

19. Datenschutz in der Privatwirtschaft

19.1 Zu den Sitzungen der obersten Datenschutzaufsichtsbehörden

Um länderübergreifend in der Bundesrepublik aber auch EU-weit einen möglichst einheitlichen Datenschutzstandard zu gewährleisten, bedarf es der Absprache unter den Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich. An den Sitzungen der obersten Aufsichtsbehörden – jeweils eine im Frühjahr und im Herbst – nehme ich regelmäßig teil. Um wirtschaftliche Belastungen der Unternehmen zu vermeiden, bin ich daran interessiert, den datenschutzrechtlichen Regelungen Geltung zu verschaffen und dabei möglichst keine zusätzlichen Arbeitsaufwände zu erzeugen. Eine über die Grenzen einheitliche Haltung der Datenschutzaufsichtsbehörden gegenüber der Wirtschaft ist auch deshalb wichtig, um gleiche wirtschaftliche Rahmenbedingungen zu erzeugen und so Wettbewerbsverzerrungen zu vermeiden. Das gilt natürlich für alle Wirtschaftszweige, im besonderem Maße aber für die, deren Geschäftsfeld ausschließlich im Bereich der Datenverarbeitung liegt.

Einige der nachfolgend aufgeführten Themen werden im weiteren Verlauf des Berichtes näher erläutert. Im Bereich der Kreditwirtschaft bestand Anlass, sich mit Themen wie Kreditscoring/Basel II, dem Verkauf von Darlehen an Unternehmer ins Ausland oder der Datenverarbeitung bei SWIFT zu befassen. Im Übrigen bestehen ständige Themen im Bereich der Telekommunikation, Tele- und Mediendienste, der Versicherungswirtschaft, dem Adress- und Versandhandel wie im Bereich des Arbeitnehmerdatenschutzes. Der Patientendatenschutz in Kooperationspraxen war ebenso Thema wie Mandantenschutz in Rechtsanwaltskanzleien, aber auch Einzelthemen wie Bonus- und Rabattkarten, Digi-Foto-Maker oder Mahnung per Computer waren Gegenstand der Beratungen. Auch bei der Gesetzgebungsberatung, z. B. der Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (hier mit Regelungen für Auskunftfeien und das Scoring) und dem Entwurf des Bundesdatenschutzauditgesetzes fand ein Meinungsaustausch statt. Soweit zu den einzelnen Themen Beschlüsse gefasst wurden, sind diese auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de abrufbar.

19.2 Kreditwirtschaft

19.2.1 Unzureichende Protokollierung von Beschäftigtenzugriffen bei einem Kreditinstitut

Ich erhielt mehrere Beschwerden unzulässiger Datenabrufe von Kundenkonten durch Beschäftigte eines Kreditinstituts.

Ich bemühte ich mich um Aufklärung des Sachverhaltes und bat das Kreditinstitut zunächst um Darstellung der von ihm verwirklichten Protokollierung der Zugriffe der Mitarbeiterinnen und Mitarbeiter. Da die Darstellung verschiedene Fragen aufwarf, besuchte ich im November 2007 schließlich das Kreditinstitut und informierte mich vor Ort über die Protokollierung.

Dabei stellte sich heraus, dass das Kreditinstitut ein im Kern seit 1971 bestehendes Datenverarbeitungssystem betreibt, bei dem die Zugriffe zwar elektronisch protokolliert, jedoch tagesaktuell auf Mikrofiche verfilmt und dem betrieblichen Datenschutzbeauftragten zur Verfügung gestellt werden. Aufgrund einer seinerzeit geschlossenen Vereinbarung mit dem Betriebsrat, um Leistungs- und Verhaltenskontrollen der Mitarbeiter auszuschließen, war es dem betrieblichen Datenschutzbeauftragten daher nicht möglich, die Mikrofiche z. B. nach den Zugriffen bestimmter Mitarbeiter oder Zeiten zu überprüfen. Auch gestaltete sich die Überprüfung der Kontrolle ohne elektronische Unterstützung durch Sichtung der Mikrofiche als äußerst mühsam, da täglich etwa 250.000 Zugriffe bremenweit protokolliert wurden.

Diese Form der Protokollierung steht nicht im Einklang mit den technisch-organisatorischen Anforderungen, die das Bundesdatenschutzgesetz für Protokollierungen aufstellt. Ich habe das Kreditinstitut, das sich bereits im Prozess der Migration auf ein neues Programm befand, hierüber in Kenntnis gesetzt und verschiedene Anforderungen an die künftige Protokollierung gestellt.

Da sich im Nachgang der Prüfung ergab, dass die verfilmten Protokolldaten zur Wiederherstellung im Katastrophenfall doch auch elektronisch vorgehalten werden, habe ich die Sicherung der Protokolldaten und eine Auswertung verlangt, um den Verdacht eines missbräuchlichen Zugriffs zu beseitigen. Dieser Vorgang ist noch nicht abgeschlossen.

19.2.2 SWIFT

Alle Auslandsüberweisungen werden weltweit über SWIFT abgewickelt. Die datenschutzrechtliche Problematik der auch auf Drittländer außerhalb der EU verteilten Datenverarbeitung von SWIFT habe ich im letzten Bericht dargestellt (vgl. 29. JB, Ziff. 18.3). Im Oktober 2007 hat SWIFT die geplante Veränderung ihrer IT-Infrastruktur bekannt gegeben. Der Art. 29-Gruppe hatte SWIFT vorher noch einige nähere Erläuterungen gegeben.

Danach soll der Systemumbau bis Ende 2009 erfolgen. Die DV soll dann auf drei Server verteilt sein. In der Schweiz wird der „globale“ Server stehen, d. h., dort werden alle Daten gespiegelt. Außerdem wird es weiterhin einen Server in den USA und einen in Europa (Niederlande) geben. Der Server in den USA wird alle Daten der „Transatlantic Zone“ speichern; auf dem europäischen Server werden alle Überweisungsdaten der „European Zone“ gespeichert werden. Zur „European Zone“ gehören alle Staaten des europäischen Wirtschaftsraums und die Schweiz. Zur „Transatlantic Zone“ gehören die USA. Alle anderen Staaten können wählen, zu welcher Zone sie gehören wollen, d. h., Länder wie Japan oder die Türkei können selbst entscheiden, ob sie zur europäischen oder transatlantischen Zone gehören wollen. Diese Frage soll von den entsprechenden nationalen Mitgliedsgruppen von SWIFT und nicht von den Regierungen entschieden werden; die entsprechenden Entscheidungen der Mitgliedsstaaten sollen öffentlich gemacht werden.

Das bedeutet: Zur Zeit werden Überweisungen innerhalb der Staaten des europäischen Wirtschaftsraumes und der Schweiz nur auf dem Server in den Niederlanden gespeichert und in der Schweiz gespiegelt. Bei Überweisungen in die USA wird eine Speicherung in den USA erfolgen.

19.3 Auskunfteien

19.3.1 Handels- und Wirtschaftsauskunfteien

Im Berichtsjahr erhielt ich Eingaben, die sich gegen die Datenverarbeitung der Auskunfteien richteten. Hier einige Beispiele:

Ein Betroffener beklagte sich bei mir, dass Daten zu einer gegen ihn gerichteten Forderung in den Auskunfteidatenbestand der für seinen Wohnort zuständigen Geschäftsstelle einer Handels- und Wirtschaftsauskunftei aufgenommen worden seien. Kenntnis von der Forderung habe er erstmalig durch das an ihn von dieser Auskunftei im Rahmen der Inkassotätigkeit des Unternehmens übersandten Mahnschreibens erhalten, dem er auch die Informationen zur Übernahme seiner Daten in den Auskunfteidatenbestand entnommen hatte.

Auch Auskunfteien dürfen nur richtige Daten verarbeiten. Ist die gegen einen Schuldner erhobene Forderung berechtigt und wurde sie termingerecht beglichen, so sind Aufnahme und Übermittlung von Angaben zu Auskunfteizwecken, nach denen der Betroffene seinen Zahlungsverpflichtungen nicht nachkommt oder es sich bei ihm um einen säumigen Schuldner handelt, nicht zulässig. Die Aufnahme und Übermittlung einer noch nicht titulierten und nicht beglichenen Forderung setzen voraus, dass der Betroffene von der bevorstehenden Nutzung für Auskunfteizwecke rechtzeitig informiert wird. Rechtzeitig ist die Unterrichtung nur, wenn dem Betroffenen noch die Möglichkeit verbleibt, in zumutbarer Weise ggf. ein berechtigtes Bestreiten der Forderung voranzubringen oder zu begleichen. Im vorliegenden Fall hätte der Betroffene keine Möglichkeit gehabt, die Berechtigung der Forderung zu überprüfen und dieser zu entsprechen bzw. sie zu bestreiten. Die Aufnahme und Übermittlung der Daten zu Auskunfteizwecken wäre daher unzulässig gewesen.

Meine Nachforschungen bei der Auskunftei ergaben, dass entgegen des Wortlauts des Mahnschreibens eine Aufnahme der den Petenten betreffenden Inkassodaten in den Auskunfteidatenbestand bislang nicht erfolgt war. Dies wurde mir auch von der für den Wohnort zuständigen Geschäftsstelle bestätigt. Die Auskunftei bedauerte, dass es durch missverständliche Formulierungen in dem Mahnschreiben zu einem falschen Eindruck gekommen war und sagte zu, die in dem Schreiben kritisierten Textpassagen künftig nicht mehr zu verwenden.

In einem anderen die Tätigkeit dieser Auskunftei betreffenden Fall beklagte sich ein Betroffener, dass seinem Anspruch auf Auskunft nach § 34 BDSG nicht entsprochen werde. Seine Bitte um Mitteilung, woher die Auskunftei seine Daten habe, werde nicht erfüllt. Erst durch mein Tätigwerden gelang es, den gesetzlichen Anspruch des Betroffenen durchzusetzen.

19.3.2 Wohnungsunternehmen als Vertragspartner der SCHUFA

Bereits 2003/2004 wurde kontrovers diskutiert, inwieweit Auskunfteien und Warndateien Auskünfte über Mietinteressenten an Vermieter vor Eingehung eines Mietverhältnisses erteilen dürfen. Zur Teilnahme von Wohnungsunternehmen am Auskunftsverfahren der SCHUFA und anderer Auskunfteien, aber auch zu Auskünften an einzelne Vermieter haben die obersten Datenschutzaufsichtsbehörden im November 2004 sich auf allgemeine Grundsätze verständigt.

Aus der Sicht des Datenschutzes sind auf branchenspezifische Daten beschränkte Auskunftssysteme vorzuziehen, bei denen die Daten gesicherte Rückschlüsse auf Mietausfallrisiken zulassen. Dies entspricht auch Vorstellungen, die derzeit im Deutschen Bundestag diskutiert werden.

Eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunftsteilen gespeicherte Daten an potentielle Vermieter ist dagegen unzulässig. an Vermieter zu übermitteln, nicht gerechtfertigt ist. Die kompletten Negativdaten etwa, wie sie anderen B-Partnern zur Verfügung gestellt werden, dürfen an Vermieter nicht weitergegeben werden.

Bei der Prüfung, in welchem Umfang nach § 29 Bundesdatenschutzgesetz an potentielle Vermieter personenbezogene Daten übermittelt werden dürfen, sind die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung in besonderer Weise zu berücksichtigen. Auskünfte über Eintragungen im Schuldnerverzeichnis sind stets zulässig.

Die obersten Datenschutzaufsichtsbehörden haben auch Zweifel an der Zulässigkeit einer Beauskunftung auf Grund einer Einwilligung. Entsprechendes gilt auch für das Verlangen gegenüber dem Mietinteressenten auf Vorlage einer Selbstauskunft. Unter den Aufsichtsbehörden ist unstreitig, dass diese rechtliche Beurteilung fortgilt.

19.3.3 Prüfung einer Auskunftsteil mit Mieterdaten in Bremen

In den Geschäftsräumen einer Mieterauskunftsteil fand die vorgenannte Prüfung statt. Prüfungsschwerpunkte waren die Datenerhebung bei Dritten, Datenspeicherung, Datenübermittlung an Dritte und die Gewährleistung der Betroffenenrechte.

Datenerhebung bei Dritten und Datenspeicherung: Die Mieterauskunftsteil erhält Daten aus unterschiedlichen Quellen, z. B. von Vermietern. Diese melden Daten über Verstöße gegen erhebliche mietvertragliche Verpflichtungen durch Mieter sowie eine Vielzahl anderer Daten an die Mieterdatenbank, z. B. Kautionsvertragsgemäß gezahlt, Mietrückstand, Mängelanzeige rechtzeitig, Tierhaltung.

Neben der Mieterdatenbank hält die Mieterauskunftsteil eine sog. Bonitätsdatenbank vor. Diese enthält den branchenübergreifenden Datenbestand einer in Baden-Württemberg ansässigen Auskunftsteil entsprechend deren Katalog über Auskunftsmerkmale und Hinweis-Meldungen. Außerdem werden Daten von anderen Auskunftsteilen branchenübergreifend in diese Bonitätsdatenbank eingestellt. Die von der Auskunftsteil in Baden-Württemberg bezogenen Daten sind nach dortiger Kategorisierung, die nicht auf die Bonitätsprüfung durch Vermieter bezogen ist, in „weiche“ (z. B. Inkasso-Mahnverfahren eingeleitet), „mittlere“ (Mahnbescheid) und „harte“ (z. B. Eröffnung des Insolvenzverfahrens) Negativmerkmale unterteilt.

Die Erhebung von Daten durch die Mieterauskunftsteil, die zusätzlich zu den Angaben über erhebliche Mietvertragsverstöße und den sog. harten Negativmerkmalen eingemeldet werden, ist aus folgenden Gründen nicht zulässig:

Bei der Frage, welche personenbezogenen Mieterdaten ein Vermieter zur Bonitätsprüfung benötigt und demzufolge erhoben bzw. in die Mieterdatenbank eingegeben werden dürfen, ist zwischen den nachstehenden Rechtsgütern des Vermieters und des Mietinteressenten angemessen abzuwägen.

Die berechtigten Interessen des Vermieters bestehen insbesondere darin, das Mietausfallrisiko zu vermindern. Insoweit ist einer Prüfung anzuerkennen, ob der Mietinteressent in der Lage ist, die Miete zu bezahlen. Bedeutsam ist hierbei auch, dass der Vermieter sog. schwarze Schafe und sog. Mietnomaden unter den Mietinteressenten erkennen möchte, um mögliche Risiken auch im Lichte des Mietvertrags abzuschätzen.

Die schutzwürdigen Interessen des Mietinteressenten bestehen aufgrund der existentiellen Bedeutung einer Wohnung als Mittelpunkt des privaten Lebensbereiches und seiner grundrechtlichen Schutzposition aus Art. 2, 13, 14 Grundgesetz (GG) und den Vorschriften des Mietrechts nach §§ 535 ff. Bürgerliches Gesetzbuch (BGB). Erfahrungsgemäß unterscheidet sich das Zahlungsverhalten im allgemeinen Geschäftsverkehr erheblich von dem Verhalten im Mietverhältnis. Gleichwohl muss hier ein Betroffener damit rechnen, als Mieter abgelehnt zu werden, wenn der Vermieter von der Auskunft über das Vorliegen eines Vollstreckungsbescheides informiert wird, der aus einer nicht bezahlten Rechnung, z. B. aus einem Kaufvertrag, resultiert.

Die Bonitätsprüfung und die daraus resultierende Datenerhebung durch den Vermieter bei Auskunfteien müssen sich an der spezifischen Situation des anzubahnenden Mietverhältnisses orientieren. Vermieter können zur Bonitätsprüfung die Vorlage von Verdienstbescheinigungen etc. durch den Mietinteressenten nach § 4 Abs. 2 Satz. 1 i. V. m. § 28 Abs. 1 Satz 1 Nr. 1 BDSG verlangen. Außerdem befinden sich Vermieter gegenüber dem Mietinteressenten im Vorteil, z. B. durch die Mietkaution, das Vermieterpfandrecht und ggf. in die Zahlungspflicht tretende Sozialbehörden, die bei Zahlungsunfähigkeit die Mietzahlung übernehmen. Daher ist die Erheblichkeitsschwelle bei mietspezifischen oder sonstigen mieterrelevanten Negativdaten hoch anzusetzen. Demzufolge benötigt ein Vermieter nicht sämtliche bei einer allgemeinen Auskunft gespeicherten Daten zur Bonitätsprüfung. Nach Abwägung beider Rechtsgüter ist nur die Erhebung bzw. Einmeldung sog. harter Daten und keiner sog. Bagatelldaten bzw. „weicher“ und „mittlerer“ Daten zulässig.

Erforderliche Angaben von Auskunfteien zur Prüfung der Bonität von Mietern: Unter Beachtung dieser Bewertung sind folgende Angaben für die Prüfung der Bonität von Mietern durch die Erhebung bei einer Auskunft erforderlich und zulässig:

- Daten aus öffentlichen Schuldnerverzeichnissen (eidesstattliche Versicherung, Haftanordnung und Insolvenz),
- rechtskräftige Titel zu Zahlungsverzug im Mietbereich,
- rechtskräftige Urteile zur fristlosen Kündigung eines Mietvertrages wegen Zahlungsverzug oder bei sonstiger Verletzung des Mietvertrages,
- rechtskräftiges Räumungsurteil wegen fristloser Kündigung,

- Daten über sog. Mietnomaden, wenn innerhalb der ersten drei Monate zwei Monatsmieten nicht gezahlt wurden und eine Strafanzeige wegen Betrugs nach § 263 Strafgesetzbuch (StGB) durch den Vermieter erstattet wurde.

Außerdem sind aus den vorgenannten Gründen zur Einhaltung des § 29 BDSG bzgl. der Mieterdatenbank die im Datenkatalog eingeteilten Daten und die Einmeldungen aus anderen Auskunfteien in die Bonitätsdatenbank entsprechend zu markieren und festzulegen, so dass nur sog. harte Daten in die Mieterdatenbank aufzunehmen sind.

Datenübermittlung an Dritte: Soweit anfragende Vermieter die in der Mieterdatenbank enthaltenen Angaben nicht für ausreichend halten, greifen sie auf die Bonitätsdatenbank der Mieterauskunftei zu. Dadurch erhalten sie neben den Angaben über Mietvertragsverstöße und den „harten“ alle über den Mietinteressenten gespeicherten sonstigen „weichen“ und „mittleren“ Daten; und zwar branchenübergreifend. Umgekehrt können Kunden, die keine Vermieter sind, auch auf die Mieterdatenbank zugreifen.

Infolge des Zugriffs auf beide Datenbanken durch die Vermieter und die übrigen Kunden erfolgt keine notwendige Trennung und Markierung der Datensätze für die Bonitätsprüfung von Mietinteressenten und für die Bonitätsprüfung außerhalb von Mietvertragsverhältnissen. Die Vermieter dürfen für den Abschluss von Mietverträgen nur Zugriff auf die hierfür benötigten Daten haben, die in der Vermieterdatenbank gespeichert sind. Die übrigen Kunden dürfen nur auf die Bonitätsdatenbank zugreifen.

Es bedarf daher einer klaren technischen und organisatorischen Trennung der Mieterdatenbank von der allgemeinen Bonitätsdatenbank, einschließlich der daraus folgenden Sperrung des jeweils unzulässigen Zugriffs auf die andere Datenbank. Zur Gewährleistung dieser Trennung sind die erforderlichen Maßnahmen nach § 9 BDSG zu treffen.

Gewährleistung der Betroffenenrechte: Bei der erstmaligen Übermittlung wird der Betroffene von der Mieterauskunftei in einem Formschreiben darüber unterrichtet, dass an einen Vermieter mit einem berechtigten Interesse Daten zu seiner Person übermittelt wurden, weil er im Begriff ist, mit ihm ggf. einen Mietvertrag abzuschließen. Über den Datensatz kann sich der Betroffene bei der Mieterauskunftei informieren.

Das verwendete Formschreiben entsprach nicht den Anforderungen des § 33 Abs. 1 Satz 2 BDSG. Eine Anpassung des Schreibens war insbesondere im Hinblick auf die Art der übermittelten Daten erforderlich.

Es besteht die Möglichkeit, Selbstauskünfte einzuholen. Diese enthalten alle über den Betroffenen gespeicherten Daten. Im Hinblick auf die Berichtigung unrichtiger Daten wurden die Betroffenen bislang an die Auskunftei verwiesen, bei der die Daten erhoben wurden. Zur Sperrung von Daten teilte die Mieterauskunftei mit, die Daten würden - so sie bestritten worden sind - bis zu einer Klärung nicht mehr übermittelt.

Die Mieterauskunftei wurde darauf hingewiesen, dass der Berichtigungsanspruch nach § 35 BDSG in vollem Umfang auch ihr gegenüber besteht und demzufolge der Geltendmachung derartiger Ansprüche zu entsprechen ist.

19.3.4 Änderung des Bundesdatenschutzgesetzes (BDSG) – Auskunfteien und Scoring

Der Handel mit bonitätsgeprüften Informationen hat sich zu einem lukrativen Markt entwickelt, da detaillierte Informationen zur wirtschaftlichen Situation einzelner Personen wertvoll sind. Während zunächst nur Waren und Kredite vergebende Unternehmen an diesen bei Auskunfteien gespeicherten Daten interessiert waren, hat sich dieser Kreis mittlerweile erheblich ausgeweitet. Vor allem auf Dienstleistungsunternehmen jedweder Art, teilweise sogar unabhängig davon, ob sie bei einem konkreten Geschäft ein wirtschaftliches Risiko tragen.

Je mehr Abnehmer die Auskunfteien für ihre Daten haben, desto umfangreicher werden ihre eigenen Dateien, da die Abnehmer zugleich Datenlieferanten sind. Die Empfänger von Daten verpflichten sich nämlich, Daten über den Geschäftsverlauf oder über Unregelmäßigkeiten beim Geschäftsverlauf den Auskunfteien mitzuteilen. So besteht seit Jahren der Trend bei Auskunfteien, ihre Geschäftsfelder zur Erhöhung des wirtschaftlichen Ertrags auszuweiten.

Dem Datenschutz wird dabei nicht immer die ausreichende Aufmerksamkeit entgegengebracht, weil die Auskunfteien in keinerlei geschäftlichen oder vertraglichen Beziehungen mit den Betroffenen stehen, deren Daten gespeichert und an Dritte übermittelt werden. Ein wachsendes Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien ermöglicht eine Profilbildung, bei der das Verhalten eines bestimmten Menschen ohne dessen Wissen und Wollen abgebildet wird und ihn so für Dritte berechenbar macht.

Angesichts dieser Tendenzen sind die sehr allgemein gehaltenen gesetzlichen Regelungen zum Datenschutz der Bürgerinnen und Bürger im Auskunfteienbereich nicht mehr ausreichend und daher ergänzungsbedürftig. Aus der Praxis der Datenschutzaufsichtsbehörden heraus haben sich Überlegungen ergeben, Regelungen zur Datenverarbeitung zu präzisieren und deren Transparenz für die Betroffenen zu verbessern.

Folgende Grundsätze sind bei Auskunftssystemen zu beachten:

- Verbot der Mitteilung über die Tatsache einer Datensperre an Dritte,
- Wegfall der Einschränkung des Auskunftsrechts unter allgemeinem Verweis auf das Geschäftsgeheimnis,
- Möglichkeit zur Selbstauskunft einmal im Jahr kostenfrei,
- Unterrichtung des Betroffenen vor einer Einmeldung durch die einmeldende Stelle zur Wahrung seiner Rechte auf u. a. Berichtigung und Sperrung seiner Daten,

- Erweiterung der Benachrichtigungspflicht auf Art und Herkunft der Daten gegenüber dem Betroffenen, die bei Dritten nur für Zwecke der Beauskunftung erhoben und hierfür kurzfristig bei der Auskunftsperson gespeichert werden,
- Benachrichtigung auch durch Auskunftspersonen bereits bei der erstmaligen Speicherung von Daten zum Betroffenen und nicht erst bei der erstmaligen Übermittlung,
- klare Anforderungen für ein ausreichendes Bestreiten der Richtigkeit der gespeicherten Daten durch den Betroffenen,
- Verkürzung der Lösungsfrist auf drei Jahre,
- Erweiterung des Bußgeldtatbestandskatalogs auf Verstöße gegen die Vorschriften zum Auskunftsrecht.

Darüber hinaus sind besondere Regelungen für branchenspezifische Auskunftssysteme erforderlich, hier insbesondere die Trennung und Beschränkung auf vertragsrelevante Daten bei Speicherung und Auskunftserteilung.

Beim Scoring, unabhängig davon, ob dies von einer Auskunftsperson oder von einem Unternehmen selbst durchgeführt wird, sind folgende Grundsätze zu beachten:

- klare Transparenz des Scorings für den Betroffenen durch entsprechende Unterrichtung durch den Scorewertschaffenden und den Scorewertverwendenden,
- Offenlegung der Merkmale und deren Gewichtung,
- Scoringverbot für vertragserfüllungsfremde Daten wie z. B. Wohnumfeld, ethnische Herkunft,
- Nutzbarkeit nur von vertragsrelevanten Daten für das Scoring.

Inzwischen hat das Bundesministerium des Innern (BMI) hierzu einen Entwurf zur Änderung der Regelungen des BDSG vorgelegt. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben sich mit dem Gesetzentwurf des BMI befasst, (vgl. Ziff. 22.7 und Ziff. 21.8 dieses Berichts). Ich habe die Senatorin für Finanzen und den Senator für Justiz und Verfassung darüber unterrichtet mit der Bitte, sich bei den Beratungen auf Bundesebene für eine Unterstützung der Forderungen einzusetzen.

19.3.5 Bericht über sonstige Themen aus der Arbeitsgruppe Auskunftspersonen

Von hervorgehobener Bedeutung in den Beratungen der AG Auskunftspersonen der Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich waren insbesondere die datenschutzgerechtere Gestaltung der SCHUFA-Klausel und des SCHUFA-Merkblatts des Zentralen Kreditausschusses (ZKA), die Einhaltung datenschutzrechtlicher Anforderungen beim Abschluss von Verträgen mit Wohnungsunternehmen durch die SCHUFA und andere Auskunftspersonen sowie die Nutzung von Daten aus dem Inkassobereich für die Auskunftserteilung. Wie unter Ziff. 19.3.3 berichtet, bestand besonderer Erörterungsbedarf auch im Hinblick auf die beabsichtigte Änderung des Bundesdatenschutzgesetzes.

Außerdem wurden u. a. die Themen rechtliche Fragen der SCHUFA-Selbstauskunft, die Verwendung des Merkmals Versandhandelskonto im SCHUFA-Verfahren, das neue Konzept der SCHUFA bei nachträglichem Bestreiten von Forderungen, die Einwilligung bei der Übermittlung des SCHUFA-Scorewertes an B-Vertragspartner, die Speicherung von Voranschriften durch die SCHUFA, die Einbeziehung gespeicherter Merkmale in die SCHUFA-Scorewertberechnung sowie Datenschutz bei Detekteien näher beraten.

19.4 Bericht aus der Arbeitsgruppe Versicherungswirtschaft

Aus der Arbeit der AG Versicherungswirtschaft der Konferenz der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich sind zwei Themen herauszugreifen, die im Berichtsjahr intensiv behandelt wurden.

Seit geraumer Zeit verhandelt die AG Versicherungswirtschaft mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) über die Formulierung wirksamer Einwilligungs- und Schweigepflichtentbindungserklärungen für Versicherungsverträge. Die Verhandlungen über eine konsensfähige Schweigepflichtentbindungserklärung sind bereits weit fortgeschritten und können ggf. in Kürze zum Abschluss gebracht werden.

Weiterhin Schwerpunkt der Beratungen ist das Hinweis- und Informationssystem (HIS) des GDV. Dabei handelt es sich um eine Warndatei, in die Versicherungen Versicherte und Dritte (ggf. Unfallbeteiligte) nach einem Punktesystem einmelden, um Auffälligkeiten, die Hinweise auf Versicherungsbetrug begründen können, bei Haftungsfällen und Anträgen auf Vertragsabschluss abzurufen. Es zeichnen sich dabei Lösungen ab, die die Tätigkeit der Versicherungen klarer strukturiert und zugleich dabei entlastet. Der aktuelle Entwurf des GDV für eine Einwilligungserklärung kann zum jetzigen Zeitpunkt jedoch noch keine Zustimmung der AG Versicherungswirtschaft finden.

19.5 Ausstellung von Energieausweisen nach der Energieeinsparverordnung

Ende Juli 2007 ist die Energiesparverordnung (EnEV) in Kraft getreten. Unter den dort genannten Voraussetzungen sind Eigentümer von Wohnungen oder Häusern verpflichtet, einen Energiepass zu erstellen. Die Verordnung eröffnet dabei zwei Möglichkeiten: Die Erstellung eines bedarfsorientierten oder die Erstellung eines verbrauchsorientierten Energiepasses. Beim bedarfsorientierten Energiepass werden bestimmte objektive bauliche Gegebenheiten festgestellt. Anders ist es bei der Erstellung eines verbrauchsorientierten Energiepasses. Hier wird der konkrete Verbrauch der letzten drei Jahre der jeweiligen Wohneinheit zur Erstellung des Energiepasses herangezogen.

Vermieterorganisationen, Energieversorgungsunternehmen, Hausverwalter, Eigentümer wie auch Mieter wandten sich an mich und wollten wissen, inwieweit bei der Ausstellung eines verbrauchsabhängigen Energieausweises bei Etagenheizungen die Verbrauchsdaten der Mieter beim jeweiligen Energieversorger dort von dem Vermieter oder von dem Aussteller des Passes abgerufen bzw. vom Energieunternehmen übermittelt werden dürfen. Da weder die EnEV noch das zugrunde liegende Energieeinsparungsgesetz (EnEG) Datenverarbeitungsregelungen für die Erstellung eines

Energiepasses enthalten, kommen die allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Anwendung. Es ist sicherlich unstrittig, dass ein berechtigtes Interesse des Eigentümers bzw. des Vermieters an den Verbrauchsdaten besteht, es ist aber nicht ausgeschlossen, dass schutzwürdige Belange der Mieter dabei beeinträchtigt sein können. Auch darf nicht passieren, dass ohne Kenntnis der Mieter Daten zwischen Energieunternehmen und Dritten über das Verbrauchsverhalten der einzelnen Mietparteien ausgetauscht werden. Es gibt daher zwei Möglichkeiten, an die verbrauchsorientierten Daten zu gelangen:

Entweder der Mieter gibt seine Verbrauchsdaten unmittelbar an den Vermieter oder den von ihm beauftragten Gutachter oder aber er erklärt in einer schriftlichen Einwilligung, dass der Vermieter oder der Gutachter berechtigt sind, die für die Erstellung des Energiepasses erforderlichen Daten beim Energieunternehmen direkt abzufragen. Ist der Mieter nicht bereit, seine Daten für die Erstellung eines Energiepasses preiszugeben, verbleibt dem Vermieter oder Eigentümer nur die Möglichkeit, mit den ihm bekannten baulichen Daten einen bedarfsorientierten Energiepass ausstellen zu lassen.

19.6 Verarbeitung personenbezogener Daten bei der Bestellung von Fotos

Im Januar 2007 wandte sich ein Petent an mich und berichtete, dass bei dem geräteunterstützten Erstellen von Foto-CDs im Einzelhandel, um anschließend Abzüge anfertigen zu lassen, ohne dass der Kunde darauf hingewiesen wird, alle Daten von dem Speichermedium, z. B. einem USB-Stick, heruntergeladen und auf die Foto-CD gespeichert werden. Der Petent beklagte, dass dadurch nicht nur alle Fotos, unabhängig davon, ob nur Abzüge gewünscht werden, sondern auch alle weiteren, unter Umständen sehr sensiblen Daten des Speichermediums in die Hände der Mitarbeiter des Einzelhandelsgeschäfts und des von ihm beauftragten Entwicklungsbüros gelangen.

Ich habe mich im Februar 2007 hiervon bei einem in Bremen ansässigen Fotogeschäft überzeugt und mich anschließend an die Geschäftsführung des Unternehmens gewandt und datenschutzgerechte Verbesserungen vorgeschlagen. Das Unternehmen hat meine Auffassung aufgegriffen und war bereit, auf den Geräten die Kunden über das vollständige Auslesen hinzuweisen. Die Verpflichtung zu einer sofortigen technischen Umstellung aller Geräte hätte aber einen Wettbewerbsnachteil bedeutet, sofern nicht andere Unternehmen in anderen Bundesländern dieselbe Transparenz herstellen, denn die Geräte von einem Hersteller in Niedersachsen werden bundesweit 10.000- bis 20.000-fach im ganzen Einzelhandel eingesetzt.

Daraufhin habe ich die Aufsichtsbehörden für den Datenschutz der anderen Bundesländer informiert mit dem Ziel, eine bundesweit einheitliche Vorgehensweise abzustimmen. Zugleich habe ich den Landesbeauftragten für Datenschutz in Niedersachsen gebeten, bei dem Hersteller die Möglichkeit einer technischen Änderung anzusprechen, bei der nur die tatsächlich für die Bestellung ausgewählten Bilder auf die CD gespeichert werden.

Der Hersteller teilte mit, dass die Geräte durch eine neue Programmversion seit Mitte Februar 2007 grundsätzlich nur noch Foto- und Videodateien kopieren und zudem die Wahl zwischen Archiv-CD (alle Bilder und Videos) und Transfer-CD (nur die für die Abzugsbestellung erforderlichen Dateien) überlässt. Damit ist mittelfristig bundesweit eine datenschutzgerechte Umstellung der Geräte in Sicht.

19.7 Teilnahme an einem Gewinnspiel der Post

Viele Bewohner und Autofahrer in Bremen wurden von der Deutschen Post per Prospekt aufgefordert, an einem Gewinnspiel teilzunehmen. Es winkten 500 Kraftstoff-Gutscheine im Werte von je 50,- € Dabei wurde neben verschiedenen Fragen rund um das Auto und über den Haushalt auch nach der beruflichen Tätigkeit und dem Netto-Einkommen der Haushalte gefragt.

Ich habe auf Anfrage öffentlich davor gewarnt, der Post leichtfertig und ungeprüft eine Vielzahl von Daten aus dem persönlichen Lebensbereich preiszugeben, zumal die weitere Nutzung der Daten durch die Post nur sehr unbestimmt beschrieben war. Für die Teilnehmer war nicht einzuschätzen, an wen die Post die Daten übermitteln würde, mit welchen anderen Daten diese verknüpft und wie die Empfänger die Daten weiter verarbeiten oder nutzen würden. Auch bestanden Bedenken, ob die Einwilligungserklärung ausreichend war, die die Post berechnete, die persönlichen Daten an unbekannte Stellen zu übermitteln. Zur Prüfung dieser Frage habe ich die zuständige Datenschutzaufsichtsbehörde, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), eingeschaltet. Dieser hat gegenüber der Deutschen Post AG einige grundsätzliche Datenschutzverbesserungen durchgesetzt, die in Zukunft bei entsprechenden Aktionen beachtet werden sollen.

19.8 Arbeitnehmerdatenschutz

19.8.1 Prüfung der Beschäftigtendatenverarbeitung im Bewerbungsverfahren

In einem Betrieb mit mehreren 100 Beschäftigten prüfte ich schwerpunktmäßig die Datenerhebung im Bewerbungsverfahren. Hierbei ging es im Wesentlichen darum, ob und ggf. welche Gesundheitsdaten (Drogentest, ärztliche Untersuchung DNA-Analyse und Schwerbehinderung) erhoben werden, ob nach einer Schwangerschaft gefragt wird, ob psychologische Testverfahren oder ein graphologischer Test durchgeführt wird, ob Daten beim bisherigen Arbeitgeber und Angaben über die finanzielle Situation (Schulden, Lohn- und Gehaltspfändung), Angaben zur Gewerkschaftszugehörigkeit und über einen strafrechtlichen Hintergrund (polizeiliches Führungszeugnis, Vorstrafen, staatsanwaltschaftliches Ermittlungsverfahren) erhoben werden.

Im Rahmen eines Prüftermins wurde festgestellt, dass hinsichtlich der Gesundheitsdaten nur eine ärztliche Untersuchung nach dem Jugendarbeitsschutzgesetz durch den Betriebsarzt durchgeführt bzw. die Vorlage eines entsprechenden Nachweises verlangt wird. Weitere der vorgenannten Gesundheitsdaten und der übrigen Daten werden nicht erhoben. Auch eine Datenerhebung bei früheren Arbeitgebern wurde verneint.

Der zur Vorbereitung der Einstellung verwendete Personalfragebogen enthielt u. a. Felder zur Staatsangehörigkeit, zum Familienstand, Angaben zum Ehepartner (vollständiger Name, Geburtsname und -datum und Konfession), zu den Kindern den Vornamen und das Geburtsdatum) sowie im Zusammenhang mit einer Schwerbehinderung die Angaben „Kriegsschaden“ oder „Arbeitsunfall“, deren Berechtigung ich näher untersuchte.

Die Erforderlichkeit der Angaben und Rechtsgrundlagen zur Konfession und zum Familienstand sowie die Felder „Kriegsschaden“ oder „Arbeitsunfall“ konnten nicht dargelegt werden, so dass die entsprechenden Felder auf dem überarbeiteten Personalfragebogen nicht mehr vorhanden sind. Die Angaben zum Ehepartner und den Kindern werden für die Pensionskasse des Unternehmens benötigt. Das Unternehmen wird auf meine Anregung hin in dem überarbeiteten Personalfragebogen zu diesen Angaben darauf hinweisen, dass sie freiwillig sind und für welchen Zweck sie benötigt werden.

Insgesamt habe ich bei der Prüfung einen guten Eindruck gewonnen, es wurden nicht in großem Umfang Daten der Bewerber mit fraglicher Eignung erhoben, sondern im Mittelpunkt der Entscheidung stand der unmittelbare Eindruck, den die Bewerberinnen und Bewerber hinterließen.

19.8.2 Ortungssystem in Firmenfahrzeugen

Beschäftigte eines Bauunternehmens haben mich darüber unterrichtet, in den Fahrzeugen ihres Arbeitgebers seien Ortungssysteme eingebaut worden, mit denen er die Beschäftigten während der Arbeitszeit und der Pausen kontrollieren könne. Es bestünden Unsicherheiten darüber, was und ggf. in welchem Ausmaß der Arbeitgeber kontrollieren dürfe. Auf Anfrage hat der Arbeitgeber dargelegt, das eingesetzte GPS-System werde zur elektronischen Arbeitszeiterfassung, zur Disposition und zum Aufspüren von gestohlenen Fahrzeugen/Geräten eingesetzt und es handele sich dabei nicht um automatisierte Datenverarbeitung. In diesem Zusammenhang hat mir die Firma, von dem das Unternehmen das System erworben hat, Informationen (Broschüre, Muster einer Betriebsvereinbarung etc.) über das System zugesandt. Es ermöglicht in vielfältiger Weise eine Überwachung der Beschäftigten.

Ich habe dem Unternehmen mitgeteilt, dass dort ein Verfahren eingesetzt wird, mit dem Daten automatisiert verarbeitet werden, die regelmäßig auf einzelne Fahrer bzw. Beschäftigte des Unternehmens bezogen werden können. Da dieses Verfahren u. a. ein Bewegungsprofil der Fahrer ermöglicht, weist dieses DV-System besondere Risiken für die Rechte der betroffenen Fahrer auf. Deshalb unterliegt das Verfahren einer Prüfung, die vor Beginn der Verarbeitung (Vorabkontrolle) nach § 4 d Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG), vom Beauftragten für den Datenschutz hätte vorgenommen werden müssen (§ 4 d Abs. 6 BDSG).

Dazu gehört insbesondere unter Abwägung mit den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Interessen der betroffenen Fahrer entsprechend § 28 Abs. 1 Nr. 2 BDSG konkret festzulegen, welche Auswertungen vorgenommen werden. Dass es dabei bleibt, ist durch technische und organisatorische Maßnahmen nach § 9 BDSG zu gewährleisten, und die Beschäftigten sind nach § 33 BDSG über Inhalt und Umfang der Datenverarbeitung und der Datenspeicherung zu benachrichtigen. Ich habe das Unternehmen aufgefordert, dies entsprechend nachzuholen. Soweit ein Betriebsrat in solchen Unternehmen vorhanden ist, empfiehlt sich der Abschluss einer entsprechenden Betriebsvereinbarung.

19.8.3 Übermittlung von Beschäftigtendaten eines Sicherheitsdienstes

Der Betriebsrat eines Sicherheitsdienstes hat mich gefragt, ob und ggf. in welchem Umfang der Arbeitgeber Daten aus der Personalakte seiner Beschäftigten an einen Auftraggeber übermitteln darf und ob dies auch ohne die Zustimmung der Beschäftigten geschehen dürfe. Geplant war die Bereithaltung der Personalakte zur Einsichtnahme durch den Auftraggeber.

Es war zu prüfen, ob die Voraussetzungen des § 28 Abs. 3 Nr. 1 BDSG vorliegen. Danach dürfen personenbezogene Daten übermittelt werden, soweit sie zur Wahrung berechtigter Interessen eines Dritten (hier: Auftraggeber) erforderlich sind und kein Grund zu der Annahme besteht, dass der Betroffene (hier: Beschäftigte) ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Grundsätzlich besteht für den Auftraggeber das berechtigte Interesse, sich ein Bild von den Beschäftigten des Sicherheitsdienstes zu machen, die für den Schutz oder die Sicherung eines bestimmten Objektes eingesetzt werden sollen. Hierbei ist der Grundsatz der Erforderlichkeit zu beachten. Keine Bedenken bestehen, wenn die Namen der Beschäftigten und ggf. - bezogen auf das zu schützende oder sichernde Objekt – Daten über dessen Qualifikation übermittelt werden, soweit diese für den Einsatz vorausgesetzt werden. Angaben zur privaten Adresse oder Telefonnummer wären nur dann erforderlich, soweit die Beschäftigten regelmäßig, kurzfristig sowie außerhalb der regulären Geschäftszeiten erreichbar sein müssen. Die Funktion eines Beschäftigten darf allenfalls im Zusammenhang mit dem zu schützenden oder zu sichernden Objekt im erforderlichen Umfang mitgeteilt werden, z. B. bei Einsatz eines Teams dessen Leiter bzw. Vertreter.

Regelmäßig nicht erforderlich sind Angaben über Funktionen im Rahmen der Personalvertretung o. a., da diese nicht in einem unmittelbaren Zusammenhang mit dem zu schützenden oder zu sichernden Objekt stehen. Das Gleiche gilt für Angaben zum Geburtsdatum, zur Betriebszugehörigkeit und für evtl. regelmäßig einzuholende polizeiliche Führungszeugnisse oder Auskünfte von Auskunfteien, z. B. der SCHUFA. Hier dürfte es ausreichen, wenn der Sicherheitsdienst sich verpflichtet, nur Beschäftigte entsprechend einzusetzen, wenn die jeweiligen vertraglich festzulegenden Anforderungen erfüllt sind. Insoweit trägt der Sicherheitsdienst die Verantwortung, dass diese Verpflichtungen eingehalten werden. In diesem Sinne hat sich der anfragende Betriebsrat des Unternehmens eingesetzt.

19.9 Einsatz von Videoüberwachung

Im Berichtsjahr erreichte mich wiederum eine Vielzahl von Anfragen, die sich gegen eine Überwachung durch Videokameras wandten. Einige Beispiele sind nachstehend aufgeführt.

In einer Modeboutique: Aufgrund von Hinweisen Betroffener habe ich mir die Videoüberwachung in einem Modegeschäft in der Bremer Innenstadt vorführen lassen und bei der Einsichtnahme in die Bilddaten auf dem Monitor Folgendes festgestellt:

Ich prüfte die Überwachung der Beschäftigten. Neben dem Verkaufsraum wird auch der Bereich an der Kasse videoüberwacht. In diesem Bereich hält sich regelmäßig zumindest ein Mitarbeiter bzw. eine Mitarbeiterin auf, so dass diese Person einer ständigen Videoüberwachung und damit einem lückenlosen Überwachungsdruck ausgesetzt ist. Sie kann nämlich nicht einschätzen, ob und ggf. wann von wem und zu welchen Zwecken eine Einsichtnahme in die Bilddaten erfolgt. Insoweit überwiegen die schutzwürdigen Interessen des Beschäftigten, so dass die Voraussetzungen des

§ 6 b BDSG nicht erfüllt sind. Ich habe den Inhaber daher gebeten, die Videoüberwachung im Kassenbereich unverzüglich einzustellen und die damit bisher aufgenommenen Bilddaten zu löschen.

Ich prüfte die Hinweise auf die Videoüberwachung. Außer einem Hinweisschild mit einem Video-Logo an der Eingangstür des Verkaufsgeschäfts, das ich erst nach längerem Hinsehen und auf den Hinweis einer Mitarbeiterin erkennen konnte, gab es im Verkaufsbereich selbst keine weiteren Hinweise auf den Umstand der Videoüberwachung, obwohl § 6 b Abs. 2 BDSG vorschreibt, dass der Umstand und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Ich habe verlangt, durch deutliche Hinweisschilder auf die Videoüberwachung aufmerksam zu machen.

Ich prüfte die Dauer der Aufzeichnung der Bilddaten und Einsichtnahme. Unklar war, wie lange die Bilddaten aufgezeichnet werden. Zwar ist von der anwesenden Mitarbeiterin erklärt worden, die Aufnahmen würden elf Tage aufbewahrt werden, Unterlagen oder sonstige Dokumentationen standen jedenfalls nicht zur Verfügung. Da die Videoüberwachung im Wesentlichen der Abwehr von Diebstählen dienen soll, habe ich verlangt, die Aufzeichnungen entsprechend § 6 b Abs. 5 Bundesdatenschutzgesetz (BDSG) unverzüglich nach Erreichen des Zwecks durch eine automatische Einstellung zu löschen, regelmäßig spätestens nach drei Tagen.

Ich prüfte die Verfahrensbeschreibung. Auch war nicht festzustellen, ob und ggf. wer unter welchen Voraussetzungen Einsicht in die Bilddaten hat bzw. haben darf und ob diese Einsichtnahme auch außerhalb des Verkaufsgeschäftes, z. B. über eine externe Verbindung o. ä., möglich ist. Es wurde lediglich auf die Firma verwiesen, die die Anlage installiert hat. Eine Einweisung sei zwar beabsichtigt gewesen, bisher jedoch nicht erfolgt. Unterlagen darüber lagen ebenfalls nicht vor. Da es sich bei dieser Videoüberwachung um ein Verfahren automatisierter Verarbeitung handelt, ist der Inhaber nach § 4 d Abs. 1 BDSG verpflichtet, eine Verfahrensbeschreibung nach Maßgabe des § 4 e BDSG zu erstellen. Hierin ist auch festzulegen, ob und unter welchen Voraussetzungen eine Einsichtnahme durch wen erfolgt und welche technischen und organisatorischen Maßnahmen nach der Anlage zu § 9 Satz 1 BDSG getroffen werden, um dies zu gewährleisten.

In einer Fahrradstation: Ich bin darüber unterrichtet worden, auf die Videoüberwachung einer Fahrradstation am Bremer Hauptbahnhof würde nicht hingewiesen. Aufgrund meiner Anfrage wurde mir erklärt, es seien nunmehr Hinweise angebracht. Die nur außerhalb der Geschäftszeiten aktivierte Aufzeichnung von Bilddaten würde bis zu zwei Monate aufbewahrt werden.

Ich habe auf § 6 b Abs. 5 Bundesdatenschutzgesetz (BDSG) hingewiesen, wonach Aufzeichnungen unverzüglich zu löschen sind, wenn sie zur Erreichung des Zieles nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Nach allgemeiner Erfahrung werden Einbrüche und Diebstähle regelmäßig am nächsten Arbeitstag zu Beginn der Geschäftszeiten festgestellt. In diesen Fällen dürfen die Aufnahmen zur Verfolgung straf- und zivilrechtlicher Ansprüche eingesehen und ausgewertet werden. Hierbei besteht regelmäßig die technische Möglichkeit, die entsprechende Sequenz auszuschneiden und separat für die genannten Zwecke zu verwenden. Die übrigen Aufnahmen sind dann unverzüglich zu löschen.

Ich habe daher gebeten, für die Aufzeichnung eine Lösungsfrist von 24 Stunden technisch und organisatorisch zu gewährleisten. Nur in dem Fall, dass die Radstation am Wochenende oder an

Feiertagen geschlossen ist, wäre eine Lösungsfrist von bis zu drei Tagen angemessen. Weiter habe ich eine Verfahrensbeschreibung nach § 4 e i. V. m. § 6 b BDSG gefordert. Dies wurde zugesichert.

19.10 Ordnungswidrigkeitsverfahren

Bei der Durchführung von Ordnungswidrigkeitsverfahren wird nur gelegentlich eine richterliche Entscheidung erforderlich. Es ist daher kein Wunder, dass in solchen Fällen die mit dem Verfahren betrauten Richterinnen und Richter, aber auch Staatsanwältinnen und Staatsanwälte mit der datenschutzrechtlichen Materie nur wenig vertraut sind. Häufig sind die Genannten auf Massenverfahren wie Verkehrsordnungswidrigkeiten spezialisiert, so dass das Verständnis für datenschutzrechtliche, insbesondere aber für datenschutztechnische Fallkonstellationen nur eingeschränkt vorhanden ist.

Um die Gerichte und Staatsanwaltschaften bei der Bearbeitung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz besser unterstützen zu können, haben sich die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich im Berichtsjahr nun darauf verständigt, eine gemeinsame Urteilssammlung aufzubauen, in die von ihnen alle erfolgreich abgeschlossenen Ordnungswidrigkeitsverfahren eingemeldet werden. Die vom Hamburgischen Datenschutzbeauftragten geführte Sammlung ist außerdem geeignet, eine vergleichbare Behandlung von Ordnungswidrigkeitstatbeständen über die Ländergrenzen hinweg zu ermöglichen und Ordnungswidrigkeitsverfahren gezielter einzusetzen.

Im Berichtsjahr erließ ich nur einen Bußgeldbescheid wegen der Nichterteilung von Auskünften gegen den Geschäftsführer eines Unternehmens. Trotz mehrfacher Aufforderung und Fristsetzung, mir die erforderlichen Auskünfte zu der von ihm betriebenen Videoüberwachung zukommen zu lassen, bekam ich diese von dem betreffenden Unternehmen nicht. Letztendlich hat der Beschuldigte das gegen ihn verhängte Bußgeld bezahlt.