



# HESSISCHER LANDTAG

28. 09. 2010

## **Vorlage der Landesregierung**

**betreffend den Dreiundzwanzigsten Bericht der Landesregierung  
über die Tätigkeit der für den Datenschutz im nicht öffentlichen  
Bereich in Hessen zuständigen Aufsichtsbehörde**

Vorgelegt mit der Stellungnahme zum Achtunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drucks. 18/2027) nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

## **Inhaltsverzeichnis**

### **Überblick und Statistiken**

- 1. Bearbeitung von Datenschutzbeschwerden und sonstige Prüfungen nach § 38 Abs. 1 BDSG**
- 1.1 Bearbeitung von aktuellen Eingaben und Beschwerden**
- 1.2 Erledigung von Eingaben und Beschwerden aus den Vorjahren**
- 1.3 Anlassabhängige und anlassbezogene Überprüfungen vor Ort nach § 38 Abs. 4 BDSG**
- 2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit**
- 2.1 Anfragebearbeitung und datenschutzrechtliche Beratung 3**
- 2.2 Öffentlichkeitsarbeit**
- 3. Register der meldepflichtigen Verfahren nach § 4d BDSG**
- 4. Ordnungswidrigkeitenverfahren**
- 5. Teilnahme an den Sitzungen des Düsseldorfer Kreises und den Arbeitsgruppen**
- 6. Überblick über die Novellen des BDSG**
- Ausgesuchte Probleme und Einzelfälle**
- 7. Auskunftfeien und deren Vertragspartner**
- 7.1 Gesetzliche Neuregelungen im Bereich Auskunftfeien und Scoring**
- 7.2 Bonitätsauskünfte über Mietinteressenten**
- 8. Banken**
- 8.1 Problematische Maßnahmen der Konzernsicherheit**
- 8.2 Bargeldtransfer und Datenschutz**
- 9. Telemedien, Internet**
- 9.1 Bewertungen von Einzelpersonen im Internet**
- 10. Auftragsdatenverarbeitung**
- 11. Aspekte internationaler Datenverarbeitung**
- 11.1 Bedeutung der Änderungen des § 11 BDSG für den internationalen Datenverkehr**
- 11.2 Mehrparteienverträge**
- 12. Beschäftigtendatenschutz**
- 12.1 Videoüberwachungsanlage in Lagerhallen**
- 12.2 Veröffentlichung von Mitarbeiterdaten im Internet**
- 12.3 Detektiveinsätze bei einem Lebensmitteldiscounter**
- 12.4 Unterlagen über Mitarbeiterprüfungen im Callcenter**
- 12.5 Veräußerung von Bewerbungsunterlagen bei Ebay**
- 13. Videoüberwachung**
- 13.1 Videobeobachtung an der "Wildschweinkirrung"**
- 14. Gesundheit**

- 14.1        Datenschutz in einer neu gegründeten ärztlichen Gemeinschaftspraxis**
- 15.        Werbung und Adresshandel**
- 15.1       Stärkung der Betroffenenrechte durch das geänderte Bundesdatenschutzgesetz**

**Der Dreiundzwanzigste Bericht der Landesregierung gibt den Sachstand im Mai 2010 wieder.**

## **Überblick und Statistiken**

### **1.        Bearbeitung von Datenschutzbeschwerden und sonstige Prüfungen nach § 38 Abs. 1 BDSG**

#### **1.1       Bearbeitung von aktuellen Eingaben und Beschwerden**

Das Regierungspräsidium Darmstadt überprüft als Aufsichtsbehörde nach § 38 Abs. 1 BDSG die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz in Hessen, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Im Berichtsjahr wurden von der Aufsichtsbehörde **in 926 Fällen** (im Vorjahr: 850) Überprüfungen von nicht öffentlichen Stellen vorgenommen, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30, 32 und § 6b BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

Telefonische Eingaben, die durch telefonische Beratung erledigt werden konnten, wurden dabei bis auf wenige Ausnahmen ebenso wenig erfasst wie solche, die durch die Versendung von Informationsmaterial und Orientierungshilfen erledigt werden konnten.

Die **926 Überprüfungen** auf Grund von Eingaben, Beschwerden und Pressemeldungen durch das Regierungspräsidium Darmstadt betrafen:

- in 165 Fällen eine große Auskunftfei,
- in 146 Fällen Unternehmen im Adresshandel- und Direktmarketingbereich,
- in 132 Fällen Telemedienanbieter (Anbieter von Internetdiensten und -inhalten, unverlangte E-Mail-Werbung),
- in 103 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 71 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 58 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 47 Fällen (andere) Handels- und Wirtschaftsauskunfteien,
- in 32 Fällen Versicherungsgesellschaften,
- in 25 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 24 Fällen Inkassounternehmen,
- in 23 Fällen Vermieter sowie Wohnungs- und Immobilienverwaltungsfirmen,
- in 22 Fällen das Gesundheitswesen (Ärzte, Krankenhäuser, Senioren- und Pflegeheime),
- in 10 Fällen den Verlags- und Medienbereich,
- in 9 Fällen Verkehrsunternehmen,
- in 8 Fällen Unternehmen des Groß- und Einzelhandels,
- in 8 Fällen Unternehmen der Versandhandelsbranche,
- in 7 Fällen Kreditkartenunternehmen,
- in 6 Fällen Unternehmen der Freizeit- und Touristikbranche,
- in 3 Fällen Politische Parteien,
- in 3 Fällen Markt- und Meinungsforschungsunternehmen,
- in 3 Fällen Anwaltskanzleien,
- in 21 Fällen sonstige Stellen (z.B. Steuerberater, Ebay-Käufer, Kfz.-Importeur, DV-Dienstleister, Auslandsdatenverarbeitung)

Bei ca. **17 v.H.** der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt **157 Fällen** wurden bei den Nachforschungen der Aufsichtsbehörde unzulässige Verarbeitungen personenbezogener Daten und andere Verstöße gegen Vorschriften des Datenschutzrechts und des Rechts der Telemedien festgestellt, die zu Beanstandungen der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten **157 Verstöße** gegen Datenschutzbestimmungen wurden festgestellt:

- in 37 Fällen bei Unternehmen im Adresshandels- und Direktmarketingbereich,
- in 30 Fällen bei Auskunftsteilen (26 Fälle betrafen dieselbe Auskunftsteil, davon war in 10 Fällen ein Verstoß durch einen Vertragspartner der Auskunftsteilen ursächlich,
- in 24 Fällen bei Anbietern von Telemedien im Internet (Content-Provider und Versender von Werbe-E-Mails),
- in 19 Fällen bei Kreditinstituten und Banken,
- in 9 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 8 Fällen bei Versicherungsgesellschaften,
- in 6 Fällen bei der Videoüberwachung,
- in 5 Fällen bei Inkassounternehmen,
- in 4 Fällen im Bereich Wohnen und Miete
- in 4 Fällen bei Versandhandelsunternehmen
- in 3 Fällen im Gesundheitswesen,
- in 2 Fällen bei Kreditkartenunternehmen,

sowie in jeweils einem Fall bei einem Verein, einem Verkehrsunternehmen, im Groß- und Einzelhandel, in der Freizeit- und Touristikbranche und bei zwei sonstigen Stellen.

Ein Teil der eingeleiteten Überprüfungen konnten im Berichtsjahr noch nicht abgeschlossen werden. Die Erledigung dieser Fälle wird in den nächsten Tätigkeitsbericht einfließen.

## 1.2 Erledigung von Eingaben und Beschwerden aus den Vorjahren

Von den noch aus den Vorjahren anhängigen Beschwerden, die oftmals sehr vielschichtige Verarbeitungszusammenhänge betrafen, wurden im Berichtsjahr **257 Fälle** abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch das Regierungspräsidium ergab, dass davon **96 Eingaben** begründet waren. Damit musste die Aufsichtsbehörde bei fast **40 v.H.** dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten **96 Verstöße** gegen Datenschutzbestimmungen wurden festgestellt:

- in 19 Fällen bei Unternehmen der Werbewirtschaft und werbenden Groß- und Einzelhändlern,
- in 16 Fällen bei Anbietern von Telemedien (Internetprovider, www-Anbieter),
- in 12 Fällen bei der Video-Beobachtung,
- in 12 Fällen bei Handelsauskunftsteilen (9 der Verstöße betrafen dieselbe Auskunftsteil, wobei 6 dieser Verstöße Vertragspartnern zuzurechnen waren),
- in 7 Fällen bei Kreditinstituten und Banken,
- in 6 Fällen im Groß- und Einzelhandel,
- in 4 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 4 Fällen bei Versicherungen,
- in 3 Fällen in Vereinen,
- in 3 Fällen im Gesundheitswesen,
- in 3 Fällen bei Unternehmen der Freizeit- und Touristikbranche,
- in 2 Fällen bei Verkehrsunternehmen,
- in 2 Fällen bei Kreditkartenunternehmen,

sowie in jeweils einem Fall bei einem Anwalt, einer politischen Partei und einem Unternehmen der Verlagsbranche.

## Anlassabhängige und anlassunabhängige Überprüfungen vor Ort nach § 38 Abs. 4 BDSG

Die Aufsichtsbehörde entscheidet nach pflichtgemäßem Ermessen, wann und in welchem Unternehmen eine Kontrolle vor Ort durchgeführt wird.

Einen besonderen Schwerpunkt bildete die Überprüfung von Videoüberwachungseinrichtungen, da hierzu erneut sehr viele Beschwerden und Anfragen eingingen und eine Bewertung oft nur nach einer Prüfung der örtlichen Gegebenheiten möglich war.

Insgesamt wurden im Berichtsjahr 53 Kontrollen vor Ort durchgeführt.

Diese betrafen folgende Branchen/Bereiche:

- Videoüberwachungssysteme	29
- Vereine/Verbände	7
- Auskunftsteilen	4
- Arbeitnehmerdatenschutz	3

- Ärztliche Praxen/Kliniken/Laboratorien/Verrechnungsstellen	3
- Adresshandel/Direktmarketing	2
- Call-Center	2
- Sonstige	3

Dabei wurden folgende Mängel am häufigsten festgestellt:

1. Voraussetzungen des § 6b Abs. 1, Abs. 3 - 5 BDSG bei der Videoüberwachung nicht erfüllt (d.h. unzulässige Videoüberwachung, keine oder zu späte Löschung der Daten etc.),
2. Voraussetzungen des § 6b Abs. 1, Abs. 3 - 5 BDSG bei der Videoüberwachung erfüllt, aber die erforderliche Information zur Videoüberwachung fehlte (§ 6b Abs. 2 BDSG),
3. fehlendes oder inhaltlich unzureichendes Verfahrensverzeichnis (§ 4g Abs. 2 BDSG),
4. im Rahmen der Auftragsdatenverarbeitung fehlende oder mangelhafte Verträge nach § 11 BDSG (wobei ab dem 1. September 2009 aufgrund der hier geltenden Neuregelungen die Beratung im Vordergrund stand, siehe hierzu Ziffer 10)
5. Mängel im Bereich der technisch-organisatorischen Maßnahmen (§ 9 BDSG und Anlage),
6. unrechtmäßige Verarbeitung (fehlende Rechtsgrundlage/Einwilligung),
7. betrieblicher Datenschutzbeauftragter nicht bestellt bzw. mangelnde Fachkunde der zum Datenschutzbeauftragten bestellten Personen (§ 4f BDSG),
8. fehlende Vorabkontrolle (§ 4d Abs. 5 und 6 BDSG).

Darüber hinaus bestand oftmals weiterer Anlass für Beanstandungen, wie auch in den vorangegangenen Tätigkeitsberichten bereits aufgezeigt wurde.

## **2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit**

### **2.1 Anfragebearbeitung und datenschutzrechtliche Beratung**

Das Regierungspräsidium Darmstadt hatte im Berichtsjahr erneut eine hohe Anzahl von Anfragen und Beratungsersuchen zu bearbeiten. In **385 Fällen** (im Vorjahr: 337 Fälle) erfolgte die Beratung und Information von Unternehmen, Vereinen und Verbänden, Bürgerinnen und Bürgern sowie Arbeitnehmerinnen, Arbeitnehmern und Betriebsräten aktenmäßig. Die direkte telefonische Erledigung von Anfragen sowie die Übersendung von Informationsmaterial und Orientierungshilfen per E-Mail wurden bis auf wenige Ausnahmen nicht statistisch erfasst.

Die statistische Auswertung der **385 Fälle** ergab folgende inhaltliche Schwerpunkte:

#### **106 Anfragen zu Auskunftfeien und Inkassounternehmen:**

Anfragen allgemeiner Art zu verschiedenen Verfahren der Auskunftfeien und neuen Produkten, Rechtmäßigkeit der Auskunftfeientätigkeit, Selbstauskünfte, zulässige Speicherdauer von verschiedenen Eintragungen, Löschfristen, Restschuldbefreiung, Informationen über Scoring und Schätzdaten, Zulässigkeit der Ermittlung und Beauskunftung von Adressdaten, auch mittels einfacher Melderegisterauskünfte, Anfragen zu Inkasso-Unternehmen, die mit der Beitreibung angeblicher Forderungen aus sogenannten "Abofallen" befasst waren.

#### **50 Anfragen zum Beschäftigten- und Bewerberdatenschutz (Arbeitnehmerdatenschutz):**

E-Mail- und Internetnutzung im Unternehmen (Zugriffsrecht des Arbeitgebers, Vertretungsregelung, Betriebsvereinbarung, Privatnutzung, Zugriff auf E-Mail-Konto eines verstorbenen Mitarbeiters), Videobeobachtung, Erstellung eines Videokonzepts, Einführung von Fingerprintsystemen zur Zugangskontrolle und Zeiterfassung, Telefondatenerfassung, Aufnahme von Konferenzen per Webcam, Mitarbeiterscreening, Übermittlung von Personaldaten in Drittstaaten, Übermittlung von Personaldaten innerhalb des Konzerns, Einführung eines zentralen Personalverwaltungssystems im Konzern, Weitergabe von Bewerbungsunterlagen, Arbeitsverträgen und Personalakten an Dritte, Outsourcing von Personalsachbearbeitung, Einführung der digitalen Personalakte, Veröffentlichung von Personaldaten im Internet, Aufdruck der Privatanschrift auf dienstlicher Visitenkarte, Mitarbeiterranking, Löschung von Bewerberdaten, SCHUFA-Eigenauskunft als Einstellungsvoraussetzung, Auswirkungen der BDSG-Novelle (§ 32 BDSG) auf den Arbeitnehmerdatenschutz.

#### **45 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände:**

Beratung des Deutschen Fußball-Bundes (DFB) u.a. hinsichtlich der Vermarktung von Adressen von Fan-Club-Mitgliedern und Abonnenten des DFB-Newsletters, Datenweitergabe im Rahmen von Doping-Überwachungsmaßnahmen, Einwilligung der Spieler, die zum Kader der Nationalmannschaft eingeladen sind hinsichtlich der Verarbeitung ihrer Gesundheitsdaten, Maßnahmen zur Sicherheit der Zugriffe auf die Schiedsrichterdatenbank, Einwilligungserklärungen für die Datenbank der Nationalmannschaft, Veröffentlichung von Spielerdaten im Internet unter Beachtung von Sportgerichtsurteilen, Veröffentlichung dieser Urteile, Verkauf von Eintrittskarten

gegen Vorlage des Personalausweises, Prüfung eines Sicherheitskonzeptes, Übermittlung von Adresslisten an Sky, Datenschutzbestimmungen und Ticketverkauf zur FIFA-Frauen-WM 2011.

Weitere Anfragen betrafen u. a. die Videoüberwachung eines Vereinsheimes, Veröffentlichung von Start- und Ergebnislisten im Internet, Veröffentlichung von Mitgliederdaten auf der Homepage des Vereins, Weitergabe dieser Daten an einzelne Mitglieder und den Kreisverband, Datenschutzerklärung für Vereine, Bestellung von Datenschutzbeauftragten, Archivierung und Löschung von Mitgliederdaten sowie die Herausgabe eines Newsletters der Hessischen Jugendfeuerwehr mit den E-Mail-Adressen der Jugendfeuerwehrwarte.

### **35 Anfragen zu Telemedien und Internet:**

Zulässigkeit von Suchmaschinen im www, insbesondere von sogenannten Personensuchmaschinen (siehe hierzu Ziffer 9.3 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 17/663) [*Berichte der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde werden im Folgenden jeweils in einer Kurzform als "Bericht der Landesregierung" zitiert.*], Informationen zur Auskunftserteilung an Betroffene im Online-Bereich nach § 13 Abs. 7 TMG i. V. m. § 34 BDSG, Unzulässigkeit der Veröffentlichung von IP-Nummern in einem Internet-Forum, Fragen zur Veröffentlichung der Daten von deutschen Domaininhabern durch den Whois-Dienst der DENIC e.G., Beratungsanfragen zur werblichen Nutzung von im www erhobenen personenbezogenen Daten, Entscheidungshilfen bei der Anwendung von Tools zur Reichweitenanalyse und zum User-Tracking im www, Schaffung von Transparenz durch Information der Betroffenen bei einer wesentlichen Änderung der Kundendatenverwaltung, Beratung bei der Erstellung eines Branchenverzeichnisses im Internet, Stellungnahmen gegenüber der Presse und Beratung von Bürgerinnen und Bürgern zu digitalen Straßenansichten im www und geodatengestützten Diensten (siehe Ziffer 9.1 des 22. Berichts der Landesregierung, Drucks. 18/1015), Informationen zum Verbot der Rufnummerunterdrückung bei Werbeanrufen, Erläuterungen der Funktionsweise von E-Mail-Diensten, keine Impressumspflicht auf privaten Homepages mit nicht-geschäftsmäßig und ohne Entgelt angebotenen Telemedien nach § 5 Abs. 1 TMG, Beratungsersuchen zur Erstellung eines Datenschutz- und Sicherheitskonzeptes, Fragen zur Zulässigkeit der Übermittlung personenbezogener Daten an Dritte sowie der Weitergabe an Auftragnehmer nach § 11 BDSG, Umgang mit den Daten von Verstorbenen bei Kunden- und E-Mail-Konten, Fragen zur Zulässigkeit spezieller Internetdienste, die nach dem Tod eines Nutzers gewährleisten sollen, dass dessen Online-Accounts und www-Seiten gelöscht und seine Freunde benachrichtigt werden, Zulässigkeitsvoraussetzungen für die Online-Erhebung personenbezogener Daten zur Veröffentlichung und zu Werbezwecken, Beratung bei der Einführung des Double-Opt-In-Verfahrens, Beratung bei der Veröffentlichung mikrogeographischer Daten, datenschutzgemäße Ausgestaltung eines Verfahrens, bei dem Neukunden von Bestandskunden gewonnen werden sollen, Informationen zu Data-Mining-Verfahren, Zulässigkeitsvoraussetzungen für die Veröffentlichung besonderer Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) im www, Nicht-Anwendbarkeit datenschutzrechtlicher Regelungen auf Daten, die mangels Personenbeziehbarkeit nicht unter § 3 Abs. 1 BDSG fallen, Beratung bei der Entwicklung eines Systems für eine mobile Mitfahrzentrale für Smartphone-Nutzer, Information über Schadsoftware auf ausländischen Internet-Seiten, Beratung und Unterstützung bei der Löschung der Daten eines Online-Accounts bei einem amerikanischen Anbieter, Hilfestellung für Opfer von Internet-Kostenfallen (siehe Ziffer 9.2 des 21. Berichts der Landesregierung, Drucks. 17/663), Beratung von Opfern diverser Telefonbetrügereien, datenschutzkonforme Erhebung und Speicherung von Daten im www, Informationen zum Vorgehen gegen unerwünschte Online-Veröffentlichungen, Gestaltung der Datenschutzerklärungen bei Internetauftritten nach § 13 Abs. 1 TMG, Zulässigkeit der Veröffentlichung von Stammbäumen im www, Veröffentlichung von Forschungsergebnissen bezüglich Familien- und Ortsgeschichte, Schutz vor Angriffen und Verunglimpfung im Internet.

### **29 Anfragen aus dem Gesundheitssektor:**

Übermittlung von Patientendaten durch die Patientenverwaltung einer Reha-Klinik an die gesetzliche Krankenversicherung, Überprüfung der Einwilligungserklärung für ein Forschungsvorhaben bei Morbus Parkinson, Fragen zur Bestellpflicht eines Datenschutzbeauftragten für Arztpraxen, Bitte eines Herstellers von Inkontinenzmitteln um Prüfung eines Mustertextes, Speicherung von personenbezogenen Daten von Personal und Betreuten einer Pflegeeinrichtung auf einem Rechner mit Internetanschluss, Aktenarchivierung von Patientenakten durch einen Dienstleister, Rechteeinschätzung zur Veräußerung von Kundendaten eines Optikers ohne Kenntnis und Einwilligung der Betroffenen, Erstellung einer medizinischen Datenbank durch einen Verein mit der Möglichkeit der Online-Abfrage, Übermittlung von Patientendaten im Rahmen der Qualitätssicherung in der stationären Patientenversorgung, Übermittlung von Anschriften von Vereinsmitgliedern an einen ambulanten Pflegedienst, Entwurf einer Broschüre "Datenschutz in Arztpraxen", Zugriffskontrolle bei der Nutzung von Versandapotheken, Fragen zu Studien im Ärztemfeld, Datenübermittlung durch Apothekenrechenzentren, Verwendung von Patientendaten eines Schlaflabors durch die betreibende Ärztin nach Ausgliederung des Schlaflabors aus dem Krankenhaus, Aufbewahrung von Akten Pflegebedürftiger nach dem Tod des Pflegedienstbetreibers.

### **23 Anfragen zum Datenschutz bei Banken:**

Klausel zur Weitergabe der Adressdaten zu Werbezwecken in einem Kreditvertrag, Identifizierung mittels Fingerprint in Tastatur, Fertigung von Ausweiskopien durch die Bank, Abfrage der persönlichen und finanziellen Verhältnisse bei Eröffnung eines Girokontos, Ausgestaltung und Übergangsfristen der Auftragsdatenverarbeitung nach der BDSG-Novelle, Datenverlust und Meldung nach § 42a BDSG, Herausgabe von Informationen zu einem Depot an eine ausländische Steuerbehörde, Informationsaustausch der Geldwäschebeauftragten, Einsatz und Verwendung der Verbund-/Allfinanzklausel, Einsatz von freien Handelsvertretern im Vertrieb, Aufzeichnung von Telefongesprächen, Fragen im Zusammenhang eines Unternehmenszusammenschlusses, Outsourcing nach KWG und Auftragsdatenverarbeitung.

**16 Anfragen zum betrieblichen Datenschutzbeauftragten:**

Fachliche Voraussetzungen für den betrieblichen Datenschutzbeauftragten, Aus- und Fortbildungsmöglichkeiten für den betrieblichen Datenschutzbeauftragten, allgemeine und spezielle Fragen bzgl. der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, Datenschutzbeauftragte in Anwaltskanzleien, mögliche Interessenkonflikte zwischen der Funktion des internen betrieblichen Datenschutzbeauftragten und anderen Tätigkeiten im Unternehmen (Geldwäschebeauftragter, Betriebsrat, IT-Leiter, Systemadministrator, sonstige IT-Mitarbeiter), Interessenkonflikt bei einem externen Datenschutzbeauftragten, der bei dem vom Unternehmen beauftragten Datenverarbeitungsdienstleister tätig ist, Vertragslaufzeit von externen Datenschutzbeauftragten, Kündigungsschutz des Datenschutzbeauftragten, Auswirkungen der BDSG-Novelle auf die Stellung des Datenschutzbeauftragten.

**15 Anfragen zur Videoüberwachung**

Anfragen zur rechtlichen Zulässigkeit der Videoüberwachung von privaten Grundstücken, Treppenhäusern, Tiefgaragen und in Ladengeschäften, zur Zulässigkeit einer Speicherung der Aufnahmen und hinsichtlich der Speicherdauer, Fragen zur Videoüberwachung des Finanzzentrums Kassel, zur Zulässigkeit von Wildkameras an Kirmungen (siehe hierzu Ziffer 13) und zum Einsatz von Webcams an Baustellen.

**13 Anfragen zur Datenverarbeitung im Ausland:**

Beratungsersuchen zu den Anforderungen an Mehrparteienverträge, die als Grundlage für den Transfer personenbezogener Daten an Stellen außerhalb der Europäischen Union und der Mitgliedstaaten des Europäischen Wirtschaftsraumes dienen sollen, Fragen zur Genehmigungsbedürftigkeit, wenn die Mehrparteienverträge auf den Standardvertragsklauseln basieren (siehe hierzu Ziffer 11.2), sonstige Fragen zum Einsatz der Standardvertragsklauseln, zu Safe Harbor und zu verbindlichen Unternehmensregelungen zum Drittstaatentransfer.

**7 Anfragen zur Werbewirtschaft**

Information zum Telemarketing, zur Löschung von Kundendaten bei Insolvenz eines Unternehmens, zum Data Mining, zur Zulässigkeit eines Kunden-werben-Kunden-Programms, zur Zulässigkeit der Adressierung von privater Post an dienstliche Adressen, zur Zulässigkeit von Postwerbung eines Steinmetzbetriebes nach Sterbefall, Prüfung eines Verfahrens zur rechtsgültigen Online-Registrierung, Anfrage zur Zulässigkeit einer Werbekampagne.

**6 Anfragen aus dem Bereich Miete und Wohnen**

Bonitätsauskünfte im Wohnungswesen, Erfassung von Heizmessdaten per Funkabruf, Frage der Rechtmäßigkeit der Herausgabe von E-Mail-Adressen und Telefonnummern von Wohnungseigentümern durch die Wohnungsverwaltung an den Verwaltungsbeirat, Abfrage des Geburtsdatums von Kunden durch ein Energieversorgungsunternehmen bei telefonischen Vertragsänderungen, Reichweite und gesetzliche Grenzen des Datenschutzes im Wohnbereich, Frage ob für Energieversorgungsunternehmen das Bundes- oder das jeweilige Landesdatenschutzgesetz anzuwenden ist.

**5 Anfragen zur Versicherungsbranche**

Beratung zur datenschutzgerechten Gestaltung der Einwilligungserklärung einer Versicherungsgesellschaft, Auskunft zur Löschung und Sperrung von Versicherungsdaten im Zusammenhang mit einem Vertragsvorverhältnis bei einem nicht zu Stande gekommenen Vertrag, Beantwortung zweier Anfragen zur Rechtmäßigkeit der Verlagerung von Versichertendaten an einen Datenverarbeitungsdienstleister in den USA, Einschätzung der Maßnahmen zur Überprüfung von Mitarbeiterinnen und Mitarbeitern einer Versicherungsgesellschaft durch eine Sicherheitsfirma.

**5 Anfragen zur Auftragsdatenverarbeitung**

Pflichten des Auftragnehmers bei Angebot einer Standesamtssoftware, Anpassung bestehender Verträge an die Anforderungen des neuen § 11 BDSG, Anwendung des § 11 Abs. 4 BDSG bei Auftragnehmern aus anderen EU-Mitgliedstaaten, Gestaltung eines Vertrags nach § 11 BDSG, Mustervereinbarungen der Aufsichtsbehörde (siehe hierzu Ziffer 10).

**4 Anfragen zum Einzelhandel**

Elektronische Erfassung der Daten in einem Möbelhaus bei Kartenzahlung, Mithören von Verkaufsgesprächen durch andere Kunden bei einem Automobilhändler, Einlesen von Personalausweisen bei einem Unternehmen der Unterhaltungselektronikbranche beim Kauf einer CD mit Altersbeschränkung.

**3 Anfragen zur Markt- und Meinungsforschung**

Datentreuhänder in der Markt- und Sozialforschung, Mithören telefonischer Interviews, Kundenbefragung in der S-Bahn, Gründung eines Markt- und Meinungsforschungsinstituts.

**23 Anfragen aus unterschiedlichen Wirtschafts- und Lebensbereichen**

Verarbeitung von Kontendaten bei Parkplatzbenutzung, Gesetzliche Anforderungen zur Erlangung eines Datenschutz-Qualitätssiegels, Übermittlung von Kundendaten an das Jugendamt, Weitergabe von Kundendaten bei Betriebsübernahme, Einrichtung einer Auskunftssperre beim Einwohnermeldeamt, Aufzeichnung von Mitgliedsdaten in einem Club, Änderungen durch die BDSG-Novellen 2009 (siehe hierzu Ziffer 6), Weitergabe der Namen von spendenden Vereinsmitgliedern an den Empfänger, Aufstellung aller potentiell personenbezogene Daten speichern den Unternehmen in Hessen, Rechtsunsicherheit bei der Anwendung des neuen § 42a BDSG, Datenschutz bei Abschluss eines Kreditvertrages, Dokumentationspflichten eines Unternehmens, Grundanforderungen an ein Geschäftsmodell mit der Möglichkeit zur Abfrage personenbezogener Daten, Datenschutz im Rahmen der Finanzberatung, Einführung einer "Geld-zurück-Garantie" beim Getränkehandel, Fragen zum Datenschutz im Versandhandel, Zulässigkeit der Erhebung von Unterschriften auf mobilen Datenerfassungsgeräten, Erfassung und Speicherung von

Trainingsdaten auf mobilen Speichermedien (Chipkarten), Sicherheitsanforderungen an die Übermittlungstechnik bei besonderen Arten personenbezogener Daten.

## **2.2 Öffentlichkeitsarbeit**

Die Aufsichtsbehörde präsentierte sich am 9. Juni 2009 mit einem Stand auf dem Hessentag in Langenselbold. Hier konnten die Mitarbeiter die Fragen vieler interessierter Bürger beantworten und diese vor Ort in datenschutzrechtlicher Hinsicht beraten.

Vertreterinnen und Vertreter des Regierungspräsidiums Darmstadt haben auch im Jahr 2009 im Rahmen von Informationsveranstaltungen diverser Veranstalter wieder Fragen zum Datenschutz beantwortet und Vorträge gehalten.

Die Aufsichtsbehörde nahm am Erfahrungsaustauschkreis Hessen der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. teil und berichtete über die Aufsichtstätigkeit sowie die Beschlüsse des Düsseldorfer Kreises und beantwortete Fragen der anwesenden betrieblichen Datenschutzbeauftragten.

Auch bei Veranstaltungen anderer Erfahrungsaustauschkreise betrieblicher Datenschutzbeauftragter in Hessen war die Aufsichtsbehörde vertreten, u.a. an einem Regionaltreffen des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Bei der Fachgruppe Einzelhandel der Gewerkschaft ver.di wurde ein Vortrag zum Mitarbeiterdatenschutz mit dem Schwerpunkt "Videoüberwachung im Arbeitsverhältnis" gehalten.

Nach Verabschiedung der Novellen zum Bundesdatenschutzgesetz entstand in Fragen des Arbeitnehmerdatenschutzes besonderer Informationsbedarf. So informierte die Aufsichtsbehörde den Hauptverband des Deutschen Einzelhandels e. V. mit einem Referat über die Änderungen im Arbeitnehmerdatenschutz durch den neuen § 32 BDSG. Dem Wunsch der Industrie- und Handelskammer (IHK) Darmstadt sowie des CAST- Forum e.V., Darmstadt nach einem Vortrag über die wichtigsten Neuerungen (siehe hierzu Ziffer 6, 7.1, 10 und 15) kam die Aufsichtsbehörde jeweils gerne nach.

Im Jahr 2010, vor Redaktionsschluss dieses Berichts, folgte das Regierungspräsidium Darmstadt auch der Einladung zur gemeinsamen Veranstaltung der IHK Frankfurt und des IHK-Forums Rhein-Main und informierte hierbei ausführlich über die BDSG-Novellen. Ferner referierte die Aufsichtsbehörde erneut beim CAST-Forum e.V.

Schon seit mehreren Jahren besteht ein regelmäßiger Kontakt mit der Hochschule Darmstadt. Auch im Sommersemester 2009 besuchten Studenten des Studiengangs "Informationswissenschaft" die Aufsichtsbehörde, um sich über deren Tätigkeit und aktuelle Themen aus der Aufsichtspraxis zu informieren.

Das Angebot an Informationsmaterial, das die Datenschutzaufsichtsbehörde zu unterschiedlichsten Fragestellungen des Datenschutzrechts u.a. auch auf den www-Seiten des Regierungspräsidiums Darmstadt unter "www.datenschutzaufsicht.hessen.de" bereithält, wurde wieder gut angenommen.

## **3. Register der meldepflichtigen Verfahren nach § 4d BDSG**

Die Aufsichtsbehörde führt gemäß § 38 Abs. 2 BDSG ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen.

Am Ende des Berichtsjahres waren 120 Verfahren von 104 verantwortlichen Stellen im Melderegister eingetragen. Nur sechs verantwortliche Stellen haben mehr als ein Verfahren gemeldet. Davon werden in 67 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler, Handels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG). Die weiteren 53 der eingetragenen Verfahren dienen dem Zweck der anonymisierten Übermittlung (§ 4d Abs. 4 Nr. 2) und dem Zweck der Markt- und Meinungsforschung (§ 4d Abs. 4 Nr. 3 BDSG).

## **4. Ordnungswidrigkeitenverfahren**

Die noch offenen Verfahren aus 2008 wurden alle im Berichtsjahr 2009 beendet. Bei drei Verfahren wurde das Bußgeld durch Beschluss des Amtsgerichts in der Sache bestätigt, aber in der Höhe jeweils von 1.000 € auf 500 € reduziert. In sechs Verfahren wurde das Bußgeld in der von der Aufsichtsbehörde verhängten Höhe bestands- bzw. rechtskräftig. Damit ist aus den vorangegangenen Berichtsjahren nur noch ein Ordnungswidrigkeitenverfahren offen, in dem das Amtsgericht der Aufsichtsbehörde den Fall zur Durchführung von weitergehenden Ermittlungen zurückgereicht hat.

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt elf Verstöße nach dem Ordnungswidrigkeitengesetz (OWiG) mit einem Bußgeldbescheid geahndet (siehe nachfolgende Tabelle). Drei Verfahren befinden sich noch im Stadium der Anhörung. Zwei Verfahren, die durch eine Anhörung eingeleitet wurden, sind auf Grund der Rücküberlegungen eingestellt worden. In mehreren Fällen hat die Aufsichtsbehörde im Jahr 2009 zwar Ermittlungen eingeleitet, der Bußgeldbescheid erging jedoch erst im Jahr 2010, bzw. in einigen Fällen dauern die Ermittlungen noch



an. In zwei Fällen wurde der Vorgang nach § 41 OWiG der Staatsanwaltschaft vorgelegt, weil Anhaltspunkte für eine Straftat nach § 44 BDSG vorlagen (siehe hierzu Ziffer 8.1).

#### Übersicht über die im Jahr 2009 erlassenen Bußgeldbescheide:

Verstoß	Grund	Rechtskraft/Bußgeldhöhe
§ 43 Absatz 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Rechtskräftig Bußgeld 1.000 €
§ 43 Absatz 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Rechtskräftig Bußgeld 3.000 €
§ 43 Absatz 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Bußgeldbescheid erteilt, Einspruch erhoben
§ 43 Absatz 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Rechtskräftig Bußgeld 3.000 €
§ 43 Absatz 1 Nr. 5	Keine Aufzeichnung des berechtigten Interesses	Rechtskräftig Bußgeld 1.000 €
§ 43 Absatz 1 Nr. 5	Keine Aufzeichnung des berechtigten Interesses	Rechtskräftig Bußgeld 1.000 €
§ 43 Absatz 1 Nr. 10	Nichterteilung von Auskünften	Rechtskräftig Bußgeld 1.000 €
§ 43 Absatz 1 Nr. 10	Nichterteilung von Auskünften	Bußgeldbescheid erteilt, Einspruch erhoben
§ 43 Absatz 1 Nr. 10	Nichterteilung von Auskünften	Bußgeldbescheid erteilt, noch offen
§ 43 Absatz 2 Nr. 1	Unbefugte Erhebung oder Verarbeitung personenbezogener Daten	Rechtskräftig Bußgeld 5.000 €
§ 43 Absatz 2 Nr. 1	Unbefugte Erhebung oder Verarbeitung personenbezogener Daten	Rechtskräftig Bußgeld 235.000 €

Wie sich aus der Übersicht ersehen lässt, beruhen die meisten Bußgeldbescheide auf Verstößen gegen § 38 Absatz 3 BDSG oder § 4f BDSG. In diesen Fällen waren der Aufsichtsbehörde die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte nicht, nicht vollständig oder nicht unverzüglich erteilt worden, oder es war trotz Vorliegen der gesetzlichen Voraussetzungen kein Beauftragter für den Datenschutz bestellt.

Das höchste Bußgeld (235.000 €) wurde gegen ein Unternehmen (juristische Person) verhängt, weil dieses Daten über Mitarbeiterinnen und Mitarbeitern unzulässig erhoben und verarbeitet hatte (siehe hierzu Ziffer 12.3). Hier wurden mehrere Einzelverstöße je nach Art und Umfang der Daten in unterschiedlicher Höhe bewertet und zu einem Bußgeld zusammengefasst.

Mit dem höchsten Bußgeld gegen eine natürliche Person (5.000 €) wurde geahndet, dass ein Mitarbeiter in leitender Position Daten von Mitarbeiterinnen und Mitarbeitern nach Beendigung seines Arbeitsverhältnisses nicht löschte und diese Daten auf den ihm vom neuen Arbeitgeber dienstlich zur Verfügung gestellten Laptop einspielte.

Zwei Bußgelder wurden wegen Nichtaufzeichnung des berechtigten Interesses verhängt. Beiden Fällen lag folgender Sachverhalt zugrunde:

Auf das Auskunftersuchen eines Betroffenen nach § 34 BDSG teilte die Auskunft diesem mit, dass sie die Unterlagen über das berechtigte Interesse des anfragenden Unternehmens vernichtet hat. Der Datenübermittlung an das Unternehmen lag kein automatisiertes Abrufverfahren nach § 10 BDSG zugrunde. Nach § 29 Absatz 2 Satz 3 BDSG sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle, also der Auskunft, aufzuzeichnen. Die nicht vorgehaltene Dokumentation bedeutet einen Verstoß gegen das BDSG, der im Rahmen eines Ordnungswidrigkeitenverfahrens nach § 43 Absatz 1 Ziffer 5 BDSG zu ahnden war. Auch die Tatsache, dass von der Firma nur in einem Einzelfall eine Anfrage gestellt wurde und keine geschäftsmäßige Verbindung zwischen Firma und Auskunft zu Stande kam, berechtigt die Auskunft nicht, die Unterlagen und die Begründung des berechtigten Interesses zu vernichten. Die stichprobenartige Überprüfung des vorliegenden Interesses und auch die Überprüfungen der Aufsichtsbehörde für den nicht öffentlichen Bereich vor Ort würden ansonsten durch die Vernichtung von Unterlagen über das berechtigtere Interesse beeinträchtigt.

#### 5. Teilnahme an den Sitzungen des Düsseldorfer Kreises und den Arbeitsgruppen

Das Regierungspräsidium Darmstadt war wieder, zum Teil gemeinsam mit dem Hessischen Ministerium des Innern und für Sport, an der Arbeit des Düsseldorfer Kreises und den von diesem gebildeten Arbeitsgruppen beteiligt und nahm an dessen Sitzungen sowie an denen der meisten Arbeitsgruppen teil (siehe Ziffer 6. des 20. Berichts der Landesregierung, Drucks. 16/7646). In der Sitzung der Arbeitsgruppe Auskunfteien im Juni 2009 führte das Regierungspräsidium Darmstadt den Vorsitz.

Die vom Düsseldorfer Kreis gefassten Beschlüsse sind auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit veröffentlicht ("<http://www.bfdi.bund.de>", Pfad: "Datenschutz/Entschlüssen/ Düsseldorf Kreis").

Einmal im Jahr treffen sich die Aufsichtsbehörden zu einem Workshop, um sich zu Fragen der praktischen Durchführung der Aufsichtstätigkeit (z.B. Durchführung der Kontrollen vor Ort) auszutauschen. Auch an dem im Berichtsjahr vom Innenministerium Baden-Württemberg veranstalteten Workshop hat das Regierungspräsidium Darmstadt teilgenommen.

## 6. Überblick über die Novellen des BDSG

Ende der letzten Legislaturperiode wurden im Deutschen Bundestag drei Novellen des Bundesdatenschutzgesetzes beschlossen. Ein Schwerpunkt der Tätigkeit der Aufsichtsbehörde beim Regierungspräsidium Darmstadt lag daher in der Information über diese Änderungen, in der Beratung über die Umsetzung sowie in der Klärung von Auslegungsfragen (siehe bereits oben Ziffer 2.1 und 2.2).

Das Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009 (BGBl. I, S. 2254, "**Novelle I**") betrifft im Wesentlichen das Auskunftswesen. Insbesondere die Kritik von Datenschutzbehörden und Verbraucherschützern an mangelnder Transparenz und unzureichender Rechtsicherheit im Auskunftswesen und im (Kredit-) Scoring hat den Gesetzgeber bewogen, mit dieser Novelle die Informations- und Auskunftsrechte der Betroffenen zu stärken und spezielle Erlaubnistatbestände einzuführen. (Näheres siehe hierzu unter Ziffer 7.1).

Das Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 14. August 2009 (BGBl. I S. 2814, "**Novelle II**") ist maßgeblich durch "Datenschutzskandale" motiviert, die insbesondere durch illegalen Datenhandel und Fälle ausufernder Mitarbeiterkontrolle gekennzeichnet waren. Dazu wurden umfangreiche Neuregelungen zur Werbung und zum Adresshandel getroffen (Näheres siehe hierzu unter Ziffer 15). Außerdem wurde eine Vorschrift zum Beschäftigtendatenschutz eingefügt (§ 32 BDSG), die aber erhebliche Auslegungsprobleme mit sich brachte. Es ist daher zu begrüßen, dass die Bundesregierung im April 2010 Eckpunkte für detailliertere Regelungen zum Beschäftigtendatenschutz veröffentlicht hat. Des Weiteren wurde der Grundsatz der Datenvermeidung und Datensparsamkeit über den Systemdatenschutz generell auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erstreckt (§ 3a BDSG). Bedeutsam sind auch die Neuregelungen für die Auftragsdatenverarbeitung (Näheres siehe hierzu unter Ziffer 10). Bei bestimmten Fällen von "Datenpannen" (unrechtmäßige Kenntniserlangung sensibler Daten) sind die verantwortlichen Stellen künftig verpflichtet, die Betroffenen und die Aufsichtsbehörde zu informieren. Zur Auslegung und damit zum Anwendungsbereich der diesbezüglichen neuen Vorschrift des § 42a BDSG bestehen viele Zweifelsfragen, die an die Aufsichtsbehörde herangetragen wurden. Die Aufsichtsbehörde verschafft sich derzeit durch entsprechende Fallsammlungen einen Überblick, um auf deren Grundlage zu Bewertungen zu gelangen. Erste Abstimmungen mit anderen Aufsichtsbehörden haben begonnen.

Durch die Novelle II wurde auch die Unabhängigkeit der betrieblichen Datenschutzbeauftragten durch die Einräumung eines Kündigungsschutzes (§ 4f Abs. 3 Satz 5 und 6 BDSG) und die explizite Aufnahme eines Rechts auf Fort- und Weiterbildung (§ 4f Abs. 3 Satz 7 BDSG) gestärkt. Es bleibt zu hoffen, dass dies zu einer Stärkung der betrieblichen Selbstkontrolle führen wird.

Auch die Datenschutzkontrolle durch die Aufsichtsbehörden wurde gestärkt. Zum einen sind die Anordnungs- und Untersagungsrechte der Aufsichtsbehörden in § 38 Abs. 5 BDSG erweitert worden. Bisher konnten die Aufsichtsbehörden nur bei festgestellten Mängeln im technisch-organisatorischen Bereich nach § 9 BDSG Anordnungen zur Mängelbeseitigung erlassen und in schwerwiegenden Fällen ggf. den Einsatz einzelner Datenverarbeitungsverfahren untersagen. Diese Befugnis hatte allerdings in der Praxis so gut wie keine Bedeutung, weil die der Kontrolle unterliegenden Stellen bei festgestellten Mängeln dieser Art in aller Regel einsichtig waren und die Mängel von sich aus behoben. Angesichts der vielen unbestimmten Rechtsbegriffe und Abwägungsklauseln im Bundesdatenschutzgesetz blieb hingegen zwischen den Aufsichtsbehörden und den verarbeitenden Stellen eher streitig, ob eine Datenverarbeitung überhaupt materiell-rechtlich zulässig war. Hier kam allenfalls unter bestimmten Voraussetzungen ein Bußgeld in Betracht. Ordnungswidrigkeitenverfahren sind aber nur begrenzt zur Klärung schwieriger Auslegungsfragen geeignet. Im Übrigen waren die Betroffenen auf den Zivilrechtsweg zu verweisen. Mit der Neuregelung in § 38 Abs. 5 BDSG verfügen die Aufsichtsbehörden nun über die Befugnis, bei jeglichen Verstößen Maßnahmen zu deren Beseitigung anzuordnen. Bei Nichtabhilfe schwerwiegender Verstöße oder Mängel kann eine Untersagungsverfügung erlassen werden.

Zum anderen erweiterte der Gesetzgeber die Sanktionsmöglichkeiten mittels Bußgeld durch neue Bußgeldtatbestände. Überdies wurde der Bußgeldrahmen auf 50.000 € (bislang 25.000 €) bei Verstößen nach § 43 Abs. 1 BDSG und auf 300.000 € (bislang 250.000 €) bei materiellen Verstößen nach § 43 Abs. 2 BDSG erhöht, wobei § 43 Abs. 2 BDSG eine "Gewinnabschöpfung" vorsieht. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die genannten Beträge nicht aus, so können sie sogar überschritten werden.

Mit Artikel 5 des Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29. Juli 2009 (BGBl. I, S. 2355, "**Novelle III**") wurde Artikel 9 der Verbraucherkreditrichtlinie umgesetzt, wonach Kreditgeber aus sämtlichen Mitgliedstaaten ein diskriminierungsfreier Zugang zu den Auskunftssystemen zu gewähren ist. Die Novelle regelt den Anspruch der Betroffenen auf Information über solche Datenbankabfragen (§ 29 Abs. 6 und 7 BDSG). Der Anspruch besteht nur, wenn der Abschluss eines Verbraucherdarlehensvertrages (§ 491 Abs. 1 BGB)

oder eines Vertrages über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft abgelehnt wird.

### **Ausgesuchte Probleme und Einzelfälle**

## **7. Auskunftfeien und deren Vertragspartner**

### **7.1 Gesetzliche Neuregelungen im Bereich Auskunftfeien und Scoring**

Nachfolgend werden die wesentlichen Änderungen der Novelle I dargestellt.

#### **a) Datenübermittlung an Auskunftfeien**

Bislang war nicht speziell geregelt, welche Daten unter welchen Voraussetzungen von Unternehmen an Auskunftfeien übermittelt werden dürfen. Maßgeblich war hier im Wesentlichen nur die Interessenabwägung zwischen den Interessen der kreditgebenden Wirtschaft an Bonitätsinformationen über (potentielle) Kunden und den schutzwürdigen Belangen der Kunden nach § 28 Abs. 1 Nr. 2 und § 28 Abs. 2 Nr. 2 BDSG. Bei Banken war ferner das Bankgeheimnis relevant. Am 1. April 2010 ist nun der neue § 28a BDSG in Kraft getreten, der speziell die Datenübermittlung an Auskunftfeien regelt.

§ 28a Abs. 1 BDSG enthält einen abschließenden Katalog der Fallgruppen, in denen eine Datenübermittlung über eine Forderung statthaft ist.

Bedeutsam ist insbesondere § 28a Abs. 1 Satz 1 Nr. 4 BDSG. Darin sind vier Voraussetzungen aufgezählt, die erfüllt sein müssen, um eine nicht titulierte und nicht ausdrücklich anerkannte Forderung bei einer Auskunftfeieinmelden zu können:

- Der Betroffene muss nach Eintritt der Fälligkeit mindestens zweimal schriftlich gemahnt worden sein.
- Der Gläubiger muss den Betroffenen rechtzeitig (frühestens jedoch mit der ersten Mahnung) über die geplante Meldung an die Auskunftfeieinfordern.
- Zwischen der ersten Mahnung und der Meldung an die Auskunftfeie müssen mindestens vier Wochen liegen.
- Die Forderung darf durch den Betroffenen nicht bestritten worden sein.

Diese Voraussetzungen entsprechen im Wesentlichen den Kriterien, die bereits vor längerer Zeit von den Aufsichtsbehörden im Düsseldorf-Kreis entwickelt wurden, damit die Interessen der Betroffenen angemessen gewahrt werden konnten. Angesichts der unbestimmten Rechtslage waren diese allerdings nicht vollständig durchsetzbar. Die Aufsichtsbehörde erhofft sich, dass durch die gesetzlichen Vorgaben künftig unzulässige Einmeldungen und Fehler bei den Vertragspartnern der Auskunftfeien vermieden werden.

Bei der Einmeldung von Forderungen, die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder für die ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt (§ 28a Abs. 1 Satz 1 Nr. 1 BDSG), ist folgendes zu beachten: Es wäre rechtsmissbräuchlich, wenn ein Gläubiger eine Forderung bei einer Auskunftfeieinmelden würde, ohne dem Schuldner eine reale Möglichkeit zu geben, die Forderung nach der Titulierung (unverzüglich) zu begleichen (siehe die Stellungnahme der Bundesregierung im Gesetzgebungsverfahren, BT-Drucksache 16/10581, Seite 2). Entsprechendes gilt auch bei der Einmeldung von Forderungen, die der Schuldner ausdrücklich anerkannt hat (§ 28a Abs. 1 Satz 1 Nr. 3 BDSG). Diese Einschränkung findet sich zwar nicht im Wortlaut des Gesetzes, ergibt sich aber daraus, dass der Gesetzgeber nur diejenigen Fallgruppen auflisten wollte, bei denen die Nichterfüllung der Forderung auf Zahlungsunfähigkeit oder Zahlungsunwilligkeit beruht. Nur unter dieser Voraussetzung haben die anderen Vertragspartner der Auskunftfeie, für welche die Daten vorgesehen sind, ein berechtigtes Interesse an der Information.

In § 28a Abs. 2 BDSG ist geregelt, unter welchen Umständen Kreditinstitute personenbezogene Daten über Vertragsverhältnisse an Auskunftfeien übermitteln dürfen. Dabei erlaubt § 28a Absatz 2 Satz 1 BDSG es den Kreditinstituten, Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunftfeien zu übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftfeie an der Kenntnis der Daten offensichtlich überwiegt.

Im Gegensatz zu "Negativdaten", also Daten über Zahlungsstörungen, die ein Indiz für die Zahlungsunwilligkeit oder -unfähigkeit sind, konnte die Übermittlung solcher "Positivdaten" nicht auf die allgemeinen Abwägungsklauseln in § 28 Abs. 1 Nr. 2 und § 28 Abs. 2 Nr. 2 BDSG gestützt werden. Daher mussten die Kreditinstitute eine Einwilligung der Betroffenen und die Befreiung vom Bankgeheimnis hinsichtlich der Datenübermittlung an die Auskunftfeieinholen. Für Verbraucher war es nicht möglich, beispielsweise einen Bankkredit zu erhalten, ohne eine entsprechende Einwilligungsklausel zu unterschreiben. In der Begründung zur Novelle ist daher ausgeführt, dass es mangels zumutbaren Alternativverhaltens zweifelhaft sein kann, ob die vom Betroffenen erteilte Einwilligung noch als freiwillig anzusehen ist. An die Stelle der Einwilligungserklärung tritt daher laut Gesetzesbegründung der neue Erlaubnistatbestand in Absatz 2 (BT-Drucksache 16/10529, Seite 15). Der Betroffene ist aber vor Vertragsabschluss über die Übermittlung zu unterrichten (§ 28a Abs. 2 Satz 2 BDSG).

Wenn Kreditinstitute auch künftig gleichwohl eine Einwilligung einholen, begeben sie sich auf unsicheres Gebiet. Die Befreiung vom Bankgeheimnis kann nach wie vor separat eingeholt werden, falls die Kreditinstitute dies für erforderlich halten.

Für Girogeschäfte ohne Kreditlinie gilt die gesetzliche Erlaubnis nicht. Ebenso stellt das Gesetz klar, dass Anfragen über Kreditkonditionen, die dem Kunden dazu dienen, Vergleiche unter den Angeboten der Kreditinstitute zu ziehen, nicht in den Auskunftsbestand einer Auskunft übermittelt werden dürfen. Damit ist der Gesetzgeber der von den Aufsichtsbehörden schon zur alten Rechtslage vertretenen Rechtsauffassung gefolgt (siehe Ziffer 7.3 des 21. Berichts der Landesregierung, Drucks. 17/663).

Da § 28a Abs. 2 BDSG nicht für Leasingunternehmen und Telekommunikationsunternehmen gilt, benötigen diese nach wie vor eine Einwilligung, die Freiwilligkeitsproblematik besteht hier fort.

**b) Nachberichtspflicht**

Nachträgliche Änderungen der einer Übermittlung zugrunde liegenden Tatsachen (also in den Vertragsverhältnissen) müssen nach § 28a Abs. 3 BDSG nunmehr innerhalb eines Monats vom Unternehmen an die Auskunft nachgemeldet werden. Damit soll gewährleistet werden, dass der Datenbestand immer aktuell gehalten wird und der Verbraucher vor Praktiken geschützt wird, seine Daten ungünstig erscheinen zu lassen, um ihn als Kunden für andere Wettbewerber nicht attraktiv zu machen. Die Bedeutung dieses Verbraucherschutzgedankens hat der Gesetzgeber noch unterstrichen und Verstöße nun mit einem Bußgeld belegt (§ 43 Abs. 1 Nr. 4a BDSG). Bisher war die Aktualisierung nur vertraglich zwischen der Auskunft und ihren Vertragspartnern geregelt und allenfalls ableitbar aus der gesetzlichen Verpflichtung, nur richtige Daten zu speichern.

**c) Schätzdaten**

Einige Auskunfteien übermitteln in einer Bonitätsauskunft zum Teil Daten, die nicht im Einzelfall konkret festgestellt wurden, sondern auf bloßen Schätzungen beruhen. Seit langem fordern die Aufsichtsbehörden, dass dies für die Empfänger der Bonitätsauskunft ersichtlich sein muss. Bislang waren die Auskunfteien aber nur bereit, in der Auskunft pauschal anzugeben, dass sich Schätzdaten in der Auskunft befinden können. Der Gesetzgeber hat hier nun erfreulicherweise klar geregelt, dass die einzelnen Daten als Schätzdaten zu kennzeichnen sind (§ 35 Abs. 1 Satz 2 BDSG).

Durch die Novelle zum Recht der Auskunfteien werden also die von den Aufsichtsbehörden auch bisher schon geforderten Voraussetzungen gesetzlich festgeschrieben und dadurch der Vollzug des Bundesdatenschutzgesetzes durch mehr Rechtsklarheit erleichtert.

**d) Zulässigkeit von Scoringverfahren und Auskunftsrechte**

Durch den neuen § 28b BDSG werden Anforderungen an Scoringverfahren aufgestellt. Implizit wird definiert, dass ein Scorewert im Sinne dieser Regelung ein "Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen" ist. Die Vorschrift gilt, wenn ein solcher Wert zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen erhoben oder verwendet wird. Die Vorschrift richtet sich also an solche Scoreverwender. Sie ist jedoch auch von Auskunfteien zu beachten, die Scores berechnen und an ihre Vertragspartner übermitteln.

§ 28b BDSG verlangt, dass die zur Berechnung des Scorewertes genutzten Verfahren unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verfahrens relevant sind. Ferner schreibt § 28b BDSG vor, dass nur solche Daten für die Berechnung verwendet werden dürfen, die von dem Unternehmen auch zulässigerweise nach den allgemeinen Vorschriften des § 28 BDSG genutzt werden dürfen. Falls eine Auskunft einen Score berechnet, darf sie nur solche Daten verwenden, die sie auch für den Zweck übermitteln dürfte. Daraus ergibt sich beispielsweise in Verbindung mit der Neuregelung in § 28a Abs. 2 Satz 3 BDSG, dass Konditionenanfragen nicht für eine Scoreberechnung verwendet werden dürfen.

Geodaten (Wohnumfeldinformationen) dürfen für das Scoring-Verfahren zwar verwendet werden, es bestehen aber verschiedene Einschränkungen. Insbesondere dürfen nicht ausschließlich diese Daten für die Berechnung des Scorewertes genutzt werden.

Durch die Neuregelungen in § 34 BDSG (insbesondere in den Absätzen 2 und 4) sowie die Änderung des § 6a BDSG wird dem dringenden Bedürfnis der betroffenen Verbraucher entsprochen, mehr Transparenz beim Scoring zu schaffen. Einblicke über das Zustandekommen des Wertes, der mitunter gravierende Auswirkungen für den einzelnen Betroffenen haben kann, blieben ihm bislang unter Hinweis auf das Betriebsgeheimnis versagt. Dies haben die Aufsichtsbehörden seit langem bemängelt. Nun hat der Gesetzgeber vorgeschrieben, dass die zur Berechnung der Wahrscheinlichkeitswertes genutzten Datenarten dem Betroffenen auf Verlangen mitzuteilen sind. In der Gesetzesbegründung sind als Beispiel und damit zugleich Orientierungsmaßstab für die Genauigkeit der Auskunft "Adressdaten" genannt (BT-Drucks. 16/10529, Seite 17). Ferner ist dem Betroffenen Auskunft über das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte zu geben, und zwar einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

e) **Kosten der Auskunftserteilung**

Der Betroffene kann nun einmal pro Jahr auch von Auskunftsteilen eine kostenlose Auskunft verlangen (§ 34 Abs. 8 Satz 2 BDSG). Zwar galt bisher schon, dass eine Auskunft grundsätzlich kostenlos zu sein hat. Anders verhielt es sich aber mit Auskünften, die zu wirtschaftlichen Zwecken genutzt werden konnten.

Die Aufsichtsbehörden begleiten nun kritisch den Umsetzungsprozess. In der Arbeitsgruppe Kreditwirtschaft und in der Arbeitsgruppe Auskunftsteilen des Düsseldorfer Kreises wurden der Wirtschaft (Kreditwirtschaft und Auskunftsteilen) Hinweise gegeben, wie die Vorschriften umzusetzen sind (teilweise sind diese Hinweise auch in der obigen Darstellung enthalten).

Die Aufsichtsbehörden haben sich dabei auf eine Koordinierung ihrer Kontrolltätigkeit in Bezug auf das Scoring verständigt.

## **7.2 Bonitätsauskünfte über Mietinteressenten**

Auch mit der Frage, unter welchen Voraussetzungen Bonitätsauskünfte über Mietinteressenten erteilt werden können, beschäftigen sich die Aufsichtsbehörden seit langem (siehe Ziffer 10.5 des 16. Berichts der Landesregierung, Drucks. 16/1680 sowie Ziffer 8.1 des 18. Berichts der Landesregierung, Drucks. 16/4752).

Das BDSG enthält keine speziellen Regelungen, sondern fordert in § 29 Abs. 2 BDSG lediglich eine Abwägung zwischen den Interessen der Vermieter und den schutzwürdigen Belangen der Mietinteressenten. In einem Beschluss des Düsseldorfer Kreises vom Oktober 2009 (**Anlage**; im Internet abrufbar unter [www.bfdi.bund.de](http://www.bfdi.bund.de), siehe Ziffer 5) wurden nun die Anforderungen formuliert, die sich aus Sicht der Aufsichtsbehörden aufgrund dieser Abwägung ergeben.

Die Vertreter der Auskunftsteile hatten Gelegenheit, sich zu den Anforderungen des Beschlusses zu äußern und Kompromissvorschläge zu unterbreiten. Hiervon haben sie jedoch keinen Gebrauch gemacht, sie lehnten den Beschluss vielmehr ab.

Eine in Hessen ansässige Verbraucherauskunft erfüllt die Anforderungen des Beschlusses teilweise bzw. in Ansätzen. Ein Score zu Mietinteressenten wird an Vermieter nicht übermittelt; generell werden nicht titulierte offene Forderungen bis 1000 €, die innerhalb eines Monats nach Einmeldung getilgt werden, sofort gelöscht, also weder an Vermieter noch an sonstige Vertragspartner übermittelt. Die Aufsichtsbehörden werden bei Beschwerden von Mietinteressenten über etwaige aufsichtsbehördliche Maßnahmen gegen die Auskunft entscheiden.

## **8. Banken**

### **8.1 Problematische Maßnahmen der Konzernsicherheit**

Eine Bank teilte in einer Presseveröffentlichung mit, dass die Führung der Bank Kenntnis davon erhalten habe, dass es in früheren Jahren im Zusammenhang mit Aktivitäten, welche die Abteilung Konzernsicherheit betreffen, möglicherweise zu Verstößen gegen interne Vorgaben oder rechtliche Anforderungen gekommen sei. Eine externe Anwaltskanzlei sei mit den Untersuchungen betraut worden, die aber noch nicht abgeschlossen seien. Auch habe die Bank die Bundesanstalt für Finanzdienstleistungen informiert.

Die Datenschutzaufsichtsbehörde beim Regierungspräsidium Darmstadt erhielt vom betrieblichen Datenschutz der Bank im Kontext mit dieser Pressemitteilung ebenfalls erste Informationen. Durch einen umfangreichen Fragekatalog verlangte die Aufsichtsbehörde sodann nach § 38 Abs. 3 BDSG unter Fristsetzung Auskunft zu dem Sachverhalt einschließlich der Verantwortlichkeiten. Die Bank versicherte zunächst ihre uneingeschränkte Bereitschaft, mit dem Regierungspräsidium zusammenzuarbeiten und dieses vollständig über die entsprechenden Sachverhalte zu informieren. Sie bat jedoch vor Fristablauf um Verständnis, dass sie noch nicht in der Lage sei, Stellung zu nehmen. Grund hierfür sei, dass die von der externen Kanzlei geführte Untersuchung noch nicht abgeschlossen werden konnte. Die Aufsichtsbehörde verdeutlichte jedoch, dass die Fragen in diesem Fall nach dem derzeitigen Stand der Erkenntnisse zu beantworten seien. Schließlich war die Bank einsichtig und legte einen entsprechenden Zwischenbericht vor. Bald danach wurde auch die Endfassung des sehr umfangreichen Abschlussberichtes der Kanzlei vorgelegt.

Die Untersuchung der Anwaltskanzlei kam dabei u. a. zu folgenden Erkenntnissen: In dem Untersuchungszeitraum (bis 1998) seien insgesamt vier Fälle mit Aktivitäten identifiziert worden, bei denen es Zweifel an der Rechtmäßigkeit im Hinblick auf den Datenschutz oder den Schutz der Privatsphäre gab. Sämtliche Aktivitäten seien aus Aufträgen entstanden, die von externen Dienstleistern im Auftrag der Abteilung Konzernsicherheit durchgeführt wurden.

In einem Fall wurden verschiedene Maßnahmen durchgeführt, um Informationen über die Motive eines kritischen Aktionärs und dessen mögliche Beziehungen zu Anlegerschützern, Rechtsanwälten und kritischen Aktionären zu beschaffen. In einem anderen Fall wurden problematische Übungen durchgeführt, um die Wirksamkeit von Personenschutzmaßnahmen für als gefährdet eingestufte Personen zu testen und gegebenenfalls zu verbessern.

Sowohl der Zwischenbericht als auch der Abschlussbericht der Anwaltskanzlei wurden vom Regierungspräsidium eingehend geprüft. Darüber hinaus führte die Aufsichtsbehörde eigene Überprüfungen vor Ort in der Bank sowie in

der beauftragten Kanzlei zur Klärung des Sachverhalts durch und unterzog diesen anschließend einer umfassenden rechtlichen Würdigung. Der personelle und zeitliche Aufwand für diese Überprüfungen war sehr erheblich.

Bei den Überprüfungen ergaben sich keine Hinweise, dass bei der Überwachung von Personen auch ehemalige Polizeibedienstete oder Beamte des Landeskriminalamts eingesetzt wurden, weder in der Sicherheitsabteilung der Bank noch bei einer privaten Sicherheitsfirma, die von der Bank beauftragt wurde.

Aufgrund der datenschutzrechtlichen Überprüfung leitete das Regierungspräsidium in zwei Fällen gegen die Bank ein Ermittlungsverfahren nach dem Ordnungswidrigkeitengesetz im Hinblick auf § 43 BDSG ein. Da sich zugleich hinreichende Anhaltspunkte dafür ergeben hatten, dass datenschutzrechtliche Straftatbestände erfüllt sein könnten, wurde der Vorgang an die zuständige Staatsanwaltschaft übergeben.

Die Staatsanwaltschaft teilte in einer Pressemitteilung vom 8. Oktober 2009 mit, dass ein Aktionär der Bank sowie ein Anwaltsbüro aus München Strafanzeige erstattet hatten. Die durch Vorlage des beim Regierungspräsidium entstandenen Vorgangs und diese Strafanzeigen veranlasste Prüfung habe ergeben, dass sich nach den vorliegenden Erkenntnissen keine Anhaltspunkte ergeben hätten, dass Vorstands- oder Aufsichtsratsmitglieder der Bank in möglicherweise strafrechtlich relevante Aktivitäten einbezogen waren. Allerdings bestünden zureichende Anhaltspunkte für einen Verstoß gegen die Strafvorschrift des Bundesdatenschutzgesetzes. Insoweit seien Ermittlungsverfahren gegen die vermutlich dafür Verantwortlichen eingeleitet worden.

Bei Redaktionsschluss dieses Berichts lag keine neue Mitteilung der Staatsanwaltschaft vor. Der Abschluss der staatsanwaltlichen Ermittlungen bleibt abzuwarten.

## **8.2 Bargeldtransfer und Datenschutz**

Beim Surfen auf einer Internetseite mit Verkaufsangeboten für PKWs entdeckte der Beschwerdeführer ein Fahrzeug, das sein besonderes Interesse weckte. Er setzte sich per E-Mail mit dem Verkäufer in Verbindung, der auch direkt antwortete und sich als älterer Herr mit grenznahem Wohnort in Dänemark zu erkennen gab. Schnell einigten sich die Parteien über Preis und die Modalitäten der Übergabe. Der Verkäufer verlangte aber dann zusätzlich eine Sicherheit dafür, dass der Käufer auch tatsächlich in die als Übergabeort vereinbarte Stadt kommen würde. Er schlug folgende Verfahrensweise vor: die Freundin des Käufers sollte den Kaufpreis des PKW auf dessen Namen bei einem Unternehmen, das Geldtransfergeschäfte durchführt, einzahlen. Dadurch sei sichergestellt, dass nur er - der Käufer - das Geld unter Vorlage seines Ausweises abholen könne. Zum Nachweis der "Sicherheitsleistung" sollte der Beschwerdeführer den Einzahlungsbeleg an den Verkäufer übermitteln. Der Beschwerdeführer handelte wie abgesprochen, zahlte das Geld ein, scannte den Einzahlungsbeleg ein und schickte diesen an den Verkäufer, wobei er allerdings die Transaktionsnummer schwärzte, da diese nach Angaben des Verkäufers zur Identifikation bei der Geldauszahlung dienen sollte.

Zum verabredeten Treffen fünf Tage später erhielt der Beschwerdeführer, als er an der Rezeption des Hotels nach dem Verkäufer fragte, die Mitteilung, dass dieser dort nicht wohne. Er wurde auch darüber informiert, dass bereits eine andere Person erfolglos nach dem betreffenden Herrn gesucht habe. Daraufhin ging der Beschwerdeführer zur nächsten Filiale des Geldtransfer-Unternehmens, um das eingezahlte Geld abzuholen. Dort wurde ihm mitgeteilt, dass bereits zwei Tage zuvor die Auszahlung an einen Mann, der den Namen des Beschwerdeführers nutzte, unter Vorlage eines auf diesen Namen ausgestellten Ausweises erfolgt war.

Der Beschwerdeführer vermutete Unregelmäßigkeiten des Finanzdienstleisters bei der Geldauszahlung und verlangte die Übersendung des Beleges über den Geldempfang. Das Geldtransfer-Unternehmen kam der Bitte nach und stellt den Beleg mit Angaben des Namens der Einzahlerin sowie des Geldempfängers, Betrag und Transaktionsnummer zur Verfügung. Die Adresse und Ausweisnummer, die bei Auszahlung des Geldes notiert wurden, schwärzte der Finanzdienstleister. Das Unternehmen begründete dies mit datenschutzrechtlichen Erwägungen. Der Beschwerdeführer wollte dies nicht hinnehmen und wendete sich an die Aufsichtsbehörde.

Der vom Beschwerdeführer genutzte Service dient dem Bargeldtransfer, wenn in einer anderen Stadt oder einem anderen Land so schnell wie möglich Bargeld benötigt wird, eine kontogebundene Überweisung aber nicht möglich ist oder zu lange dauern würde. Er ist so ausgestaltet, dass der Empfänger alle wesentlichen Transaktionsdetails mitteilen muss, um seine Berechtigung zum Empfang des Geldes nachzuweisen. Dies sind der Name des Absenders, der Name des Empfängers, die Überweisungssumme sowie das Einzahlungsland. Die Transaktionsnummer ist hilfreich bei der Durchführung, aber in Deutschland keine Auszahlungsbedingung. Die Details der Transaktion sind bei Einhaltung der Allgemeinen Geschäftsbedingungen nur dem Einzahler und dem Geldabholer bekannt, da Dritte nicht von den auftragsbezogenen Details in Kenntnis gesetzt werden sollen. Die Identifikation durch Vorlage eines Ausweises nimmt das Unternehmen allein auf Grund der Regelungen des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vor.

Nach dem eigenen Vortrag des Beschwerdeführers konnten die notierten Ausweis- und Adressdaten nicht seine eigenen sein, eine Datenweitergabe mit Einwilligung des Beschwerdeführers kam daher nicht in Betracht.

Als Erlaubnistatbestand bot sich nur § 28 Abs. 3 Nr. 1 BDSG an. Hiernach ist die Übermittlung oder Nutzung für einen anderen Zweck auch zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Das berechnigte Interesse des Beschwerdeführers, der durch kriminelle Aktivitäten einen Geldverlust erlitten hat, liegt eindeutig vor. Fraglich ist jedoch, ob es schutzwürdige Aspekte gibt, die gegen die Herausgabe der notierten Ausweisdaten sprechen. Hier sind verschiedene Fallkonstellationen denkbar.

1. Der vorgelegte Ausweis wurde als Blanko-Formular entwendet und war nie als amtliches Dokument für eine Person ausgestellt. Für die Tat wird er mit dem Namen des Beschwerdeführers versehen. Die verwendete Adresse hat keinen Bezug zu einer realen Person. Einer Übermittlung entgegenstehende schutzwürdige Belange sind hier nicht ersichtlich.
2. Der Inhaber des Ausweises ist in den Prozess des Geldempfangs involviert und hat seinen Ausweis zur Verfügung gestellt. Lediglich der Name wurde auf den Beschwerdeführer geändert. Ausweisnummer und Adressdaten sind dem Betroffenen zuordenbar. Hier ist ein schutzwürdiges Interesse äußerst zweifelhaft.
3. Es handelt sich um ein ursprünglich echtes Identifikationspapier das dem Inhaber abhanden gekommen ist. Lediglich der Name wurde für die Tat abgeändert. Hier ist der rechtmäßige Ausweisinhaber schutzwürdig. Kennt der Beschwerdeführer die Anschrift des Betroffenen so wäre er möglicherweise Schadensersatzforderungen oder Konfrontationen ausgesetzt. Davor ist der Unbeteiligte zu schützen.

Die Hintergründe im Einzelfall sind dem Finanzdienstleister nicht bekannt. Er hat daher grundsätzlich von einem schutzwürdigen Interesse im Hinblick auf die Adress- und Ausweisdaten auszugehen. Der Beschwerdeführer ist hier auf die Erstattung einer Strafanzeige zu verweisen. Der Finanzdienstleister hat versichert, dass er den Strafverfolgungsbehörden alle Unterlagen zur Verfügung stellt. Im Zuge der Ermittlungen kann dann festgestellt werden, ob eine Tatbeteiligung des Ausweisinhabers vorliegt. Dieser ist auf diesem Weg nur mit den Strafverfolgungsbehörden konfrontiert. Auch der Beschwerdeführer kann über eine Akteneinsicht seines Rechtsanwalts Daten für mögliche Schadensersatzforderungen erhalten.

Im vorliegenden Fall hat der Beschwerdeführer auf diesem Weg erfahren, dass ein osteuropäischer Pass mit Adresse in Deutschland vorgelegt wurde. Die staatsanwaltschaftlichen Ermittlungen waren erfolglos. Das Verhalten des Finanzdienstleisters war datenschutzrechtlich nicht zu beanstanden.

## **9. Telemedien, Internet**

### **9.1 Bewertungen von Einzelpersonen im Internet**

Das Internet bietet wie kein anderes Medium für Verbraucherinnen und Verbraucher optimale Möglichkeiten, Preise und Qualität von unterschiedlichsten Produkten und Dienstleistungen zu vergleichen. So existiert bereits seit vielen Jahren eine große Vielfalt von Portalen, bei denen die Preise von Produkten bei verschiedenen Händlern gegenübergestellt werden und bei denen Nutzer zusätzlich die Möglichkeit haben, ein bereits gekauftes Produkt zu bewerten. Diese Bewertung soll künftigen Käufern entweder als Empfehlung oder als Warnung eine praktische Entscheidungshilfe für den Kauf an die Hand geben.

Durch den großen Erfolg dieser Portale ist es zu erklären, dass in letzter Zeit immer öfter Bewertungsportale im www angeboten werden, bei denen nicht nur Preis und Qualität von Produkten, sondern die unterschiedlichsten Dienstleistungen von Personen, z.B. Lehrern, Professoren, Handwerkern, Ärzten, Friseuren oder Rechtsanwälten bewertet werden. Da bei diesen Bewertungen immer ein Personenbezug gegeben ist, beschäftigen sich die Datenschutzaufsichtsbehörden schon seit längerem mit der Problematik, wie hierbei eine Verletzung des Rechts auf informationelle Selbstbestimmung und eine Beeinträchtigung des Persönlichkeitsrechts der Betroffenen vermieden werden kann. In dem am 17./18. April 2008 gefassten Beschluss des Düsseldorfer Kreises wurden die datenschutzrechtlichen Mindestanforderungen an solche Internet-Angebote formuliert:

#### **Internet-Portale zur Bewertung von Einzelpersonen**

1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.
2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.
3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Am 23. Juni 2009 erging ein Urteil des BGH zum Lehrerbewertungsportal "www.spickmich.de" (Az.: VI ZR 196-08). Das Urteil zeigt auf, unter welchen datenschutzrechtlichen Bedingungen das Grundrecht der Meinungsfreiheit nach Art. 5 GG nach Auffassung des Gerichts Vorrang vor dem Recht auf informationelle Selbstbestimmung nach Art. 1, 2 GG hat. Aus der Urteilsbegründung lassen sich aber auch datenschutzrechtliche Mindestanforderungen ableiten, welche die im o.a. vorherigen Beschluss des Düsseldorfer Kreises enthaltenen Forderungen der Aufsichtsbehörden zum Teil präzisieren.

Das Angebot einer Bewertungsplattform im Internet unterliegt demnach den Regelungen des § 29 BDSG. Es handelt sich dabei um geschäftsmäßiges Erheben, Speichern, Verändern und Nutzen personenbezogener Daten. Hierbei ist eine Abwägung zwischen dem berechtigten Interesse des Anbieters bzw. dem Informationsinteresse der Öffentlichkeit und den schutzwürdigen Interessen des Betroffenen vorzunehmen.

Das Regierungspräsidium Darmstadt hat aufgrund einiger Beschwerden betroffener Ärzte ein von einem in Hessen ansässigen Unternehmen geführtes Ärztebewertungsportal auf die Kriterien des "Spickmich-Urteils" untersucht und dabei einige datenschutzrechtliche Defizite und Unzulänglichkeiten festgestellt. So dürfen die von Portalnutzern abgegebenen Bewertungen keine Schmähkritik, Verleumdungen oder Beleidigungen enthalten. Dies ist beispielsweise durch automatisierte Wortfilter und Plausibilitätsprüfungen aber auch durch manuelle Einzelfallprüfung vor der Veröffentlichung zu erreichen. Die Bewertungskriterien sind nachvollziehbar und angemessen zu gestalten, müssen mit der beruflichen Sozialsphäre der Betroffenen zu tun haben und dürfen nicht zu Missbrauch verleiten. Sie sind nach Ablauf einer bestimmten Zeit zu entfernen, da sie zwischenzeitliche Veränderungen, z.B. Neuausstattung einer Praxis oder zusätzliches Personal, nicht abbilden.

Eine Nutzung der Daten außerhalb der Zweckbindung (hier: gezielte Suche nach Informationen zu einem bestimmten Arzt) ist zu verhindern. Daher dürfen Suchmaschinen nur die Anschrift eines Arztes finden, die Bewertung selbst darf für Suchmaschinen nicht auffindbar sein. Erst ein gezieltes Aufrufen der Adress-Seite darf den Zugang zu Bewertungen eröffnen.

Nach § 29 Abs. 2 BDSG, der sich ursprünglich an Auskunfteien und andere Unternehmen richtet, die Datenverarbeitung zum Zweck der Übermittlung betreiben, darf die Übermittlung der bereitgehaltenen Daten an Dritte nur erfolgen, wenn der Dritte ein berechtigtes Interesse nachweist und kein schutzwürdiges Interesse entgegensteht. Der Bundesgerichtshof hat nun im "Spickmich-Urteil" klargestellt, dass eine einzelfallbezogene Überprüfung, ob das berechtigte Interesse bei den Nutzern der Internet-Plattform vorliegt, anders als es das Gesetz vorgibt, im Internet faktisch nicht stattfinden kann. Stattdessen müssen bei Online-Bewertungsportalen allerdings gewisse grundsätzliche Vorkehrungen getroffen werden, wie z.B. die genannten Zugangs- und Suchmaschinenbeschränkungen, um zumindest im Ansatz die Zweckbestimmungsbegrenzungen einzuhalten.

Unabhängig von den im "Spickmich-Urteil" konkret erwähnten datenschutzrechtlichen Aspekten, die nur mit der Bewertung des schutzwürdigen Interesses zu tun hatten, weil es um die Frage ging, ob die Klageführerin einen zivilrechtlichen Unterlassungsanspruch gegenüber den Betreibern der Bewertungsplattform hat, sind noch weitere grundsätzliche Punkte zu beachten.

Nach § 33 Abs. 1 Satz 2 BDSG ist ein Betroffener zu unterrichten, soweit nach § 29 BDSG zur Übermittlung bereitgehaltene Daten erstmalig übermittelt würden. Übertragen auf das Internet heißt das, sobald eine Website erstmalig aufgerufen wird, also im Grunde genommen, sobald die Daten abrufbar sind. Eine Ausnahme gilt bei Stellen, die Daten zur Übermittlung bereithalten, nur in den Fällen nach § 33 Abs. 2 Nr. 8 BDSG. Danach kann von einer Benachrichtigung abgesehen werden, soweit es sich um Daten aus allgemein zugänglichen Quellen bzw. listenmäßig zusammengefasste Daten handelt und gleichzeitig eine Benachrichtigung wegen der Vielzahl der Fälle unverhältnismäßig ist. Da die Bewertungen nicht aus allgemein zugänglichen Quellen stammen, kann diese Ausnahmeregelung von der Benachrichtigungspflicht von den Anbietern von Bewertungsplattformen allerdings nicht in Anspruch genommen werden.

Nach § 35 Abs. 1 BDSG sind falsche Daten zu berichtigen, sobald diese Tatsache bekannt wird. Darüber hinaus haben Stellen, die Daten zur Übermittlung bereithalten, die Richtigkeit der Daten auch turnusmäßig zu überprüfen (§ 35 Abs. 2 Nr. 4 BDSG).

Das hessische Arztbewertungsportal bietet zwar bereits Möglichkeiten, Falscheingaben selbst zu korrigieren und auf Missbrauchsfälle hinzuweisen. Auch beziehen sich die vorgegebenen Kriterien auf dem Online-Bewertungsformular auf die Sozialsphäre der Betroffenen. Andere Kriterien wurden aber nicht erfüllt. Daher wurde das Unternehmen aufgefordert,

- auf dem Bewertungsformular kein unmoderiertes Freitextfeld mehr anzubieten, das im vorliegenden Fall erfahrungsgemäß immer wieder genutzt wurde und wird, um zweifelhafte und rufschädigende Äußerungen zu verbreiten. Alternativ kann das Unternehmen geeignete Wortfilter einbauen bzw. andere Plausibilitätsprüfungen und strenge manuelle Kontrollen der Freitextbeiträge vor der Veröffentlichung einer Bewertung durchführen;
- die gesamten Datenbestände turnusmäßig zu überprüfen, die Bewertungen aktuell zu halten und veraltete Bewertungen zu löschen;
- die www-Seiten, welche die abgegebenen Bewertungen enthalten, mit einem Suchmaschinenschutz zu versehen;
- grundsätzlich bei Aufnahme einer Arztanschrift, erst recht jedoch bei Aufnahme einer Bewertung, den Betroffenen zu benachrichtigen. Das Vorliegen etwaiger Ausnahmetatbestände ist zu prüfen und zu dokumentieren.

Die vielen datenschutzrechtlichen Probleme, die das Aufkommen der Online-Bewertungsplattformen mit sich gebracht haben, werden unter den Aufsichtsbehörden der Länder noch intensiv in der Arbeitsgruppe Telekommunikation und Telemedien des Düsseldorfer Kreises diskutiert. Es bleibt zu hoffen, dass eine weitere Novellierung des BDSG die bestehenden rechtlichen Unklarheiten und Regelungslücken beheben und sowohl im Sinne der Anbieter als auch der Datenschutzaufsichtsbehörden künftig eine sichere Rechtsgrundlage für solche Internet-Veröffentlichungen bieten wird. Bis dahin werden die Aufsichtsbehörden die Rechtsprechung in diesem Bereich



weiter beobachten. Im Übrigen bleibt abzuwarten, ob das für Datenschützer eher enttäuschende "Spickmich-Urteil" Gegenstand der Klage eines Betroffenen vor dem Bundesverfassungsgericht werden wird.

## 10. Auftragsdatenverarbeitung

Auf Vorschlag des Bundesrates wurde die Vorschrift des § 11 BDSG über die Auftragsdatenverarbeitung ergänzt. Anlass hierfür waren zum einen mehrere Fälle, bei denen Auftragsdatenverarbeiter rechtswidrig mit personenbezogenen Daten umgegangen waren, sowie zum anderen die Erfahrung der Aufsichtsbehörden, dass Unternehmen bei der Beauftragung von Datenverarbeitungsdienstleistern die bisherige Vorschrift häufig missachteten. Dies geschah oft aus Unkenntnis der Vorschrift oder deren Bedeutung.

§ 11 Abs. 2 Satz 2 BDSG wurde daher so gefasst, dass die gesetzlichen Anforderungen an die Ausgestaltung des Auftrages besser erkennbar werden. Ferner wurde § 11 Abs. 2 Satz 4 BDSG dahingehend konkretisiert, dass der Auftraggeber sich erstmals "vor Beginn der Datenverarbeitung und sodann regelmäßig" von der Einhaltung der beim Auftraggeber getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Verstöße gegen § 11 Abs. 2 Satz 2 und 4 BDSG sind auch bußgeldbewehrt (§ 43 Abs. 1 Nr. 2b BDSG).

Das Regierungspräsidium Darmstadt hatte bereits vor der Novelle einen Mustervertrag zur Auftragsdatenverarbeitung auf seiner Internetseite zum Abruf bereitgehalten. In diesem waren die meisten Festlegungen, die § 11 Abs. 2 Satz 2 BDSG nun explizit fordert, schon enthalten bzw. vorgesehen. Dieser Mustervertrag ging davon aus, dass erforderliche Präzisierungen in einem separaten Dienstleistungsvertrag, einer Leistungsbeschreibung oder in schriftlichen Weisungen vorgenommen werden. Aufgrund der Ergänzung des § 11 BDSG, die am 1. September 2009 in Kraft trat, überarbeitete das Regierungspräsidium Darmstadt umgehend seinen Mustervertrag und veröffentlichte diesen auf der Website des Regierungspräsidiums. Zwischenzeitlich gewonnene praktische Erfahrungen sind in die weitere Überarbeitung eingeflossen. Die aktuelle Fassung des Mustervertrags ist diesem Bericht als **Anlage** beigelegt.

Zur Neufassung des § 11 BDSG erreichten das Regierungspräsidium Darmstadt eine Vielzahl von Fragen. Die dringlichste und am häufigsten gestellte Frage war, ob die Neuregelung auch auf Verträge anwendbar ist, die vor dem 1. September 2009 geschlossen wurden. Diese Frage wurde bejaht, denn nach einvernehmlicher Auffassung aller Aufsichtsbehörden im Bundesgebiet ist die Vorschrift so auszulegen, dass auch "Altverträge" anzupassen sind. Soweit auf der Grundlage von Altverträgen weiterhin Datenverarbeitungen erfolgen, stellt dies eine fortgesetzte Beauftragung dar. Da die Neuregelung kurze Zeit nach der Verabschiedung des Gesetzes (am 14. August 2009) in Kraft trat, aber keine Übergangsfrist eingeräumt wurde, sahen sich die Auftraggeber vielfach vor kaum zu bewältigende Herausforderungen gestellt. In vielen Unternehmen bzw. Konzernen waren Hunderte von Verträgen anzupassen. Dem Wunsch, eine verbindliche Übergangs- oder Duldungsfrist zu nennen, vermochte die Aufsichtsbehörde nicht zu entsprechen. Sie stellte jedoch klar, dass Sanktionen nicht verhängt werden, soweit es Unternehmen unmöglich ist, die gesetzlichen Anforderungen einzuhalten. Es war offensichtlich, dass die Verträge nicht von heute auf morgen umgestellt werden konnten. Maßgeblich ist daher, dass Unternehmen unverzüglich und systematisch an die Anpassung herangehen.

Weitere Fragen betrafen die neuen bzw. konkretisierten Kontrollpflichten des Auftraggebers. Hier verwies die Aufsichtsbehörde auf die aufschlussreichen Ausführungen in der Gesetzesbegründung. Darin heißt es unter anderem: "Zugleich erscheint es auch gerechtfertigt, dass sich der Auftraggeber noch vor Beginn der tatsächlichen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch den Auftragnehmer davon überzeugt, dass dieser die erforderlichen technischen und organisatorischen Maßnahmen vorgenommen hat. Durch die zusätzlich vorgesehene "regelmäßige" Kontrolle wird überdies zum Ausdruck gebracht, dass insbesondere bei längerfristigen Auftragsdatenverarbeitungen eine einmalige Kontrolle nicht ausreicht. Eine starre Frist, z.B. eine jährliche Kontrolle, würde der in der Praxis vorkommenden Bandbreite an Auftragsdatenverarbeitungen nicht gerecht. Nur durch eine Dokumentation lässt sich der Handlungszeitpunkt nachweisen und kann sich der Auftraggeber z.B. gegenüber der Aufsichtsbehörde entlasten. Eine nähere Ausgestaltung der Art und des Umfangs der Dokumentation erscheint nicht erforderlich und würde wiederum der Bandbreite an Auftragsdatenverarbeitungen nicht gerecht. Beispielsweise kann der Umfang je nach Größe und Komplexität der Auftragsdatenverarbeitungen variieren. Es wird nicht verlangt, dass sich der Auftraggeber unmittelbar beim Auftragnehmer vor Ort oder selbst in Person überzeugt. Dies wäre regelmäßig nicht angemessen und mit einem Verlust an Flexibilität verbunden, z.B. wenn der Auftraggeber ein Testat eines Sachverständigen einholen möchte oder wenn eine schriftliche Auskunft des Auftragnehmers ausreicht." (BT-Drucks. 16/13657).

Maßgeblich für Art und Umfang der Kontrollen sind somit die Umstände des Einzelfalles, also unter anderem die Art der Datenverarbeitung und die vorhandenen Erfahrungen mit dem Auftragsdatenverarbeiter.

Häufig werden Unterauftragnehmer in die Erbringung von Datenverarbeitungsdienstleistungen eingeschaltet. Hierzu wurde die Frage gestellt, ob und ggf. inwieweit der Auftraggeber unmittelbar selbst den Unterauftragnehmer kontrollieren muss. Nach Auffassung der Aufsichtsbehörde erfordert § 11 BDSG, dass ein direktes Prüfrecht des Auftraggebers auch beim Unterauftragnehmer besteht. Gerade die Datenskandale, die Veranlassung für die Änderung des § 11 BDSG gaben, betrafen überwiegend Missstände bei Unterauftragnehmern. Der Auftraggeber kann seine Verantwortung nicht vollständig auf den Auftragnehmer delegieren. Zwar wird der Auftraggeber seiner Kontrollpflicht nach § 11 Abs. 2 Satz 4 BDSG im Falle einer Unterbeauftragung meist Genüge tun, wenn er sich vom Auftragnehmer konkret nachweisen lässt, dass dieser die Prüfungen beim Unterauftragnehmer vorgenommen hat,

allerdings muss er die Möglichkeit haben, notfalls selbst beim Unterauftragnehmer zu prüfen (ggf. in Begleitung eines Vertreters des Auftraggebers).

Die Vorschrift des § 11 Abs. 2 Satz 4 BDSG lässt zwar einen Spielraum, inwieweit und in welchem Umfang tatsächlich Prüfungen vor Ort erforderlich sind, sie stellt die Auftraggeber aber nicht frei, völlig auf Überprüfungen vor Ort zu verzichten. Würde man § 11 Abs. 2 Satz 4 BDSG dahin auslegen, dass der Auftraggeber nur beim (unmittelbaren) Auftragnehmer kontrollieren muss, würde in den Fällen, in denen beim Auftragnehmer selbst gar keine Datenverarbeitung erfolgt, die Prüfpflicht des Auftraggebers insoweit zum Teil ins Leere laufen. Auch dies spricht dafür, dass § 11 BDSG ein "Durchgriffsprüfrecht" beim Unterauftragnehmer erfordert. Zu bedenken ist in diesem Zusammenhang, dass die Verpflichtung des § 42a BDSG in jedem Fall den Auftraggeber trifft, also - entgegen dem missverständlichen Wortlaut - nicht den Auftragnehmer und nicht einen Unterauftragnehmer. Auch aus diesem Grund muss der Auftraggeber die Möglichkeit haben, notfalls selbst vor Ort die konkrete Datenverarbeitung zu prüfen.

Weitere Fragen betrafen die Relevanz der Änderungen des § 11 BDSG beim internationalen Datenverkehr (siehe hierzu nachfolgend Ziffer 11.1).

## **11. Aspekte internationaler Datenverarbeitung**

### **11.1 Bedeutung der Änderungen des § 11 BDSG für den internationalen Datenverkehr**

Wenn sich ein deutscher Auftraggeber eines Datenverarbeitungsdienstleisters bedient, der in einem anderen Mitgliedstaat der Europäischen Union oder des europäischen Wirtschaftsraumes ansässig ist, findet § 11 BDSG unmittelbar Anwendung. Folglich gelten auch die neuen Anforderungen.

Ein betrieblicher Datenschutzbeauftragter stellte die Frage, ob somit ein Auftraggeber nach § 11 Abs. 2 Satz 2 Nr. 5 in Verbindung mit Absatz 4 Nr. 2 BDSG auch dann seinen Auftragnehmer verpflichten muss, einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn dies in dem europäischen Land, in dem der Auftragnehmer ansässig ist, gesetzlich nicht vorgeschrieben ist. Diese Frage war nach einhelliger Auffassung aller Mitglieder der Arbeitsgruppe internationaler Datenverkehr des Düsseldorfer Kreises zu verneinen, denn § 4f BDSG ist für den Auftragnehmer nicht anwendbar. Maßgeblich ist hier das Recht des jeweiligen EU-Staates.

Beindet sich der Dienstleister in einem sogenannten Drittstaat, also außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes, ist § 11 BDSG zwar nicht unmittelbar, aber entsprechend anwendbar als Anforderung der "Ersten Stufe" im Rahmen der Abwägung nach § 28 Abs. 1 Nr. 2 BDSG. Daher sind auch die neuen Anforderungen des § 11 BDSG einzuhalten. Wenn also der Dienstleister ein Safe-Harbor-zertifiziertes Unternehmen in den USA ist, sind entsprechende vertragliche Regelungen zu treffen. Wenn mit dem Dienstleister der EU-Standardvertrag vom Dezember 2001 abgeschlossen wurde oder der neue EU-Standardvertrag vom Februar 2010 (im Internet abrufbar unter "[http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_de.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_de.htm)") abgeschlossen werden soll, ist festzustellen, dass die Anforderungen des § 11 BDSG dadurch bereits zum Teil erfüllt werden. Erforderliche Präzisierungen können durch ausführliche Festlegungen und ggf. Ergänzungen in den Anhängen zum Standardvertrag erfolgen. Alternativ hierzu können die erforderlichen Präzisierungen auch in einem separaten Dienstleistungsvertrag mit zugehöriger Leistungsbeschreibung oder ggf. in schriftlichen Weisungen vorgenommen werden. Hierauf sollte entsprechend Bezug genommen werden. Aus den Standardverträgen selbst geht hervor, dass ihre Regelungen nicht so konkret sind, dass sie abschließend beinhalten, was der Auftragnehmer zu tun hat; so werden an mehreren Stellen die Weisungen des Auftraggebers erwähnt und damit Konkretisierungen vorausgesetzt (siehe Ziffer 11.1 des 19. Berichts der Landesregierung, Drucks. 16/5892 zur Gesamthematik nach der alten Rechtslage).

Werden die EU-Standardverträge ergänzt oder geändert, drängt sich natürlich die Frage nach der Genehmigungspflicht auf, die daher auch häufig der Aufsichtsbehörde gestellt wurde. Grundsätzlich besteht nur Genehmigungsfreiheit, wenn die Klauseln wörtlich verwendet werden (siehe Ziffer 7.2 des 15. Berichts der Landesregierung, Drucks. 15/4659). Geringfügige Änderungen, die dazu dienen, den Anforderungen der "1. Stufe" Rechnung zu tragen, können vorgenommen werden, ohne dass dies die Genehmigungspflicht auslöst (siehe hierzu den Beschluss des Düsseldorfer Kreises vom April 2007 zu Fragen des internationalen Datenverkehrs und Ziffer 9 des 20. Berichts der Landesregierung, Drucks. 16/7646 sowie Ziffer 11. des 22. Berichts der Landesregierung, Drucks. 18/1015). Nach den Erwägungsgründen in den jeweiligen Entscheidungen der EU-Kommission zu den Standardvertragsklauseln können im Übrigen "geschäftszugehörige Klauseln" aufgenommen werden, sofern diese nicht im Widerspruch zu den Klauseln stehen.

In der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises bestand Einigkeit, dass daher auch Ergänzungen oder Präzisierungen, die erfolgen, um § 11 Abs. 2 Satz 2 BDSG umzusetzen, keine Genehmigungspflicht auslösen. Wird der alte Standardvertrag nach dem 15. Mai 2010 um solche Regelungen ergänzt, handelt es sich nicht um relevante Änderungen im Sinne des Artikel 7 Nr. 2 Satz 2 der Kommissionsentscheidung vom 5. Februar 2010, welche die Vertragsparteien zwingen könnte, den neuen Standardvertrag abzuschließen.

### **11.2 Mehrparteienverträge**

Internationale Unternehmensgruppen und Konzerne schließen vielfach einen Mehrparteienvertrag zwischen ihren Mitgliedsunternehmen, der als Grundlage für Datenübermittlungen innerhalb der Gruppe bzw. des Konzerns dienen

soll. Mit dem Vertrag sollen insbesondere die speziellen datenschutzrechtlichen Voraussetzungen beim Datentransfer in sogenannte Drittstaaten (Staaten außerhalb der Europäischen Union und außerhalb der Mitgliedstaaten des Europäischen Wirtschaftsraumes) erfüllt werden. Handelt es sich um individuelle Verträge, bedürfen die Übermittlungen der aufsichtsbehördlichen Genehmigung nach § 4c Abs. 2 BDSG.

Im letzten Tätigkeitsbericht wurde über ein solches Genehmigungsverfahren und die hierbei gestellten Anforderungen an derartige Verträge berichtet (siehe Ziffer 3.1 des 22. Berichts der Landesregierung, Drucks. 18/1015).

Mehrparteienverträge können jedoch auch auf den EU-Standardverträgen basieren. Mehrparteien-Standardverträge ("multilaterale Standardverträge") sind also möglich. Aufgrund der beim Regierungspräsidium Darmstadt eingegangenen zahlreichen Anfragen hierzu wurde in der Arbeitsgruppe Internationaler Datenverkehr die Frage behandelt, ob und unter welchen Voraussetzungen hier Genehmigungsfreiheit besteht.

Die Aufsichtsbehörden waren sich einig, dass auch hier unter den oben genannten Bedingungen, d.h. grundsätzlich nur bei wörtlicher Verwendung, eine Genehmigungsfreiheit besteht. Minimale redaktionelle Änderungen, mit denen dem Umstand Rechnung getragen wird, dass es jeweils mehrere Exporteure und mehrere Importeure gibt, wären ebenfalls akzeptabel, würden also keine Genehmigungspflicht auslösen. Es muss aber auf den ersten Blick erkennbar sein, dass der Standardvertrag unverändert gilt. Wenn die Änderungen umfangreich sind, sodass nur durch eingehende Prüfungen festgestellt werden kann, dass es sich lediglich um redaktionelle Änderungen handelt, ist im Zweifel Genehmigungspflicht anzunehmen. Werden Regelungen aus verschiedenen EU-Standardverträgen kombiniert, besteht Genehmigungspflicht. Genehmigungsfreiheit kann nur bestehen, wenn ein Standardvertrag in Gänze übernommen wird. Aber es ist durchaus möglich, dass verschiedene Standardverträge zu Bestandteilen eines Gesamtvertragswerkes werden. Allerdings müssen die Bestimmtheitsanforderungen gewahrt werden (siehe hierzu unten Näheres).

Häufig wird den Standardvertragsklauseln ein "Hauptvertrag" ("Intra Group Agreement" o. ä.) vorangestellt und die Standardvertragsklauseln sind nur ein Anhang hierzu. Sofern durch einen solchen Hauptvertrag oder Rahmenvertrag die Standardvertragsklauseln nicht modifiziert werden, d.h. nicht in einem für die Genehmigungsfrage maßgeblichen Umfang im Sinne der obigen Erläuterungen, dann bleibt es bei der Genehmigungsfreiheit. In diesem Zusammenhang wird auch auf die Ausführungen unter Ziffer 3 des 19. Berichts der Landesregierung, Drs. 16/5892 verwiesen. Diese betreffen zwar nicht Mehrparteienverträge, sind aber gleichermaßen relevant. Wie dort ausgeführt, wäre es möglich, in einen Hauptvertrag Begriffsbestimmungen oder sonstige Vorgaben zur praktischen Umsetzung der EU-Standardvertragsklauseln im Konzern voranzustellen, aber es muss klargestellt werden, dass die EU-Standardvertragsklauseln inhaltlich unberührt bleiben. Die Genehmigungspflicht kann nur entfallen, wenn bei einem Rechtsstreit letztlich die Interpretation der EU-Standardvertragsklauseln maßgeblich ist. Insoweit muss von vornherein klargestellt werden, was gewollt ist. Daher kann es geboten sein, vorsorglich die Regelung aufzunehmen, dass im Falle von Unstimmigkeiten, Widersprüchen oder Zweifeln zwischen den konkreten Umsetzungsvorgaben im Hauptvertrag und den EU-Standardvertragsklauseln auf jeden Fall die Regelungen des EU-Standardvertrages Vorrang haben.

Bei Mehrparteien-Standardverträgen ist stets zu beachten, dass die erforderliche Bestimmtheit gewährleistet sein muss. Es muss klar geregelt werden, wer an wen welche Daten zu welchem Zweck übermittelt.

- Dies bedeutet, es muss zunächst einmal ersichtlich sein, welche Unternehmen (Stellen) Datenexporteure und welche Unternehmen Datenimporteure sind.
- Ferner muss eindeutig festgelegt sein, welche Rolle der Importeur einnehmen soll, ob er also als eigenständige verantwortliche Stelle ("Controller") fungieren soll oder nur als Datenverarbeitungsdienstleister ("Processor"). Dies ist dann von Bedeutung, wenn einem Hauptvertrag sowohl die Controller-Processor-Standardvertragsklauseln (EU-Standardvertrag vom Dezember 2001 oder neuer Controller-Processor-Standardvertrag vom Februar 2010) als auch die Controller-Controller-Standardvertragsklauseln (EU-Standardvertrag vom Juni 2001 oder alternativer Standardvertrag vom Dezember 2004) angefügt sind (als zwei separate Anhänge). Hier muss unzweifelhaft festgelegt werden, auf welche Übermittlung welche Standardvertragsklauseln anwendbar sind. Abstrakte Vorgaben etwa in der Art, dass bei Datentransfers an einen Datenverarbeitungsdienstleister die Controller-Processor-Klauseln gelten, reichen nicht.
- Die in den Anlagen zu den Standardvertragsklauseln geforderten Angaben müssen in der Weise gemacht werden, dass sie bezüglich des jeweiligen Datentransfers zwischen jedem Exporteur und jedem Importeur dokumentiert sind.

Idealerweise sind die o. g. Bestimmtheitsanforderungen in der Weise zu erfüllen, dass so viele Anlagen (pro Standardvertrag) ausgefüllt werden, wie es unterschiedliche Datentransfers gibt, also eine Anlage je Datentransfer, ggf. unterschiedlich je nach Verwendungszweck von einem Exporteur an einen Importeur. Allerdings erscheint es akzeptabel, wenn zunächst das Maximum der Übermittlungen je Standardvertrag festgelegt wird, also die Gesamtheit aller Daten, die in der Summe von allen Exporteuren in Europa zu der Gesamtheit der Zwecke übermittelt werden, dies wäre dann quasi der Rahmen. Spezifizierungen müssten dann separat vorgenommen werden. Es könnte in einem Länderzusatz für Deutschland festgelegt werden, was für die Datentransfers aus Deutschland gilt. Weitere Präzisierungen entsprechend den obigen Anforderungen könnten in sonstiger Weise dokumentiert werden. Dies müssten also verbindliche Präzisierungen sein, aber es wäre akzeptabel, wenn diese nicht von den gleichen Personen erstellt werden, welche den eigentlichen Mehrparteien-Vertrag unterzeichnet haben. Hier wäre also eine Delegation denkbar. Die entsprechende Präzisierung muss aber spätestens erfolgen, bevor die konkrete Übermittlung erfolgt.

Auf die bei individuellen Mehrparteiverträgen bestehenden besonderen Anforderungen, die im Hinblick auf die Genehmigungspflicht gelten, wurde bereits im letzten Tätigkeitsbericht (siehe Ziffer 3.1 des 22. Berichts der Landesregierung, Drucks. 18/1015) hingewiesen.

## **12. Beschäftigtendatenschutz**

### **12.1 Videoüberwachungsanlage in Lagerhallen**

Bei einem großen Internet-Versandhandelsunternehmen konnte die Aufsichtsbehörde hinsichtlich der Installation einer Videoüberwachungsanlage in einer neugebauten Lagerhalle beratend tätig werden. Der Betriebsrat des Unternehmens war mit einer entsprechenden Bitte an die Aufsichtsbehörde herangetreten. Wie sich herausstellte, war auch die Geschäftsführung an einer solchen Beratung vor Inbetriebnahme der Anlage interessiert.

Die Notwendigkeit einer Videoüberwachung wurde von der Geschäftsleitung mit Diebstählen in großem Umfang in den Lagern begründet. Die Videoüberwachung sollte sowohl der Abschreckung als auch der Aufklärung dienen. Aus datenschutzrechtlicher Sicht wurde das berechnigte schutzwürdige Interesse an der Videoüberwachung grundsätzlich anerkannt.

Bei einer Überprüfung vor Ort wurden neben der neu errichteten Lagerhalle auch die alten Lagerhallen, die ebenfalls mit einer Überwachungsanlage ausgestattet waren, in Augenschein genommen. An der Begehung der Lagerhallen nahmen ein Mitglied der Geschäftsleitung, ein Betriebsratsmitglied und die betriebliche Datenschutzbeauftragte teil.

Seitens der Aufsichtsbehörde konnte festgestellt werden, dass sowohl bei den bereits vorhandenen Kameras als auch bei der Installation der Kameras im Neubau in den meisten Fällen der Grundsatz der Verhältnismäßigkeit beachtet wurde.

Gegen die Anbringung bzw. Ausrichtung von vier Kameras in der neuen Lagerhalle mussten aus datenschutzrechtlicher Sicht allerdings Bedenken geltend gemacht werden, da diese Kameras jeweils direkt auf einen Arbeitsplatz gerichtet gewesen wären, d.h. hier hätte eine permanente Überwachung des dort tätigen Mitarbeiters stattgefunden oder zumindest stattfinden können. Eine solche ständige Kontrolle ist mit dem Anspruch des Arbeitnehmers auf Schutz seiner Persönlichkeitsrechte nicht vereinbar.

Auch eine über dem Raucherbereich im Außenbereich des Altbaus angebrachte Domkamera wurde beanstandet, da die Videoüberwachung von Mitarbeitern in einem Sozialbereich unzulässig ist. Das Unternehmen wurde aufgefordert, diese Kamera zu entfernen.

Die übrigen Videokameras waren aus datenschutzrechtlicher Sicht nicht zu beanstanden. Der Unternehmensleitung wurde empfohlen, unter Beteiligung der betrieblichen Datenschutzbeauftragten und des Betriebsrats ein Videokonzept zu erarbeiten. Ebenso wurde der Abschluss einer Dienstvereinbarung angeraten. Beide Empfehlungen der Aufsichtsbehörde wurden von dem Unternehmen umgesetzt.

Es wäre wünschenswert, wenn sich mehr Unternehmen bereits vor der Installation einer Videoüberwachungsanlage an die Aufsichtsbehörde wenden und von ihr beraten lassen würden.

### **12.2 Veröffentlichung von Mitarbeiterdaten im Internet**

An die Aufsichtsbehörde wurde telefonisch eine Beschwerde über die Homepage eines Reisebüros herangetragen, auf der neben den Kontaktdaten der Mitarbeiter mit Angabe über den jeweiligen Zuständigkeitsbereich auch die Kontaktdaten eines Auszubildenden veröffentlicht wurden, die darüber hinaus die zusätzliche Information: "Herr X befindet sich zur Zeit im Krankenstand" enthielten. Die Veröffentlichung dieser Daten stellte einen Verstoß nach § 28 Abs. 6 BDSG dar, wonach u. a. die Übermittlung sensibler Daten, zu denen auch Gesundheitsdaten gehören, nur unter ganz bestimmten Voraussetzungen zulässig ist.

Die Aufsichtsbehörde wurde in diesem Fall unverzüglich tätig und konnte durch einen Anruf in dem Reisebüro erreichen, dass die Angaben über den Auszubildenden noch am selben Tag von der Website gelöscht wurden. Aufgrund der schnellen Reaktion durch die verantwortliche Stelle wurde von aufsichtsbehördlichen Maßnahmen abgesehen.

Darüber hinaus war aber noch zu prüfen, ob überhaupt die Zulässigkeitsvoraussetzungen zur Veröffentlichung der Kontaktdaten der Mitarbeiter vorlagen. Einen speziellen Fall der Übermittlung von Personaldaten stellt deren Veröffentlichung dar. Trotz der grundsätzlichen Vertraulichkeit von Mitarbeiterdaten ist deren Veröffentlichung in herkömmlicher Form (Briefbogen, Prospekten, Werkszeitungen etc.) ohne Einwilligung der Betroffenen zulässig, wenn dies in der Zweckbestimmung des Arbeitsverhältnisses liegt.

Die Berechtigung oder Verpflichtung zur Publikation in herkömmlicher Form schließt aber keineswegs die Befugnis zur Einstellung dieser Daten in das Internet ein. Wegen der globalen Zugriffs- und Missbrauchsmöglichkeiten ist die Einstellung der Daten ins Internet mit besonderen Datenschutzrisiken für den Betroffenen verbunden. Daher ist eine Veröffentlichung von Name, Titel, Funktion oder Telefonnummer von Mitarbeitern im Internet nur mit Einwilligung der Betroffenen zulässig, es sei denn, es handelt sich um Funktionsträger, die auf Grund ihrer dienstlichen Tätigkeit auch Außenstehenden bekannt sein sollten. Gleichwohl wäre es wünschenswert, auch Funktionsträ-

gern eine Widerspruchsmöglichkeit einzuräumen. Die Veröffentlichung soll sich auf die Basiskommunikationsdaten beschränken. Eine darüber hinausgehende Veröffentlichung bedarf immer der Einwilligung der Mitarbeiter.

Im Falle des Reisebüros hat die Aufsichtsbehörde die Zulässigkeitsvoraussetzungen für eine Veröffentlichung der Kontaktdaten der festangestellten Mitarbeiter als erfüllt angesehen - nicht aber für die des Auszubildenden. Dieses Problem hatte sich aber - wie oben ausgeführt - zwischenzeitlich erledigt.

### **12.3 Detektiveinsätze bei einem Lebensmitteldiscounter**

Bereits im Herbst des Jahres 2008 hatte die Aufsichtsbehörde ein datenschutzrechtliches Überprüfungsverfahren gegen einen in Hessen ansässigen großen Lebensmitteldiscounter eingeleitet, dem - Presseberichten zufolge - die Überwachung seiner Mitarbeiter durch Detektive vorgeworfen wurde. Dieser Vorwurf war vergleichbar mit den Verstößen der rechtlich selbständigen und auf zwölf Bundesländer verteilten Vertriebsgesellschaften eines anderen Lebensmitteldiscounters, gegen die schon im Jahr 2008 Bußgelder in einer Gesamthöhe von rd. 1,5 Mio. € festgesetzt wurden (siehe Ziffer 12.1 des 22. Berichts der Landesregierung, Drucks. 18/1015).

Aufgrund von Inventurverlusten, die anders nicht aufgeklärt werden konnten, hatte sich das Unternehmen zum Einsatz von Detektiven entschlossen. Nach Darstellung des Unternehmens richteten sich die Detektiveinsätze nicht gegen Mitarbeiter, sondern gegen Kunden. Tatsächlich konnte die Aufsichtsbehörde bei Auswertung der noch vorhandenen Einsatzprotokolle der Detektive feststellen, dass sich diese ausschließlich auf Einsätze zur Kundenüberwachung bezogen. Obwohl sich der Überwachungsauftrag in keinem Fall auf die Mitarbeiter erstreckte, ergab sich aus den Detektivberichten, dass dennoch Mitarbeiter beobachtet wurden - wenn auch ohne Auftrag. Die Einsatzberichte enthielten neben allgemeinen Zustandsbeschreibungen insbesondere auch Beobachtungen bezüglich persönlicher Verhaltensweisen und Befindlichkeiten sowie privater Verhältnisse von Mitarbeitern. Bei den gespeicherten Daten handelte es sich teilweise um schwerwiegende Eingriffe in das Persönlichkeitsrecht der Betroffenen.

Seitens des Unternehmens wurde versichert, dass die Protokolle in keinem Fall in Bezug auf das Mitarbeiterverhalten ausgewertet wurden. Allerdings wurde bei Durchsicht der Protokolle die erforderliche Sorgfalt außer Acht gelassen, denn die Einsatzberichte wurden weder gegenüber der beauftragten Detektei beanstandet noch wurden die personenbezogenen Daten aus den Protokollen gelöscht oder innerhalb eines Protokolls zumindest geschwärzt. Die verantwortliche Stelle hätte auch erkennen müssen, dass durch die unbefugte Speicherung das Persönlichkeitsrecht der betroffenen Personen verletzt werden würde.

Die mit der unzulässigen Speicherung von Mitarbeiterdaten begangenen datenschutzrechtlichen Verstöße erfüllten den Ordnungswidrigkeitstatbestand nach § 43 Abs. 2 Nr. 1 BDSG und wurden mit einer Geldbuße von 235.000 € geahndet (siehe bereits oben Ziffer 4).

### **12.4 Unterlagen über Mitarbeiterprüfungen im Callcenter**

In vielen Callcentern ist die hohe Fluktuationsrate der Mitarbeiter nicht zu übersehen. Dies wurde auch für die Aufsichtsbehörde offensichtlich, als ihr eine Vielzahl von Unterlagen übergeben wurden, die in der Hauptsache Beurteilungen von einzelnen Mitarbeitern eines Callcenters enthielten. Vor allem aber wurde offenkundig, dass mit den Beschäftigendaten nicht sorgsam umgegangen wurde. Die Unterlagen waren nämlich in einem Müllcontainer, der auf einem frei zugänglichen Gelände stand und zum Teil sogar auf dem Erdboden um den Müllcontainer herum, gefunden worden. Der Finder händigte die Unterlagen der Aufsichtsbehörde aus.

Neben den Beurteilungen der Mitarbeiter befand sich dabei auch eine Anleitung zur Telefongesprächsführung. Aus dieser ging hervor, wie man die Angerufenen zum Vertragsabschluss für eine Lotterie überreden soll, und mit welchen Tricks die Angerufenen dazu gebracht werden sollen, ihre Bankverbindungsdaten anzugeben. Zu den Daten über die Mitarbeiter gehörten u. a. Angaben zur Stimmqualität, zur Wortwahl und insbesondere, wie gut die Überredungskünste des Mitarbeiters sind.

Wie und insbesondere von wem diese Unterlagen in den Papiercontainer entsorgt worden waren, war nicht mehr aufzuklären. Weitere aufsichtsbehördliche Maßnahmen, um eine ordnungsgemäße Datenverarbeitung bei dem Callcenter herbeizuführen, erübrigten sich, denn das Unternehmen existierte nicht mehr. Der Missstand war dem ehemaligen Geschäftsführer anzulasten, da es keine Nachweise zur Entsorgung sensibler Unterlagen im Unternehmen gab und die ehemaligen Mitarbeiter nach eigenen Aussagen auch nicht in irgendeiner Form dazu von der Geschäftsleitung geschult worden waren. Nachdem der Name und die Anschrift des ehemaligen Geschäftsführers ermittelt waren, wurde ein Ordnungswidrigkeitenverfahren gegen ihn eingeleitet. Dies dauerte bei Redaktionsschluss für diesen Bericht noch an.

### **12.5 Veräußerung von Bewerbungsunterlagen bei Ebay**

Eine Tageszeitung übergab der Aufsichtsbehörde Bewerbungsunterlagen von ca. 500 Arbeitssuchenden, die bei Ebay verkauft worden waren. Es handelte sich dabei um komplette Bewerbungen, in denen auch häufig die Bitte der Bewerber um Rücksendung enthalten war. Auch in diesem Fall existierten das oder die Unternehmen nicht mehr. Nach umfangreichen Recherchen konnten ein ehemaliger Geschäftsführer und sein Nachfolger als verantwortliche Personen ausfindig gemacht werden.

Der ehemals verantwortliche Geschäftsführer sah kein Problem darin, die Bewerbungsunterlagen seinem Nachfolger zu überlassen, obwohl dieser die konkrete Geschäftstätigkeit gar nicht übernehmen, sondern eine andere Geschäftstätigkeit ausüben wollte. Aber selbst bei einer Übergabe des Unternehmens hätten die Bewerberdaten nicht ohne weiteres an ein anderes Unternehmen weitergegeben werden dürfen.

Der neue Geschäftsführer wollte noch etwas Geld aus den Unterlagen herausholen und bot deshalb die kompletten Unterlagen als wenig gebrauchte Bewerbermappen an, ohne sich um den Inhalt zu kümmern. Gegen beide Geschäftsführer wurden Ordnungswidrigkeitenverfahren eingeleitet.

### **13. Videoüberwachung**

#### **13.1 Videobeobachtung an der "Wildschweinkirrung"**

Es scheint durchaus verbreitet, dass private Jäger die Wildschweinkirrung (Fütterung) im Wald mit einer Videokamera überwachen. Sie wollen sich dadurch die zeitraubende Beobachtung und den Ansitz vor Ort ersparen und trotzdem darüber informiert sein, wie viele und welche Wildschweine (Keiler, Bachen oder Frischlinge) sich im Jagdgebiet aufhalten. Ein Jagdpächter im Taunus bemerkte bei der Auswertung der Videoaufnahmen nicht nur die erwarteten Wildschweine, sondern auch den Nachbarjagdpächter, der sich an der Kirrung zu schaffen machte und wohl nachschaute, was der Kollege da füttert. Aufgrund der verbreiteten Konkurrenz zwischen benachbarten Jagdpächtern kam es zum Ärger, weil der beobachtende Jagdpächter bei der Jagdgenossenschaftsversammlung die Bilder des beobachteten Nachbarn herumzeigte und sich darüber aufregte, was "der" in seinem Revier zu suchen habe. Dies wurde dem gefilmten Jagdpächter von Dritten zugetragen, worauf dieser Unterlassung und die Herausgabe der Bilder forderte. Dies geschah zunächst über Rechtsanwälte bis dann auch der Bürgermeister der betroffenen Gemeinde und darüber hinaus die untere Jagdbehörde beim Rheingau-Taunus-Kreis und sodann die obere Jagdbehörde beim Regierungspräsidium Kassel eingeschaltet wurden. In diesem Zusammenhang prüfte die obere Jagdbehörde aus jagdlicher Sicht, ob der Jagdpächter eine Kamera anbringen darf. Hierbei stellte sich die Frage, ob die Kamera eine jagdliche Einrichtung - wie ein Hochsitz - ist und nach § 22 Hessischen Jagdgesetz geduldet werden muss. Der Leiter der oberen Jagdbehörde in Kassel wandte sich zugleich an das Regierungspräsidium Darmstadt und bat um Prüfung aus datenschutzrechtlicher Sicht.

Die jagdrechtliche Frage legte die obere Jagdbehörde wegen der grundsätzlichen Bedeutung dem Ministerium für Umwelt, Energie und Landwirtschaft vor. Dieses kam letztlich zu der Bewertung, dass eine Wildbeobachtungskamera keine jagdliche Einrichtung im Sinne des § 22 Hessisches Jagdgesetz ist. Es gibt somit keine spezialgesetzliche Regelung, die das Anbringen einer solchen Kamera erlaubt.

Aus datenschutzrechtlicher Sicht handelt es sich bei der Beobachtung im Wald durch den Jagdpächter um die Beobachtung des öffentlichen Raums. Für die Videoüberwachung des öffentlichen Raums gibt es spezielle Regelungen in § 14 HSOG. Daraus und aus den Wertungen des § 6b BDSG ist abzuleiten, dass Privatpersonen oder sonstige nicht öffentliche Stellen nicht befugt sind, den öffentlichen Bereich zu überwachen. Der Jagdpächter hat die Kamera schließlich abgebaut und die Bilddaten des Nachbarjagdpächters vernichtet.

Möglich wäre eine Wildbeobachtung mittels Webcam nur, wenn die Bilder so gering aufgelöst werden, dass Personen nicht identifizierbar sind und lediglich zwischen Mensch, Wildschwein, Hirsch usw. unterschieden werden kann.

### **14. Gesundheit**

#### **14.1 Datenschutz in einer neu gegründeten ärztlichen Gemeinschaftspraxis**

Eine ärztliche Gemeinschaftspraxis ist eine ärztliche Kooperationsform, in der üblicherweise alle Ärzte Zugriff auf die Daten aller dort behandelten Patienten nehmen können. Der gegenseitige Zugriff der Ärzte auf die Patientendaten bedarf aber einer Rechtfertigung. Die Rechtfertigung kann in der mutmaßlichen Einwilligung eines Patienten bestehen. Zumindest sollte ihm ein Widerspruchsrecht zustehen (siehe Ziffer 14.1 des 22. Berichts der Landesregierung, Drucks. 18/1015). Mitunter wünscht ein Patient nicht, dass ein bestimmter Arzt Zugriff auf seine Daten nehmen kann. Dieser Fall kann insbesondere dann auftreten, wenn sein behandelnder Arzt einer Gemeinschaftspraxis beiträgt bzw. mit anderen Ärzten eine solche Praxis gründet. Dieses Problem sollte über eine schriftliche Einwilligung des Patienten gelöst werden, aus welcher klar hervorgeht, welchen Ärzten der Gemeinschaftspraxis er den Zugriff auf seine Daten gestattet respektive nicht gestattet. Zudem ist von den Gemeinschaftspraxen eine Lösung zu finden, die sicherstellt, dass ein solcher "unerwünschter" Arzt nicht auf die Patientendaten des betreffenden Patienten zugreifen kann.

In einem aktuellen Fall legte ein empörter Beschwerdeführer der Aufsichtsbehörde den Entwurf einer Einverständniserklärung vor, da er diese nicht für datenschutzgerecht hielt.

In der Erklärung wurden die Patienten darüber informiert, dass die Gemeinschaftspraxis mit sechs Ärzten gegründet wurde und in wenigen Monaten den Betrieb aufnehmen werde. Die Patienten sollten ihr Einverständnis erklären, dass alle Ärzte der neuen Gemeinschaftspraxis ihre Krankenunterlagen einsehen dürfen. Für den Fall, dass sie hiermit nicht einverstanden waren, wurde ihnen erklärt, dass eine Behandlung durch ihren bisherigen Arzt nicht mehr möglich sei. Der Patient hätte somit keine Möglichkeit gehabt, von seinem bisherigen behandelnden Arzt weiterhin behandelt zu werden, wenn er den anderen Ärzten den Zugriff auf seine Daten verwehren wollte. Die

Beschwerde zeigt, dass bei Patienten durchaus sowohl eine Sensibilität hinsichtlich ihrer Patientendaten besteht, als auch die Erwartung, dass sie Einfluss auf die Zugriffsmöglichkeiten von Ärzten einer Gemeinschaftspraxis auf ihre Daten nehmen können.

Die Aufsichtsbehörde machte die Ärzte der künftigen Gemeinschaftspraxis, welche zu dieser Zeit noch in unterschiedlichen Praxen praktizierten, darauf aufmerksam, dass ein Patient auch in einer Gemeinschaftspraxis das Recht haben muss, einzelne Ärzte vom Zugriff auf seine Daten auszuschließen, ohne dass ihm deswegen die Behandlung in dieser Praxis verwehrt wird.

Es stellte sich heraus, dass man inzwischen von dem ursprünglichen Plan bereits Abstand genommen hatte und den Patienten die Möglichkeit geben wollte, einzelne Ärzte vom Zugriff auf ihre Patientendaten auszuschließen. Zudem wurde mitgeteilt, dass bezüglich der Zugriffstrennung in der EDV Lösungsvorschläge in Ausarbeitung seien. Die vorgelegte geänderte Einverständniserklärung war jedoch noch weiter überarbeitungsbedürftig. Der Patient konnte zwar erklären, dass er mit einem gemeinsamen Zugriff aller Ärzte einverstanden ist, oder dass er es nicht ist, es fehlte jedoch die Erläuterung, wie verfahren werden soll, wenn er nicht mit dem gemeinsamen Zugriff einverstanden ist.

Die Einverständniserklärung wurde schließlich in Abstimmung mit der Aufsichtsbehörde dahingehend geändert, dass der Patient selbst darüber entscheidet, welche Ärzte der Gemeinschaftspraxis Zugriff auf seine Daten nehmen dürfen, und dass die Möglichkeit der Behandlung unabhängig davon ist, ob er sich für den Zugriff durch alle oder nur durch bestimmte Ärzte entscheidet. Hierauf wurde in der Einwilligungserklärung ausdrücklich hingewiesen. Durch Ankreuzen kann sich der Patient für die eine oder die andere Zugriffsmöglichkeit entscheiden. Falls nur bestimmte Ärzte Zugriff auf seinen Daten nehmen sollen, werden diese namentlich von ihm in der Einverständniserklärung benannt.

Als Problem für die Praxis erwies sich die zunächst avisierte technische Zugriffstrennung, da nach Angabe des federführenden Arztes weder der Hersteller des in der Praxis verwendeten Programms noch der lokale Support eine Möglichkeit der Datentrennung im Rahmen einer Gemeinschaftspraxis darstellen könnten. Es wird auf eigenes Betreiben der Ärzte nunmehr so verfahren, dass Daten von Patienten, die nicht mit dem Zugriff aller Ärzte einverstanden sind, aus der EDV gelöscht und in Papierform beim Arzt ihrer Wahl unter Verschluss aufbewahrt werden. Diese Regelung wurde von der Aufsichtsbehörde akzeptiert.

## **15. Werbung und Adresshandel**

### **15.1 Stärkung der Betroffenenrechte durch das geänderte Bundesdatenschutzgesetz**

Im Bereich Werbung und Adresshandel lag das Hauptgewicht der praktischen Arbeit auch 2009 wieder in der Durchsetzung der Betroffenenrechte auf Auskunft und Sperrung der für Werbezwecke verwendeten Daten. Zur Stärkung eben dieser Rechte hat der Bundestag am 3. Juli 2009 das Gesetz zur Änderung datenschutzrechtlicher Vorschriften verabschiedet ("Novelle II", siehe bereits oben Ziffer 6). Dabei wurde das Listenprivileg nach § 28 Abs. 3 Satz 1 Nr. 3 BDSG a. F. zwar nicht vollkommen aufgehoben, aber insbesondere durch die Einführung neuer Transparenz- und Speicherpflichten eingeschränkt und neu gestaltet. Neue Spezialregelung für Werbung und Adresshandel ist jetzt § 28 Abs. 3 bis 4 BDSG. Für den Adresshandel ist ferner § 29 BDSG maßgeblich, worin auf § 28 Abs. 3 bis 3b BDSG Bezug genommen wird. Die Neuregelungen werfen viele Auslegungsfragen auf und haben zu einiger Rechtsunsicherheit geführt.

#### **a) Einwilligungsvorbehalt**

In § 28 Abs. 3 Satz 1 BDSG hat der Gesetzgeber die Verarbeitung oder Nutzung personenbezogener Daten unter einen Einwilligungsvorbehalt gestellt: "Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat..." Für die Erhebung der Daten muss auf § 28 Abs. 1 BDSG zurückgegriffen werden.

Von Beginn des Gesetzgebungsverfahrens an war die Frage, inwieweit es Ausnahmen von dem Einwilligungserfordernis (opt-in-Prinzip) geben sollte, Gegenstand intensiver Diskussionen. Im parlamentarischen Verfahren hat der ursprüngliche Entwurf der Bundesregierung noch bedeutende Änderungen erfahren. Letztlich bestehen nun eine Reihe von Ausnahmen, sodass in der Praxis (de facto) weitgehend das Widerspruchsprinzip (opt-out-Prinzip) gilt. Diese Ausnahmen sind in § 28 Abs. 3 Satz 2 bis 5 BDSG geregelt.

#### **b) Ausnahmen vom Einwilligungsvorbehalt**

##### **§ 28 Abs. 3 Satz 2 BDSG**

Der Katalog der Ausnahmen wird eingeleitet mit der Formulierung "Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken..."

Werden ausschließlich die zuvor genannten Listendaten verwendet, gibt es also Ausnahmen vom Einwilligungserfordernis, die den Handlungsrahmen für die schriftliche Kundenansprache künftig abdecken.

## **Verarbeitung und Nutzung für eigene Angebote (§ 28 Abs. 3 Satz 2 Nr. 1)**

### **1. Alternative**

Stammen die Daten vom Betroffenen selbst und wurden sie im Rahmen eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses (insbesondere Vertrag, Vertragsverhandlungen) bei ihm erhoben, bedarf die schriftliche werbliche Ansprache auch weiterhin keiner gesonderten Einwilligung. Dies setzt voraus, dass das Unternehmen ausschließlich für eigene Angebote wirbt. Hier gilt dann ausnahmsweise nicht die Beschränkung auf Listendaten, da nach Satz 3 das Hinzuspeichern erlaubt ist. Hiermit ist das Speichern weiterer Daten zur Selektion gemeint, Merkmalskombinationen sind also erlaubt. Das Hinzuspeichern schließt die Erlaubnis zur Verarbeitung und Nutzung dieser Daten ein, sofern eine Abwägung nach Satz 6 getroffen wurde.

### **2. Alternative**

Fremde Adressen dürfen für eigene Angebote ohne Einwilligung und ohne Quellkennzeichnung genutzt werden, wenn die Daten aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben wurden. Der Begriff ist enger als "allgemein zugängliche Quellen" und betrifft beispielsweise nicht Daten, die einer Website des Beworbenen entnommen werden könnten. Ist der Beworbene jedoch in einem im Internet bestehenden Verzeichnis zu finden, so bedarf es keiner Einwilligung zur werblichen Nutzung der Daten. Nach § 28 Abs. 3 Satz 3 in Verbindung mit Satz 6 BDSG dürfen auch hier weitere Daten hinzugespeichert werden, sofern die schutzwürdigen Interessen des Betroffenen nicht entgegenstehen.

## **Werbung für berufliche Zwecke (§ 28 Abs. 3 Satz 2 Nr. 2 BDSG)**

Keine Einwilligung ist erforderlich für Werbung im Hinblick auf die berufliche Tätigkeit eines Betroffenen. Diese Ausnahme für Geschäftswerbung erfasst nicht nur die Werbung gegenüber freiberuflich oder gewerblich Tätigen unter deren Geschäftsadresse, sondern gilt nun z.B. auch für die bei ihnen Beschäftigten, etwa den Leiter der Entwicklungsabteilung oder die Sekretärin der Geschäftsführung (BT-Drucks. 16/13657). Allerdings darf die Werbung nur an die berufliche Anschrift gerichtet sein. Wichtig ist hier der geschäftliche Bezug, denn nicht immer lässt sich der Adresse eindeutig entnehmen, ob es sich um Geschäftsadresse oder das Büro zu Hause handelt.

## **Werbung für Spenden (§ 28 Abs. 3 Satz 2 Nr. 3 BDSG)**

Steuerbegünstigten Spendenorganisationen wie gemeinnützigen Organisationen und Parteien ist die schriftliche Kundenansprache ohne Einwilligung der Adressaten gestattet.

Die Ausnahmeregelungen in § 28 Abs. 3 Satz Nr. 3 und 4 BDSG bedeuten, dass für Geschäftswerbung und Spendenwerbung unter den genannten Voraussetzungen die Transparenzanforderungen des § 28 Abs. 3 Satz 4 und 5 BDSG nicht gelten.

## **Transparente Übermittlung (§ 28 Abs. 3 Satz 4 BDSG)**

Im Gesetzgebungsverfahren wurde insbesondere erörtert, ob eine Datenübermittlung für fremde Werbezwecke ohne Einwilligung der Betroffenen möglich sein soll. Dabei erwies sich der Gedanke als kompromissfähig, dass der Betroffene zumindest wissen sollte, woher seine für die Werbung verwandten Adressdaten stammen. Es wurde daher Einigung darüber erzielt, dass eine Einwilligung ferner nicht erforderlich sei für die Übermittlung von Listendaten an Dritte zu Werbezwecken, wenn in jedem Werbeschreiben des Dritten (anderen) die erstmalig erhebende Stelle (die Datenquelle) eindeutig erkennbar benannt werde.

Nach § 34 Abs. 1a BDSG ist jede Datenübermittlung mit Angabe der Lieferkette, also mit Herkunft und Empfänger der Daten, für zwei Jahre zu speichern. Dem Betroffenen ist auf Verlangen entsprechende Auskunft über die Herkunft und den Empfänger der Daten zu erteilen. Die Speicherung der erstmalig erhebenden Stelle muss solange erfolgen, wie die Daten für Werbezwecke verwendet werden, ist also nicht auf zwei Jahre begrenzt, da sowohl zeitliche Gründe, wenn die übermittelten Daten länger als zwei Jahre genutzt werden sollen, als auch andere Gründe, z.B. Quelle und Herkunft der Daten fallen durch Folgeübermittlungen auseinander, einer Begrenzung der Speicherdauer entgegenstehen können. Die in § 28 Abs. 3 Satz 4 Halbsatz 2 BDSG geforderte Kennzeichnungspflicht unterliegt zudem keiner zeitlichen Beschränkung. Auch hieraus folgt, dass die erstmalig erhebende Stelle dauerhaft zu speichern ist.

Ein Verstoß gegen die Speicher- und Auskunftspflicht nach § 34 Abs. 1a BDSG ist gemäß § 43 Abs. 1 Nr. 8 a BDSG bußgeldbewehrt. Wird die erstmalig erhebende Stelle nicht in der Werbung angegeben, stellt dies eine unzulässige Übermittlung dar, die - ebenso wie andere unzulässige Datenverarbeitungen - ggf. nach § 43 Abs. 2 Nr. 1 BDSG mit einem Bußgeld geahndet werden kann.

## **Transparente Nutzung (§ 28 Abs. 3 Satz 5 BDSG)**

Eine weitere Ausnahme vom Erfordernis der Einwilligung erlaubt die **Nutzung** (keine Übermittlung) von Daten zur Bewerbung von fremden Angeboten, wenn bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle, also der Adresseigner, eindeutig erkennbar ist. Laut Gesetzesbegründung umfasst diese Ausnahme die Beipackwerbung ebenso wie die Empfehlungswerbung. Darüber hinaus gilt sie für das sogenannte Lettershop-Verfahren.

Zur Kennzeichnungspflicht heißt es in den Gesetzesmaterialien: "Eine Erkennbarkeit bei der Ansprache ist nicht gegeben, wenn der Betroffene anhand eines Kennzeichens oder einer Nummer lediglich die Möglichkeit erhält, durch weiteres Tätig werden die Stelle zu identifizieren. Einer eindeutigen Erkennbarkeit bei der Ansprache genügt nur eine Bezeichnung im Klartext." (BT-Drucks. 16/13657, Seite 31). Durch diese Bestimmung soll dem Beworbenen erleichtert werden, von seinem Recht auf Widerspruch Gebrauch zu machen. Es ist daher sinnvoll, den Ad-



resseigner in der Widerspruchsbelehrung zu nennen. Es muss ferner auch, wie bisher, der Nutznießer der Werbung (das werbende Unternehmen) eindeutig erkennbar aus dem Werbeschreiben hervorgehen. Dies ergibt sich bereits aus der alten Vorschrift des § 28 Abs. 4 Satz 2 Halbsatz 2 BDSG, in der insoweit mit der verantwortlichen Stelle nicht der Adressseigner gemeint war.

Die etwas missverständlich gewählte Einleitung des Satzes 5 "Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2..." meint wohl nicht, dass die Begrenzung auf die in Satz 2 genannten "Listendaten" aufgehoben ist (so Meltzian, Der Betrieb, S. 2643 ff). Die Abstimmung im Düsseldorfer Kreis zu dieser Frage war bei Redaktionsschluss für diesen Bericht noch nicht abgeschlossen.

**c) Einwilligung (§ 28 Abs. 3a und 3b BDSG)**

Wie sich aus obigen Ausführungen ergibt, ist eine Einwilligung dann erforderlich, wenn die vorgenannten Ausnahmen nicht greifen. An diese werden in § 28 Abs. 3a BDSG besondere Anforderungen gestellt. Wird eine schriftliche Einwilligung zusammen mit anderen Erklärungen verlangt, ist diese durch drucktechnisch deutliche Gestaltung hervorzuheben. Wird eine Einwilligung telefonisch erteilt, muss deren Inhalt schriftlich bestätigt werden. Wird eine Einwilligung elektronisch erteilt, ist sie zu protokollieren, muss jederzeit abrufbar und mit Wirkung für die Zukunft widerruflich sein. Diese Vorschrift entspricht § 13 Abs. 2 TMG. Nach § 28 Abs. 3b BDSG darf der Abschluss eines Vertrages in bestimmten Fällen nicht von der Einwilligung des Betroffenen in die Verwendung seiner Daten für Werbung und Adresshandel abhängig gemacht werden (begrenztes Koppelungsverbot).

**d) Recht auf Widerspruch (§ 28 Abs. 4 BDSG)**

Für alle oben genannten Ausnahmen vom Einwilligungserfordernis gilt weiterhin die Widerspruchslösung (opt-out-Prinzip). Der Betroffene muss widersprechen, wenn er nicht will, dass seine Daten für Werbung verwendet werden. Die Regelung findet sich in § 28 Abs. 4 Satz 1 BDSG: "Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung- oder der Markt- und Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig." Neu ist, dass die Verarbeitung und Nutzung entgegen § 28 Abs. 4 Satz 1 BDSG nach § 43 Abs. 2 Nr. 5b BDSG bußgeldbewehrt ist.

Nach § 28 Abs. 4 Satz 2 BDSG muss der Hinweis auf das Widerspruchsrecht nicht nur bei der werblichen Ansprache (wie bisher), sondern auch schon bei der Begründung eines Vertrages oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erfolgen.

Für die Ausübung des Widerspruchs darf gemäß § 28 Abs. 4 Satz 4 BDSG keine strengere Form verlangt werden als für das Rechtsgeschäft. Ein Verstoß hiergegen ist ebenfalls gemäß § 43 Abs. 1 Nr. 3a BDSG bußgeldbewehrt.

**Zusammenfassend** ist festzuhalten, dass mit der Verabschiedung der BDSG-Novelle II eine Stärkung der Rechte der Betroffenen, insbesondere durch die neu eingeführten bzw. verbesserten

- Transparenzpflichten nach § 28 Abs. 3 Satz 4 und 5 BDSG und § 28 Abs. 4 Satz 2 BDSG
  - Speicherpflichten nach § 28 Abs. 3 Satz 4 2. Halbsatz BDSG i. V. m. § 34 Abs. 1a BDSG
  - Anforderungen an Einwilligungen nach § 28 Abs. 3a BDSG
  - Bußgeldvorschriften für den Werbebereich nach § 43 Abs. 1 Nr. 3a und 8a, § 43 Abs. 2 Nr. 5b BDSG
- erreicht wurde.

Über die zahlreichen Auslegungsfragen der Novelle II steht die Datenschutzaufsichtsbehörde seit September 2009 in intensivem Kontakt mit dem in Wiesbaden ansässigen Deutschen Dialogmarketing Verband. In einer Reihe von Punkten wurde bereits Übereinstimmung erzielt, diese sind zum Teil in die obige Darstellung eingeflossen. Die Abstimmung mit dem Verband und mit anderen Aufsichtsbehörden soll fortgeführt werden.

Wiesbaden, 27. September 2010

Der Hessische Ministerpräsident:

**Bouffier**

Der Hessische Minister des  
Innern und für Sport:  
**Rhein**