahl von Ereignissen vorgegeben werden, zu denen Daten gespeichert werden.
- Es dürfen nur erforderliche Daten gespeichert werden.
- Die Daten sind zu löschen, wenn sie nicht mehr benötigt werden. Folglich muss auch gelöscht werden, wenn die Daten längere Zeit (z. B. sechs Wochen) nicht ausgewertet wurden.
- Eine Definition von Löschprioritäten muss möglich sein.
- Es muss eine festgelegte Speicherdauer für Daten geben, die aus der Blackbox für eine Untersuchung entnommen werden.
- Die Schnittstellensicherheit und die Datenintegrität müssen ein hohes Niveau haben.
- Ein Zugriff auf Daten darf nur Personen möglich sein, die die Berechtigung dazu haben.
- Die Datenverarbeitung muss für den Fahrer transparent sein.

Nach umfassender Beratung der Aufsichtsbehörde wirkte der Datenschutzbeauftragte des Unternehmens auf die notwendigen Regelungen und insbesondere die Transparenz für die Betroffenen hin.

Das bislang allein in Sachsen-Anhalt angebotene Produkt stieß nach seiner Etablierung auf bundesweites Interesse. Vor diesem Hintergrund fand Anfang des Jahres eine erneute Beratung statt. Neben der Erörterung der bisherigen Ausführungen und der möglichen Risiken des Produktes aus datenschutzrechtlicher Sicht, betonte die Aufsichtsbehörde nochmals die Notwendigkeit ausreichender Transparenz des Verfahrens gegenüber den Betroffenen.

### 4.1.8 Übermittlung personenbezogener Daten

Öffentliche Stellen, z. B. Landkreise oder Staatsanwaltschaften, wenden sich in bestimmten Situationen an nicht-öffentliche Stellen und bitten um Auskünfte. Soweit eine Auskunft erteilt wird und diese personenbezogene Daten beinhaltet, findet eine Übermittlung personenbezogener Daten statt.

**Begriffserläuterungen:**
*Übermitteln* ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass a) die Daten an den Dritten weitergegeben werden oder b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Übermitteln stellt neben dem Speichern, Verändern, Sperren und Löschen personenbezogener Daten eine Form der *Verarbeitung* dar.

**Ein Wohnungsunternehmen** wandte sich an die Aufsichtsbehörde, da es nicht einschätzen konnte, ob es die von einer öffentlichen Stelle erbetenen Auskünfte erteilen darf. Konkret wurde das Unternehmen als Vorvermieter eines Mieters angeschrieben, da eine Couchgarnitur auf der Straße entdeckt und vermutet wurde, dass der Mieter diese unzulässig entsorgt habe. Es wurde – soweit vorhanden – um Übersendung von Fotografien der Couch des Vormieters gebeten bzw. eine Beschreibung der Couchgarnitur. Sowohl aus den der Wohnung des Mieters zuzuordnenden Fotos als auch der Beschreibung dort vorhandener Objekte ergeben sich personenbezogene Daten.

Die beabsichtigte Datenverarbeitung - Übermittlung - darf nur erfolgen, wenn sie nach § 4 Abs. 1 BDSG zulässig ist. Folglich nur, soweit dies das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift erlaubt oder anordnet oder der Betroffene eingewilligt hat. Im vorliegenden Fall kam allein § 28 Abs. 2 Nr. 2 BDSG als Zulässigkeitsalternative in Frage. Allerdings soll diese Vorschrift keine Auffangklausel darstellen, sondern als Ausnahme gesehen und deshalb restriktiv interpretiert werden. Da davon auszugehen ist, dass der abfallrechtliche Vorgang im Rahmen eines Ordnungswidrigkeitenverfahrens relevant ist, müsste die anfragende Stelle zunächst von den eigenen Ermittlungsmöglichkeiten Gebrauch machen. Da

dies nicht erfolgte, ergab sich keine Zulässigkeit nach § 28 Abs. 2 Nr. 2a BDSG. Ähnlich verhält es sich in Bezug auf § 28 Abs. 2 Nr. 2b BDSG. Der Rückgriff auf diese Vorschrift unter Hinweis auf die Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit ist nur zulässig, wenn es keine anderen, spezialgesetzlichen Regelungen gibt. Grundsätzlich soll sich aus der Vorschrift eine Befugnis zur Datenübermittlung beim Vorliegen von Straftaten ergeben, dies gilt jedoch nicht bei der Verfolgung von Ordnungswidrigkeiten.
Im Ergebnis vermochte die Aufsichtsbehörde daher keine Übermittlungsbefugnis des Wohnungsunternehmens erkennen.

**Ein Einwohnermeldeamt** bat ein Wohnungsunternehmen um Übermittlung personenbezogener Daten aller Neumieter in einem gewissen zeitlichen Turnus. Die entsprechende Aufforderung wurde auf § 12 Abs. 1, 2 bzw. hinsichtlich des Umfanges der Datenerhebung auf § 11 Abs. 2 des Meldegesetzes des Landes Sachsen-Anhalt (MG LSA) gestützt. Das Unternehmen war der Auffassung, dass eine entsprechende Datenübermittlung auf der genannten Grundlage nur im Einzelfall zu erfolgen hat und bat um Bewertung der Angelegenheit aus aufsichtsbehördlicher Sicht.
Die Aufsichtsbehörde bestätigte die Rechtsauffassung des Unternehmens.

Auch bei der **Veräußerung einer Arztpraxis** kommt es zur Übermittlung personenbezogener Daten. Denn sowohl der die Praxis aufgebende Arzt als auch der Arzt, der die Praxis übernimmt, stellen jeweils sog. verantwortliche Stellen i. S. des Bundesdatenschutzgesetzes dar. Eine Übermittlung personenbezogener Daten muss daher auf der Grundlage des § 4 Abs. 1 BDSG, dem sog. Verbot mit Erlaubnisvorbehalt, zulässig sein.
Die Aufsichtsbehörde wies darauf hin, dass es keine spezialgesetzliche Regelung gibt, die die Übermittlung sämtlicher Patientendaten des die Praxis aufgebenden Arztes an den „Nachfolger“ normiert. Im Hinblick auf die Zulässigkeitsnormen des BDSG, speziell § 28 BDSG, ist stets eine Interessenabwägung im Einzelfall vorzunehmen. Eine Übermittlung der Patientendaten ist nur erforderlich, wenn sich die Patienten vom „Nachfolger“ weiterbehandeln lassen wollen.
Im Ergebnis muss der Patient immer die Möglichkeit haben, mitzubestimmen. Seit dem Urteil des BGH vom 11.12.1991, Az. VIII ZR 4/91, ist unbestritten, dass die Übermittlung der Patientendaten wegen der möglichen Verletzung der ärztlichen Schweigepflicht und des Rechts auf informationelle Selbstbestimmung des Patienten (Datenschutz) der ausdrücklichen Entscheidung des jeweiligen Patienten bedarf. Zuvor war es üblich, dass Ärzte beim Verkauf ihrer Praxis die Patientenunterlagen ohne Einwilligung der betroffenen Patienten an den Nachfolger übergaben.

Die Aufsichtsbehörde wies darauf hin, dass es sich bei den einzuholenden Einwilligungen nicht um konkludente Einwilligungen handeln darf, da § 4a BDSG solche nicht vorsieht. Vielmehr müssen die Einwilligungen zu ihrer Wirksamkeit den Voraussetzungen des § 4a BDSG genügen. Somit genügt z. B. ein Informationsschreiben an den Patienten nicht, da Schweigen nicht als Zustimmung gewertet werden kann.

**TIPP:**
Für die praktische Umsetzung der Einholung von Einwilligungen aller Patienten hat sich ein sog. „Zwei-Schränke-Modell“ durchgesetzt. Dies bedeutet, dass sich der Nachfolger verpflichtet, die Daten des Vorgängers in einem verschlossenen Schrank zu verwahren. Beim ersten „Neu“besuch eines Patienten beim „Nachfolger“ wird dessen Einwilligung eingeholt und seine Daten ggf. ins neue System eingefügt.

### 4.1.9 Nutzung personenbezogener Daten – Einführung einer Beförderungschipkarte

**Eine Verkehrsgesellschaft** beabsichtigte eine Chipkarte mit Daten und einem Lichtbild einzuführen, um sich zukünftig mit der Chipkarte die Fahrberechtigung nachweisen zu lassen. Die um Beratung gebetene Aufsichtsbehörde stellte zunächst fest, dass aus den bisher ausgegebenen Berechtigungskarten allein Name, Vorname, Anschrift, Geburtsdatum, Fahrstrecke und Gültigkeitszeitraum ersichtlich sind. Diese Daten werden auch im Rahmen des eingesetzten Abrechnungsprogramms gegenüber dem Beförderungsdienstleister genutzt.
Zu diesen Daten sollte nunmehr zusätzlich das Lichtbild hinzukommen. Mit der Anfertigung der Lichtbilder sollte ein zentraler Fotograf beauftragt werden. Die vorgelegte Vereinbarung mit dem Fotografen ließ erkennen, dass diesem eine weitere Nutzung der Fotos für andere Zwecke untersagt wurde und eine Verpflichtung auf das Datengeheimnis erfolgte. Neben der Vereinbarung wurde auch die erbetene Programmbeschreibung für das Verwaltungsprogramm vorgelegt.

Aus den vorgelegten Unterlagen ergab sich, dass der Einsatz der Beförderungschipkarte zu einem umfassenden Umgang mit personenbezogenen Daten führen würde. So findet eine Veränderung personenbezogener Daten statt, wenn Änderungen eintreten und diese im Verkehrsunternehmen eingepflegt werden. Im Rahmen von Kontrollen der Fahrtberechtigungen kommt es zur Übermittlung personenbezogener Daten an die Kontrolleure. Wenn die Berechtigungen der Beförderten in Bezug auf die Beförderungsleistung eingeschränkt werden, führt dies zur Sperrung personenbezogener Daten - oder wenn keine Berechtigung mehr

besteht - zur Löschung. Auch eine Nutzung der Daten ist mit der Karte verbunden, denn Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Die beschriebenen Verarbeitungsprozesse wurden grundsätzlich als zulässig eingestuft. Es wurde ein berechtigtes Interesse des Unternehmens anerkannt, Maßnahmen zu ergreifen, die sicherstellen, dass nur Personen befördert werden, für die ein Beförderungsanspruch besteht. Dieses Ziel kann nicht ohne die personenbezogenen Informationen erreicht werden. Die damit verbundene Datenerhebung, -verarbeitung und -nutzung ist im Allgemeinen erforderlich. Überwiegende schutzwürdige Belange der Fahrgäste waren nicht ersichtlich. Das Unternehmen wurde allerdings darauf hingewiesen, dass im Einzelfall die Zulässigkeit nochmals konkret auf der Grundlage des § 28 Abs. 1 S. 1 Nr. 2 BDSG geprüft werden müsse. Zudem wurde darauf hingewiesen, dass gemäß § 28 Abs. 1 S. 2 BDSG die Zwecke, für die die erhobenen Daten verarbeitet und genutzt werden sollen, konkret festzulegen sind. Da die Daten zudem nicht bei den Betroffenen selbst erhoben werden, wurde an die bestehende Benachrichtigungspflicht des § 33 Abs. 1 BDSG erinnert. Abschließend wurde die entsprechende Ergänzung des ohnehin vorgesehenen Informationsblattes empfohlen.

## 4.2 Was ist zulässig und was nicht – ausgewählte Beschwerdeverfahren

### 4.2.1 Videoüberwachung quer Beet

„Vorsicht Kamera“, der Eigenname für eine Fernsehshow, ist aber auch bezeichnend für den seit Jahren ansteigenden Einsatz von Videoüberwachungssystemen. Die Technik wird immer günstiger und ist so einfach zu handhaben, dass auch „der Feierabendhandwerker mit zwei linken Händen“ die Kamera installieren kann. Zudem finden sich in fast jeder Baumarktwerbung Angebote für Videoanlagen, und wenn es dann noch 20 Prozent auf alles gibt, treten Bedenken wegen des Datenschutzes in den Hintergrund. Die sich aus rechtlicher Sicht ergebenden Fragen – auch bei der privaten Videoüberwachung – waren bereits mehrfach Gegenstand gerichtlicher Verfahren. Der Bundesgerichtshof führte in seinem Urteil vom 16. März 2010 (Az.: VI ZR 176/09) unter anderem zur Beeinträchtigung des Persönlichkeitsrechts des Grundstücksnachbarn aus, wenn auf einem Privatgrundstück Überwachungskameras installiert sind.

Gerade diese Problematik beschäftigt auch die Aufsichtsbehörde, wenn Petenten den Eindruck haben, dass auch der öffentlich zugängliche Raum erfasst wird.

Der Bundesgerichtshof bestätigte, dass die Herstellung von Bildnissen einer Person, insbesondere Aufzeichnungen mit einer Videokamera, auch in der Öffentlichkeit zugänglichen Bereichen (z. B. auf einem öffentlichen Weg) einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht eines Betroffenen darstellen kann, selbst wenn keine Verbreitungsabsicht bestehe. Eine abschließende Beurteilung und damit die Feststellung, ob eine Verletzung des Persönlichkeitsrechts gegeben ist, habe jedoch unter Würdigung aller Umstände des Einzelfalls und durch Vornahme einer die (verfassungs-)rechtlich geschützten Positionen der Beteiligten berücksichtigenden Güter- und Interessenabwägung zu erfolgen.
Wird bei der Installation von Videoüberwachungsanlagen auf einem Privatgrundstück sichergestellt, dass weder der angrenzende öffentliche Bereich noch benachbarte Privatgrundstücke oder ein gemeinsamer Zugang von Kameras erfasst werden, überwiegen keine Persönlichkeitsrechte erfasster Personen. Andernfalls sei die Beobachtung nur zulässig, wenn im Rahmen der Abwägung feststeht, dass das Persönlichkeitsrecht der Betroffenen nicht den Interessen des Betreibers überwiegt. Ein Eingriff in das Persönlichkeitsrecht Dritter liege vor, wenn diese durch die Überwachung tatsächlich betroffen sind oder wenn der Dritte eine Überwachung objektiv ernsthaft befürchten muss („Überwachungsdruck“). Letzteres sei gegeben, wenn dies aufgrund konkreter Umstände als nachvollziehbar und verständlich erscheine. Allein die hypothetische Möglichkeit der Überwachung genüge dagegen nicht. Dies sei der Fall, wenn ein Betroffener die Anfertigung von Aufnahmen lediglich befürchte, objektiv allerdings feststehe, dass öffentliche und fremde private Flächen nicht erfasst werden, und die Kameras und deren Erfassungsbereich nur mit erheblichen und äußerlich wahrnehmbarem Aufwand und nicht nur durch einfache Betätigung der Steuerungsanlage verändert werden können.

**ZU BEACHTEN:**
Die vorgenannten Ausführungen gelten auch für bloße Kameraattrappen. Für Betroffene ist nicht erkennbar, ob sie tatsächlich gefilmt werden oder nicht. Vielmehr wird auch bei Aufstellen einer Attrappe, die einer funktionsfähigen Videokamera gleicht, bei den Betroffenen der Eindruck erweckt, sie müssten ständig mit einer ihren Privatbereich überwachenden Aufzeichnung rechnen.

Wie bereits erwähnt, haben sich die Anfragen zur Zulässigkeit der Beobachtung mit optisch-elektronischen Einrichtungen gehäuft, wo der Eindruck bestand, dass der öffentlich zugängliche Raum erfasst werde.

**Begriffsbestimmung:**
Unter *öffentlich zugänglichen Räumen* sind umbaute Flächen zu verstehen, die ihrem Zweck nach dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Öffentlich zugängliche Räume sind beispielhaft die Ausstellräume eines Museums, Schalterhallen, Tankstellen, Cafés, Parkhäuser u. v. m.. Maßgeblich für den Begriff des Raumes, wie er in § 6 b des Bundesdatenschutzgesetzes genutzt wird, ist, dass der Betroffene nur über begrenzte Möglichkeiten verfügt, der Videoüberwachung auszuweichen. Unter diesem Gesichtspunkt können „Räume“ auch außerhalb von Gebäuden liegen, wenn sie umgrenzt sind (*Däubler* in Däubler/Klebe/Wedde/Weichert (Hrsg.), Kommentar zum BDSG, § 6b Rn. 21 m. w. N.).

Die Aufsichtsbehörde prüfte wiederholt die Zulässigkeit einer Kamera am Fenster eines Miethauses bei der der Eindruck vorlag, dass ein Großteil eines öffentlichen Marktplatzes überwacht wurde. Eine Mieterin des Hauses gab an, sich von der Kamera auf Schritt und Tritt beobachtet zu fühlen und Angst zu haben, dass Fotos ins Internet gestellt werden. Die Aufsichtsbehörde ermittelte die tatsächlichen Gegebenheiten (Anbringungsort, Erfassungsbereich, Beobachtungszeiten etc.). Zudem wurde die für die Kamera verantwortliche Stelle um Mitteilung des Zweckes der Videoüberwachung und Ausführungen zur Zulässigkeit gebeten. Der Inhaber der Wohnung teilte zunächst mit, dass das Gerät „lediglich der Abschreckung von eventuellen Straftätern als Konsequenz in der Vergangenheit gehäuft vorgekommener polizeibekannter Einbrüche und Sachbeschädigungen am Wohnobjekt“ diene. Zudem handele es sich ohnehin um eine Attrappe, so dass schutzwürdige Interessen Dritter nicht verletzt würden. Die Aufsichtsbehörde wies darauf hin, dass es zur Beurteilung der Zulässigkeit der Kamera nicht entscheidend sei, ob es zu einer konkreten Verletzung schutzwürdiger Interessen Dritter kommt, sondern ob diese ggf. gegenüber den eigenen berechtigten Interessen überwiegen. Durch eine vermeintliche Beobachtung sämtlicher Passanten würden diese unter Generalverdacht gestellt. Dies nahm der Inhaber der Kamera zum Anlass die Kamera zu entfernen.

Circa ein halbes Jahr später wurde die Aufsichtsbehörde jedoch darüber informiert, dass die Kamera wieder installiert worden sei. Erneut teilte der Inhaber der Kamera mit, dass die Kamera entfernt wurde. Das Gerät diene allein zur gelegentlichen Beobachtung öffentlicher Ereignisse. Die Aufsichtsbehörde teilte dem Verantwortlichen daraufhin mit, dass derzeit keine weiteren Ermittlungen in der Angelegenheit erfolgen, jedoch künftig Vorortkontrollen erfolgen. Soweit er erneut die Installation der Kamera beabsichtigte, wurde die vorherige Abstimmung mit der Aufsichtsbehörde empfohlen, da die Anbringung der Kamera nach dem Ergebnis der bisherigen Prüfung nicht zulässig gewesen ist.

In einem anderen Fall wurde die Aufsichtsbehörde wiederum auf eine, an einem Fenster angebrachte, Kamera hingewiesen. Diese Kamera erweckte den Eindruck, eine Fußgängerpassage werde überwacht. Der Petent – ein Arzt, der im selben Gebäude praktiziert – wandte sich an die Aufsichtsbehörde, da sich seine Patienten überwacht fühlen. Der Verantwortliche teilte mit, dass es sich bei der installieren Kamera lediglich um eine Beobachtungshilfe handele und keine Aufnahmen stattfinden. Sie diene allein dazu, zu sehen, wer vor dem Haus stehe.
Die Zulässigkeit der Beobachtung wurde auf der Grundlage von § 6b Abs. 1 Nr. 3 BDSG geprüft. Das Anliegen, Einlass begehrende Personen identifizieren zu können, kann zwar als berechtigtes Interesse gesehen werden, jedoch muss die Beobachtung zur Erreichung dieses Zieles auch erforderlich sein. Dies ist der Fall, wenn es kein milderes und ebenfalls geeignetes Mittel gibt, mit dem der Zweck erreicht werden kann. Eine solche Erforderlichkeit stellte die Aufsichtsbehörde nicht fest. Neben der vorhandenen Gegensprechanlage genügt der Blick aus dem Fenster. Auch lagen Anhaltspunkte dafür vor, dass schutzwürdige Interessen der Betroffenen überwiegen. Passanten der Fußgängerpassage können der vermuteten Beobachtung zwar ausweichen, die Besucher des Wohn- und Geschäftshauses jedoch nicht. Die Beobachtung mit der Kamera war daher nicht zulässig. Die Aufsichtsbehörde gab der verantwortlichen Stelle auf, die Kamera zu entfernen. Dieser Forderung kam der Verantwortliche ausweislich eines Vororttermins nach.

Mit dem Einsatz von optisch-elektronischen Einrichtungen werden auch Arbeitnehmer an ihrem Arbeitsplatz konfrontiert. Sei es die Kamera am Eingangsbereich, um Besucher identifizieren zu können oder Kameras im eigentlichen Arbeitsbereich. Selten ist die Beobachtung der Arbeitnehmer bezweckt. Dies macht die sog. Mitbeobachtung der Arbeitnehmer aber nicht ohne weiteres zulässig. Dass die Persönlichkeitsrechte der betroffenen Arbeitnehmer – die einem erheblichen Überwachungsdruck ausgesetzt werden – verletzt werden können, ist nämlich nicht von der Hand zu weisen. Eine Überwachung, die jede Regung und Bewegung der Mitarbeiter zur Kenntnis nimmt und dokumentiert, ist nicht mit der Menschenwürde vereinbar. Allerdings kann es in Ausnahmefällen zulässig sein, Videoüberwachung im Hinblick auf Arbeitnehmer vorzunehmen, insbesondere wenn ein hinreichend konkreter Verdacht auf begangene strafbare Handlungen besteht, der nicht oder nur schwer mit anderen, das Persönlichkeitsrecht des Überwachten wahrenden Mitteln, geklärt werden kann. Die **gezielte dauerhafte Überwachung** von Arbeitnehmern ist nicht zulässig.

### 4.2.2 Nachtsichtgeräte im Kino: Nur lästig oder ein datenschutzrechtlicher Verstoß?

**Können Nachtsichtgeräte Licht ins Kinodunkel bringen?**

**Kino-Besucher mit Nachtsichtgeräten beobachtet**

**Harry-Potter-Fans mit Nachtsichtgeräten ausspioniert**

Der Mitte 2009 in die Kinos gekommene „Harry-Potter"-Film zog nicht nur Kinogänger an, sondern auch eine Prüfung der Aufsichtsbehörde nach sich.

Einer Kinobesucherin war nämlich aufgefallen, dass während der Filmvorführung links und rechts der Leinwand Mitarbeiter einer Sicherheitsfirma „den Besucherraum mit Hilfe kameraähnlicher Geräte beobachten". Auf ihre Nachfrage erfuhr die Kinobesucherin, dass die Besucher nicht gefilmt, sondern mittels Nachtsichtgeräten im Auftrag der Filmverleihfirma Warner Bros. beobachtet wurden.

Zum Einsatz dieser Nachtsichtgeräte in einem Magdeburger Kino hat das Landesverwaltungsamt als zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich den Einzelsachverhalt geprüft. In dem Kino wurden Mitarbeiter einer Sicherheitsfirma eingesetzt, die mittels Nachtsichtgeräten kontrollierten, ob Zuschauer technische Mittel zum Fertigen von Mitschnitten des Filmes nutzen. In der Vergangenheit ist es in diesem Kino nachweislich zu einem Mitschnitt (Raubkopie) gekommen. Dieses illegale Mitschneiden und Verbreiten von Kinofilmen verursacht der Filmindustrie einen ernormen Schaden, deshalb soll mit dieser Maßnahme das Mitschneiden verhindert werden. Dieser Vorgang war Anlass des Einsatzes der Nachtsichtgeräte. Der Drei-Tage-Zeitraum wurde festgelegt, da erfahrungsgemäß gerade am Eröffnungswochenende Raubkopien gefertigt werden.

Für die Aufsichtsbehörde steht fest, dass grundsätzlich ein berechtigtes Interesse an der Beobachtung von Kinobesuchern bei Previews – auch unter Einsatz von Nachtsichtgeräten – besteht.

Vor diesem Hintergrund hat das Landesverwaltungsamt den konkret bekannt gewordenen Einsatz der Nachtsichtgeräte vom 15.07.2009 bis 19.07.2009 in dem Magdeburger Kino während des neuen Harry Potter Filmes beurteilt. Da es nur zu einem punktuellen Einsatz der Nachtsichtgeräte zur reinen Beobachtung (Aufzeichnungsmöglichkeiten waren technisch nicht gegeben) kam, um bei Verdacht mögliche Täter ansprechen zu können, wurden die Kinobesucher nicht unter Generalverdacht gestellt. Zudem wurden die Kinobesucher nach Feststellung der Aufsichtsbehörde – wie notwendig – bereits an den Kinokassen mittels Auf-

steller darauf hingewiesen, dass die Vorstellung mit Nachtsichtgeräten überwacht wird. Auf den gleichen Aufstellern wurde auch nochmals darauf hingewiesen, dass Kameras und andere Aufnahmegeräte im Kinosaal nicht verwendet werden dürfen und jeder Verstoß zur Anzeige gebracht wird.

Zugegeben, ein ungutes Gefühl bleibt, wenn man weiß, es beobachtet mich jemand – wenn auch nur kurz - im Schutz der Dunkelheit. Gleichwohl ist nicht jedes „ungute Gefühl“, das durch Dritte erzeugt wird, rechtlich relevant.

Die Aufsichtsbehörde beurteilte, dass § 6b BDSG – Beobachtung des öffentlich zugänglichen Raumes mit optisch-elektronischen Einrichtungen – nicht zur Anwendung kommt, da die Nachtsichtgeräte keine Aufzeichnungsfunktion hatten. Schließlich hat der Gesetzgeber durch die Definition „Videobeobachtung“ in § 6b BDSG den Anwendungsrahmen eingegrenzt. Ansonsten müsste auch das Beobachten des Rosenmontagszuges in der Kölner Innenstadt mit einem Opernglas unter den Schutzzweck der Norm fallen!

### 4.2.3. Erhebung personenbezogener Daten

**Begriffsbestimmungen:**

*Erheben* ist das Beschaffen von Daten über den Betroffenen. Auf die Art und Weise der Beschaffung kommt es nicht an. Denkbare Wege zum „Beschaffen von Daten“ sind die Befragung einer Person, das Anfordern von Unterlagen oder das elektronische Abrufen von Daten. Allerdings muss das Beschaffen gezielt erfolgen, d. h. die beiläufige zufällige Wahrnehmung führt ebenso wenig wie die aufgedrängte Unterrichtung (Zusendung eines unaufgeforderten schriftlichen Dokumentes oder eine Information auf dem Anrufbeantworter). Werden auf diesem Wege erlangte Informationen allerdings nicht gelöscht, erhalten sie nachträglich eine Zweckbestimmung und gelten als erhoben (*Weichert* in Däubler/Klebe/Wedde/Weichert (Hrsg.), Kommentar zum BDSG, § 3 Rn. 23 m. w. N.).

In welchen Bereichen die Aufsichtsbehörde die Zulässigkeit der Datenerhebung prüfte, ist den nachfolgenden Beispielen zu entnehmen.

**In zwei Fällen** beschäftigte sich die Aufsichtsbehörde mit der Datenerhebung beim Parken auf Privatparkplätzen. Das Abstellen eines Fahrzeuges auf solchen Plätzen kann dazu führen, dass das Fahrzeug abgeschleppt wird oder eine Zahlungsaufforderung an das geparkte Fahrzeug geheftet wird. Mit dieser wird um die eigenständige Überweisung einer „Ersatzgebühr“ gebeten. Dabei werden auch das Kfz-Kennzeichen und der Zeitpunkt des Parkens als maßgebliche Daten erhoben. Verstreicht die gesetzte Zahlungsfrist, übergibt der Parkplatzbetreiber die Angelegenheit unter Mitteilung der erhobenen Daten an einen Anwalt. Dieser ermittelt Name und Anschrift des Fahrzeughalters und erinnert an die offene Forderung.
Die Aufsichtsbehörde prüfte, ob der Rechtsanwalt als „Nichtbehörde“ aufgrund des bekannten Kfz-Kennzeichens bei den Zulassungsstellen Auskunft zu den weiteren Daten des Fahrzeughalters erhalten darf. Der Rechtsanwalt hatte sich schriftlich an die zuständigen Zulassungsstellen gewandt und um Mitteilung von Vor- und Zunamen des Halters, Straße, Postleitzahl und Ort gebeten, um Rechtsansprüche gemäß § 39 Straßenverkehrsgesetz (StVG) geltend machen zu können.
§ 39 Abs. 1 StVG beinhaltet eine spezielle Rechtsgrundlage für die Datenübermittlung durch die Zulassungsbehörde an den Rechtsanwalt. Diese Rechtsvorschrift erlaubt somit nicht direkt die Datenerhebung durch den Rechtsanwalt.
Im vorliegenden Einzelfall ist die Datenerhebung allerdings auf der Grundlage des § 28 Abs. 1 Nr. 2 BDSG unter Beachtung der Rechtsvorschrift des § 39 Abs. 1 StVG zulässig gewesen. Danach ist das Erheben personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse lag vor. Zudem wurden mit Name und Anschrift nur die erforderlichen Daten erhoben. Auch überwogen keine schutzwürdigen Belange der Betroffenen. Es ist folgerichtig, dass eine Datenerhebung erlaubt ist, wenn die Datenübermittlung an die erhebende Stelle bereits zulässig ist.

**Vermehrt** erreichten uns Beschwerden, weil Betroffene um die Vorlage einer Kopie des Personalausweises gebeten wurden. Eine solche Verfahrensweise wurde häufig bei der Geltendmachung des Auskunftsrechtes nach § 34 BDSG festgestellt. In einem weiteren Fall soll sogar das Scannen des Ausweisdokumentes Zugangsvoraussetzung für das Betreten einer Diskothek gewesen sein. Die Betroffenen zogen allerdings im Moment der entsprechenden Aufforderung die richtige Konsequenz. Sie entschieden sich gegen den Besuch der Disko und baten die Aufsichtsbehörde um Prüfung der Zulässigkeit der Verfahrensweise. Die verantwortliche Stelle bestritt das Scannen eines Ausweisdokumentes als Zugangsvorausset-

zung für die Disko. In anderen Fällen gingen die verantwortlichen Stellen dagegen davon aus, dass die praktizierte Verfahrensweise zur Identitätsprüfung zulässig sei.

Datenschutzrechtlich führt das Kopieren und Scannen von Ausweisdokumenten zu einer Erhebung personenbezogener Daten. Aufgrund des sog. Verbotes mit Erlaubnisvorbehalt ist dies nur zulässig, wenn 1. eine spezialgesetzliche Grundlage dies erlaubt, 2. eine Einwilligung des Betroffenen vorliegt oder 3. eine Zulässigkeit auf Basis des Bundesdatenschutzgesetzes gegeben ist.

Gesetzlich ausdrücklich zugelassen ist die Vervielfältigung von Ausweisdokumenten
z. B.

- beim Abschluss von Telekommunikationsdienstleistungsverträgen (§ 95 Abs. 4 S. 2 TKG),

- beim Bestehen von Aufzeichnungs- und Aufbewahrungspflichten für bestimmte Transaktionen (§ 8 Abs. 1 S. 3 des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG)),

- zum Nachweis der Identität bei Anforderung einer Auskunft (§ 64 Abs. 1 Nr. 2 Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnis-Verordnung (FeV)),

- zur Anfertigung von Ausweiskopien i. R. v. behördlichen Beglaubigungen (§ 33 Abs. 1 S. 1 i. V. m. Abs. 4 Nr. 1 VwVfG)

***§ 95 Abs. 4 TKG – Vertragsverhältnisse***

*Der Diensteanbieter kann im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Teilnehmers erforderlich ist. Er kann von dem Ausweis eine Kopie erstellen. Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten. Andere als die nach Absatz 1 zulässigen Daten darf der Diensteanbieter dabei nicht verwenden.*

***§ 64 FeV- Identitätsnachweis***

*(1) Als Identitätsnachweis bei Auskünften nach § 30 Absatz 8 oder § 58 des Straßenverkehrsgesetzes werden anerkannt*
*1. die amtliche Beglaubigung der Unterschrift,*
*2. die Ablichtung des Personalausweises oder des Passes oder*
*3. bei persönlicher Antragstellung der Personalausweis, der Pass oder der behördliche Dienstausweis.*
*(2) Für die Auskunft an einen beauftragten*

*Rechtsanwalt ist die Vorlage einer entsprechenden Vollmachtserklärung oder einer Fotokopie hiervon erforderlich.*

**Mit einer Datenerhebung** in dieser Form wurde ein Petent konfrontiert, als er zur Verbesserung des Internet-Zuganges einen UMTS-Stick erwerben wollte. Er gab an, sich beim Abschluss des entsprechenden Nutzungsvertrages mit seinem Personalausweis legitimiert und seine Kontoverbindung angegeben zu haben, um die Einziehung der monatlichen Rechnung zuzulassen. Dabei seien sein Personalausweis und seine EC-Karte kopiert worden. Auf seine Nachfrage zur Rechtmäßigkeit der Verfahrensweise sei ihm lediglich mitgeteilt worden, dass die Anweisung des Shop-Inhabers umgesetzt wurde.

Sowohl der Shop-Inhaber als auch der Telekommunikationsdienstleister, der der Aufsicht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit untersteht, haben in der Angelegenheit übereinstimmend Stellung genommen. Die Anfertigung einer Kopie von amtlichen Ausweisen sei von § 95 Abs. 4 TKG gedeckt. EC-Karten würden nur in Ausnahmefällen fotokopiert und zwar, wenn sich ein Kunde nur über einen Reisepass oder ein ausländisches Ausweispapier ausweisen könne. Die kopierten Unterlagen würden im Rahmen des monatlichen Versandes an den Telekommunikationsdienstleister weitergegeben und im Zuge des weiteren Prozesses von dem Telekommunikationsdienstleister vernichtet. Eine papiergebundene oder elektronische Speicherung der Unterlagen finde nicht statt, da diese allein der Legitimationsprüfung dienen.

Im Ergebnis wurde festgestellt, dass die Erstellung einer Kopie und kurzzeitige Aufbewahrung von amtlichen Ausweisdokumenten durch § 95 Abs. 4 TKG gedeckt sein kann. Die Fertigung einer Kopie der EC-Karte ist jedoch nicht durch diese Rechtsgrundlage legitimiert. Allerdings werden durch das Kopieren der EC-Karte grundsätzlich nicht mehr Daten erhoben, als bereits im Rahmen des Vertrages selbst angegeben wurden.

**Für gesetzlich** nicht geregelte Sachverhalte besteht grundsätzlich ein Vervielfältigungsverbot von Ausweisdokumenten. Dies beugt dem Entstehen von Ausweiskopie-Registern vor und es entstehen keine zusätzlichen Sicherheitsprobleme. Bei dem neuen Personalausweis würde dies beispielsweise dazu führen, dass die allein auf dem Ausweis abgedruckte Berechtigungsnummer in Umlauf gerät. Allerdings zeigt die praktische Notwendigkeit, dass ein striktes Kopierverbot nicht praktikabel ist. So kann bei der Einholung einer Auskunft auf der Grundlage des § 34 BDSG eine Person allein mit Name und Anschrift nicht eindeutig identifizierbar sein. Dies z. B. dann, wenn zu einem Namen mehrere Wohnaderessen gespeichert

sind. Hier lässt sich nicht ohne Weiteres erkennen, ob es sich um eine Namensgleichheit unterschiedlicher Personen handelt oder ob eine missbräuchliche Anfrage unter fremden Namen vorgenommen wird. Entscheidend ist aber, dass es sich um Ausnahmefälle handelt. In Anerkennung des praktischen Bedürfnisses für die Verwendung von Ausweiskopien wird erwogen, dem Gesetzgeber bei der nächsten Novelle des Personalausweis- und Passgesetzes ausdrückliche Regelungen zu Art und Umfang von Ausnahmen vom Kopierverbot vorzuschlagen. Dies würde zu einer spezialgesetzlichen Zulässigkeitsnorm führen.

Bis zu einer gesetzlichen Regelung ist **ZU BEACHTEN:**

Die Vorlage einer Kopie eines Ausweisdokumentes kann in begründeten Einzelfällen erforderlich sein. Ist es Ihnen nicht möglich, Ihre Identität persönlich durch Vorlage des Ausweisdokumentes zu belegen, achten Sie bitte darauf, dass die verantwortliche Stelle allein die Daten erhält, die zu Identifizierungszwecken unumgänglich sind (Name, Anschrift, Geburtsdatum). Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden und ist unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist. Eine automatisierte Speicherung der Pass-/Ausweisdaten ist unzulässig.

Sonstige Daten wie Zugangs- und Seriennummern, Angaben zur Größe, Augenfarbe, Passfoto sowie die maschinenlesbare Zone sollten geschwärzt werden.

Die Aufsichtsbehörde wird auch zukünftig verantwortliche Stellen darauf aufmerksam machen, dass die Betroffenen auf die Möglichkeit des Schwärzens hinzuweisen sind. Nur auf diesem Weg können die Grundsätze der Datensparsamkeit und Erforderlichkeit eingehalten werden.

Keine Bedenken bestehen im Übrigen hinsichtlich der Anfertigung einer „Sicherungskopie“ für und durch den Dokumenteninhaber (z. B. für Auslandsreisen) wenn diese dazu dient, im Falle des Diebstahls/Verlusts ein neues Ausweisdokument zu beantragen.

**In diesem Zusammenhang** ist ein Fall darzustellen, auf den ein LKW-Fahrer die Aufsichtsbehörde aufmerksam gemacht hat. Ein Stahlhandelunternehmens hatte abzuholende Ladung gegenüber dem Fahrpersonal von beauftragten Subunternehmen nur freigeben, nachdem der Personalausweis vorgelegt und kopiert worden war.

Zur Aufklärung des Sachverhaltes bat die Aufsichtsbehörde das Unternehmen um Ausführungen, zu welchem Zweck die Vorlage des Personalausweises verlangt wird und warum der Personalausweis kopiert wird. Zudem wurde gebeten, darzustellen, wie die Aufbewahrung der kopierten Unterlagen (Ort, Zugriffsregelungen, Löschfristen) erfolgt.

Das Stahlhandelsunternehmen sah die Datenerhebung auf Grundlage des § 7c des Güterkraftverkehrsgesetzes (GüKG) als zulässig an.

§ 7c GüKG ordnet jedoch weder eine Datenerhebung ausdrücklich an noch erlaubt es eine solche. Die Vorschrift stellt daher keine eigenständige Zulässigkeitsnorm dar und das Kopieren der Ausweise kann nicht darauf gestützt werden.

Da der originäre Zweck eines Frachtvertrages die Beförderung des Frachtgutes ist, diente das Kopieren von Ausweisdaten auch nicht der Vertragserfüllung. Folglich schied auch die Zulässigkeit der Erhebung der Daten auf der Grundlage des § 28 Abs. 1 Nr. 1 BDSG aus.

Im Ergebnis wurde festgestellt, dass die Zulässigkeit aus § 28 Abs. 1 Nr. 2 BDSG resultieren kann, allerdings allein hinsichtlich der zur Dokumentation erforderlichen Daten. Nach einer Kontrolle der Ausweise genügt eine schriftliche Aufzeichnung einzelner Daten wie Name, Anschrift, Geburtsort und Staatsangehörigkeit der Fahrer ohne gleichzeitiges Kopieren. Um sicherzustellen, dass die Ausweise kontrolliert worden sind, ist zudem beispielsweise das Notieren einzelner Ziffern der Ausweisnummern möglich.

***§ 7c GüKG - Verantwortung des Auftraggebers -***

*Wer zu einem Zwecke, der seiner gewerblichen oder selbständigen beruflichen Tätigkeit zuzurechnen ist, einen Frachtvertrag oder einen Speditionsvertrag mit einem Unternehmen abgeschlossen hat, darf Leistungen aus diesem Vertrag nicht ausführen lassen, wenn er weiß oder fahrlässig nicht weiß, dass der Unternehmer*

1. *nicht Inhaber einer Erlaubnis nach § 3 oder einer Berechtigung nach § 6 oder einer Gemeinschaftslizenz ist, oder die Erlaubnis, Berechtigung oder Lizenz unzulässig verwendet,*
2. *bei der Beförderung Fahrpersonal einsetzt, das die Voraussetzungen des § 7b Abs. 1 Satz 1 nicht erfüllt, oder für das er nicht über eine Fahrerbescheinigung nach Artikel 3 Abs. 1 der Verordnung (EWG) Nr. 881/92 verfügt,*
3. *einen Frachtführer oder Spediteur einsetzt oder zulässt, dass ein solcher tätig wird, der die Beförderungen unter der Voraussetzung von*
   *a) Nummer 1*
   *b) Nummer 2*
   *durchführt.*

*Die Wirksamkeit eines zu diesem Zwecke geschlossenen Vertrages wird durch einen Verstoß gegen Satz 1 nicht berührt.*

Die Aufsichtsbehörde empfahl zudem ein Merkblatt für die kontrollierten Fahrer zu fertigen, welches diesen von den Kontrolleuren bei Fragen zur Verfahrensweise vorgelegt werden kann. Erfahrungsgemäß können Kontrolleure bei Rückfragen nicht immer alle Bedenken der Kontrollierten hinsichtlich der Rechtmäßigkeit einer Verfahrensweise ausräumen. Ist jedoch aus einem Merkblatt ersichtlich, zu welchem Zweck die Daten erhoben werden, wie sie aufbewahrt werden, unter welchen Umständen ein Umgang mit den Daten erfolgt und wer für weitere Fragen als Ansprechpartner zur Verfügung steht, wird eine Vertrauensbasis geschaffen. So werden auch die obliegenden Unterrichtungspflichten nach § 4 Abs. 3 BDSG erfüllt. Darüber hinaus wurde für den Fall der nachfolgenden Nutzung der Daten empfohlen, zu dokumentieren, wer wann und aus welchem Grund ein vorhandenes Prüfprotokoll aus dem verschließbaren Aktenschrank entnommen hat.

**In einem anderen Fall** informierte eine Patientin die Aufsichtsbehörde über die Verfahrensweise eines Arztes. Dieser habe vor der Behandlung die Vorlage ihres Personalausweises erbeten und diesen fotokopiert. Soweit sich ein/e Patient/in mit dieser Vorgehensweise nicht einverstanden erklärte, wurde er/sie nicht behandelt.
Die nachfolgenden Ermittlungen der Aufsichtsbehörde dienten der Klärung, zu welchem Zweck die Personalausweise kopiert werden und ob alle aus dem Dokument ersichtlich werdenden Daten für diesen Zweck benötigt werden. Die Aufsichtsbehörde bat um Ausführungen zur Aufbewahrung der kopierten Unterlagen (Ort, Zugriffsregelungen, Löschfristen) und Zulässigkeit der Datenerhebung und -speicherung.
Die beschriebene Verfahrensweise betraf nach Angabe des Arztes eine kleine Gruppe von Patienten, die privat versichert sind und keinerlei Nachweis ihrer Versicherung erbringen. Die Vorlage des Personalausweises sei notwendig, um dem Erschleichen ärztlicher Leistungen durch unkorrekte Abrechnungsdaten vorzubeugen. Die Ausweiskopien wurden nach Begleichung der Arztrechnung zurückgegeben oder vernichtet. Sämtliche auf einer Ausweiskopie enthaltenen Daten (Personalausweisnummer, Lichtbild, Größe, Augenfarbe etc.) seien nicht erforderlich, die Unzulässigkeit der Erhebung und Speicherung bestimmter Daten wurde eingeräumt. Der Arzt teilte auch eine geänderte Verfahrensweise mit. Zukünftig werde – soweit dies nach Auffassung der Aufsichtsbehörde datenschutzkonform ist – die Vorlage des Personalausweises erbeten und von diesem Name, Adresse und Geburtsdatum als notwendige Daten notiert.
Eine solche Verfahrensweise ist auf Grundlage des § 28 Abs. 1 S. 1 Nr. 2 BDSG zulässig. Das Löschkonzept nach Begleichung der Rechnung für die erhobenen Daten ist dem Zweck angemessen gewesen.

**Schließlich wurden** der Aufsichtsbehörde Fälle bekannt, bei denen beim Kauf bestimmter Produkte, z. B. eines Handys ohne Kartensperre oder einer Kamera, unter Verweis auf etwaige Garantieansprüche, Name und Anschrift des Kunden notiert bzw. notiert werden sollten. Ein Elektronikunternehmen erläuterte, in welchen Verkaufsfällen es insbesondere zu einer Datenerhebung komme:

> Allgemein erfolge ein Verkauf von Waren gegen Kassenbon, daher sei hier keine Verarbeitung personenbezogener Daten erforderlich. Im Gewährleistungsfall reiche die Vorlage von Kassenbon und Ware aus.
>
> Beim Verkauf von „Prepaid-Handys“ würden auf der Grundlage von § 111 TKG Name, Vorname, Anschrift und Geburtsdatum erfasst.
>
> Bei hochpreisigen Waren (ggf. bereits ab 50,00 EUR) werde eine Rechnung gestellt und ausgedruckt. Dies diene der Zuordnung eines Gerätes mit Seriennummer im Rahmen eine Garantieabwicklung. Die Daten würden im Warenwirtschaftsystem erfasst.

Für den Verkauf eines Handys ohne Kartensperre mit einem Warenwert von ca. 40,00 EUR war keine Datenerhebung vorgesehen. Daher empfahl die Aufsichtsbehörde dem Unternehmen, seine Mitarbeiter hierüber durch ein Merkblatt zu unterrichten. Dieser Empfehlung kam das Unternehmen mit einer Organisationsmitteilung nach.

### 4.2.4 Speicherung/Aufbewahrung personenbezogener Daten

Häufig wenden sich Privatpersonen an die Aufsichtsbehörde, wenn sie von einer Auskunftei ein Schreiben erhalten haben, dass Daten über sie erstmalig übermittelt worden sind. Dadurch erhalten die Betroffenen Kenntnis darüber, dass die Auskunftei Daten über sie gespeichert hat und mit diesen Daten handelt. Damit kommen die Unternehmen ihrer Benachrichtigungspflicht aus § 33 Abs. 1 BDSG nach. In einem solchen Fall informiert die Aufsichtsbehörde zunächst die Betroffenen über die allgemeine Rechtslage und bietet an, gegebenenfalls die Zulässigkeit der Speicherung bestimmter Einzeldaten zu prüfen.

Bei den informierenden Unternehmen handelt es sich typischerweise um solche Unternehmen, welche sich in Bezug auf die Zulässigkeit der Datenerhebung und -verarbeitung im Rahmen der Geschäftstätigkeit auf § 29 BDSG – geschäftsmäßige Datenerhebung und -speicherung – berufen können. Aus diesem Grund ist nicht von vornherein davon auszugehen, dass der Umgang der Unternehmen mit personenbezogenen Daten grundsätzlich unzulässig erfolgte.

*Auskunfteien* sind Unternehmen, die Daten über Privatpersonen oder Unternehmen, insbesondere zu deren wirtschaftlicher Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit „sammeln“ und auf dieser Datenbasis Auskünfte über die wirtschaftlichen Verhältnisse erteilen. Derartige Auskünfte werden i. d. R. eingeholt, um wirtschaftliche Risiken zu senken. Die wohl bekannteste Auskunftei ist die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung). Sie ist eine Gemeinschaftseinrichtung der kreditgebenden Wirtschaft, d. h. solcher Unternehmen, die Kreditrisiken eingehen, z. B. Kreditinstitute, Kreditkartengeber, Leasinggesellschaften und Handels- und Telekommunikationsunternehmen. Weitere große Auskunfteien sind beispielsweise die Creditreform oder Bürgel.

Der Umgang mit personenbezogenen Daten durch Auskunfteien vollzieht sich typischerweise in verschiedenen Phasen. Zunächst erfolgt eine Erhebung von Daten bzw. eine Datenübermittlung von dem Geschäftspartner der Auskunftei zum Zweck der Speicherung und Beauskunftung der Daten durch die Auskunftei (Einmeldung).
Die Daten stammen jedoch nicht nur aus übermittelten Daten, sondern aus allgemein zugänglichen Quellen wie Telefon- und Adressbüchern, Branchenverzeichnissen oder öffentlichen Registern wie dem Handelsregister oder dem Schuldnerverzeichnis (§ 915e Abs. 1 ZPO).

Erheben, verarbeiten oder nutzen Auskunfteien personenbezogene Daten, unterliegen sie den Datenerhebungs- und Verwendungsvorschriften des BDSG. Die Zulässigkeit der einzelnen Verarbeitungsschritte richtet sich, sofern keine entsprechende Einwilligung nach § 4a BDSG der Betroffenen vorliegt, nach § 29 BDSG – Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung.

Neben Namen, Anschrift und Geburtsdatum werden gegebenenfalls auch Daten zum Einkommen und Vermögen, z. B. Tätigkeit, Arbeitgeber, Umsatz, Grundbesitz, Bankverbindung und Schulden gespeichert. Gespeichert wird auch, ob eine eidesstattliche Versicherung abgegeben, ein Zwangsversteigerungsverfahren betrieben, gegen den Betroffenen wegen Säumigkeit ein Haftbefehl angeordnet wurde oder ob vollstreckbare Schuldtitel vorliegen. Bei Unternehmen und gewerblich tätigen Einzelpersonen werden bei einigen Auskunfteien bei fehlenden Informationen auch „Schätzdaten“ gespeichert.

Die Aufsichtsbehörde empfiehlt Betroffenen von ihrem Auskunftsrecht gemäß § 34 BDSG gegenüber Auskunfteien Gebrauch zu machen. Denn nur wenn man weiß, wer, welche Daten, zu welchem Zweck über die eigene Person gespeichert hat, können etwaige Folgerechte (Datenberichtigung oder –löschung gemäß § 35 BDSG bei unrichtig oder unzulässig ge-

speicherten Daten) geltend gemacht werden. Sobald Anhaltspunkte bestehen, dass die gespeicherten Daten unrichtig oder unzulässig gespeichert werden, kann die Aufsichtsbehörde kontaktiert werden.

Zur Beurteilung der Zulässigkeit der Erhebung und Speicherung von personenbezogenen Daten hat sich in der Praxis die Einteilung der Daten in verschiedene Kategorien durchgesetzt. Unterschieden wird zwischen den sog. Negativdaten, welche weiche und harte Negativdaten umfassen, und den sog. Positivdaten. Letztere werden nicht von allen Auskunfteien in ihren Datenbestand aufgenommen.
Unter Positivdaten versteht man in der Regel alle Daten, die sich nicht auf vertragswidriges Verhalten des Betroffenen beziehen (z. B. Daten über die Beantragung, die Aufnahme, ordnungsgemäße Abwicklung und Beendigung einer Vertragsbeziehung). Die Positivdaten dürfen den Auskunfteien von ihren Geschäftspartner grundsätzlich nur aufgrund einer ausdrücklichen vorhergehenden Einwilligung i. S. d. § 4a BDSG übermittelt werden.
Negativdaten sind dagegen solche, die Auskunft über die nicht vertragsgemäße Abwicklung eines Vertrages geben und Rückschlüsse auf die Zahlungsunfähigkeit oder -unwilligkeit zulassen. Dabei sind harte Negativmerkmale solche, die aufgrund objektiver Tatsachen den Rückschluss auf die Zahlungsunfähigkeit oder -unwilligkeit erlauben (beispielsweise Angaben über die Durchführung eines Zwangsvollstreckungsverfahrens oder die Eröffnung eines Insolvenzverfahrens). Weiche Negativmerkmale lassen dagegen einen solchen Rückschluss nicht ohne Weiteres zu. Es handelt sich dabei um Angaben, die auf einer einseitigen Rechtsausübung des Geschäftspartners der Auskunftei beruhen, also etwa Angaben über Mahnungen, Kreditkündigungen, den Lohnabzug im Pfändungsverfahren oder Mahnbescheide. Die Erhebung und Speicherung der Negativmerkmale ist grundsätzlich nach § 29 Abs. 1 BDSG zulässig. Die „Einmelder“ müssen prüfen, ob die Voraussetzungen für eine Übermittlung der Daten an die Auskunftei vorliegen. Durch die Einführung des § 28a BDSG wird nunmehr seit dem 01.04.2010 gesetzlich definiert, unter welchen Voraussetzungen eine Datenübermittlung an Auskunfteien zulässig ist.

Neben Positiv- und Negativdaten gibt es noch die sog. Identifizierungs- oder Personenstammdaten (z. B. Name, Anschrift und Geburtsdatum/-ort).

Die Zulässigkeit der Speicherung personenbezogener Daten kann strittig sein. So prüfte die Aufsichtsbehörde einen Fall, in dem ein Kunde einen PC gekauft hatte, der nicht fehlerfrei arbeitete. Dies führte dazu, dass der Kunde einen Werkstattauftrag mit dem Inhalt „Hardwaretest durchführen zum Nachvollziehen des angegebenen Fehlers, Rückabwicklung bei Hardwarefehler“ bei dem Unternehmen, wo er den PC gekauft hatte, auslöste. Aus den

Schreiben des Unternehmens an den Petenten wurde ersichtlich, dass lediglich Softwarefehler festgestellt werden konnten. Aus Kulanz wurde der Kauf dennoch rückabgewickelt, der PC dem Petenten jedoch nicht zum Löschen der bereits auf dem PC gespeicherten Daten herausgegeben. Der Petent äußerte gegenüber der Aufsichtsbehörde den Verdacht, dass die auf dem PC vorhandenen Dateien unzulässig im Unternehmen gespeichert seien.

Im aufsichtsbehördlichen Verfahren ermittelte die Aufsichtsbehörde, dass das Unternehmen ein Testprotokoll als Nachweis dafür, dass der Rechner über mehrere Tage fehlerfrei gelaufen ist und somit keinen Hardwaredefekt aufweist, gespeichert hatte. Zudem wurde ein Systemprotokoll vorgehalten, aus dem hervorging, dass der Rechner vor der Überprüfung mit Viren verseucht war und fehlerhafte Installationen vorlagen. Diese Unterlagen waren unter dem Namen des Petenten gespeichert. Daher setzte die Aufsichtsbehörde durch, dass der Petent die vorgenannten Protokolle auf der Grundlage des § 34 BDSG erhielt.
Die Aufsichtsbehörde bezog in ihre Prüfung ein, dass nach der Rückabwicklung auf dem PC personenbezogene Daten gespeichert waren. Da der Computer nach den Ausführungen des Unternehmens nicht defekt war, musste das Unternehmen dafür Sorge tragen, dass die gespeicherten Daten gelöscht werden. Daher wurden die beschriebenen Prozesse zur Löschung etwaiger Daten innerhalb des Landesverwaltungsamtes fachlich beurteilt. Es wurde festgestellt, dass es nach Absolvieren des Prozesses zur Datenlöschung nicht möglich ist, Daten auf der Festplatte wiederherzustellen.
Im Ergebnis gab es bezogen auf den Umgang mit den auf dem zurückgegebenen Rechner gespeicherten personenbezogenen Daten und den übrigen gespeicherten personenbezogenen Daten keinen Grund zu Beanstandungen. Dem Auskunftsanspruch hätte das Unternehmen jedoch auch ohne aufsichtsbehördliches Einschreiten nachkommen müssen.

### 4.2.5. Übermittlung personenbezogener Daten

Eine Übermittlung personenbezogener Daten findet gemäß § 3 Abs. 4 Nr. 3 BDSG nicht nur bei der bloßen Übergabe von personenbezogenen Daten statt, sondern auch wenn Einsichts- oder Abrufmöglichkeiten geschaffen werden. Auf die Art der Bekanntgabe kommt es nicht an. Diese kann z. B. schriftlich, mündlich, fernmündlich, durch körperliche Weitergabe von Datenträgern oder mit Hilfe elektronischer Medien erfolgen. Eine Übermittlung setzt auch nicht voraus, dass der Empfänger konkret bekannt ist.

Auch in der vergangenen Berichtsperiode wurden der Aufsichtsbehörde zahlreiche Sachverhalte geschildert, die eine Übermittlung darstellen. Die Fallbeispiele reichen vom Anruf eines neuen Arbeitgebers beim alten Arbeitgeber bis zur Entsorgung von Unterlagen mit personenbezogenen Daten im Hausmüll oder in der Papiertonne.

Quedlinburg-**AUSVERKAUF**

Alles muss raus… Aber müssen Unterlagen mit personenbezogenen Daten (z. B. Bewerbungsunterlagen) in der Papiertonne jedermann zugänglich sein?

Quelle: Bild

In nebenstehendem Fall prüfte die Aufsichtsbehörde zunächst, ob die Unterlagen sichergestellt wurden. Gleichzeitig wurde eine Vorortprüfung am Fundort durchgeführt, da auch die Beschaffenheit und die Zugänglichkeit des Entsorgungscontainers für die Aufsichtsbehörde relevant waren.
Nachdem der Aufsichtsbehörde die sichergestellten Unterlagen übergeben wurden, ermittelte die Aufsichtsbehörde gegenüber der verantwortlichen Stelle.

Im Ergebnis wurde festgestellt, dass das Unternehmen Bewerbungsunterlagen, die nicht berücksichtigt werden konnten, grundsätzlich an die Bewerber zurücksandte. Im Rahmen der Geschäftsräumung sollten die noch vorhandenen Unterlagen einer ordnungsgemäßen Vernichtung zugeführt werden. Sie seien in entsprechend bezeichnete Kartons verpackt worden, jedoch versehentlich von einem Umzugshelfer im Container entsorgt worden. Der Vorfall wurde bedauert.
Die Aufsichtsbehörde führt diesbezüglich ein Ordnungswidrigkeitenverfahren wegen unzulässiger Datenübermittlung durch.

**Die Aufsichtsbehörde** prüfte weiterhin Sachverhalte, in denen Privatpersonen personenbezogene Daten ins Internet stellten, so z. B. ausführliche Berichte über Rechtsstreitigkeiten mit dem Ex-Vermieter und Werturteile über die Persönlichkeit des Ex-Vermieters.
In derartigen Sachverhalten sind zwei Grundrechtspositionen betroffen, das Recht auf freie Meinungsäußerung und das im Datenschutzrecht relevante Persönlichkeitsrecht. Da beim Zusammentreffen von Grundrechten weder dem einen noch dem anderen Vorzug zu gewähren ist, hatte die Aufsichtsbehörde das Recht auf freie Meinungsäußerung bei der Prüfung ebenfalls einzubeziehen. Da keine Einwilligungserklärung des Betroffenen zur Datenübermittlung vor und auch keine andere Rechtsvorschrift die umfassende Datenübermittlung erlaubte, konnte sich die Zulässigkeit allein aus dem Bundesdatenschutzgesetz selbst ergeben. Die Vorschriften waren allerdings unter dem Aspekt auszulegen, dass vorrangig eine Abwägung der Schwere der Persönlichkeitsrechtsverletzung durch die Äußerung/en einer-

seits und der Einbuße an Meinungsfreiheit durch die Untersagung der Äußerung andererseits vorzunehmen ist. Für die Intensität der Beeinträchtigung des Persönlichkeitsrechts kommt es auf die Art und Weise der Darstellung, insbesondere auf den Grad der Verbreitung des Mediums an.
Im zu beurteilenden Fall lösten zeitlich weit zurückliegende rechtliche Streitigkeiten eine derart spekulative Berichterstattung aus, zu der keine hinreichenden Gründe des Gemeinwohls vorliegen, die das Recht auf informationelle Selbstbestimmung zulässig beschränken. Ins Gewicht fällt dabei auch, dass die Internetveröffentlichung weltweit von jedem Rechner mit Internetzugang abgerufen werden kann und nicht nur von etwaigen Betroffenen des regionalen Umfeldes. Im zu prüfenden Fall lag bereits ein Urteil vor und der zu Grunde liegende Sachverhalt wurde abschließend behandelt. Die Aufsichtsbehörde sah die schutzwürdigen Belange des Betroffenen als überwiegend an und beurteilte die Übermittlung trotz Meinungsäußerungsfreiheit als unzulässig.

**Nicht unerwähnt** soll folgender Fall bleiben: Ein Rechtsanwalt informierte den Arbeitgeber eines privaten Vermieters darüber, dass der Vermieter im Rahmen eines Verfahrens auf Eigenbedarfskündigung den Briefkopf des Auftraggebers im privaten Bereich nutzte. Darüber hinaus übermittelte er durch die Übersendung der entsprechenden Schreiben in ungeschwärzter Form auch sämtliche Angaben zu der privaten Auseinandersetzung des Vermieters mit seinem Mandanten. Eine solche Verfahrensweise ist nicht erforderlich gewesen und daher unzulässig.

### 4.2.6. Nutzung personenbezogener Daten für Zwecke der Werbung

Um den eigenen Briefkasten vor kostenlosen Zeitungen und Prospekten zu „retten“, nutzen zahlreiche Haushalte den Aufkleber am Briefkasten mit der Aufschrift „Bitte keine Werbung“. Dieser hilft in der Regel, den Einwurf von Flyern, Prospekten und „an alle Haushalte“ adressierten Schreiben zu verhindern. Andere Haushalte stehen dieser Art von Werbung aufgeschlossen gegenüber, da sie Informationsmöglichkeiten bietet. Zudem sind diese Werbematerialien schnell entsorgt. Dies gilt allerdings nicht für adressierte Schreiben, hinter denen zunächst etwas Wichtiges, Persönliches vermutet wird. Umso größer ist die Verärgerung, wenn man die Briefe öffnet und Werbung für Kredite, Arznei- und Potenzmittel offenbar wird. Unverlangte adressierte Werbung wird zunehmend als störend empfunden, zumal sich häufig die Frage stellt, woher der Absender die genutzte Anschrift hat.

Die Wege für den Bezug von Adressdaten sind verschieden. Einige Unternehmen führen Preisausschreiben, Verlosungen oder Informationsveranstaltungen durch, um an Anschriften und werberelevante Informationen zu gelangen. Auch Kundenbindungs- und Rabattsysteme dienen häufig diesem Zweck. Viele Werbende greifen darüber hinaus auch auf Adressbestände von sogenannten Adresshändlern zurück. Diese vermieten oder verkaufen speziell nach den Wünschen ihres Kunden, den werbenden Unternehmen, zugeschnittene Adressdaten, die sie meist aus der Auswertung öffentlich zugänglicher Quellen (Adress- und Telefonbücher, Branchenverzeichnisse, Handels- und Vereinsregister etc.) ermittelt haben. Manche Unternehmen erhalten die Werbebotschaft vom werbenden Unternehmen und versenden die Schreiben selbst, indem sie jeweils die Anschriften ergänzen (sog. Lettershop-Verfahren). In derartigen Fällen ist es möglich, dass das werbende Unternehmen noch gar keine personenbezogenen Daten von dem von der Werbung Betroffenen erhält. In den Besitz der Daten gelangt das Unternehmen erst durch den Betroffenen selbst, nämlich indem dieser auf die Werbung reagiert.

Die Aufsichtsbehörde überprüfte im vergangenen Berichtszeitraum auch zahlreiche Fälle im Zusammenhang mit unerwünschter Werbung.

**Ein Ehepaar** wurde von einem Unternehmen für Büroorganisation telefonisch kontaktiert. Die Eheleute beschwerten sich direkt beim Unternehmen und baten, auch weil unaufgeforderte Werbung per Telefon untersagt ist, um Auskunft über die Herkunft der genutzten Daten. Sie verwiesen auf § 34 BDSG und baten um sofortige Löschung der Daten. Binnen einer Woche teilte das Unternehmen den Eheleuten den Verkäufer der Firmendatei mit. Unter den gekauften 1.000 Firmenadressen seien ca. 10 Privatanschlüsse unwissend kontaktiert worden. Das Unternehmen entschuldigte sich. Geschäfte mit Privatpersonen seien zu keinem Zeitpunkt beabsichtigt gewesen, daher habe die Mitarbeiterin auch nachgefragt, wer in dem Haus der Familie – der vermuteten Firma – für Bürobedarf zuständig sei. Da das Ehepaar schon länger das Problem hat, dass die private Telefonnummer mit einer nicht bestehenden geschäftlichen Tätigkeit verknüpft ist, baten sie die Aufsichtsbehörde um nähere Prüfung.
Im Rahmen der aufsichtsbehördlichen Ermittlungen wies die verantwortliche Stelle nach, dass allein Daten von Firmen und Freiberuflern erworben werden sollten. Die gelieferten Daten wurden vorgelegt und geprüft.
Ein vorsätzlicher oder fahrlässiger Verstoß des Unternehmens gegen datenschutzrechtliche Bestimmungen konnte nicht festgestellt werden. Das Unternehmen hat sich für die unzulässige, aber unbeabsichtigte Nutzung der Telefondaten der Betroffenen entschuldigt und die Konsequenz gezogen, von dem Adresslieferanten keine Daten mehr zu beziehen.

**In weiteren Fällen** erhielten Privatpersonen jeweils eine Gewinnbenachrichtigung eines Unternehmens. Aus der Gewinnbenachrichtigung ging hervor, dass das Unternehmen sowohl die Anschrift als auch die Telefonnummer der Betroffenen besitzt und diese Daten aus der Teilnahme an einem bestimmten Kreuzworträtsel resultieren sollen. Beide Betroffene gaben bei der Aufsichtsbehörde jedoch an, weder das Unternehmen zu kennen, noch an einem Kreuzworträtsel teilgenommen zu haben. Ein Betroffener beurteilte das Vorgehen des Unternehmens als betrügerische Handlung, mit der „unbedarfte Menschen zu etwas verleitet werden sollen".
Die Aufsichtsbehörde konnte ihre Ermittlungen leider nicht abschließen, da das Unternehmen im Laufe des Verfahrens das Gewerbe abmeldete.

Die Aufsichtsbehörde rät nicht von der Teilnahme an Gewinnspielen ab, gibt jedoch folgende Hinweise:

1. Auf Gewinnbenachrichtigungen, denen kein eigenes aktives Handeln vorausgegangen ist, sollte nicht reagiert werden. Niemand hat etwas zu verschenken!
2. Sofern an einem Gewinnspiel teilgenommen werden soll, wird empfohlen, insbesondere die Ausführungen zum Datenschutz bzw. der Datenverarbeitung genau zu lesen. Sollte die Verarbeitung der angegebenen Daten über die Gewinnabwicklung hinaus vorgesehen sein, empfiehlt es sich, von dem Werbewiderspruchsrecht Gebrauch zu machen. Dies kann durch Streichen einer entsprechenden Passage oder zu jedem späteren beliebigen Zeitpunkt ohne Angabe von Gründen erfolgen.

Über die datenschutzrechtlich relevanten Aspekte hinaus entdeckte die Aufsichtsbehörde in Verbraucherschutzforen **„pfiffige Hinweise"**, die sich auf eine Gewinnbenachrichtigung im Zusammenhang mit sog. Kaffeefahrten beziehen:

„Bei diesen Benachrichtigungen geht es weder um die Übergabe eines Gewinns noch um einen Ausflug, sondern um eine Verkaufsveranstaltung.
Wenn Sie möchten, schicken die die Antwortkarte **ohne** Porto unter Nennung mehrer Personen ab. Fahren Sie aber **nicht** mit!
Informieren Sie die lokale Presse, damit potentielle Interessenten gewarnt werden können."

**Neben Werbung per Post** wird auch Werbung mittels E-Mail verschickt. Der Versand eines Unternehmensnewsletters ist dabei eine häufige Werbemaßnahme. In zwei der Aufsichtsbehörde geschilderten Fälle vermittelte der Newsletter den angeschriebenen Personen den Eindruck, diese hätten sich selbst durch Anmeldung beim werbenden Unternehmen für den Newsletter-Service entschieden bzw. per „Double Opt In" bei einem Partner für den Service eingetragen.

**Begriffserläuterung:**
Das „Double Opt In“ Verfahren ist zweistufig aufgebaut. In einem ersten Schritt erfolgt eine Anmeldung zum Newsletter oder die Bestellung einer Ware auf einer Website. Der Anmelder/Besteller muss dann in einer Bestätigungsmail bzw. in einem Aktivierungslink seine Anmeldung/Bestellung bestätigen.

Die Ermittlungen der Aufsichtsbehörde bestätigten die Aussagen der Betroffenen. Diese hatten weder mit dem werbenden Unternehmen noch mit etwaigen Partnern in Kontakt gestanden. Die Daten waren gekauft worden. Auf das Tätigwerden der Aufsichtsbehörde wurden die Datensätze der Betroffenen beim werbenden Unternehmen gelöscht und das Vertragsverhältnis mit dem Datenlieferanten gelöst. Die Aufsichtsbehörde ermittelte weiterhin, aus welchen Quellen der Vertragspartner die Daten der Betroffenen – bestehend aus Anrede, Vorname, Nachname, Straße und Hausnummer, Postleitzahl und Ort, E-Mail-Adresse und IP-Adresse – erhalten hat. Zudem rügte die Aufsichtsbehörde, dass die Betroffenen entgegen § 28 Abs. 4 BDSG nicht über das ihnen zustehende Werbewiderspruchsrecht unterrichtet worden waren.

**Formulierung Ihres Werbewiderspruchs**

„Ich widerspreche der Nutzung oder Übermittlung meiner Daten für Zwecke der Werbung und/oder für die Markt- oder Meinungsforschung.“

Auch können Sie bereits bei Vertragsabschlüssen auf Vertragsformularen folgenden handschriftlichen Vermerk anbringen: „Bitte keine Übermittlung oder Nutzung meiner Daten zu Werbezwecken!“. Seriöse Vertragspartner respektieren diesen Vermerk.

**Weitere praktische Tipps**

Der Briefkastenaufkleber „Keine Werbung bitte“ schützt vor Werbematerial, das **nicht persönlich** an Sie adressiert ist. Die Zusteller von Werbematerial müssen sich an Ihren auf diesem Weg geäußerten Wunsch halten. Tun sie es nicht, können Sie selbst oder ein Verbraucherverband gegen das Verteiler- bzw. Werbeunternehmen rechtlich vorgehen.

Um sich vor adressierten Werbezuschriften zu schützen, bietet der private Deutsche Dialog-Marketing-Verband (DDV) Verbraucherinnen und Verbrauchern an, sich in die sogenannte Robinsonliste eintragen zu lassen. Ein Formular für die Aufnahme in die Robinsonliste erhalten Sie bei DVV Robinsonliste, Postfach 1401, 71243 Ditzingen oder online auf der Verbraucherwebsite www.ichhabediewahl.de. Die dem DDV angeschlossenen Unternehmen erhalten dann die Nachricht, dass Sie keine Werbung wünschen. In der Regel überprüfen die ange-

schlossenen Unternehmen ihre Adresslisten anhand der Robinsonliste.

Auch können Sie die Annahme an Sie adressierter Werbebriefe verweigern. Dazu streichen Sie Ihre Adresse durch, vermerken Sie „Zurück an Absender“ und schicken den Brief unfrankiert zurück. Gewissenhafte Unternehmen werden nachfolgend Ihre Anschrift auf ihre interne „Sperrliste“ setzen.

**In zahlreichen** Fällen informierten Betroffene die Aufsichtsbehörde über unerwünschte Werbeanrufe. Eine Betroffene wies auf Anrufe einer „Bundeszentrale Berlin“ hin. In den Anrufen bot das Unternehmen ihr an, sie gegen Zahlung eines Mitgliedsbeitrages von unerwünschten Werbeanrufen „zu befreien“. Die Aufsichtsbehörde konnte in diesem Fall jedoch keine verantwortliche Stelle ermitteln und daher nur allgemeine Hinweise geben.

Bei Werbeanrufen sind sowohl das Bundesdatenschutzgesetz und das Gesetz gegen unlauteren Wettbewerb zu beachten. Die Bundesagentur, die unerlaubte Werbeanrufe nach dem Gesetz gegen unlauteren Wettbewerb ahndet, benötigt für ihre Ermittlungen ebenso wie die Aufsichtsbehörde für den Datenschutz, detaillierte und nachvollziehbare Anzeigen, die möglichst folgende Angaben beinhalten sollten:

- genaue Information über das Datum, die Uhrzeit des Anrufs sowie die ggf. angezeigte Rufnummer und
- sofern bekannt, konkrete Namen der Anrufer, beworbene Produkte und Dienstleistungen sowie Information über das anrufende oder werbende Unternehmen.

**Die** Aufsichtsbehörde stellte auch fest, dass die anrufenden Unternehmen oft bereits über Bankverbindungsdaten verfügen. Im Rahmen der Anrufe sollen Dienstleistungen vermittelt und versucht werden, die Kontodaten zu „legalisieren“. Zum Beispiel wird der Angerufene nach bestimmten Daten gefragt, damit er diese gegebenenfalls korrigiert. Die Aufsichtsbehörde kann in diesem Zusammenhang nur raten, keine Bankverbindungsdaten am Telefon preiszugeben. Jedes seriöse Unternehmen wird bei Bedenken des Angerufenen bereit sein, diese Daten gesondert und schriftlich zu erfassen. Denn können Sie sich sicher sein, dass hinter dem Anrufer auch tatsächlich das Unternehmen steht, für das sich ausgegeben wird?

Sofern sich Betrüger als Datenschützer ausgeben, hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in seiner Pressemitteilung vom 14. Mai 2010 Folgendes geraten:

•Keine Datenschutzaufsichtsbehörde würde von sich aus Bürgerinnen und Bürger anrufen, um ihre Hilfe anzubieten. Notieren Sie sich, falls ersichtlich, die Rufnummer und beenden das Gespräch sogleich durch Auflegen des Telefonhörers.
•Machen Sie auf keinen Fall persönliche Angaben und hüten Sie sich insbesondere davor, Bankverbindungsdaten bekannt zu geben.
•Sollte durch das Telefongespräch doch ein Vertrag zustande gekommen sein, können Betroffene, die nicht ordnungsgemäß über ihr Widerrufsrecht belehrt worden sind, alle per Telefon geschlossenen Verträge über Dienstleistungen noch bis zur vollständigen Bezahlung schriftlich widerrufen.
•Kontrollieren Sie regelmäßig Ihre Bankauszüge. Da Banken Lastschriftberechtigungen nicht prüfen, sollte spätestens bei der Kontrolle der Kontoauszüge und einer unberechtigten Lastschrift gehandelt und unverzüglich der Lastschrift widersprochen werden. Zu Unrecht abgebuchtes Geld kann bei der Bank bis zu sechs Wochen nach der Abbuchung ohne Begründung zurückgerufen werden.
•Sollten Sie zuvor bereits auf die unseriösen Anrufe eines Gewinnspielunternehmens hereingefallen sein, wenden Sie sich deswegen an eine Verbraucherschutzzentrale.
•Melden Sie Rufnummernmissbrauch und unerlaubte Telefonwerbung der Bundesnetzagentur als zuständiger Aufsichtsbehörde. Formblätter für entsprechende Beschwerden werden auf deren Internetseite angeboten.

### 4.2.7 Gewinnspiele

Wie das Gewinnspiel zu einem Minusspiel werden könnte, veranschaulicht folgender Sachverhalt: Ein Unternehmen rief bei einer Betroffenen an und verlangte 380,00 EUR von ihr. Grund dafür sei, dass sich die Betroffene nach Abschluss eines Gewinnspielvertrages im November 2008 nicht bei dem Unternehmen gemeldet habe. Als die Betroffene antwortete, von dem bezeichneten Vertrag keine Kenntnis zu haben, drohte die Anruferin, den Vorgang einem Anwalt zu übergeben. Nach Diskussionen offerierte die Anruferin, ein Angebot welches jedoch „nicht verraten“ werden solle – „Wenn ein dreimonatiger Vertrag mit monatlicher Zahlung von 34,80 EUR akzeptiert werde, würden die 380,00 EUR aus dem vorgenannten Vertrag erlassen werden“. Weiterhin wurden die Daten der Betroffenen, darunter auch die Kontoverbindung, abgeglichen. Die Betroffene notierte sich die Telefonnummer der Anruferin und die Anschrift des Unternehmens. Nachfolgend rief sie die Telefonnummer an, um zu prüfen, ob sich die verantwortliche Firma meldet. Die Telefonnummer war einem Privatanschluss zugeordnet. Der Inhaber des Anschlusses war bereits mehrfach angerufen worden und hatte auf diese Art und Weise bereits von der „Praxis der Bedrohung mit 380,00 EUR“ Kenntnis erlangt.

Dieser Fall belegt anschaulich, mit welchen Methoden Betroffene bei unerwünschten Telefonanrufen konfrontiert werden. Nicht selten stellt sich beim Anruf heraus, dass Kontodaten des Verbrauchers bereits bekannt sind. Bei den Anrufen sollen typischerweise die persönlichen Daten abgeglichen werden und/oder Gewinnspielabonnements, die Teilnahme an Lotterien oder sonstige Dienstleistungsverträge aufgeschwatzt oder untergeschoben werden. Obwohl die Betroffenen die telefonischen Angebote meist ablehnen, kommt es vor, dass kurze Zeit später Abbuchungen von dem abgeglichenen Bankkonto vorgenommen werden. Kontrolliert ein Betroffener seine Abbuchungen nicht regelmäßig und macht unerlaubte Ab-

buchungen nicht rückgängig, hat er neben dem unzulässigen Umgang mit seinen personenbezogenen Daten auch einen materiellen Schaden.
Um an Daten der Betroffenen zu gelangen, gibt es verschiedene „Geschäftsmodelle“. Am verbreitetsten ist das „Ja-Modell“: Die Betroffenen werden stets in Gespräche verwickelt, bei denen zunächst Fragen gestellt werden, die vom Angerufenen erwartungsgemäß nur mit „ja“ beantwortet werden. (Sind Sie Frau Müller? Ist es nicht schlimm, wie Griechenland die Euro-Krise verursacht? Ist das nicht ein scheußliches November-Wetter?). Sodann wird versucht, den Angerufenen so viele Informationen wie möglich zu entlocken. So wird etwa eine falsche Bankverbindung genannt, damit sie der überrumpelte Verbraucher ohne nachzudenken korrigiert. Sofern den Betroffenen bereits die korrekte Kontoverbindung mitgeteilt wird, stellt sich die Frage, woher diese Daten resultieren. Eine allgemeingültige Antwort auf diese Frage gibt es kaum, denn die Wege der illegalen Datenbeschaffung sind vielfältig. In der Vergangenheit stammten die meisten Datensätze aus Beständen von Glücksspielunternehmen. Entweder haben unzuverlässige Mitarbeiter Firmendatenbestände kopiert und weiterverkauft oder ein zwischengeschaltetes Call-Center hatte die Daten nach Abschluss ihrer Aufträge nicht gelöscht, sondern gesammelt und unbefugt weiterverwendet. Die Datenbestände können allerdings auch aus der Inanspruchnahme von Internetdiensten, aus dem Zeitschriftenvertrieb, aus Spendensammlungen, von Preisausschreiben oder aus Kundenbeständen anderer Unternehmen resultieren.

Verständlicherweise stellt sich der eine oder andere Leser die Frage, wie es möglich sein kann, mit illegal erworbenen Kontodaten Abbuchungen zu erwirken. Denn grundsätzlich dürfen Dritte ohne eine zuvor erfolgte Einzugsermächtigung des Kontoinhabers keine Beträge vom fremden Konto abbuchen. Im sog. Lastschriftverfahren ist dies dennoch möglich, da dies wie folgt abläuft:
Der Einzugsberechtigte übergibt seinem Geldinstitut ein als Lastschrift ausgewiesenes Formular, in dem Name und Bankverbindung des Zahlungspflichtigen sowie der abzubuchende Betrag angegeben sind. Das Geldinstitut wendet sich daraufhin an die Bank des Zahlungspflichtigen, die aufgrund der erklärten Einzugsermächtigung das Konto des Zahlungspflichtigen belastet. Im Massenverfahren der Lastschrifteinlösung werden Abbuchungen im Wege einer sog. Inkassovereinbarung zugelassen. Die Ermächtigung des Kontoinhabers zum Einzug der Lastschrift wird daher nur stichprobenartig und nicht in jedem Einzelfall überprüft. Der Zahlungsempfänger muss sich nur vorab verpflichten, die Einzugsermächtigung auf Verlangen vorzulegen. Wie Sie sich dennoch gegen derartige Geschäfte mit Ihren Bankdaten zur Wehr setzen können, zeigt die nachfolgende Übersicht:

## Was kann ich tun?

- **Was kann ich tun, wenn bereits Geld von meinem Konto abgebucht wurde?**

Nachdem Sie von einer rechtswidrigen Lastschriftabbuchung Kenntnis erlangt haben, können Sie diese bei Ihrem Geldinstitut innerhalb von einer Frist von 6 Wochen ohne Begründung widerrufen. Der abgebuchte Betrag wird Ihrem Konto problemlos wieder gutgeschrieben. Dies setzt voraus, dass Sie Ihre Kontobewegungen regelmäßig kontrollieren.

- **Wie kann ich zukünftig unerlaubte Abbuchungen verhindern?**

Im Fall des Missbrauchs Ihrer Kontodaten kann es u. U. angezeigt sein, von Ihrer Bank den Wechsel Ihrer Kontonummer zu verlangen. Denn sind Ihre Daten einmal im Umlauf und kann weder von der Quelle, noch von weiteren Empfängern eine effektive Datenlöschung verlangt werden, kann es erneut zu unberechtigten Abbuchungen kommen.

- **Sollte ich einen Strafantrag stellen?**

Sollte von Ihrem Konto unberechtigerweise Geld abgebucht worden sein, kann dies sowohl den Tatbestand des Betruges erfüllen, als auch eine strafbewehrte unbefugte Datenverarbeitung (§ 44 BDSG) darstellen. Daher ist **unbedingt** zu empfehlen, nach dem Zurückholen des Geldes (**1. Priorität**) Strafantrag zu stellen.

- **Wie kann ich zukünftig vermeiden, dass meine Adresse, Telefon- und Kontonummer in Umlauf gelangen?**

Zum präventiven Schutz ist immer wieder zu empfehlen, mit dem Angeben persönlicher Daten sparsam umzugehen.

Vermeiden Sie die Weitergabe Ihrer Daten am Telefon und im Internet (Achtung: sog. Pishing-Mails erwecken den Eindruck, dass Sie Ihre Zugangsdaten [z. B. der Bank] bestätigen sollen. Derartiges würde ein seriöser Anbieter jedoch nicht per Internet veranlassen).

Geben Sie insbesondere Konto- und Telefonverbindungsdaten nur an, wenn dies zwingend notwendig ist und Ihnen Ihr Vertragspartner zuverlässig erscheint.

Weiterhin wird dringend empfohlen, bei Vertragsabschlüssen nicht in die Weitergabe Ihrer Daten an Dritte einzuwilligen, auch nicht im „Kleingedruckten“. Sofern Ihnen etwas nicht plausibel erscheint, sollten Sie nachfragen. Erhalten Sie auf Ihre Fragen keine befriedigende, sondern eine ausweichende oder sogar abweisende Antwort, sollten Sie Ihrem „Bauchgefühl des Misstrauens“ folgen und keine näheren Angaben machen. Unternehmen sind nämlich gesetzlich verpflichtet, Sie zu informieren, zu welchem Zweck Ihre Daten verwendet werden.

Schließlich kann nur davon abgeraten werden, am Telefon Kontodaten preiszugeben. Seriöse Unternehmen werden auch nach einem telefonisch zustande gekommenen Kontakt die für die Bezahlung notwendigen Informationen schriftlich einholen.

- **An wen kann ich mich bei einem Missbrauch meiner Daten wenden?**

Wenn es um Verbraucherschutzfragen im Allgemeinen geht, können Sie sich an die örtlichen Verbraucherzentralen wenden. Für konkrete Fragen im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten sind die Aufsichtsbehörden für den Datenschutz die richtigen Ansprechpartner.

### 4.2.8 Löschung personenbezogener Daten

In vielen der Aufsichtsbehörde bekannt gewordenen Fällen wird statt der Berichtigung oder der Sperrung personenbezogener Daten die Löschung personenbezogener Daten erbeten. Das Recht auf Löschung ist ein den Betroffenen zustehendes Recht. Es ermöglicht dem Betroffenen ggf. rechtswidrige Verarbeitungen personenbezogener Daten zu unterbinden und damit sein Recht auf informationelle Selbstbestimmung durchzusetzen.

Welche Bedeutung der Gesetzgeber den Rechten der Betroffenen beimisst, wird dadurch deutlich, dass die Rechte auf Berichtigung, Löschung und Sperrung nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können und die Ausübung der Rechte für den Betroffenen grundsätzlich keine Kosten verursacht.

**Begriffserläuterungen:**

Die *Löschung* personenbezogener Daten bedeutet die Unkenntlichmachung der bei einer verantwortlichen Stelle gespeicherten Daten.

Die Betroffenen machen diese Rechte in der Regel dann geltend, wenn sie der Auffassung sind, dass ein Unternehmen ihre Daten nicht mehr benötigt, z. B. weil ein Rechtsgeschäft nicht zustande gekommen ist oder weil sie nicht wissen, wofür ihre Daten nachfolgend genutzt werden.

Eine verantwortliche Stelle ist nur in den in § 35 Abs. 2 S. 2 BDSG normierten Fällen zur Löschung personenbezogener Daten verpflichtet. Unabhängig davon kann die verantwortliche Stelle eine Löschung grundsätzlich jederzeit vornehmen. An die Stelle der Löschung kann allerdings auch die Sperrung der Daten gemäß § 35 Abs. 3 BDSG treten. Dies ist z. B. der Fall,

***§ 35 BDSG – Berichtigung, Löschung und Sperrung von Daten***

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

wenn sich aus den Regelungen des Handelsgesetzbuches (§ 257 HGB) und der Abgabenordnung (§ 147 AO) Aufbewahrungsfristen für die folgenden bestimmten Daten ergeben: Kundenadresse, Auftragsdatum, bestellte Artikel, Lieferdatum und Datum des Ausgleichs des Kundenkontos.

Spezialgesetzliche Aufbewahrungsfristen führen allerdings nicht dazu, dass die davon betroffenen Daten weiter für Zwecke der Werbung genutzt werden dürfen, wenn ein Betroffner das ihm zustehende Werbewiderspruchsrecht geltend gemacht hat. 28 Abs. 3 Nr. 3 BDSG erlaubt die Nutzung von bestimmten Daten für Zwecke der Werbung nämlich nur so lange wie der Betroffene der Nutzung nicht widerspricht. § 35 Abs. 3 BDSG führt allein dazu, dass die Daten für die spezialgesetzlich vorgesehenen Zwecke aufbewahrt werden dürfen.

Eine Sperrung führt zum Kennzeichnen gespeicherter personenbezogener Daten, deren weitere Verarbeitung und Nutzung einzuschränken ist.

*1. ihre Speicherung unzulässig ist,*
*2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,*
*3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder*
*4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.*

*Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.*

*Abs. 3: An die Stelle einer Löschung tritt eine **Sperrung**, soweit*

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

Personenbezogene Daten, die eine verantwortliche Stelle im Zusammenhang mit einem Bewerbungsverfahren erhalten hat, sind grundsätzlich nach Abschluss eines Bewerbungsverfahrens **zu löschen**.

Auch im vergangenen Berichtszeitraum wandten sich Betroffene an die Aufsichtsbehörde mit der Bitte um Klärung des „Verbleibs von Bewerbungsunterlagen".

Konkret hatte sich eine Frau auf eine Stellenanzeige beworben und ihren Unterlagen sogar einen Freiumschlag beigefügt. Trotz mehrfacher schriftlich geäußerter Bitte um Rücksendung der Unterlagen, habe das Unternehmen nicht reagiert.

Bewerbungsunterlagen einer Person (ausgenommen das an den potentiellen Arbeitgeber gerichtete Anschreiben), egal ob sie per Post oder auf elektronischen Wege übersandt werden, bleiben grundsätzlich weiterhin deren Eigentum. Eine Firma ist daher verpflichtet, die Unterlagen sorgfältig aufzubewahren und diskret zu behandeln. Wenn ein Anstellungsverfahren abgeschlossen ist, müssen die Unterlagen der nicht berücksichtigten Bewerber zurückgegeben bzw. vernichtet werden. Die im Rahmen des Bewerbungsverfahrens erhobenen personenbezogenen Daten sind nach § 35 Abs. 2 Ziffer 3 BDSG zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die Art und Weise der Löschung ist gesetzlich nicht vorgeschrieben. Zurückbehalten darf der Arbeitgeber allein die Unterlagen, die an ihn gerichtet sind, wie z. B. Bewerbungsanschreiben, Personalfragebögen, graphologische Gutachten und Referenzauskünfte. Die Löschungsverpflichtung wirkt daher differenziert.

Ggf. können Bewerbungsunterlagen für eine bestimmte, im Voraus festgelegte Dauer, mit Zustimmung der Bewerber aufbewahrt werden, wenn anzunehmen ist, dass sie demnächst z.B. für eine später zu besetzende Stelle wieder gebraucht werden.

In dem geschilderten Fall teilte die verantwortliche Stelle mit, dass nach eingehender Prüfung weder Bewerbungsunterlagen der Betroffenen vorliegen, noch personenbezogene Daten zu ihr gespeichert seien. Soweit die Betroffene nähere Anhaltspunkte zu der Bewerbung in dem Unternehmen habe, z.B. eine Eingangsbestätigung oder einen Zustellnachweis, werde erneut geprüft. Da die Petentin keine weiteren Auskünfte zur Sachverhaltsklärung machen konnte, prüfte die Aufsichtsbehörde den Umgang des Unternehmens mit Bewerberunterlagen allgemein. Relevant waren, inwieweit Ein- und Ausgang der Post registriert werden, ob es im Unternehmen Regelungen und Dokumentationen zur internen Weitergabe von Bewerbungen gibt etc. .

Nach Angaben des Unternehmens wird jegliche Eingangspost vom zuständigen geschulten Personal der „Allgemeinen Verwaltung“ geöffnet, vorsortiert und entsprechend verteilt. Bewerbungen werden nach den Empfängerbereichen sortiert und in ein eigenes Bewerbungseingangsbuch eingetragen. Bewerbungen aus dem Bereich Vertrieb (i. d. Regel Verkäufer/innen) würden an den zuständigen Verkaufsleiter der in Betracht kommenden Filiale weitergeleitet, dies werde notiert. Der zuständige Verkaufsleiter lade die Bewerber sodann entweder zu einem Vorstellungsgespräch ein oder sende nicht berücksichtigte Bewerbungsunterlagen mit einer Absage versehen an den Bewerber zurück. In dem geführten Verzeichnis war die in Rede stehende Bewerbung nicht verzeichnet.
Im Ergebnis stellte die Aufsichtsbehörde fest, dass die organisatorischen Maßnahmen im Umgang mit Bewerberdaten in dem Unternehmen nicht zu beanstanden und die Ermittlungen des Unternehmens sachkonform gewesen sind. Ein Verstoß gegen die Verpflichtung zur Löschung lag nicht vor.

### 4.2.9 Betroffenenrechte

Die Betroffenenrechte sind unter anderem in den §§ 34 und 35 BDSG geregelt. Während das Auskunftsrecht des § 34 BDSG die Betroffenen in die Lage versetzt, zu wissen, wer, was, aus welchem Grund über sie gespeichert hat, gibt die Vorschrift des § 35 BDSG – Berichtigung, Löschung und Sperrung von Daten – dem Betroffenen verschiedene Befugnisse, um den weiteren Umgang mit „seinen“ Daten in Einklang mit seinen berechtigten Interessen bringen zu können. Dazu zählt der Berichtigungsanspruch nach § 35 Abs. 1 BDSG. Danach sind personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

Das Bundesdatenschutzgesetz gibt allerdings nicht vor, wie Daten zu berichtigen sind. Da es stets auf den Einzelfall ankommt, kann eine gesetzliche Vorschrift diese Vorgaben auch nicht treffen. In jedem Fall sind geeignete Maßnahmen zu treffen, um eine unrichtige Information über den Betroffenen zu korrigieren. Nach § 35 Abs. 7 BDSG ist eine verantwortliche Stelle zudem verpflichtet, Stellen an die Daten übermittelt wurden, über die Berichtigung unrichtiger Daten zu verständigen, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

**Zahlreiche Petenten** wandten sich an die Aufsichtsbehörde, da sie wissen wollten, woher bestimmte Unternehmen ihre Daten bezogen haben. Regelmäßig hatten die Betroffenen versucht, diese Information bereits über das ihnen zustehende Auskunftsrecht gemäß § 34 Abs. 1 BDSG zu erhalten, jedoch keine Antwort vom angeschriebenen Unternehmen erhalten. Die Aufsichtsbehörde wirkte erfolgreich auf die Erfüllung zahlreicher Auskunftsansprüche hin.

Eine Ausprägung des Auskunftsrechtes ist die Einsichtnahme des Betroffenen in Patientenunterlagen. Im Gesundheitswesen (ob im Krankenhaus, im Pflegeheim oder beim Arzt) besteht aus verschiedenen Gründen die Notwendigkeit, personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Dokumentiert werden grundsätzlich die wichtigsten diagnostischen und therapeutischen Maßnahmen und Verlaufsdaten. Auch im Gesundheitsbereich gilt der Grundsatz, dass nur zu erheben ist, was auch erforderlich ist. Diese Bewertung kann sich an dem Merksatz von Reinhard Lay orientieren: „Was praxisrelevant, vergütungsrelevant, prüfungsrelevant oder juristisch erforderlich ist, wird vollständig, wahr und klar dokumentiert." (Reinhard Lay: „*Ethik in der Pflege*. Ein Lehrbuch für die Aus-, Fort- und Weiterbildung." Schlütersche Verlagsgesellschaft, Hannover 2004, S. 157). Zu beachten ist weiterhin, dass die Dokumentation vor nachträglicher Veränderung und vor unbefugtem Zugriff zu schützen ist.
Selbstverständlich hat ein Patient das Recht, Einsicht in die ihn betreffenden Behandlungsunterlagen zu nehmen. Dies bedeutet nach zivilrechtlichen Grundsätzen, dass die Möglichkeit zu geben ist, die Dokumentation in Augenschein zu nehmen. Darüber hinaus ergibt sich dieses Recht auch aus § 34 BDSG – Auskunft an den Betroffenen. Nähere Ausführungen hierzu finden Sie unter Abschnitt 2, Punkt 2.3 „Rechte der Betroffenen" dieses Berichtes. Es gilt allerdings zu beachten, dass das Einsichtsrecht nur sog. objektivierbare Befunde bzw. Bewertungsfakten betrifft, nicht aber sog. subjektiv wertende Aufzeichnungen (z. B. Aufzeichnungen über persönliche Eindrücke vom Patienten im Rahmen einer psychiatrischen Behandlung).

# 5 Aktuelles zum Datenschutzes

## 5.1 Google Street View, Bing Maps Streetside & Co.

Im vorhergehenden 4. Tätigkeitsbericht wurde über den Geodienst Google Street View berichtet. Inzwischen gibt es zahlreiche sog. Panorama- und Geodatendienste, die Geodaten nutzen.

Straßenansichten, die dem Internetnutzer bei einem virtuellen Spaziergang ermöglichen, einen Straßenzug aus der Perspektive des Fußgängers zu betrachten, werden maßgeblich von Street View (Google) und Bing Maps Streetside (Microsoft) zur Verfügung gestellt. Die schutzwürdigen Interessen der Eigentümer und Bewohner sind bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet zu berücksichtigen.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) hat einen Datenschutz-Kodex für Geodatendienste vorgelegt, der für alle Anbieter einen einheitlichen Datenschutzstandard erzeugen sollte. Der Kodex entspricht allerdings in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt. Von besonderer Bedeutung dabei ist, dass ein Widerspruchsrecht gegen die weitergehende Veröffentlichung erst nach der Veröffentlichung vorgesehen ist. Das Recht auf informationelle Selbstbestimmung wird allerdings bereits mit der Veröffentlichung verletzt, weshalb die Einräumung eines Vorabwiderspruchsrechts unumgänglich ist. Eine Möglichkeit des Vorabwiderspruches wird auch von Microsoft vorgesehen.
**Aus Sicht der Aufsichtsbehörden sind die aus dem Beschluss des Düsseldorfer Kreises vom 08. April 2011 bereits am 13./14. November 2008 aufgeführten Punkte entscheidend**:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.
- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor und nach der Veröffentlichung bestehen.
- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

## 5.2 Webanalysedienstleistungen - Google Analytics & Co.

Webanalysedienste dienen dazu, auf Websites zu Zwecken der Werbung und Marktforschung oder zur bedarfsgerechten Gestaltung von Internetangeboten das Surfverhalten der Nutzer zu analysieren. Der bekannteste Dienst dieser Art ist Google Analytics. Dies ist ein Programmcode, den Webseitenbetreiber auf ihre Website integrieren. Wird die Seite aufgerufen, wird der Browser des Besuchers von der Seite angewiesen, zusätzlich ein Programm, ein sog. Script vom Google-Server, herunterzuladen und auszuführen. Es wird auf dem Rechner des Nutzers eine kurze Analyse durchgeführt und die gewonnenen Informationen an Google in die USA zurückgeschickt, dort gespeichert sowie ausgewertet.

Bei der Erstellung von Nutzungsprofilen durch Webseitenbetreiber sind die Bestimmungen des Telemediengesetzes (TMG) zu beachten. Entsprechend dürfen Nutzungsprofile nur bei der Verwendung von Pseudonymen erstellt werden, wobei die vollständige IP-Adresse kein Pseudonym i. S. d. TMG darstellt. In jedem Fall muss der Betreiber einer Website als verantwortliche Stelle die Nutzer des eigenen Angebotes über den Einsatz des Analysewerkzeugs unterrichten und ein Widerspruchsrecht gegen die Erstellung eines Nutzungsprofiles einräumen (§ 15 Abs. 3 TMG). Welche weiteren Vorgaben aus dem TMG im Einzelnen zu beachten sind, ist im Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 zur „Datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ (abrufbar: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile) zu entnehmen. Zudem hat der Nutzer eines Webanalysewerkzeuges mit dem Anbieter einen den Anforderungen des § 11 BSDG entsprechenden Vertrag zu schließen.

Beim Webanalysewerkzeug Google Analytics können durch das Zusammenführen der in die USA übermittelten Daten verschiedener Google Dienstleistungen umfassende Nutzungsprofile erstellt werden. Aus datenschutzrechtlicher Sicht sind folgende Maßnahmen notwendig, damit z. B. das Produkt Google Analytics datenschutzkonform eingesetzt werden kann:

- Sicherstellung, dass keine IP-Adressen der Nutzer an Google übermittelt werden, wenn diese das vom Unternehmen zur Verfügung gestellte plug-in nutzen, mit dem jeder Betroffene einen Widerspruch gegen die Übermittlung seiner Daten an Google Analytics erklären kann
- Verkürzung der IP-Adressen – Übermittlung vollständiger IP-Adressen in USA ist mangels Rechtsgrundlage ohne Einwilligung der Nutzer unzulässig

- Sicherstellung, dass bei Vertragsende die Daten des jeweiligen Auftraggebers auf den Servern von Google gelöscht werden
- transparente Nutzungsbedingungen des Produktes.

### 5.3 Sicheres Surfen im Internet

Ein Alltag ohne Internet ist kaum noch denkbar. Viele der neuen Entwicklungen sind nützlich. Aber jede neue Technologie bringt auch Gefahren mit sich, vor denen sich Nutzer wirksam schützen sollten.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bietet einen Selbsttest an, der den Teilnehmern verrät, ob die eigenen Daten wirksam geschützt sind (abrufbar: http://gsb.download.bva.bund.de/BFDI/id_theft/index.html).
Daneben hat der BfDI die wichtigsten Regeln für sicheres Surfen im Internet zusammengefasst. Das entsprechende Dokument ist abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/SicheresSurfen.pdf?__blob=publicationFile.

Ein Website-Besucher hat zwar keinen direkten Einfluss auf die Art und Weise der Datenverarbeitung durch den Betreiber einer Website, dennoch kann der Einzelne aktiven Selbstschutz betreiben, indem:

- **Datenschutzerklärungen gelesen werden**
- **Websites von Betreibern, die keine akzeptable Datenschutzerklärung abgegeben haben, gemieden werden**
- **Dateneingaben auf das erkennbare Minimum reduziert werden und allein erforderliche Pflichtfelder ausgefüllt werden und**
- **etwaige Verstöße bei der zuständigen Aufsichtsbehörde oder den Verbraucherzentralen angezeigt werden.**

Um sich gegen die Datensammlung schützen zu können, wird der Einsatz eines Internetbrowsers empfohlen, der Skripte nur nach Aufforderung ausführt. Mit folgenden einfachen und kostenlosen Mitteln können Privatpersonen und Unternehmen ihre Surfspuren verringern:
- Browser so einstellen, dass Cookies höchstens für die aktuelle Sitzung angenommen werden

- Bei sensiblen Themen einen Anonymisierungsdienst verwenden.
- Bei Nutzung von Mozilla Firefox die Skripte selektiv mit der Firefox-Erweiterung „noscript“ steuern, so dass Cookies von Google und Co. gar nicht erst gesetzt werden können und der „Gefällt mir - Button“ von Facebook ebenfalls gar nicht erst angezeigt wird.
- Keine Toolbar von Google, Yahoo, Alexis u. a. im Browser einsetzen, da diese Toolbars das Surfverhalten protokollieren.

### 5.4 Smartphones

***iPhone und iPad Besitzer werden überwacht und geortet***

In der Presse wurde wiederholt auf das Problem hingewiesen, dass von den Herstellern von Smartphones unbemerkt Positionsangaben von Handynutzern erhoben und gespeichert würden. Selbst bei Deaktivierung entsprechender Funktionen (Apps) würden Ortsinformationen gesammelt.

Sog. **Smartphones** sind mobile Geräte, die neben der obligatorischen Telefonierfunktion weitergehende Nutzungen ermöglichen.
Klassische Anwendungen von Smartphones sind die mobile Internet- und E-Mail-Nutzung, das Abspielen von Audio- und Videodateien, Aufnehmen von Fotos sowie Versenden von Kurznachrichten.
Smartphone-Apps sind kleine Programme, die auf dem Smartphone installiert sind, um bestimmte Funktionalitäten zur Verfügung zu stellen, z.B. um die Verbindung zu anderen Geräten herzustellen (Bluetooth) oder die eigene aktuelle Position bzw. die einer gewünschten Dienstleistung darzustellen.

Die datenschutzrechtliche Problematik der nützlichen Funktionen liegt darin, dass neben der grundsätzlich legitimen Datennutzung ein erheblicher Teil der Apps verschiedene personenbezogen Daten (wie z. B. Gerätenummer, Telefonnummer, Kontaktdaten aus dem Adressbuch) an den jeweiligen App-Hersteller übermittelt, ohne dass dies für den jeweiligen Dienst erforderlich ist. Auch ist der Nutzer nicht über diese Tatsache informiert. Zudem besteht die Gefahr der Entstehung umfangreicher Interessens- und vollständiger Bewegungsprofile.

Bisher sind die Möglichkeiten des Selbstschutzes begrenzt. Teilweise können die Rechte von Apps eigenständig beschränkt werden, z.B. die Festlegung, ob ein App auf die Lokalisie-

rungsfunktionalität zurückgreifen darf. Allerdings erfordert dies eine Transparenz der Funktionsweise der App. Denn nur auf diese Art und Weise kann bestimmt werden, welche Rechte eine App erhalten muss, um noch zu funktionieren und welche Rechte bzw. Daten überflüssig sind.

## 5.5 Soziale Netzwerke

Nach wie vor boomen soziale Netzwerke. In solchen Online-Kontaktnetzwerken haben Internetnutzer die Möglichkeit, sich kennenzulernen, sich zu „treffen“, zu chatten, sich online auszutauschen, Partner fürs Leben oder für kürzere Zeitabschnitte zu finden und hierfür auch eigene Inhalte bis zum ausführlichen Persönlichkeitsprofil samt Interessen und Aktivitäten einzustellen.

Nicht immer bleibt alles so privat, wie es sein sollte. Dies zeigt sich bereits daran, dass sich Unternehmen über Bewerber häufig im Web informieren. Ausweislich einer BITKOM-Presseinformation vom 09.11.2010 (vollständig abrufbar unter http://www.bitkom.org/de/presse/66442_65790.aspx) gewinnen 45 Prozent aller Unternehmen zusätzliche Informationen über Bewerber mittels Google, Bing oder speziellen Personensuchmaschinen. 21 Prozent recherchieren in sozialen Online-Netzwerken, die einen beruflichen Schwerpunkt haben. 17 Prozent suchen sogar in sozialen Netzwerken, die einen eher privaten Charakter haben. Bislang gibt es keine konkreten Einschränkungen für Internet-Recherchen über Bewerber. Dies soll allerdings in gesetzlichen Regelungen zum Beschäftigtendatenschutz nachgeholt werden. Rechtlich zulässig soll künftig allein die Recherche über Bewerber mit Suchmaschinen sowie in sozialen Online-Netzwerken mit eindeutig beruflichem Charakter sein. BITKOM beurteilte allerdings, dass die Überprüfbarkeit etwaiger Recherchen in privaten Online-Netzwerken in der Praxis schwierig sein dürfte.

Nach wie vor ist das Wichtigste eine starke Eigenverantwortung der Nutzer von sozialen Netzwerken. Die bereits im 4. Tätigkeitsbericht aufgeführten Tipps gelten weiter:

**Tipps zur Nutzung von sozialen Netzwerken:**

- Das Auftreten im sozialen Netzwerk sollte grundsätzlich unter Verwendung von Pseudonymen (Spitznamen) – ggf. vollständiger Vorname, abgekürzter Nachname - erfolgen! Der „echte“ Name sollte nur zur ersten Kontaktaufnahme genutzt werden.
- Fotos, auf denen die Person deutlich erkennbar ist, sollten vermieden werden.
- Der Grundsatz der Datensparsamkeit ist zu beachten. Die Daten, die man offenbaren

möchte, sollten dem Zweck des Profils angepasst sein.

- Kontaktdaten sollten grundsätzlich nicht angegeben werden!
- Die Standardeinstellungen des Netzwerkbetreibers sollten auf „Privatsphäre hoch“ gesetzt werden, so dass der Zugriff auf die Profildaten nicht für die allgemeine Öffentlichkeit möglich ist.
- Die Daten des sozialen Netzwerkes sollten nicht in Suchmaschinen auffindbar sein. Einige Netzwerke ermöglichen den Zugriff auf Profildaten grundsätzlich nur anderen Mitgliedern, andere ermöglichen den Ausschluss der Recherche über Suchmaschinen oder die Beschränkung des Zugriffs zumindest als Option.
- Anwendungen von Drittanbietern sollte kein Zugriff auf die Profildaten ermöglicht werden.
- Vorsicht bei netzwerkübergreifenden Verknüpfungen! Soziale Netzwerke oder andere Dienstleister ermöglichen die gemeinsame Pflege oder Nutzung der Profildaten in mehreren Netzwerken.
- Die Rechte Dritter müssen beachtetet werden. So dürfen z. B. Fotos anderer Personen nur mit deren Zustimmung eingestellt werden.

## 5.6 Cloud Computing

„Wer klaut in der Cloud“ ist ein ansprechendes Wortspiel, doch welche datenschutzrechtlichen Risiken ergeben sich aus der Cloud bzw. dem Cloud Computing?

Cloud Computing bezeichnet das Bereitstellen benötigter Rechenkapazitäten, Datenspeicher oder fertiger Programmpakete über Netze, insbesondere über das Internet. Daher kann ein Endnutzer von einem Anbieter flexibel die notwendige Menge an Rechenkapazität weltweit einkaufen, bei Bedarf weitere Kapazitäten hinzumieten bzw. wieder freigeben, wenn diese nicht mehr benötigt werden. Der Endnutzer kann so die Investitionen in den Ausbau der eigenen Infrastrukturen gering halten. Anbieter der benannten Kapazitäten sind Rechenzentren oder andere Dienstleister, die über Überkapazitäten verfügen und diese mittels Cloud Computing anderen Stellen zur Verfügung stellen.
Dabei kann zwischen Clouds, die nur einer geschlossenen Nutzergruppe zur Verfügung stehen – Private Clouds – und solchen, die frei zugänglich sind – Public Clouds – unterschieden werden. Beim offenen, globalen Modell, bei dem Kapazitäten aus weltweit verteilten Rechenzentren genutzt werden, hat der Nutzer regelmäßig keine gesicherte Kenntnis, wo auf der Welt die Daten aktuell gespeichert sind, auf welchen Rechnern die Daten verarbeitet werden, in welchem wirtschaftlichen und politischen System die Rechenzentren sich örtlich

befinden etc.. Wie soll beispielsweise das Datenschutzniveau in Juba, der Hauptstadt vom Südsudan, eingeschätzt werden? Entsprechend hoch sind die datenschutzrechtlichen Bedenken, wenn es sich bei den zu verarbeitenden Daten um personenbezogene Daten handelt. Das Hauptproblem liegt in der Integrität (Unverletzlichkeit) und der Vertraulichkeit der verarbeiteten personenbezogenen Daten. Es ist unklar, wer – ggf. auch unbefugt – Zugriff auf die Daten hat.

Die datenschutzrechtliche Verantwortung obliegt dem Nutzer der angebotenen Kapazitäten und nicht dem Anbieter der Leistungen. Die verantwortliche Stelle ist gesetzlich verpflichtet zu gewährleisten, dass die gesetzlichen Vorgaben über den Datenschutz eingehalten werden. Dies führt dazu, dass ein Anbieter des Cloud Computing nur als Auftragsdatenverarbeiter in Anspruch genommen werden kann, wenn dieser Gewähr dafür bietet, dass dessen getroffenen technischen und organisatorischen Maßnahmen einen hinreichenden Schutz der zu verarbeitenden personenbezogenen Daten gewährleisten. Insbesondere ist ein Vertrag zwischen dem Nutzer als Auftraggeber und dem Anbieter als Auftragsdatenverarbeiter zu schließen, der den Anforderungen des § 11 BDSG genügt. Hauptproblematik einer entsprechenden Regelung ist wegen der ad hoc Zuweisung freier Serverkapazitäten, dass der Auftraggeber im Detail wissen muss, welche Daten, wo, unter welchen Bedingungen verarbeitet werden. Denn allein auf dieser Basis lassen sich die notwendigen technischen und organisatorischen Maßnahmen und die weiteren Festlegungen nach § 11 Abs. 2 BDSG umsetzen. Zudem muss dann, wenn der Auftragnehmer die Daten außerhalb der EU oder des EWR verarbeitet, zusätzlich ein angemessener Datenschutz in den jeweiligen Drittstaaten gewährleistet und ggf. eine Genehmigung bei der für die verantwortliche Stelle zuständige Datenschutzbehörde eingeholt werden. Eine solche Genehmigung kann regelmäßig entfallen, wenn sog. Standardvertragsklauseln verwendet werden. Diese Klauseln sollen den Schutz persönlicher Daten standardisiert sicherstellen, wenn Unternehmen personenbezogene Daten an andere Unternehmen außerhalb der EU zur Weiterverarbeitung übersenden. Die EU-Kommission hat am 05.02.2010 einen Beschluss zur Aktualisierung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern gefasst (abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:01:DE:HTML).
Mithin sollten Dienstleistungen nur dann unter Nutzung des Cloud Computings realisiert werden, wenn bestimmte rechtliche, technische und organisatorische Voraussetzungen erfüllt sind.
In den „Sicherheitsempfehlungen für Cloud Computing Anbieter“ des Bundesamtes für Sicherheit in der Informationstechnik

(veröffentlicht
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile)
werden sowohl Basisanforderungen, als auch Anforderungen an hohe Vertraulichkeit und hohe Verfügbarkeit auf Grundlage des IT-Grundschutzes beim Einsatz von Cloud Computing aufgeführt. Diese sollten bei der Prüfung der Beauftragung eines entsprechenden Anbieters vom Auftraggeber – also dem Endnutzer – entsprechend beachtet werden.

### 5.7 Der neue Personalausweis

Der neue Personalausweis im Scheckkartenformat wird inzwischen seit dem 01. November 2010 ausgestellt. Auf dem Ausweis befinden sich sichtbar abgedruckte Daten und zusätzlich ein Chip für den elektronischen Identitätsnachweis (eID). Auf dem Chip sind alle auf dem Ausweis aufgedruckten Daten gespeichert, außer den Angaben zur Größe, zur Augenfarbe und zur Unterschrift des Ausweisinhabers, also auch das biometrische Gesichtsbild. Lediglich die Speicherung des Fingerabdruckes erfolgt nur auf ausdrücklichen Wunsch des Inhabers des Ausweisdokumentes.

Der elektronische Identitätsnachweis ermöglicht es, sich im Rahmen von E-Government und auch E-Commerce gegenüber berechtigten Stellen auszuweisen. Ziel ist es, Internetnutzern mehr Sicherheit und besseren Datenschutz zu bieten. Der Ausweisinhaber kann selbstbestimmt entscheiden, ob er die eID-Funktion nutzen will. Soll die Funktion nicht genutzt werden, kann die standardmäßig aktivierte eID-Funktion gebührenfrei von der jeweiligen Personalausweisbehörde deaktiviert werden. Ein Nachteil ist mit der Deaktivierung nicht verbunden. Wer die Funktion nutzen möchte, sollte nach den Hinweisen des Bundesbeauftragten für Datenschutz und Informationsfreiheit (siehe www.bfdi.bund.de) darauf achten, dass der eigene Rechner über einen aktuellen Virenscanner sowie eine Firewall verfügt und Sicherheitsupdates regelmäßig durchgeführt werden. Die sechsstellige Ausweis-PIN soll ein sicheres Passwort sein. Daher ist nicht zu empfehlen, die PIN aus dem Geburtsdatum oder ähnlichen leicht recherchierbaren Daten zu erstellen.

Umfassende Informationen zum neuen Personalausweis sind den Ausführungen des Bundesbeauftragten für Datenschutz und Informationsfreiheit auf www.bfdi.bund.de zu entnehmen.

# 6 Ausblick

Immer wieder kommt es zu sog. Datenschutzskandalen. Die Arbeit der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich gewinnt immer mehr an Bedeutung, nicht zuletzt wegen der sich rasant entwickelnden Technik. Wer hätte vor ein paar Jahren gedacht, dass eines Tages die Häuserfronten ganzer Städte im Internet verfügbar sind und daraus ganz neue datenschutzrechtliche Probleme entstehen? Und nicht im Traum hätte man damit gerechnet, sich eines Tages mit dem Datenschutzniveau von Burkina Faso zu beschäftigen, nur weil in Ouagadougou ein über Cloud Computing genutzter Server steht!

Beim Datenschutz geht es nicht darum, die Bürger im Umgang mit ihren Daten zu bevormunden, sondern Wege aufzuzeigen, wie sie – insbesondere bei Nutzung des Internets – selbstbestimmt mit ihren Daten umgehen können. Dazu gehören auch die Möglichkeiten, datenschutzfreundliche Grundeinstellungen der Technik zu nutzen. Auch dieses Anliegen hat das Landesverwaltungsamt als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt gern und nachhaltig verfolgt.

Vor dem Hintergrund der Entscheidung des Europäischen Gerichtshofes wurde die Datenschutzaufsicht in Sachsen-Anhalt neu geregelt. Am 01. Oktober 2011 ging die Aufgabe der Datenschutzkontrolle im nicht-öffentlichen Bereich auf den Landesbeauftragten für den Datenschutz Sachsen-Anhalt über.

# Abkürzungsverzeichnis

| | |
|---|---|
| Abs. | Absatz |
| AiB | Arbeitsrecht im Betrieb (Zeitschrift) |
| Art. | Artikel |
| Az. | Aktenzeichen |
| BAG | Bundesarbeitgericht |
| BGB | Bürgerliches Gesetzbuch |
| BGH | Bundesgerichtshof |
| BR-Drs. | Drucksache des Bundesrats |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BT-Drs. | Drucksache des Bundestags |
| BVerfGE | Entscheidung des Bundesverfassungsgerichts |
| bzw. | beziehungsweise |
| d.h. | das heißt |
| EG | Europäische Gemeinschaft |
| etc. | et cetera (= und so weiter) |
| EU | Europäische Union |
| e.V. | eingetragener Verein |
| EWR | Europäischer Wirtschaftsraum |
| f. | folgende(r) |
| ff. | folgende |
| ggf. | gegebenenfalls |
| GPS | Global Positioning System (Navigationssystem) |
| Hrsg. | Herausgeber |
| Hs | Halbsatz |
| incl. | inklusive |
| i. R. v. | im Rahmen von |
| i. S. | im Sinne |
| i. S. v. | im Sinne von |
| i. V. m. | in Verbindung mit |
| juris PR-ArbR | juris Praxis Report – Arbeitsrecht (Zeitschrift) |
| MMR | Multimedia und Recht (Zeitschrift) |
| m. w. N. | mit weiteren Nachweisen |
| Nr. | Nummer |
| NZA | Neue Zeitschrift für Arbeitsrecht |
| o. ä. | oder ähnlichem |

| | |
|---|---|
| PIN | persönliche Identifikationsnummer |
| Rs. | Rechtssache |
| S. | Satz |
| SGB | Sozialgesetzbuch |
| sog. | sogenannte(n/r/s) |
| u. a. | unter anderem |
| UMTS-Stick | Universal Mobile Telecommunications System - Stick |
| u. v. m. | und vieles mehr |
| u. U. | unter Umständen |
| vgl. | vergleiche |
| z. B. | zum Beispiel |
| ZPO | Zivilprozessordnung |

## Notizen

## Hier sind wir erreichbar

Hauptsitz
Ernst-Kamieth-Straße 2, 06112 Halle [Saale]
Telefon [0345] 514 –0

Dienstgebäude Halle
Dessauer Straße 70, 06118 Halle [Saale]
Telefon [0345] 514 –0

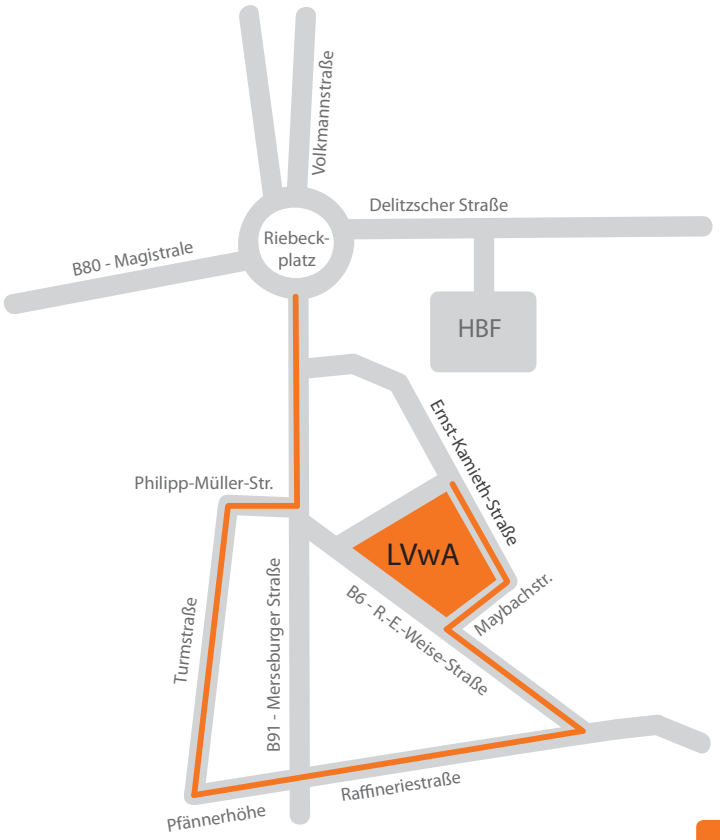
Dienstgebäude Halle
Maxim-Gorki-Straße 7, 06114 Halle [Saale]
Telefon [0345] 514 –0

Nebenstelle Dessau - Roßlau
Kühnauer Straße 161, 06846 Dessau - Roßlau
Telefon [0340] 6506 –0

Dienstgebäude Magdeburg
Olvenstedter Straße 1-2, 39108 Magdeburg
Telefon [0391] 567 –02

Nebenstelle Magdeburg
Hakeborner Straße 1, 39112 Magdeburg
Telefon [0391] 567 –02

## Anfahrtsskizze Hauptsitz




Impressum: Landesverwaltungsamt
Ernst-Kamieth-Straße 2
06112 Halle [Saale]
Tel.: [0345] 514 0
Fax: [0345] 514 1477
E-Mail: poststelle@lvwa.sachsen-anhalt.de
Internet: www.lvwa.sachsen-anhalt.de