1. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 5. Dezember 2011 bis 31. Dezember 2013
Zitiervorschlag: 1. TB LfDI Thüringen

Der 1. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Mai 2014

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

B Nicht-öffentlicher Bereich

B Nichtöffentlicher Bereich

Vorwort

Dr. Lutz Hasse

Mit Inkrafttreten der Novellierung des Thüringer Datenschutzgesetzes, also seit dem 9. Dezember 2011, konnte der Thüringer Landesbeauftragte für den Datenschutz gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz die Funktion der Aufsichtsbehörde nach § 38 Abs. 6 Bundesdatenschutzgesetz im nicht-öffentlichen Bereich wahrnehmen. Bereits am 9. März 2010 hatte der Europäische Gerichtshof (EuGH, Rechtssache C-518/07) Artikel 28 Abs. 1 der Europäischen Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. I. 281 S. 31 bis 50)) dahingehend ausgelegt, dass die Datenschutzaufsicht in völliger Unabhängigkeit wahrgenommen werden müsse. Eine solche Unabhängigkeit schließe jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, aus, durch die die Aufgabenerfüllung der Datenschutzaufsicht in Frage gestellt werden könnte. Der EuGH attestierte insoweit, dass die staatliche Aufsicht, der die für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Kontrollstellen in Deutschland unterworfen waren bzw. sind, *nicht* mit dem Unabhängigkeitserfordernis vereinbar sei. Damit gab der Europäische Gerichtshof vor, dass die datenschutzrechtliche Aufsicht vom Thüringer Landesverwaltungsamt auf den Thüringer Landesbeauftragten für den Datenschutz zu übertragen war. Der besondere Reiz dieser neuen Aufgabe liegt darin, „ein Feld zu beackern“, das in den zurückliegenden 20 Jahren vom Thüringer Landesverwaltungsamt nur mit 0,85 so

genannten Vollbeschäftigungseinheiten bestellt werden konnte. Um diese „Brache“ in eine „blühende Landschaft“ zu verwandeln, bedarf es besonderer Anstrengungen. Die Fallzahlen im nicht-öffentlichen Bereich haben sich von 2011 zu 2013 vervielfacht, insbesondere die Zahl der Ordnungswidrigkeitenverfahren ist derart stark angestiegen, dass trotz guten Arbeitsklimas und hoch motivierter Arbeitnehmer die Behörde des TLfDI deutlich an ihre Kapazitätsgrenzen stößt. Geplant ist daher die Einrichtung eines vierten Referates „Datenschutz im nicht-öffentlichen Bereich“. Denn gerade in diesem Bereich werden sowohl Verwaltungs- als auch Ordnungswidrigkeitenverfahren geführt, die rechtlich in aller Regel hohe Anforderungen stellen; bei ca. 80 % der Verfahren ist auf Seiten der datenschutzrechtlich verantwortlichen Stelle (Unternehmen) eine anwaltliche Beteiligung zu verzeichnen. Dies ist auch naheliegend, verfolgen doch die nicht-öffentlichen Stellen in der Regel wirtschaftliche Interessen und können bzw. wollen Bußgelder oder Zwangsgelder nicht widerstandslos hinnehmen. Verfahren im nicht-öffentlichen Bereich sind mithin sehr viel aufwendiger als Verfahren im öffentlichen Bereich. Der Prozentsatz der Bescheide des TLfDI, die mit einem Rechtsbehelf angegriffen werden, ist hoch. Gleichwohl wurden sämtliche Verfahren bisher erfolgreich geführt. Hinzu kommt, dass parallel zum vermehrten Arbeitsanfall in den Rechtsreferaten auch das Technik-Referat in verstärktem Maße gefordert ist – etwa bei Kontrollen oder Stellungnahmen gerade auch im nicht-öffentlichen Bereich. Waren beim Datenschutzbeauftragten im Jahr 2012 noch 449 Vorgänge zu bearbeiten, waren es im Jahr 2013 bereits 810. In den nächsten Jahren wird diese Zahl weiterhin ansteigen. Der TLfDI hofft mit Blick auf die Gewährung neuer Personalstellen auf die weitere konstruktive Unterstützung durch die Landtagsfraktionen, die Landtagspräsidentin und den Personalrat der Thüringer Landtagsverwaltung.

Auf der Grundlage des 2012 gefassten Beschlusses des Beirates beim TLfDI erfasst der Tätigkeitsbericht zum nicht-öffentlichen Bereich zusätzlich den Monat Dezember des Jahres 2011.

Der TLfDI hat in seiner Funktion als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich die Befugnis, verantwortliche Stellen in seinem Zuständigkeitsbereich anlasslos zu kontrollieren, § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG). Um diese Kontrolle wirksam durchführen zu können, hat der Gesetzgeber dem TLfDI und seinen Mitarbeitern eine Reihe an Werkzeugen an die

Hand gegeben. So darf der TLfDI von Unternehmen umfassende Auskunft verlangen und die einzelnen Betriebe vor Ort kontrollieren. Dabei hat er Zutritt zu allen Geschäftsräumen und das Recht, in alle Unterlagen Einsicht zu nehmen, § 38 Abs. 4 Satz 1 BDSG. Während den meisten vom TLfDI durchgeführten Kontrollen ein bestimmter Anlass, meist ein Hinweis durch einen Bürger, zu Grunde liegt, hat der TLfDI einige anlasslose Kontrollen in Wirtschaftsunternehmen durchgeführt. Dabei wurde sowohl auf die regionale Verteilung als auch darauf geachtet, dass sowohl große als auch kleine Unternehmen kontrolliert wurden. Ein Schwerpunkt wurde hierbei auf Unternehmen aus der Recycling-Branche gelegt. Alle Unternehmen wurden dabei nach dem im Anhang unter Anlage 1 beigefügten Fragenkatalog geprüft. Der Fragenkatalog wird fortlaufend durch den TLfDI unter Berücksichtigung der bei den Kontrollen gewonnenen praktischen Erfahrungen überarbeitet. In den folgenden Beiträgen werden die Ergebnisse der Kontrollen dargelegt. Auf der Internetseite des TLfDI werden fortlaufend weitere Hinweise eingestellt werden.

Als unabhängige Behörde darf der TLfDI die Funktion der Aufsichtsbehörde im nicht-öffentlichen Bereich wahrnehmen. Trotz bester Motivationslage der Arbeitnehmerinnen und Arbeitnehmer des TLfDI sollte die personelle Ausstattung dem Aufgabenzuwachs entsprechen (§ 36 Abs. 5 ThürDSG).
Der TLfDI hat in seiner Funktion als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich die Befugnis, verantwortliche Stellen in seinem Zuständigkeitsbereich aufgrund eines besonderen Anlasses oder auch anlasslos zu kontrollieren. Hierzu hat er Zutritt zu allen Geschäftsräumen und das Recht in alle Unterlagen Einsicht zu nehmen.

1 Schwerpunkte im Berichtszeitraum

Datenschutz
© Coloures Pic – Fotolia.com

Die aufsichtsbehördliche Tätigkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im nicht-öffentlichen Bereich war im Wesentlichen durch drei Schwerpunkte beansprucht:
Den größten Einschnitt stellte die Übernahme der aufsichtsbehördlichen Tätigkeit im nicht-öffentlichen Bereich mit dem Inkrafttreten des Gesetzes zur Änderungen des Thüringer Datenschutzgesetzes (ThürDSG) Ende des Jahres 2011 dar. Bis zu diesem Zeitpunkt war diese Tätigkeit dem Thüringer Landesverwaltungsamt zugeteilt, welches für die datenschutzrechtliche Aufsicht aller Unternehmen in Thüringen 0,8 Vollzeitstellen eingeplant hatte. Die sich aus dieser Unterbesetzung ergebende Vakanz in Sachen datenschutzrechtlicher Aufsichtstätigkeit und den sich daraus entwickelnden Folgen war eine der Herausforderungen, mit denen der TLfDI zu kämpfen hatte und hat. So war „der Datenschutz“ in vielen Thüringer Unternehmen, die der TLfDI seit seiner Aufgabenübernahme kontrollierte, ein unbekanntes Feld, von dem man bestenfalls ungenaue Vorstellungen hatte. Dass das Bundesdatenschutzgesetz für diese Unternehmen seit der Wende Anwendung fand, diese Tatsache aber unbekannt ist, war und ist leider sehr häufig festzustellen.
Aus diesem Grund hat sich der TLfDI nach seiner Amtsübernahme um einen steten und intensiven Austausch zu den in Thüringen vertretenen Industrie- und Handelskammern bemüht. Er legte großen Wert darauf, die Unternehmen in Thüringen in datenschutzrechtlicher Hinsicht auf den richtigen Weg zu bringen. Es wurden unter anderem Informationsveranstaltungen durch den TLfDI initiiert.
Einen weiteren Eckpunkt des Berichtszeitraumes stellt der Aufbau des Ordnungswidrigkeitenverfahrens dar. Auch hier lag bislang die Zuständigkeit beim Thüringer Landesverwaltungsamt. Das Ordnungswidrigkeitenverfahren als besonderes Verwaltungsverfahren

stellte den TLfDI und seine Behörde vor besondere Herausforderungen. Es sind wenige Parallelen zu den bisherigen Verfahrensweisen vorhanden. Vielmehr handelt es sich um ein streng formalisiertes Verfahren mit festem Aufbau. Um auch diese Verfahren von Anfang an erfolgreich zu betreuen, hat der TLfDI einen Juristen angestellt, der primär mit dem Aufbau und der Durchführung dieses Verfahrens betraut ist. Der Aufbau des Verfahrens konnte zwischenzeitlich hinsichtlich der gängigsten Verfahrensformen abgeschlossen werden; die bisherigen Ordnungswidrigkeitenverfahren verliefen erfolgreich.
Schließlich stellt die Videoüberwachung in all ihrer Vielfalt einen weiteren Schwerpunkt aus dem Berichtszeitraum dar. Ständig in Quantität steigend, ständig in technischer Sicht besser und damit auch in der Qualität zunehmend, stellt diese Art der Datenerhebung und in meisten Fällen auch -speicherung eines der größten datenschutzrechtlichen Probleme und damit eine Herausforderung für den TLfDI auch in Zukunft dar. Ein Großteil der Fälle im nicht-öffentlichen Bereich, der zu einer aufsichtsbehördlichen Reaktion führt, steht im Zusammenhang mit Videoüberwachung. In den seltensten Fällen ist die Überwachung zulässig. Ebenso selten ist die Einsicht der Unternehmen, die die Überwachung durchführen.

Die Schwerpunkte im Berichtszeitraum waren der erfolgreiche Start der aufsichtsbehördlichen Kontrolltätigkeit des TLfDI, die Durchführung des oftmals daraus resultierenden Ordnungswidrigkeitenverfahrens in neuer eigener Zuständigkeit sowie die immer stärker zunehmende Videoüberwachung in allen nicht-öffentlichen Bereichen.

2 Düsseldorfer Kreis

Runder Tisch Business
© fotomek – Fotolia.com

Ursprünglich war der Düsseldorfer Kreis das Gremium der obersten Datenschutzaufsichtsbehörden in Deutschland. Nachdem die Datenschutzaufsicht bis auf den Ausnahmefall des Bayrischen Landesamtes für Datenschutzaufsicht auf die Landesdatenschutzbeauftragten übergegangen ist, ist der Düsseldorfer Kreis nunmehr ein Arbeitskreis der Datenschutzkonferenz. Im Düsseldorfer Kreis treffen sich die Datenschutzaufsichtsbehörden, um ihre Aufsichtstätigkeit im nicht-öffentlichen Bereich zu koordinieren. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen hat den Vorsitz. Jede Datenschutzaufsichtsbehörde kann Themen in den Düsseldorfer Kreis einbringen, die nach ihrer Auffassung ein bundeseinheitliches Vorgehen erfordern. Sofern eine Einigkeit erzielt werden kann, fasst der Düsseldorfer Kreis einstimmige Beschlüsse, die veröffentlicht werden. Gegenstand der Beschlüsse ist eine datenschutzrechtliche Bewertung eines bestimmten Sachverhalts aus dem nicht-öffentlichen Bereich, die der Wirtschaft Rechtssicherheit geben sollen. Unternehmen können davon ausgehen, dass die angesprochenen Themen von den Datenschutzaufsichtsbehörden in Deutschland einheitlich behandelt werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) veröffentlicht die Beschlüsse des Düsseldorfer Kreises auf seiner Homepage unter http://www.tlfdi.de/tlfdi/berichte/duesseldorf/. Die im Berichtszeitraum gefassten Beschlüsse des Düsseldorfer Kreises sind im Anhang veröffentlicht.

Der Düsseldorfer Kreis fasst Beschlüsse, in denen eine einheitliche datenschutzrechtliche Bewertung eines bestimmten Sachverhalts aus dem nicht-öffentlichen Bereich bundeseinheitlich festgeschrieben wird.

3 Wirtschaftsunternehmen in Thüringen

Warnschild Videoüberwachung
© bilderzwerg – Fotolia.com

3.1 Gründung des Runden Tisches "Orientierungshilfe Aktenaufbewahrung (OHA)"

Nachdem sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Anschluss an das Immelborn-Aktenlagerungs-Desaster an einem Runden Tisch mit thüringischen Archivierungsdienstleistern einen Überblick über die branchenspezifischen Probleme verschafft hatte, gelang es ihm, „big player“ aus der Branche der Archivierungsdienstleister und von Seiten der betrieblichen Datenschutzbeauftragten an einen Runden Tisch zu bitten, um zu erörtern, wie konzeptionell ein zweiter Fall Immelborn verhindert werden kann. Als Ziel kristallisierte sich zügig heraus, dass es zur Konkretisierung unpräziser gesetzlicher Vorgaben dringend einer „Orientierungshilfe Aktenaufbewahrung (OHA)“ bedarf. Sie soll einerseits Archivierungsdienstleistern, andererseits aber auch Unternehmen, die diese Dienstleister beauftragen wollen, eine Richtschnur an die Hand geben, auf welche Weise die rechtlichen Vorgaben einzuhalten sind und wie sich Auftraggeber (vorab) von der Einhaltung dieser Vorgaben unterrichten können. Die gemeinsam erarbeitete Orientierungshilfe soll sodann mit dem zuständigen Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgestimmt werden, um so die bundesweite Anwendung der Orientierungshilfe zu gewährleisten.
Die Arbeiten an der Orientierungshilfe gestalten sich aufwendig, sodass bis zur „Marktreife“ der Orientierungshilfe noch einige Zeit vergehen wird.
Allen Beteiligten ist jedoch daran gelegen, ein weiteres Datenschutz-Desaster wie in Immelborn (siehe hierzu Punkt 3.7) zu verhindern – das ist aller Mühen wert!

Der Runde Tisch „Orientierungshilfe Aktenaufbewahrung (OHA)“ wird eine Orientierungshilfe entwickeln, die zum einen Archivierungsdienstleister in die Lage versetzen soll, datenschutzrechtlich korrekt zu arbeiten, und zum anderen Unternehmen, die diese Dienstleister beauftragen wollen, dazu befähigen soll, etwa anhand von Checklisten die Archivierungsdienstleister einer qualifizierten Bewertung unterziehen zu können.

3.2 Dialog mit den Handwerkskammern (HWK) – Reanimation notwendig

Während die Kooperation mit den Industrie- und Handelskammern (IHK) etwas an Fahrt aufnimmt, gestaltet sich der Dialog mit den Handwerkskammern (HWK) zäh, bzw. ein Desinteresse der HWKs an einem datenschutzrechtlichen Dialog mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wird deutlich signalisiert. Das ist bedauerlich, da die HWKs auf diese Weise ihren Mitgliedern die Chance nehmen, mit dem TLfDI z. B. an Runden Tischen über Datenschutzthemen aus Sicht der Handwerksbetriebe sowie aus Sicht des Datenschutzbeauftragten zu diskutieren. Es fand unter anderem ein Gesprächstermin in der Handwerkskammer Erfurt statt, bei dem der TLfDI sich vorstellte und anbot, einen Datenschutz-Flyer zu gestalten, der speziell für Handwerksbetriebe datenschutzrechtliche Fragen und Probleme aufgreift. Zur Vorbereitung sollten fünf repräsentative Handwerksbetriebe besucht werden, um sich einen Überblick über die datenschutzrechtliche Situation und die datenschutzrechtlichen Anforderungen in Handwerksbetrieben zu verschaffen. In der Folge wurden ein Autohaus und ein Café besucht. Trotz mehrmaliger Nachfrage des TLfDI fanden sich keine weiteren Handwerksbetriebe, bei denen eine repräsentative Kontrolle durchgeführt werden konnte.
Aufgrund der bisher gemachten Erfahrungen im Bereich der Handwerksbetriebe ist die Erstellung von Informationen für diese Zielgruppe noch nicht möglich gewesen. Gleichwohl wird der TLfDI weiterhin versuchen, die „leblose“ Kommunikation „zu reanimieren“, um datenschutzrechtliche Informationen an die Handwerksbetriebe heranzutragen. Dessen ungeachtet werden die Handwerksbetriebe künftig verstärkten Kontrollen ausgesetzt sein, um auch auf diese Weise den ausgeprägten Datenschutzdefiziten entgegen wirken zu können.

Im Gegensatz zur Kommunikation mit den IHKs gestaltet sich der Dialog zwischen den HWKs und dem TLfDI als noch verbesserungswürdig. Eine Ausblendung des Datenschutzes gehört jedoch der Vergangenheit an. Der TLfDI wird daher weiterhin den Dialog suchen, daneben aber auch andere Wege finden, den Datenschutzgedanken in die Handwerksbetriebe zu tragen.

3.3 Neue Besen ….

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war nach der Amtsübernahme klar, dass bei den Unternehmen in Thüringen in Sachen Datenschutz einiges im Argen liegt, stand doch für diese Aufgabe im Thüringer Landesverwaltungsamt nicht einmal eine Person mit ihrer gesamten Arbeitskraft zur Verfügung (siehe Vorwort). In dem Bewusstsein, dass diese Situation nicht durch die Unternehmen verursacht worden ist, wollte der TLfDI nicht mit „harter Hand“ vorgehen, sondern suchte zunächst Kontakt zu den Wirtschaftsverbänden (siehe hierzu auch Punkt 3.2). Er nahm zu allen drei Industrie- und Handelskammern (IHK) in Thüringen Kontakt auf, und führte mit den Geschäftsführern ein persönliches Gespräch. Hierbei legte er dar, dass er großen Wert darauf legt, die Unternehmen in Thüringen datenschutzrechtlich auf den richtigen Weg zu bringen. Er bot an, über seine Behörde und sein Anliegen z. B. im Rahmen einer Mitgliederversammlung der IHK zu berichten. Zunächst wurde vereinbart, dass der TLfDI in der Mitgliederzeitung der IHK über den Datenschutz im Unternehmen berichtet. Dann war die Teilnahme an einigen Veranstaltungen der IHK zu Informationszwecken vorgesehen. Die Verwirklichung gestaltete sich jedoch sehr unterschiedlich. So war der TLfDI in beiden Berichtsjahren auf dem Ostthüringer Unternehmer- und Gründertag vertreten. Er hielt einen Vortrag zu Chancen und Risiken des Datenschutzes für Unternehmen auf dem Seminar der IHK Ostthüringen zum Thema „Sind Ihre Unternehmensdaten sicher?“ Ebenfalls besuchte der TLfDI eine Veranstaltung der IHK Südthüringen, in der er Unternehmern zunächst in einem Vortrag, dann in einer Gesprächs- und Fragerunde das Thema Datenschutz näherbrachte. Ansonsten erfolgten jedoch keine Einladungen an den TLfDI zu Informationsveranstaltungen. Dies ist etwas bedauerlich, da den Arbeitnehmern des TLfDI bei Vor-Ort-Kontrollen in Unter-

nehmen des Öfteren mitgeteilt wurde, dass es hilfreich gewesen wäre, wenn diese über datenschutzrechtliche Anforderungen vorab informiert gewesen wären.
Mit der IHK Erfurt erarbeitete der TLfDI einen Flyer zum „Datenschutz im Unternehmen“ der unter dem Link:
http://www.tlfdi.de/tlfdi/wir/info/datenschutz_im_unternehmen/
eingesehen werden kann. Ein aufwendiges Unterfangen stellte die Erarbeitung einer Broschüre zu § 28 Bundesdatenschutzgesetz (BDSG) dar. Diese wurde vom TLfDI erstellt, während die IHK Erfurt das Layout und den Druck übernahm. Diese Broschüre ist unter
http://www.tlfdi.de/imperia/md/content/datenschutz/themen/unternehmen/datenschutz_f__r_unternehmen_pdf_19.03.2014.pdf auf der Homepage des TLfDI veröffentlicht. Sie richtet sich an Unternehmerinnen und Unternehmer, um diesen einen verhältnismäßig schnellen Einblick in das Datenschutzrecht zu ermöglichen. Die für Unternehmen wichtige, aber sehr komplizierte Vorschrift des § 28 BDSG wird darin in einzelnen Fallbeispielen aus dem Unternehmeralltag hoffentlich verständlich dargestellt; Rückmeldungen dazu aus der Unternehmerschaft werden fortlaufend eingearbeitet.
Nach diesem ersten Aufschlag hat der TLfDI dann im zweiten Berichtsjahr damit begonnen, Unternehmen in Thüringen auch anlassunabhängig zu kontrollieren. Hierzu wurde die im Anhang unter Anlage 1 beigefügte Frageliste verwendet, mit der alle datenschutzrechtlich relevanten Bereiche im Unternehmen abgefragt werden sollten. Die Ergebnisse dieser Kontrollen sind in den nachfolgenden Tätigkeitsberichtsbeiträgen nachzulesen.

Nach seiner Amtsübernahme nahm der TLfDI zunächst Kontakt mit den IHKs auf, um sein Anliegen zum Datenschutz im Unternehmen bekannt zu machen. Er bot den IHKs Unterstützung in Form von Informationsveranstaltungen und der Veröffentlichung von Beiträgen an; ein wichtiger Schritt ist die Erstellung der Broschüre zu § 28 BDSG.

3.4 ERFA-Kreis

Im Berichtszeitraum nahm der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an vier Sitzungen des Erfahrungsaustausch-Kreises (ERFA-Kreises) teil. Dabei handelt

es sich um eine Zusammenkunft von vornehmlich betrieblichen Datenschutzbeauftragten, mit dem Zweck des gegenseitigen Austausches. Gebildet wurden diese regionalen Kreise durch die Gesellschaft für Datenschutz und Datensicherheit e. V.
Die ERFA-Kreise stehen grundsätzlich allen Interessierten offen, bedürfen jedoch der vorherigen Anmeldung. Eingeladen sind in erster Linie Datenschutzbeauftragte.
Der TLfDI hat bei seinen Besuchen dieser Tagungskreise jeweils unterschiedliche Schwerpunkte seiner Tätigkeit vorgestellt und aktuelle Fragen und Problemstellungen der Teilnehmer geklärt.

Der ERFA-Kreis ist ein gutes Instrument zur Klärung datenschutzrechtlicher Fragen aus dem nicht-öffentlichen Bereich.

3.5 Der TLfDI rät: Widerspruch gegen Werbungsschreiben nach § 28 Abs. 4 BDSG nutzen – sonst ist Werbung einer Schuldnerberatung zulässig

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit wurde darüber informiert, dass eine in Thüringen ansässige Schuldnerberatung Anschreiben versandt hatte, mit denen über das Privatinsolvenzverfahren informiert wurde. Im Raum stand die damit verbundene Frage, wie solche Schreiben datenschutzrechtlich zu bewerten sind und ob die Nutzung personenbezogener Daten für solche Schreiben zulässig ist.
Das von der Schuldnerberatung versandte Anschreiben diente dazu, über die Möglichkeit zu informieren, sich durch ein Privatinsolvenzverfahren zu entschulden. Insofern war das Anschreiben als Werbungsschreiben für die Schuldnerberatung anzusehen.
Die Nutzung personenbezogener Daten für Werbungszwecke ohne schriftliche Einwilligung richtet sich nach § 28 Abs. 3 Bundesdatenschutzgesetz (BDSG). Da sich die Nutzung der personenbezogenen Daten auf den Namen sowie die Anschrift beschränkte, bewegte sich auch das Werbungsschreiben der Schuldnerberatung innerhalb des rechtlich zulässigen Rahmens. Darüber hinaus konnte der betroffenen Person mitgeteilt werden, dass die Schuldnerberatung die für das Werbungsschreiben benötigten personenbezogenen Daten nicht gespeichert hatte.

Möchten Sie Ihren Briefkasten entlasten? Dann machen Sie von Ihrem Widerspruchsrecht Gebrauch:
Zur Abwehr unerwünschter Werbung räumt § 28 Abs. 4 BDSG dem Betroffenen ein uneingeschränktes Widerspruchsrecht gegenüber der verantwortlichen Stelle bezüglich der Verarbeitung und Nutzung seiner Daten zu Zwecken der Werbung oder Markt- und Meinungsforschung ein. Das Widerspruchsrecht besteht unabhängig davon, ob die Werbung ohne oder mit Einwilligung des Betroffenen erfolgt. Ein solcher Widerspruch ist an keine Form gebunden, wonach er telefonisch, konkludent oder auch durch einen Vermerk auf dem Werbungsschreiben „Annahme verweigert“ gegenüber der verantwortlichen Stelle geäußert werden kann.
Für weitere Informationen zum Widerspruch siehe: http://www.bfdi.bund.de/DE/Themen/GrundsaetzlichesZumDatenschutz/BDSGAuslegung/Artikel/Widerspruchsrecht.html?nn=409922.

3.6 Auch wenn Du nicht willst, …ich schreib´ Dir trotzdem – Wann ist die Nutzung personenbezogener Daten zu Werbezwecken unzulässig?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde eines promovierten Universitätsmitarbeiters. Nach seinen Angaben erhielt er von einem Verein in Thüringen unaufgefordert Werbe-Mails, in denen ihm die Möglichkeit der Teilnahme an Veranstaltungen angeboten wurde. Trotz mehrfacher Aufforderung des Beschwerdeführers, dies zu unterlassen, erhielt er weiterhin unerwünschte Nachrichten per E-Mail an seine dienstliche E-Mail-Adresse.
Der TLfDI hat sich daraufhin an den Verein gewandt und um Auskunft zu den zum Beschwerdeführer gespeicherten Daten sowie zu der Herkunft dieser Daten gebeten. Ferner interessierten den TLfDI die Empfänger oder Kategorien von Empfängern, an die diese Daten weitergegeben werden bzw. worden sind, sowie der Zweck der Speicherung dieser Daten (§ 6 Abs. 1 i. v. m. § 34 Abs. 1 BDSG). Da eine Verarbeitung und Nutzung personenbezogener Daten des Betroffenen für Zwecke der Werbung bei Widerspruch des Betroffenen unzulässig ist (§ 28 Abs. 4 BDSG), forderte der TLfDI den Verein auf, mitzuteilen, warum der Löschaufforderung des Betroffenen bislang nicht nachgekommen wurde.

Zwar zeigte sich der Verein reumütig und sagte zu, die Beschwerde zum Anlass zu nehmen, die Daten des Betroffenen unverzüglich zu löschen und keine weiteren E- Mails an den Beschwerdeführer zu versenden, ging aber davon aus, dass das Bundesdatenschutzgesetz (BDSG) im vorliegenden Fall keine Anwendung finde. Weder die Datenerhebung noch die Datenverarbeitung erfolge beim Verein mittels automatisierter Datenverarbeitung, sondern durch manuelle Eingabe der selbständig gesammelten Daten. Zudem handele es sich bei den vom Betroffenen gespeicherten Daten allein um allgemein zugängliche Daten nach § 28 Abs. 1 Nr. 3 BDSG (die E-Mail-Adresse sei z. B. auch auf der Internetseite einer Universität zu finden). Weitere Daten seien nicht erhoben oder gespeichert worden.
Der TLfDI hat die Anwendbarkeit des BDSG als gegeben angesehen und ist davon ausgegangen, dass zumindest die Datenverarbeitung automatisiert erfolgte, sodass eine weitere Verarbeitung und Nutzung der personenbezogenen Daten des Beschwerdeführers für Zwecke der Werbung (für Veranstaltungen und ähnliches), bedingt durch das Vorliegen seines Widerspruchs, unzulässig war (§ 28 Abs. 4 BDSG). Auch eine Zulässigkeit der Datenspeicherung nach § 28 Abs. 1 Nr. 3 BDSG wurde seitens des TLfDI verneint, da das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse des Vereins überwiege.
In Anbetracht dessen, dass die personenbezogenen Daten des Betroffenen umgehend gelöscht wurden, hat der TLfDI die Angelegenheit als erledigt betrachtet und den Beschwerdeführer entsprechend informiert. Der Verein wurde aufgefordert, zukünftig bei Widersprüchen von Betroffenen die weitere Verarbeitung oder Nutzung dieser Daten gemäß § 28 Abs. 4 BDSG zu unterlassen.

Auch bei Einladungen zu einer – wenn auch kostenlosen – Veranstaltung müssen der Datenschutz und das Interesse des Betroffenen berücksichtigt werden.

3.7 Akten außer Kontrolle

Auf den Hinweis eines Arztes hin, dass er an seine Patientenakten nicht mehr heran käme, kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Sommer 2013 die Geschäftsräume des betreffenden Aktenarchivie-

rungsunternehmens in Immelborn und stellte dabei desaströse Zustände fest. Problematisch war hierbei, dass sich das Unternehmen seit einigen Jahren in Insolvenz befand und sich der ehemalige Geschäftsführer und jetzige Liquidator ins Ausland abgesetzt hat. Auf drei Etagen und insgesamt ca. 3000 qm Nutzfläche stehen hunderttausende Akten in Regalen und in Kartons verpackt. Teilweise sind die Aufbewahrungsfristen für die Akten (vermutlich) bereits abgelaufen, teilweise aber auch nicht. Das größte Problem ergibt sich jedoch aus der Tatsache, dass das Unternehmen nach dem sogenannten „chaotischen System“ eingelagert hat. Dies ist in dieser Branche durchaus üblich und aus deren Sicht vermutlich sinnvoll, da so der vorhandene Lagerplatz effektiver genutzt werden kann. Dabei werden Akten nicht nach einlagerndem Unternehmen geordnet, sondern kommen dorthin, wo grade Platz ist. Wo einzelne Akten stehen, ist im Computer abgelegt. Leider wurde jedoch, soweit der TLfDI durch Dritte informiert worden ist, durch den vom Gericht bestellten Insolvenzverwalter zunächst die EDV verwertet, möglicherweise aber auch von Dritten gestohlen. Jedenfalls ist die Computertechnik nicht mehr vorhanden. Damit ist aus dem chaotischen System das „System“ verschwunden und das „Chaos“ geblieben. Die Folge ist, dass die Aktenbestände mühsam von Hand gesichtet und registriert werden müssen, bevor sie – wie datenschutzrechtlich vorgesehen – an die Personen und Firmen, die die Akten dort eingelagert haben, zurückgeführt werden können. Hierfür muss jeder Aktenordner in die Hand genommen werden. Für einen kleineren Teil der Akten ist dies im Berichtszeitraum bereits erfolgt. Hintergrund ist, dass das rechtliche Konstrukt hinter einer solchen Aktenverwahrung ein Vertrag über die Auftragsdatenverarbeitung ist. Richtig angewendet erlaubt ein derartiger Vertrag es dem Auftraggeber (z. B. Arzt oder sonstiger Unternehmer), personenbezogene Daten an den Auftragnehmer (Archivierungsunternehmen) weiterzugeben, ohne dass die besonderen Voraussetzungen für eine Übermittlung im Sinne des Bundesdatenschutzgesetzes gegeben sein müssen. Allerdings bleibt der Auftraggeber weiterhin für die ordnungsgemäße Verarbeitung der personenbezogenen Daten verantwortlich, was weitestgehend unbekannt ist. So auch in diesem Fall. Ansprechpartner sind für den TLfDI daher die einlagernden Stellen oder Personen.
Doch bevor mit der eigentlichen Aufgabe, der Rückführung der Akten begonnen werden kann, musste sich der TLfDI nach dem Hinweis einen Überblick über die dort herrschenden Zustände ma-

chen. Da staatliches Handeln in einem Rechtsstaat wie Thüringen nur mit einer Rechtsgrundlage möglich ist, konnte der TLfDI nicht einfach „mit der Tür ins Haus fallen“. Da in diesem Fall davon auszugehen war, dass der Eigentümer der Immobilie und Geschäftsführer des insolventen Unternehmens nicht zur Kontrolle anwesend sein wird, musste zunächst das rechtskonforme Öffnen der Türen vorbereitet werden. Dies konnte mit einem öffentlich zugestellten Bescheid – eine Meldeadresse des Unternehmers war nicht ermittelbar – erreicht werden, indem das Unternehmen über die bevorstehende Kontrolle in Kenntnis gesetzt und verpflichtet wurde, den TLfDI das Gelände und die Geschäftsräume betreten zu lassen. Für den Fall der Nichtbefolgung wurde das Zwangsmittel der Ersatzvornahme, konkret das Öffnen der Türen, angedroht.

Auf den oben bereits erwähnten drei Etagen und 3000 qm Nutzfläche bot sich dem TLfDI und seinen Mitarbeitern dann ein unerwartetes Ausmaß an Chaos. Akten waren aus Regalen gestoßen und lagen auf dem feuchten Boden, teilweise waren Regale im Einsturz begriffen. Auf der obersten Etage erwartete den TLfDI dann noch eine Steigerung: Stellen Sie sich vor, Sie nehmen einen großen Raum (ca. 1000 qm), stellen diesen bis unter die Decke voll mit auf Paletten gestapelten und mit Akten gefüllten Kartons und schütteln diesen solange, bis kaum noch ein Karton auf dem anderen steht. Ein professioneller Aktenverwahrer, der im Auftrag einer vom TLfDI angeschriebenen verantwortlichen Stelle das Objekt besichtigt hat, um die Abholung bestimmter Akten vorzubereiten, teilte mit, dass er so etwas, trotz langjähriger Arbeit in diesem Metier, noch nicht erlebt hätte.

Selbstverständlich können die Akten nicht einfach vernichtet werden, schon gar nicht auf Kosten des Steuerzahlers. Vielmehr sind die einzelnen Akten der jeweils verantwortlichen Stelle, also der Person oder dem Unternehmen, welches die Einlagerung vorgenommen hat, zuzuordnen. Dazu hat der TLfDI zwei Herkulesaufgaben zu bewältigen: Er muss feststellen, wer Akten eingelagert hat und dokumentieren, wo diese im Gebäude liegen.

Um diese Aufgabe, der die immer noch viel zu kleine Behörde des TLfDI in personeller Hinsicht nicht gewachsen ist, bewältigen zu können, hat der TLfDI sich über das Thüringer Innenministerium an die Polizei gewandt, mit der Bitte Amtshilfe zu leisten. Vorgesehen war, dass einige Bereitschaftspolizisten für das Herstellen arbeitsfähiger Zustände und das Sichten bereitgestellt werden. Dieses Ersu-

chen wurde abgelehnt, denn leider sei die Polizei nicht in der Lage, auf ihre Beamten zu verzichten. Sie könne ihre sonstigen Aufgaben ansonsten nicht mehr wahrnehmen. Nur am Rande sei bemerkt, welch trauriges Bild das Innenministerium hier über den Zustand der Thüringer Polizei zeichnet, dem Exekutivorgan, das eigentlich die Aufgabe hat, die öffentliche Sicherheit und Ordnung zu gewährleisten und nötigenfalls bei Rechtsverstößen gegen das Datenschutzrecht, wie zum Beispiel im Immelborner Aktenlager, die Rechtsordnung wiederherzustellen.

Bisher versucht der TLfDI, so gut es geht, mit seiner kleinen Behörde auf eigene Faust in Immelborn wieder ordnungs- und datenschutzrechtlich ordnungsgemäße Zustände herbeizuführen. Bei einem geschätzten Aktenbestand von ca. 250.000 Akten ist dies jedoch eine langwierige Aufgabe. Für etwa 80.000 Akten ist diese Arbeit erledigt. Jedoch wartet auch das sonstige beträchtliche Tagesgeschäft des TLfDI nicht solange, bis die Akten in Immelborn aufbereitet sind.

Sobald alle Akten registriert sind, können die verantwortlichen Stellen bzw. Personen vom TLfDI aufgefordert werden, die jeweiligen Akten abzuholen. Es kann dann geplant werden, in welcher Reihenfolge und auf welche Art und Weise dies sinnvoll ist.

Auch hier drohen Verzögerungen. Nicht jede Stelle wird akzeptieren, dass sie für die teilweise vor langer Zeit eingelagerten Akten verantwortlich ist. Die Einlagerungsgebühren wurden in der Regel im Voraus für teilweise zehn Jahre gezahlt. Eine erneute Einlagerung oder Vernichtung ist mit erneuten Kosten verbunden, die von der verantwortlichen Stelle getragen werden müssen.

Zwar kann und wird der TLfDI die Verantwortlichen mittels Anordnung zum Handeln zwingen, jedoch steht den verantwortlichen Stellen selbstverständlich gegen solche Verwaltungsakte der Rechtsweg offen. Streitigkeiten vor dem Verwaltungsgericht binden wiederum Personal und sind vor allem eines: langwierig.

Wann „die Akte Immelborn“ geschlossen werden kann, steht derzeit noch in den Sternen. Ohne die Unterstützung anderer Behörden bleibt dem TLfDI nichts anderes übrig, als sich Hilfe im privaten Bereich zu holen. Dies wird den Steuerzahler aber einiges kosten. Vernünftiger wäre es daher, wenn sich das Thüringer Innenministerium (TIM) doch zum Helfen durchringen und Personal, Generatoren für Licht, große Leuchter, Hubwagen etc. zur Verfügung stellen könnte. So könnte wenigstens der erste Schritt, die eigentliche Sich-

tung des Aktenbestands, zügig und erfolgreich erledigt werden. Bei weiterer Verweigerung der Amtshilfe seitens des TIM wird der TLfDI diese Unterstützung gerichtlich einklagen.

Wenn Akten ausgelagert werden müssen, sollte der Preis nicht das einzige Kriterium für die Auswahl des zu beauftragenden Unternehmens sein. Auch wenn die Akten nicht mehr im Schrank des einlagernden Unternehmens stehen, bleibt dieses verantwortliche Stelle. Deswegen ist es notwendig und gesetzlich vorgeschrieben, sich vor und auch nach dem Auslagern darüber zu versichern, dass die Akten in einer Art und Weise gelagert werden, die auch dem Datenschutz genügt.
Auch muss ein Vertrag über eine Auftragsdatenverarbeitung (vgl. 5. TB Anlage 23 - Mustervertrag) geschlossen werden, der den gesetzlichen Anforderungen genügt. Ansonsten ist mit einem Ordnungswidrigkeitenverfahren wegen unerlaubter Verarbeitung von personenbezogenen Daten zu rechnen.

3.8 Wahrnehmung des Hausrechts darf nicht vorgeschoben werden: Videogaga 1

Ein anonymer Hinweis brachte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf die Spur eines Cafés, das seinen Gastraum durch Videokameras überwacht. In der daraufhin durchgeführten Vorortkontrolle bestätigte sich die vermutete unzulässige Videoüberwachung. Auch bei einem Café handelt es sich um einen öffentlich zugänglichen Bereich, auch hier gilt die abschließende Regelung des Gesetzgebers in § 6 b Bundesdatenschutzgesetz zur Zulässigkeit von Videoüberwachungen in diesen Bereichen. Der auf Nachfrage mitgeteilte Zweck der Videoüberwachung war die Überwachung des Eingangs zum Café, also die Ausübung des Hausrechts. Unglücklich war allerdings, dass die Kameras die Bilder auf einen Tablet-PC übertrugen. Dieser lag zumeist mit entladener Batterie und nicht eingeschaltet in der Wohnung des Betreibers. Mit anderen Worten, die Videokameras filmten zwar, konnten aber den mit Ihnen verfolgten Zweck gar nicht erfüllen. Die Videoüberwachung muss nach dem Gesetz auch für den Zweck der Ausübung des Hausrechts geeignet und erforderlich sein. Das ist nur dann der Fall, wenn durch die Videoüberwachung die Ausübung des Hausrechts zumindest unterstützt wird und kein ande-

res Mittel zur Verfügung steht, das in die Rechte der Gäste weniger stark eingreift. Ebenfalls darf kein Anhaltspunkt dafür erkennbar sein, dass schutzwürdige Interessen der Betroffenen überwiegen. Die hier festgestellte Videoüberwachung war schon deswegen unzulässig, da sie überhaupt nicht geeignet war, den angestrebten Zweck zu erreichen. Aber selbst wenn dies der Fall gewesen wäre, sind in Gaststätten immer Anhaltspunkte dafür erkennbar, dass die Interessen der gefilmten Gäste überwiegen. Dabei kommt es auch nicht darauf an, ob und wie gefilmt wird bzw. ob aufgezeichnet wird. Es handelt sich um einen Ort, der der Freizeitgestaltung dient. Hier muss eine Entfaltung der Persönlichkeit möglich sein, die nicht unter dem Eindruck der ständigen Beobachtung steht. Der TLfDI hat hier die Demontage der Kameras angeordnet.

Die Videoüberwachung muss für den von ihr verfolgten Zweck geeignet und erforderlich sein. Videokameras in Gaststätten, die im Gastraum aufgebaut sind bzw. in diesen hineinfilmen, sind grundsätzlich datenschutzrechtswidrig.

3.9 Ich weiß, was Du isst, also weiß ich, was Du bist: Videogaga 2

So oder so ähnlich scheinen es derzeit mehrere Gastronomen in Thüringen zu betrachten. Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) laufen derzeit mehrere Verwaltungsverfahren hinsichtlich Videoüberwachung im Gastronomiebereich, die alle auf Hinweise aus der Bevölkerung zurückzuführen sind. Ganz besonders genau scheint es ein Erfurter Unternehmen zu nehmen, wenn es große Teile des Gastraums und den überwiegenden Teil des Arbeitsbereiches der Gaststätte überwacht. Dabei kann man fast pauschal sagen, dass diese Art der Videoüberwachung rechtswidrig ist.
Die Überwachung im Gastraum ist ohnehin rechtswidrig, da eine Videoüberwachung im öffentlich zugänglichen Bereich schon dann unzulässig ist, wenn Anhaltspunkte darüber vorhanden sind, dass schutzwürdige Interessen Betroffener das Interesse des Betreibers an der Beobachtung überwiegen, § 6 b Abs. 1 Bundesdatenschutzgesetz. Dies ist im Gastraum eines Cafés, einer Bar oder eines Restaurants immer der Fall, weil dies ein Ort ist, an dem eine ungestörte

Entfaltung der Persönlichkeit im Rahmen der Freizeitgestaltung möglich sein muss.
Die Videoüberwachung von Arbeitnehmern ist in aller Regel ebenfalls unzulässig. Ein Umgang mit Arbeitnehmerdaten ist nämlich immer nur dann erlaubt, wenn dies zur Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Eine Videoüberwachung im Rahmen eines Arbeitsverhältnisses kann zum Beispiel dann erforderlich sein, wenn extreme (Arbeits-)Umstände vorliegen, wie beispielsweise eine lebensbedrohliche Arbeitsumgebung, bei der der oder die Arbeitnehmer ständig beobachtet werden müssen, um im Fall eines Unfalls sofort eingreifen zu können. Umstände also, die im Arbeitsbereich von Gastronomiebetrieben eher selten gegeben sein dürften.
Der TLfDI hat dem – uneinsichtigen – Unternehmen gegenüber eine Anordnung erlassen, in der die Deinstallation der Kameras verlangt wird, um wieder rechtskonforme Zustände herzustellen.

Videoüberwachung im Gastronomiebereich ist in der Regel unzulässig. Sollten Sie eine solche Anlage bemerken, wenden Sie sich bitte an den TLfDI, damit dieser der Sache nachgehen kann.

3.10 Busfahrer im Visier: Videogaga 3

Auf einen anonymen „Wink“ hin wurde die Aufmerksamkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf ein Thüringer Nahverkehrsunternehmen gelenkt. In dem Hinweis wurde von einer umfangreichen Videoüberwachung sämtlicher Busse gesprochen. Nicht nur das Betriebsgelände, sondern auch die Busfahrer selbst sollten überwacht werden. Insgesamt seien ca. 40 Videokameras in Betrieb.
Im Laufe der Kontrolle wurde durch die Arbeitnehmer des TLfDI in der Tat eine umfangreiche Videoüberwachungsanlage festgestellt. Hervorzuheben ist dabei insbesondere die festgestellte Kamera im Bus, die den Busfahrer bei seiner Arbeit filmt. Diese Kamera ist rechts oberhalb des Busfahrers angebracht und filmt nach links Richtung vordere Einstiegstür. Aufgenommen werden dabei auch Bereiche außerhalb des Busses und zwar sowohl in Fahrtrichtung sowie auf der Einstiegsseite. Allerdings ist auch das Lenkrad mit den Armen und Händen des Busfahrers zu erkennen. Teilweise – jeweils von Bus und Fahrer abhängig – auch der Kopf des Fahrers.

Rechtlich gesehen sind ein Bus und die Straße um diesen herum nicht anders zu beurteilen als sonstige Bereiche, die öffentlich zugänglich sind. Dabei kommt es nämlich nicht darauf an, ob es sich um Privatbesitz handelt oder nicht. Vielmehr ist maßgeblich, ob die jeweiligen Flächen vom äußeren Erscheinungsbild her den Eindruck erwecken, von jedermann betreten werden zu dürfen. Umso mehr unter den Begriff der öffentlich zugänglichen Bereiche fallen dann Bereiche, die dazu gedacht sind, von jedermann betreten zu werden: Busse zum Beispiel.
Videoüberwachung in diesen Bereichen ist problematisch, wie man auch daran erkennen kann, dass dieser Komplex immer wieder in diesem Tätigkeitsbericht zur Sprache kommt. Der Gesetzgeber hat nämlich erkannt, dass Videoüberwachungsanlagen in besonderem Maße in die Grundrechte der Bürger eingreifen und deren Gebrauch in öffentlich zugänglichen Bereichen daher abschließend reglementiert. Nur in den gesetzlich zulässigen Fällen ist eine Videoüberwachung zulässig, wenn diese erforderlich ist und keine Anhaltspunkte dafür bestehen, dass Interessen der jeweils Betroffenen dem entgegenstehen, so der Gesetzgeber in § 6 b Bundesdatenschutzgesetz (BDSG).
Nach dieser Regelung (§ 6 b BDSG) sind die Aufnahmen außerhalb des Busses nur dann zulässig, wenn dies zur Durchsetzung des Hausrechts bzw. wegen berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Beide Alternativen scheiden hier aus: das Hausrecht, weil ein Busunternehmen auf Straßen und Fußwegen kein Hausrecht ausübt; besondere Interessen, weil diese nicht für konkrete Zwecke festgelegt wurden.
Hinsichtlich der hier beleuchteten Kamera über dem Busfahrer kommen auch noch Arbeitnehmerdatenschutzaspekte hinzu. So ist eine Erhebung von Arbeitnehmerdaten immer nur dann erlaubt, wenn dies zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist.
Unter beiden Gesichtspunkten ist die über dem Fahrer installierte Kamera in der derzeitigen Installation unzulässig.
Die Zulässigkeit dieser Aufnahmen scheitert schon offensichtlich daran, dass diese nicht für die Durchführung des Arbeitsverhältnisses von Belang sind.
Aber auch die Aufnahmen der Bereiche außerhalb des Busses sind datenschutzrechtlich problematisch. So werden Fahrzeuge (und deren Kennzeichen) vor dem Bus genauso erfasst, wie auf den Fußwe-

gen laufende und an Haltestellen stehende Menschen. Diese Beobachtung des öffentlich zugänglichen Bereiches ist jedoch nur unter den oben beschriebenen Voraussetzungen möglich, wenn diese zur Durchsetzung des Hausrechts oder eines besonderen Interesses für festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für überwiegende schutzwürdige Interessen Betroffener bestehen.
Insoweit ist die juristische Prüfung noch nicht abgeschlossen, jedoch sind die Kameras, die den Busfahrer und die Außenbereiche aufnehmen, nach summarischer Prüfung mit dem BDSG nicht zu vereinbaren.
Der TLfDI wird nach Abschluss der Prüfung dem Unternehmen das Ergebnis mitteilen. Reagiert das Unternehmen hierauf nicht und belässt es bei den festgestellten rechtswidrigen Verfahrensweisen, wird der TLfDI gegenüber dem Unternehmen eine Anordnung erlassen, mit der er diesem die entsprechenden Verhaltensweisen untersagt. Sofern im Ergebnis nach Abschluss der juristischen Prüfung eine unzulässige Videoüberwachung festgestellt werden sollte, wird der TLfDI ebenfalls die Einleitung eines Ordnungswidrigkeitenverfahrens prüfen.

Wenn Arbeitnehmer bei ihrer Tätigkeit permanent videoüberwacht werden, ist dies in aller Regel unzulässig. Auch die Aufnahme des öffentlichen Verkehrsraums ist regelmäßig rechtswidrig.

3.11 Wertvoller Schrott im Blick: Videogaga 4

Im Rahmen seiner Tätigkeit führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) verschiedene anlassunabhängige Kontrollen durch. Mit Übernahme der Zuständigkeit im nicht-öffentlichen Bereich Ende 2011 durch den TLfDI führte dieser mehrere Informationskampagnen für Unternehmen durch. Im Anschluss an diese Informationsphase, die mit einer Art „Schonfrist“ für die Unternehmen verbunden war, begann der TLfDI mit anlasslosen Kontrollen bei Unternehmen. In diesem Zusammenhang wurden auch diverse Recyclingunternehmen kontrolliert, weil es aus dieser Branche bereits diverse Beschwerden beim TLfDI gab. Bei diesen Unternehmen ergaben sich vielfältige, auf den ersten Blick nicht ersichtliche datenschutzrechtliche Problemstellungen. Eine davon ist der umfangreiche Einsatz von Videoüberwachungstechnik.

So auch in diesem Fall. Zwar ist die juristische Bewertung bislang noch nicht abgeschlossen, allerdings wird auch in diesem Fall von einer Videotechnik in einem Umfang Gebrauch gemacht, der nach summarischer Prüfung nicht mit dem Bundesdatenschutzgesetz (BDSG) vereinbar ist.
So ist unter anderem eine umfangreiche Videoüberwachung im Außenbereich eingerichtet, die möglicherweise nicht den gesetzlichen Voraussetzungen entspricht und damit unzulässig ist. Durch eine solche Videoüberwachungsanlage werden personenbezogene Daten erhoben und gespeichert. Dies ist jedoch nur zulässig, wenn die betroffenen Personen in die Datenerhebung und -speicherung eingewilligt haben, was bei einer Videoüberwachung wirklichkeitsfremd wäre, oder das Gesetz eine entsprechende Erlaubnisnorm für den konkreten Fall des Einsatzes bereithält.
Im hiesigen Fall ist die einschlägige Erlaubnisnorm § 6 b Bundesdatenschutzgesetz (BDSG). Diese regelt den Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen. Zu solchen zählt auch der Betriebshof eines Recyclingunternehmens, soweit dieser so gestaltet ist, dass jedermann diesen betreten kann. In solchen Bereichen ist eine Videoüberwachung durch ein nicht-öffentliches Unternehmen nur dann zulässig, wenn diese zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke durchgeführt wird und hierfür auch erforderlich ist.
Während diese Voraussetzungen zumeist vorliegen mögen bzw. deren Hürde nicht sonderlich schwer zu nehmen ist, stellt § 6 b BDSG noch eine weitere Anforderung an eine zulässige Videoüberwachung. So dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener die Interessen des Videoüberwachenden überwiegen. Im Gegensatz zu den vorherigen Voraussetzungen stellt dies eine hohe Hürde für die Zulässigkeit einer Videoüberwachung im nicht-öffentlichen Bereich dar. Bereits Anhaltspunkte dafür, dass Interessen Betroffener überwiegen, führen zur Unzulässigkeit der Anlage. Daher ist eine Videoüberwachung in solchen Bereichen nur dann zulässig einsetzbar, wenn es dafür wirklich triftige und schwerwiegende Gründe gibt, die eventuelle schutzwürdige Interessen Betroffener in jedem Fall überwiegen.
Der TLfDI wird in diesem Fall nach Abschluss der Prüfung dem Unternehmen in einem Kontrollergebnis mitteilen, welche Mängel festgestellt wurden. Sollte das Unternehmen daraufhin die entspre-

chenden Mängel nicht abstellen, wird der TLfDI dem Unternehmen gegenüber eine Anordnung erlassen, mit der die Beseitigung der Mängel durchgesetzt werden. Darüber hinaus muss das Unternehmen wegen des hohen Eingriffspotentials von Videoaufnahmen in das Persönlichkeitsrecht der Betroffenen mit der Einleitung von Ordnungswidrigkeitenverfahren rechnen.

Bevor Investitionen zur Einrichtung einer Videoüberwachungsanlage getroffen werden, sollte genau geprüft werden, ob diese mit dem BDSG vereinbar ist. Hierbei sollte man nicht nur auf die Aussagen des installierenden Unternehmens vertrauen, da diese in erster Linie ihr Produkt und ihre Dienstleistung verkaufen möchte. Die Voraussetzungen für eine zulässige Videoüberwachung sind oftmals hoch und bedürfen der Prüfung durch Fachpersonal. Dabei sind unbedingt die Voraussetzungen, die das Gesetz an die jeweilige Art der Videoüberwachung richtet, einzuhalten. Unternehmen sollten erwägen, vor einer Videoinstallation den TLfDI zu Rate zu ziehen.

3.12 Schrott unter Beobachtung: Videogaga 5

Im Rahmen der anlasslosen durchgeführten Kontrolle suchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein größeres Recyclingunternehmen auf. Dieses Unternehmen besaß keinen betrieblichen Datenschutzbeauftragten. Es war bislang nicht üblich, die Arbeitnehmer, die mit der Verarbeitung von personenbezogenen Daten betraut sind, auf das Datengeheimnis zu verpflichten. Nach § 5 Bundesdatenschutzgesetz (BDSG) muss jedes Unternehmen seine mit der Verarbeitung von personenbezogenen Daten betrauten Arbeitnehmer auf das Datengeheimnis verpflichten. Auf der Homepage des TLfDI findet sich eine Mustervorlage zur Verpflichtung auf das Datenschutzgeheimnis. Das Unternehmen wird diese Verpflichtung der Arbeitnehmer nachholen.
Das Verfahrensverzeichnis befand sich im Aufbau. Es gab bereits Festlegungen des Qualitätsmanagements, die sich mit den Verfahren der Verarbeitung von personenbezogenen Daten befassen. Diese müssen jedoch noch strukturiert und zusammengefasst werden, um den gesetzlichen Anforderungen zu genügen. Nach § 9 BDSG muss das Unternehmen die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung datenschutzrechtlicher Bestimmungen zu gewährleisten. Im Nachgang zur Kontrolle

reichte das Unternehmen bereits umfangreiche Unterlagen ein, diese werden derzeit geprüft.
Auf dem Gelände des Unternehmens gab es eine umfangreiche Videoüberwachung mit 10 Dome-Kameras, die sich sowohl innerhalb des Firmengebäudes als auch außerhalb befanden. Die Zwecke für die Videoüberwachung waren bei den einzelnen Kameras unterschiedlich. Sie wurden bei der Begehung erläutert, waren jedoch nicht im Rahmen eines Sicherheitskonzeptes dokumentiert. Eine Videoaufzeichnung fand nicht statt, die Bilder waren in einem separaten Wachraum durch den Wachmann live zu sehen. Auch das reine Monitoring fällt unter den Begriff der Videoüberwachung nach § 6 b BDSG. Es handelt sich hierbei um die Beobachtung mit optisch-elektronischen Einrichtungen nach § 6 b Abs. 1 BDSG. Gegenüber der Videoaufzeichnung stellt das reine Monitoring einen geringeren Eingriff in die Rechte der Betroffenen dar, da die Aufnahme der Person nur in Echtzeit erfolgt und nachträglich nicht mehr wieder herstellbar ist. Gleichwohl muss die durchgeführte Videoüberwachung den Anforderungen des § 6 b BDSG genügen, soweit sie in öffentlich zugänglichen Räumen erfolgt, ansonsten müssen die Anforderungen des § 28 BDSG erfüllt oder, wenn die Beobachtung von Mitarbeitern im Fokus steht, die Voraussetzungen des § 32 BDSG gegeben sein. Der TLfDI hat die Prüfung der Zulässigkeit der Videoüberwachung in dem Unternehmen noch nicht abgeschlossen. Für jede einzelne Kamera muss festgestellt werden, ob diese den jeweils geltenden rechtlichen Anforderungen entspricht. Jedenfalls wird der TLfDI vom Unternehmen die Erstellung eines Verfahrensverzeichnisses nach § 4 g Abs. 2 bzw. 2 a BDSG verlangen. Außerdem müssen die konkreten Zwecke der Videoüberwachung nach § 6 b Abs. 1 bzw. 28 Abs. 1 Satz 2 BDSG schriftlich festgelegt werden.

Zwar stellt die reine Videobeobachtung einen geringeren Eingriff dar als die Videoaufzeichnung. Auch sie ist jedoch nur bei Vorliegen einer gesetzlichen Ermächtigung zulässig. Vor Beginn der Videoüberwachung ist der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen und es sind die erforderlichen technischen und organisatorischen Maßnahmen zur Einhaltung datenschutzrechtlicher Anforderungen zu treffen.

3.13 Schrott-Video: Videogaga 6

Im Zuge der anlasslos durchgeführten Unternehmenskontrollen suchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein Unternehmen auf, dessen Hauptgeschäft das Elektronikschrott-Recycling ist. In diesem Unternehmen gab es etliche datenschutzrechtliche Probleme:
Das rechtlich selbstständige Unternehmen ist Tochter eines größeren Konzerns, der die Personalverwaltung für das Unternehmen übernommen hat. Nach § 11 Bundesdatenschutzgesetz (BDSG) bleibt weiterhin das auftraggebende Unternehmen für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. In diesem Fall ist ein schriftlicher Auftrag zu erteilen, der den Anforderungen des § 11 Abs. 2 Satz 2 BDSG entsprechen muss. Es müssen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, der Umfang der Weisungsbefugnis, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält und vieles mehr geregelt werden. Ein solches Vertragsverhältnis existierte zwischen Konzerntochter und Konzernmutter jedoch nicht.
Zwar hatte das Unternehmen einen Datenschutzbeauftragten, dieser hatte jedoch noch keine speziellen Datenschutzkenntnisse erworben. Es gab im Betrieb auch keine Richtlinien bzw. Anweisungen zur Einbeziehung des Datenschutzbeauftragten. Es fehlten schriftliche Festlegungen zur Sperrung und Löschung von nicht mehr erforderlichen Daten. Ein schriftliches Konzept zu allgemeinen technischen und organisatorischen Maßnahmen existierte ebenso wenig wie ein Konzept über die Gesamtheit der Sicherheitsmaßnahmen (IT-Sicherheitskonzept).
Weiterhin wurde auf dem Gelände eine Videoüberwachung mit vier Kameras durchgeführt. Eine Kamera filmte dabei Arbeitnehmer auf einem dauerhaft eingerichteten Arbeitsplatz an einem Förderband. Zwar ist der von der Kamera überwachte Bereich öffentlich zugänglich, jedoch steht hier der Beschäftigte im Fokus der Überwachung. In diesen Fällen haben sich die Aufsichtsbehörden der Länder darauf geeinigt, die Zulässigkeit der Videoüberwachung an den Vorausset-

zungen des § 32 BDSG zu messen. Danach dürfen personenbezogene Daten eines Arbeitnehmers für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses zu dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Arbeitnehmers nur dann erhoben, verarbeitet oder genutzt werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Da beide Voraussetzungen nicht vorlagen, war die Kamera in dieser Ausrichtung nicht zulässig.
Eine weitere Kamera wurde auf Wunsch eines Kunden installiert. Dieser wollte dokumentiert haben, dass seine Produkte, die geheimhaltungsbedürftige Daten enthielten, ordnungsgemäß geschreddert bzw. vernichtet worden sind. Hier reicht es aus Sicht des TLfDI im Rahmen der Erforderlichkeit aus, die Kamera nur bei der Auftragstätigkeit für diesen Kunden zu aktivieren.
Die Zulässigkeit der übrigen Kameras war, da das Betriebsgelände während der Geschäftszeiten für den Publikumsverkehr geöffnet war, an § 6 b BDSG zu messen. Nach § 6 b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht mit einem anderen (wirtschaftlich oder organisatorisch) zumutbaren, in die Rechte der Betroffenen weniger einschneidenden Mittel, erreicht werden kann.
Eine weitere Kamera, die den Eingangsbereich absichern sollte, war teilweise auch auf den öffentlichen Verkehrsgrund gerichtet. Hier war nicht ersichtlich, wieso die Aufnahme dieses Bereiches für die verfolgten Zwecke erforderlich sein sollte. Die Kamera sollte dazu dienen, eine Annahmestelle für Elektroschrott, die sich vor dem Tor auf dem Betriebsgelände befand, zu überwachen. Wer außer seinem Grundstück auch öffentlichen Raum, wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt.

Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten oder sonstige Verkehrsteilnehmer, zurück.

Eine weitere Kamera wurde angebracht, um einen Bereich zu überwachen, der schlecht einsehbar war. Es sei in der Vergangenheit häufiger dazu gekommen, dass Personen nachts über den Zaun auf das Gelände gelangt sind. Hier hielt der TLfDI eine Überwachung während der Geschäftszeiten für nicht erforderlich.
Die aufgezeichneten Bilder wurden von dem Unternehmen 84 Stunden gespeichert. Nach § 6 b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erfüllung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Das bedeutet, Videoaufzeichnungen sind grundsätzlich nach 48 Stunden zu löschen.
Das Unternehmen forderte von sämtlichen Kunden Kopien der Personalausweise. Dies ist grundsätzlich unzulässig und nicht erforderlich (hierzu wird auf den Beitrag unter Punkt 3.48 verwiesen).
Der TLfDI teilte dem Unternehmen das Ergebnis seiner Kontrolle mit und gab diesem Gelegenheit zur Stellungnahme. Es bleibt abzuwarten, ob das Unternehmen alle datenschutzrechtlichen Forderungen des TLfDI erfüllt oder eine verwaltungsrechtliche Anordnung erforderlich sein wird. Derzeit wird geprüft, ob ein Bußgeldverfahren eingeleitet wird.

Für Unternehmen in Thüringen bestehen zahlreiche datenschutzrechtliche Anforderungen. Es ist beispielsweise im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret anzugeben und die gesetzlichen Voraussetzungen sind für jede Kamera gesondert zu prüfen. Diese Festlegungen sind Teil der durch das Unternehmen zu treffenden technischen und organisatorischen Maßnahmen nach § 9 BDSG.

3.14 Der nicht privilegierte Konzern

Im Rahmen seiner Tätigkeit führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) verschiedene anlassunabhängige Kontrollen durch. In diesem Zusammenhang wurden auch diverse Recyclingunternehmen kontrolliert. In dieser Branche ergeben sich vielfältige, auf den ersten Blick nicht ersichtliche datenschutzrechtliche Problemstellungen. Im Fall des nunmehr kontrollierten Unternehmens wurden mögliche Probleme hinsichtlich der Auftragsdatenverarbeitung festgestellt. Dies ist insbesondere bei solchen Unternehmen ein Problemschwerpunkt, die in eine umfangreiche Konzernstruktur eingebunden sind. Ein Konzern entsteht immer dann, wenn mehrere Unternehmen zusammenarbeiten und eines davon die anderen beherrscht. Typischerweise werden in solchen Strukturen beispielsweise Arbeitnehmerdaten an eine beherrschte Verwaltungsgesellschaft weitergeleitet, die dann alle damit verbundenen Aufgaben, wie Lohnsteuerberechnungen übernimmt.
Im Zusammenhang mit dem Datenschutz führt dies oftmals zu Problemen, je nachdem, wie die Aufgabenteilung im jeweiligen Konzern organisiert ist. Denn, woran man denken muss: Das Bundesdatenschutzgesetz (BDSG) kennt keine Sonderregelungen für Konzerne. Demensprechend gibt es auch kein „Konzernprivileg“ im BDSG.
Während es sich also auf den ersten Blick so „anfühlt“, als würden personenbezogene Daten innerhalb eines Unternehmens bleiben, weil man diese innerhalb der selben Unternehmensgruppe „verschiebt“, werden datenschutzrechtlich betrachtet personenbezogene Daten zwischen verschiedenen Unternehmen übermittelt. Hierfür gelten dieselben Einschränkungen, die auch für Unternehmen gelten, die nicht durch einen Beherrschungsvertrag verbunden sind.
Dieses falsche Gefühl führt oftmals dazu, dass zwischen den konzerneigenen Unternehmen keine oder nur mangelhafte Auftragsdatenverarbeitungsverträge geschlossen werden. Tatsächlich ist eine solche Verarbeitung von Daten aber nur dann zulässig, wenn entweder ein solcher Auftragsdatenverarbeitungsvertrag geschlossen wurde, der Betroffene einwilligt oder es eine entsprechende Erlaubnisnorm gibt. Hinsichtlich der Einwilligung bestehen aber wegen der sozialen und wirtschaftlichen Abhängigkeit des Arbeitnehmers vom Arbeitgeber hohe Anforderungen. Die Versuchung, sämtliche Maß-

nahmen des Arbeitgebers „abzunicken“, um diesem zu gefallen, wird als hoch eingeschätzt. Da die Einwilligung nach den gesetzlichen Vorgaben freiwillig erfolgen muss, aber solche autonomen Gründe, die vom Arbeitnehmer selbst stammen und zur Einwilligung geführt haben müssen, fehlen, scheidet eine Einwilligung als Zulässigkeitsgrund im Arbeitsverhältnis in der Regel aus. Der Wille, zu gefallen, oder sonstiger Anpassungsdruck von außen stellt nämlich keinen autonomen Grund dar.
Auch der Weg über die Erlaubnisnorm ist holprig. Zwar stellt das Gesetz mit § 28 BDSG bzw. bei Arbeitnehmerdaten mit § 32 BDSG Normen bereit, die für diesen Anwendungsbereich in Frage kommen, jedoch müssen die Unternehmen hierbei jedes Mal erneut umfangreich prüfen, ob eine Übermittlung oder sonstige Verarbeitung von personenbezogenen Daten noch von der jeweiligen Norm gedeckt ist.
Einfacher stellt sich hier die Auftragsdatenverarbeitung, geregelt in § 11 BDSG, dar. Für ein solches Rechtsverhältnis schreibt das BDSG Form und Inhalt vor. Dieser Auftrag zur Datenverarbeitung ist schriftlich zu erteilen, wobei nach § 11 Abs. 2 Satz 2 BDSG insbesondere im Einzelnen festzulegen sind:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Wesentlicher Vorteil für den Datenverkehr innerhalb des Konzerns ist der, dass bei einem Auftragsdatenverarbeitungsverhältnis kraft gesetzlicher Fiktion keine Datenübermittlung erfolgt und somit die Voraussetzungen der entsprechenden Erlaubnisnorm (für die Übermittlung) entfallen. Allerdings ist zu beachten, dass der Auftraggeber eines solchen Vertragsverhältnisses auch datenschutzrechtlich verantwortliche Stelle bleibt. Werden beim Auftragnehmer datenschutzrechtswidrige Zustände festgestellt, bleibt folglich dennoch der Auftraggeber Ansprechpartner der Aufsichtsbehörde.
Im hiesigen Fall konnten bis heute die entsprechenden Verträge nicht nachgereicht werden. Dies kann unter Umständen dazu führen, dass die jeweils vorgenommenen Übermittlungen in unbefugter Art und Weise erfolgten. Wenn sich diese Annahme bestätigt, muss das Unternehmen mit der Einleitung entsprechender Ordnungswidrigkeitenverfahren durch den TLfDI rechnen.

Auch innerhalb eines Konzerns gelten die Regelungen des BDSG zum Datenschutz im nicht-öffentlichen Bereich ohne Einschränkungen. Hier bietet es sich oftmals an, Verträge über eine Auftragsdatenverarbeitung zwischen Unternehmen zu schließen, die regelmäßig personenbezogene Daten übermitteln sollen. Allerdings sind dabei die gesetzlichen Mindeststandards für einen solchen Vertrag einzuhalten

3.15 Teurer Schrott

Die wenigsten Unternehmen können alle Bereiche, bei denen personenbezogene Daten verarbeitet werden müssen, selber abwickeln. Hierzu bedient man sich dann anderer Unternehmen, die sich auf den entsprechenden Bereich spezialisiert haben. Typisches Beispiel hierfür ist die Altpapiervernichtung. Ein vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) kontrolliertes Unternehmen setzte einen Dienstleister ein, um seine alten Datenträger zu vernichten, auf denen personenbezogene Daten

gespeichert waren. Hierbei handelt es sich um ein so genanntes Auftragsdatenverhältnis, an das das Bundesdatenschutzgesetz (BDSG) bestimmte Anforderungen stellt. Allerdings entsprach der diesem Auftragsverhältnis zu Grunde liegende Vertrag nicht den vom Gesetz vorausgesetzten formalen und inhaltlichen Ansprüchen. Zwar entsprach der Vertrag der vom Gesetz geforderten Schriftform, jedoch war weder der Gegenstand des Auftrags ausreichend bezeichnet, noch wurde auf den Umfang, die Art und den Zweck der vorgesehenen Verarbeitung der Daten, die Art der Daten und die Betroffenen eingegangen. Die zu regelnden notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG waren ebenso nicht enthalten, wie ein dem Auftraggeber einzuräumendes Kontrollrecht. Auch fehlte eine Regelung, die den Auftragnehmer dem Weisungsrecht des Auftraggebers unterwirft und ersteren verpflichtet, Verstöße gegen den Datenschutz seinem Auftraggeber zu melden. Letztlich fehlte auch eine Regelung über die Rückgabepflicht von personenbezogenen Daten nach Ende des Vertragsverhältnisses an den Auftraggeber. Die Folge ist, dass kein Auftragsdatenverarbeitungsverhältnis im Sinne des Datenschutzrechts besteht und es sich bei der Weitergabe der Festplatten zum Zweck der Vernichtung damit um eine Übermittlung personenbezogener Daten im Sinne des BDSG handelt. Allerdings um eine Übermittlung, für die keine Rechtsgrundlage besteht und die damit unbefugt erfolgte. Eine unbefugte Übermittlung von personenbezogenen Daten ist allerdings mit einem Bußgeld von bis zu 300.000 Euro bedroht. Der TLfDI hat das Unternehmen aufgefordert, ein dem BDSG entsprechendes Vertragswerk aufzusetzen, um so den Anforderungen des BDSG zu genügen. Ob ein Ordnungswidrigkeitenverfahren eingeleitet werden soll, wird derzeit geprüft.

Wenn personenbezogene Daten im Auftrag verarbeitet werden sollen, müssen Unternehmen unbedingt darauf achten, dass ein wirksamer und inhaltlich richtiger Vertrag über die Auftragsdatenverarbeitung geschlossen wird. Liegt kein Auftragsdatenverarbeitungsvertrag im Sinne des Datenschutzrechts vor, handelt es sich um eine Datenübermittlung, die einer eigenen Rechtsgrundlage bedarf. Fehlt diese, kann es ganz schnell teuer werden.

3.16 Zwei Fliegen mit einer Klappe

Eines der vielen vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen einer anlasslosen Kontrollreihe kontrollierten Unternehmen war ein Hersteller großer industrieller Fertigungsanlagen.
Bereits zu Beginn der Kontrolle war offensichtlich, dass der Geschäftsführer des Unternehmens vom Datenschutz, wie ihn das Gesetz versteht, noch nichts gehört hatte. Der Unternehmer verstand unter dem Begriff vielmehr den Schutz der Unternehmensdaten vor Zugriffen von außen und von innerhalb des Unternehmens und dabei vor allem Daten, die für das Unternehmen von Wert sind, wie z. B. Konstruktionspläne. Sicherlich sind solche Datensätze für Unternehmen schützenswerte Daten, handelt es sich doch im Kern um das Kapital des Unternehmens. Leider ist diese fehlerhafte, zumindest aber unvollständige Auffassung hinsichtlich des Begriffes Datenschutz weit verbreitet und zumindest zu kurz gegriffen.
Mit dem Bundesdatenschutzgesetz (BDSG) hat der Gesetzgeber Unternehmern und anderen privaten Stellen aufgegeben, mit personenbezogenen Daten Dritter nur insoweit umzugehen, wie es das Gesetz vorsieht oder der Einzelne es zulässt. Sonstige schützenswerte Daten, wie z. B. Geschäftsgeheimnisse, hatte der Gesetzgeber nicht im Sinn. Dennoch sind beide Bereiche nicht völlig voneinander zu trennen. Wer, so wie es das Gesetz vorschreibt, für den Schutz von personenbezogenen Daten ein Sicherheitskonzept erstellt und den Zugang zu unterschiedlichen Bereichen sowie Programmen regelt, um den Zugriff Unbefugter auf personenbezogene Daten zu verhindern und eine ausschließliche Verarbeitung im Rahmen der gesetzlichen Vorschriften zu gewährleisten (Zugriffs- und Zutrittsregelungen), wird seine Überlegungen ohne größere Umstände auch auf die nicht personenbezogenen Daten des Unternehmens ausweiten können.
Im hiesigen Fall stellte es sich genau anders herum dar. Das Unternehmen hatte einiges an Mitteln in den Schutz der unternehmenseigenen Konstruktionspläne investiert. Zwar wurden vom TLfDI und seinen Mitarbeitern der eine oder andere Mangel festgestellt, jedoch war das Unternehmen dann auch hinsichtlich der personenbezogenen Daten weit besser aufgestellt als die meisten anderen kontrollierten Unternehmen. So waren alle Maßnahmen zum technischen und organisatorischen Datenschutz bereits getroffen und mussten nur noch

auf die eigentlich zu schützenden personenbezogenen Daten ausgeweitet werden. Insbesondere existierte ein detailliertes IT-Sicherheitskonzept, was zwar notwendig, aber nach den bisherigen Erfahrungen in Thüringen leider noch nicht selbstverständlich ist.
Die detaillierten Unterlagen liegen dem TLfDI zur Prüfung vor und werden noch ausgewertet. Sodann wird dem Unternehmen in einem Schreiben mitgeteilt werden, welche Veränderungen und Maßnahmen noch notwendig sind, um die Einhaltung des BDSG zu gewährleisten. Sofern bei der Detailprüfung keine schwerwiegenden Verstöße mehr festgestellt werden und den Forderungen des TLfDI Folge geleistet wird, ist das Verfahren damit abgeschlossen.

Ein datenschutzrechtlich ordnungsgemäß arbeitendes Unternehmen hat auch aus unternehmerischer Sicht einen Marktvorteil. Zunächst danken es einem die Arbeitnehmer, Lieferanten und Kunden, wenn mit ihren Daten ordnungsgemäß umgegangen wird, gleichzeitig können aber auch sonstige Daten des Unternehmens in das technisch-organisatorische Schutzkonzept des Unternehmens mit eingebunden werden. So schlägt man zwei Fliegen mit einer Klappe.

3.17 Problemzonen im Autohaus: Videogaga 7

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte im Rahmen seiner Tätigkeit ein Autohaus. Die juristische Bewertung ist bislang noch nicht abgeschlossen. Es ist allerdings ersichtlich, dass sich die datenschutzrechtlichen „Problemzonen“ dieses Autohauses nicht von den sonstigen Problemen im Einzelhandel unterscheiden. So ist unter anderem eine umfangreiche Videoüberwachung im Außenbereich eingerichtet, die möglicherweise nicht den gesetzlichen Voraussetzungen entspricht und damit unzulässig ist. Durch eine solche Videoüberwachungsanlage werden personenbezogene Daten erhoben und gespeichert. Dies ist jedoch nur zulässig, wenn die betroffenen Personen in die Datenerhebung und -speicherung eingewilligt haben, was fallbezogen bei der Videoüberwachung wirklichkeitsfremd wäre, oder das Gesetz eine entsprechende Erlaubnisnorm für den konkreten Fall des Einsatzes bereithält. Im hiesigen Fall ist die einschlägige Erlaubnisnorm § 6 b Bundesdatenschutzgesetz (BDSG). Diese regelt den Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen. Zu solchen zählt auch das Areal eines Autohauses, da es

einem nicht näher bestimmbaren Personenkreis zugänglich ist und der Betreiber sogar möchte, dass Kundschaft das Gelände bzw. die Räumlichkeiten betritt. In solchen Bereichen ist eine Videoüberwachung durch ein nicht-öffentliches Unternehmen nur dann zulässig, wenn diese zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke durchgeführt wird und hierfür auch erforderlich ist. § 6 b BDSG stellt daneben noch eine weitere Anforderung an eine zulässige Videoüberwachung: So dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener die Interessen des Videoüberwachenden überwiegen. Hierbei muss der Unternehmer im Vorfeld die beeinträchtigten Interessen der Personen, die zukünftig und gegen seine Interessen an der Videoüberwachung abwägen. Stellt er hierbei fest, dass seine Interessen die der Betroffenen nicht überwiegen könnten, so ist die angedachte Videoüberwachung unzulässig. Mit dieser Anforderung an eine Videoüberwachung in öffentlich zugänglichen Bereichen wirkt der Gesetzgeber flächendeckenden Videoüberwachungen entgegen. Es soll also nur dann eine Videoüberwachung in solchen Bereichen durchgeführt werden, wenn ein wirklich triftiger Grund vorliegt.

Der TLfDI wird nach Abschluss der Prüfung dem Unternehmen mitteilen, welche Mängel festgestellt wurden. Sollte das Unternehmen daraufhin die entsprechenden Mängel nicht beheben, wird der TLfDI dem Unternehmen gegenüber eine Anordnung erlassen, mit der die Beseitigung der Mängel durchgesetzt wird. Darüber hinaus wird, sofern im Ergebnis feststeht, dass die Videoüberwachung in unzulässiger Art und Weise durchgeführt wurde, die Einleitung eines Ordnungswidrigkeitenverfahrens geprüft.

Bevor Investitionen zur Einrichtung einer Videoüberwachungsanlage getroffen werden, sollte genau geprüft werden, ob diese mit dem BDSG vereinbar ist. Hierbei sollte man nicht nur auf die Aussagen des installierenden Unternehmens vertrauen, da diese in erster Linie ihr Produkt und ihre Dienstleistung verkaufen möchte. Stellt der TLfDI später fest, dass die Videoüberwachung nicht mit dem BDSG vereinbar ist, kann dies ein Ordnungswidrigkeitenverfahren nach sich ziehen.
Daher sollte zuvor vom Unternehmen erwogen werden, den TLfDI um eine Stellungnahme zur geplanten Videoinstallation zu bitten.

3.18 Die Pause ist für die Videoüberwachung tabu: Videogaga 8

Die Videoüberwachung war auch Thema bei der Kontrolle eines in der Lebensmittelbranche tätigen Produktionsunternehmens. Neben einer umfangreichen Videoüberwachung innerhalb der Produktionsgebäude waren auch außerhalb des Gebäudes Videokameras angebracht. Dabei muss zunächst darauf hingewiesen werden, dass es sich um ein Unternehmen handelte, welches den Datenschutz ernst nimmt. Dies war bereits daran erkennbar, dass die Videoüberwachung innerhalb des Gebäudes vorbildlich eingerichtet ist. Eine Arbeitnehmerüberwachung findet nicht statt. Alle Bereiche in denen sich Arbeitnehmer aufhalten und aufhalten könnten, sind geschwärzt und damit bereits vom Aufzeichnungsvorgang ausgeschlossen. Die Überwachung richtet sich allein auf die Produktion und ist damit zulässig. Für die Kontrollierenden, die eher weitgehende datenschutzrechtliche Verstöße gewöhnt sind, sehr ungewohnte Umstände. Allerdings sind auch in diesem Betrieb Mängel festgestellt worden: Im Zuge der Einführung eines betriebsweiten Rauchverbots war ein Unterstand für Raucher eingerichtet worden. Allerdings wurde dabei nicht bedacht, dass sich dieser im Aufnahmebereich der Außenkameras befindet. Pausenräume für Arbeitnehmer dürfen selbstverständlich nicht überwacht werden. Ebenfalls war die Aufzeichnungsdauer der gesamten Videoüberwachung zu lang gestaltet. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit steht mit dem Unternehmen in Kontakt, um datenschutzrechtlich konforme Zustände zu erreichen. Sollte dies nicht gelingen, werden entsprechende Maßnahmen per Anordnung auf verwaltungsrechtlichem Wege durchgesetzt werden.

Im Regelfall ist die dauerhafte Videobeobachtung von Arbeitnehmern unzulässig. Dies gilt insbesondere für Rückzugsräume. Dabei kommt es auch nicht darauf an, ob die Videokamera zu diesem Zweck eingerichtet worden ist. Die theoretische Möglichkeit der Beobachtung reicht für einen Verstoß aus.

3.19 Online-Präsenz? Datenschutz nicht vergessen!

In einem kontrollierten Unternehmen, das im Einzelhandel tätig ist, wurde neben dem eigentlichen Ladengeschäft auch ein Online-Handel mit eigener Internetpräsenz betrieben. Die dafür benötigte

Hardware wurde bei einem der vielen Hoster auf dem Markt zusammen mit der Domain angemietet. Datenschutzrechtlich problematisch daran ist, dass jeder Kunde, der über diesen Shop etwas kauft, seine hierfür notwendigen Daten angeben muss. Diese darf zwar der Betreiber des Onlineshops erheben und speichern, allerdings werden in diesem Fall die Daten nicht durch den Betreiber des Shops gespeichert, sondern liegen, zumindest physisch, auf den Festplatten des Hosters. Damit speichert der Hoster personenbezogene Daten für den Betreiber des Onlineshops. Diese Art der Datenverarbeitung ist nur zulässig, soweit zwischen dem Hoster als Auftragnehmer und dem Onlineshopbetreiber als Auftraggeber ein Auftragsdatenverarbeitungsverhältnis nach § 11 Bundesdatenschutzgesetz (BDSG) vereinbart wurde. Sobald also durch die Internetpräsenz personenbezogene Daten verarbeitet werden, muss ein solcher Vertrag geschlossen werden. Der Vertrag hat dem Schriftformerfordernis zu genügen. Dies setzt also voraus, dass der Vertrag in Papierform existiert und von beiden Parteien unterzeichnet wird. Eine E-Mail oder ein Fax genügt dieser Form nicht. Darüber hinaus muss der Gegenstand des Auftrags ausreichend bezeichnet, der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung der Daten, die Art der Daten und die Betroffenen angegeben sein. Die zu regelnden notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG müssen ebenso enthalten sein, wie ein dem Auftraggeber einzuräumendes Kontrollrecht. Auch eine Regelung, die den Auftragnehmer dem Weisungsrecht des Auftraggebers unterwirft und ersteren verpflichtet, Verstöße gegen den Datenschutz seinem Auftraggeber zu melden, muss enthalten sein.

Einen solchen Vertrag hat das Unternehmen mit seinem Hoster nicht geschlossen. Der Thüringer Landesbeauftragte hat das Unternehmen aufgefordert, diesen rechtswidrigen Zustand zu beenden. Dies kann entweder durch Abschalten des Internetshops, den Umzug der Präsenz auf eigene Hardware oder am einfachsten durch Abschluss eines entsprechenden Vertrages über eine Auftragsdatenverarbeitung geschehen.

Jedes Mal, wenn Datenverarbeitungsvorgänge ausgelagert werden und das übernehmende Unternehmen dabei weisungsgebunden bleiben soll, ist ein Vertrag über eine Auftragsdatenverarbeitung zu schließen. Es ist unerheblich, ob die Auslagerung nur vorüberge-

hend, einmal oder regelmäßig erfolgt. Sobald Datenverarbeitungsvorgänge an Dritte gegeben werden, muss ein solcher Vertrag nach § 11 BDGS geschlossen werden.

3.20 Sagst Du es mir nicht, frag‘ ich jemand anderen

Die Mutter eines Betroffenen hat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf ein Gebaren der Arbeitgeberin ihres Sohnes aufmerksam gemacht, welches nicht mit dem Bundesdatenschutzgesetz (BDSG) zu vereinbaren war.
Der Arbeitgeber hatte dem Arbeitnehmer gekündigt. Dieser stellte im Rahmen eines Kündigungsschutzprozesses den Antrag auf Feststellung der Unwirksamkeit eben jener Kündigung. Um sich nunmehr seiner Beweisnot (der Arbeitgeber ist für die Darlegung der Kündigungsgründe beweisbelastet) zu entziehen, nutzte der Arbeitgeber personenbezogene Daten des Arbeitnehmers, die er bei einem weiteren Arbeitnehmer erhoben oder von diesem erlangt hat.
Der TLfDI nahm sodann dahingehend Stellung, dass, soweit die personenbezogenen Daten bei einem Dritten erhoben wurden, dies gegen den Grundsatz der Direkterhebung (beim unmittelbar Betroffenen, dem Sohn) verstoße. Der Gesetzgeber hat die Erhebung von personenbezogenen Daten eines Betroffenen bei Dritten nur in abschließend geregelten Fällen zugelassen, die hier nicht greifen, § 4 Abs. 2 BDSG. Folge sei eine rechtswidrige Erhebung, weswegen auch die darüber hinausgehende Nutzung der Daten unzulässig sei.
Das Gericht nahm die Stellungnahme des TLfDI, die durch den Kläger in den Prozess eingeführt wurde, zur Kenntnis. Allerdings gelangte das Gericht zur Überzeugung, dass die personenbezogenen Daten der beklagten Arbeitgeberin ohne eigenes Zutun durch einen Dritten zugespielt wurden. Mit anderen Worten, nach Feststellung des Gerichts hat die Beklagte die Herausgabe der Daten an sie weder verlangt noch sonst wie gefördert. Damit handelt es sich nicht um eine Erhebung, weswegen auch nicht gegen den Direkterhebungsgrundsatz verstoßen werden kann. Gleichwohl hat sich das Gericht auf Grund der Stellungnahme des TLfDI entschieden, den entsprechenden personenbezogenen Daten eine untergeordnete Rolle zuzuordnen. Dies ist umso mehr begrüßenswert, als dass das Gericht an Aussagen des TLfDI gegenüber einer Prozesspartei ohnehin nicht

gebunden ist und einfache Rechtsverstöße im Zivilrecht kein Beweisverwertungsverbot nach sich ziehen.
Ebenso wie das Gericht nicht an die rechtliche Bewertung des TLfDI gebunden ist, ist dieser auch nicht an die Verlautbarungen des Gerichts gebunden. In einem Ordnungswidrigkeitenverfahren wird derzeit der für den TLfDI maßgebliche Sachverhalt erforscht.

Personenbezogene Daten dürfen grundsätzlich nur beim Betroffenen direkt erhoben werden. Die hiervon zu machenden Ausnahmen sind vom Gesetzgeber in § 4 Abs. 2 BDSG geregelt. So darf man hiervon abweichen, wenn der Gesetzgeber dies in einem anderen Gesetz ausdrücklich geregelt hat oder wenn die Erhebung beim Betroffenen mit einem unverhältnismäßigen Aufwand verbunden ist. Letztere Variante ist aber nur sehr eingeschränkt anwendbar und mit einer strengen Verhältnismäßigkeitsabwägung verbunden.
Wird gegen diesen Direkterhebungsgrundsatz verstoßen, führt dies zur Rechtswidrigkeit der Datenerhebung und deren Nutzung bzw. Speicherung. Ein Ordnungswidrigkeitenverfahren kann die Folge sein.

3.21 Aus der Röhre geguckt: Videogaga 9

Aufgrund eines Hinweises erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon, dass in einem Unternehmen im Raucherraum eine Kamera versteckt angebracht sein sollte. Eine Kontrolle vor Ort ergab, dass es sich um eine Videokamera handelte, die in einer in den Pausenraum ragenden Rohrhülse verborgen war. Dem Unternehmen wurde mitgeteilt, dass der Einsatz dieser Kamera mit dem geltenden Datenschutzrecht nicht vereinbar ist. Eine Videoüberwachung ist nur dann möglich, wenn das Gesetz eine entsprechende Erlaubnisnorm bereithält. Dies deshalb, weil das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig ist, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat eingewilligt (sogenanntes Verbot mit Erlaubnisvorbehalt).
Eine Einwilligung der Arbeitnehmer lag selbstverständlich nicht vor, sie wäre auch unwirksam gewesen, da es im Beschäftigungsverhältnis in der Regel an der Freiwilligkeitsvoraussetzung des § 4 a Absatz 1 Satz 1 BDSG fehlt. Da es sich bei dem Raucherraum

in einem Unternehmen nicht um öffentlich-zugänglichen Raum handelt, kommt als Erlaubnisnorm nicht § 6 b BDSG, sondern nur § 32 BDSG in Betracht. Nach dieser Vorschrift können personenbezogene Daten eines Arbeitnehmers für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Diese Voraussetzungen sind in den allermeisten Fällen der Arbeitnehmerüberwachung nicht gegeben. So auch im vorliegenden Fall. Eine heimliche Videoüberwachung ist nur in absoluten Ausnahmefällen zulässig. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Arbeitnehmers nach § 32 Abs. 1 Satz 2 BDSG nur dann erhoben, verarbeitet oder genutzt werden, wenn vorab zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Arbeitnehmers an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. In der Abwägung wird auch gewichtet, ob den Arbeitnehmern überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich verbleibt. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind ebenfalls von der Überwachung auszunehmen.
Die Kamera wurde laut Aussage des Unternehmens nicht mehr genutzt. Auch wenn eine ungenutzte Kamera keine Daten erhebt, ist sie dennoch unzulässig (siehe hierzu näher Punkt 3.22).
Bei der Vorort-Kontrolle teilte das Unternehmen mit, die Kamera abbauen zu wollen. Dies ist mittlerweile geschehen.

Eine heimliche Videoüberwachung von Arbeitnehmern ist nur in absoluten Ausnahmefällen zur Aufdeckung von Straftaten zulässig. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind von der Überwachung stets auszunehmen.

3.22 Videokameras fast im Wohnzimmer: Videogaga 10

Ganz soweit ist es noch nicht, dass Eigentümer versuchen, Videokameras in den Wohnungen ihrer Mieter unterzubringen. Allerdings hat die digitale Revolution auch nicht vor Wohnblöcken halt gemacht. Vielerorts werden Videokameras in Wohnanlagen installiert, oftmals, ohne dass sich die verantwortliche Stelle Gedanken über die datenschutzrechtliche Zulässigkeit solcher Einrichtungen macht.
Etwas harmloser stellte sich ein Fall dar, der dem TLfDI 2012 zur Bearbeitung vorlag. Auf einen Hinweis hin wurde ein Wohnhaus kontrolliert, welches umfangreich videoüberwacht sein sollte. Tatsächlich wurde im Rahmen der Kontrolle allerdings lediglich eine Kamera festgestellt. Noch dazu war diese nicht einmal in Betrieb. Vielmehr sollte sie als Attrappe eingesetzt werden. Positioniert war die Kamera im Eingangsbereich, wo sich ebenfalls die Klingeltafel sowie die Concierge befanden.
Datenschutzrechtlich sind Videoaufnahmen in Wohnhäusern alles andere als einfach und von Einzelfall zu Einzelfall differenziert zu betrachten. Je nach den festgestellten Umständen finden unterschiedliche, im Bundesdatenschutzgesetz (BDSG) befindliche Normen Anwendung, die die (Un-)Zulässigkeit der jeweiligen Videoüberwachung regeln.
Um das Ergebnis vorweg zu nehmen: Im hiesigen Fall erachtete der TLfDI die eingesetzte Kameraattrappe für zulässig. In ihrer datenschutzrechtlichen Prüfung unterscheiden sich solche Attrappen aber kaum von richtigen Kameras. Dies liegt daran, dass es subjektiv für den Betroffenen keinerlei Unterschied macht, ob eine Kamera in Betrieb oder ausgeschaltet ist. Denn dieser Zustand ist von Außen nicht erkennbar, womit der Überwachungsdruck für den Betroffenen gleichbleibt. Dieser Überwachungsdruck hat in der Regel eine Verhaltensänderung zur Folge, was wiederum einen Eingriff ins allgemeine Persönlichkeitsrecht darstellt. Nach § 1 Abs. 1 BDSG ist Zweck dieses Gesetzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Da durch die täuschend echte Simulation (Attrappe) des Umgangs mit personenbezogenen Daten auch eine Beeinträchtigung des Persönlichkeitsrechts gegeben ist, sind die Grundsätze des BDSG entsprechend heranzuziehen.
Allerdings konnte in diesem Fall nachgewiesen werden, dass im Vorfeld in Form von wiederholtem Vandalismus und ähnlichen

Vorkommnissen zu Lasten des Eigentümers große Schäden entstanden sind, die auch eine echte Kamera zur Ausübung des Hausrechts rechtfertigen würden. Die Videoüberwachung ist zulässig, wenn der Vermieter schwerwiegende Beeinträchtigungen seiner Rechte auf diese Weise verhindern kann und das Recht des Mieters, sich in sämtlichen allen Bewohnern zugänglichen Bereichen unbeobachtet zu bewegen, nicht überwiegt. Die im Einsatz befindliche Videoattrappe im Haupteingangs- und Conciergebereich erschien unter Berücksichtigung der dargelegten bisherigen Schäden und Vorkommnisse in dem Gebäude als zulässig.

Kameras in Wohnbereichen sind wegen des besonders privaten Aufstellungsorts aus datenschutzrechtlicher Sicht besonders heikel. Die Beurteilung der datenschutzrechtlichen Zulässigkeit ist kompliziert, da die rechtliche Einordnung von unterschiedlichen Umständen des Einzelfalls abhängig ist. Zulässig kann eine Kamera im Eingangsbereich sein, wenn es zuvor zu wiederholtem Vandalismus und ähnlichen Vorkommnissen gekommen ist.

3.23 Der betriebliche Datenschutzbeauftragte – woher nehmen?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte ein IT-Unternehmen, dessen primäres Aufgabenfeld in der Auftragsdatenverarbeitung für andere Unternehmen liegt. Die Kontrolle verlief erfreulich, die juristische Prüfung ist noch nicht abgeschlossen, aber soweit ersichtlich, ergaben sich mit einer Ausnahme aus datenschutzrechtlicher Sicht keine tiefgreifenden Bedenken. Das Angebot des Unternehmens beinhaltet auch Dienstleistungen für Auftraggeber, die als automatisierte Datenverarbeitung unter Umständen einer Vorabkontrolle unterfallen. Dabei handelt es sich in der Regel um automatisierte Verfahren, die in besonderem Maße in Grundrechte Betroffener eingreifen. In solchen Fällen verlangt das Bundesdatenschutzgesetz auch vom Auftragnehmer eines solchen Vertragsverhältnisses, dass dieser einen betrieblichen Datenschutzbeauftragten beschäftigt und zwar, ohne dass es irgendwelcher Mindestanzahlen von Arbeitnehmern bedarf, § 4 f Abs. 1 Satz 6 Bundesdatenschutzgesetz (BDSG).
Zwar hat das kontrollierte Unternehmen einen betrieblichen Datenschutzbeauftragten bestellt, jedoch handelt es sich hierbei um einen der Geschäftsführer, die gleichzeitig auch die einzigen Arbeitnehmer

des Unternehmens darstellen. Genau hierin liegt die Krux. An einen betrieblichen Datenschutzbeauftragten werden zwar keine besonderen Voraussetzungen im Sinne einer besonderen Ausbildung gesetzt, jedoch verlangt das Gesetz in § 4 f Abs. 2 BDSG, dass dieser die erforderliche fachliche Eignung und Zuverlässigkeit besitzt. An der fachlichen Eignung des Geschäftsführers war nichts auszusetzen, doch gehört zur Zuverlässigkeit eines betrieblichen Datenschutzbeauftragten, dass dieser eine gewisse Unabhängigkeit besitzt. Nicht ohne Grund kann einem solchem Datenschutzbeauftragten auch nur unter sehr strengen Voraussetzungen gekündigt werden. Stellt nun ein Mitglied der Geschäftsführung den betrieblichen Datenschutzbeauftragten, ist zumindest ein Interessenkonflikt zwischen den Interessen der Geschäftsführung und denjenigen des Datenschutzes nicht auszuschließen. Daher geht die herrschende Meinung und mit dieser der TLfDI davon aus, dass es in einer solchen Konstellation an der notwendigen Zuverlässigkeit des betrieblichen Datenschutzbeauftragten mangelt. Rechtsfolge ist, dass die Abberufung des betrieblichen Datenschutzbeauftragten verlangt werden kann. Außerdem folgt aus den hier dargestellten Umständen, dass Unternehmen, die nur aus geschäftsführenden Gesellschaftern bestehen, aber gleichzeitig der Bestellung eines Datenschutzbeauftragten bedürfen, entweder für diese Aufgabe einen Arbeitnehmer einstellen oder diese Aufgabe extern vergeben müssen. Sollte die derzeitige Annahme des TLfDI auch nach Abschluss der juristischen Prüfung weiter bestehen, so wird dieser dem Unternehmen gegenüber anordnen, einen Datenschutzbeauftragten wirksam zu bestellen. Darüber hinaus muss das Unternehmen in diesem Fall mit der Einleitung eines Ordnungswidrigkeitenverfahrens rechnen.

Es ist von unbedingter Wichtigkeit, dass Unternehmen selbstständig prüfen, ob sie einen betrieblichen Datenschutzbeauftragten benötigen. Zwar wird auch der TLfDI eine Notwendigkeit der Bestellung feststellen, jedoch ist eine solche mit erheblichen Verwaltungskosten verbunden und kann ein empfindliches Bußgeld nach sich ziehen. Die gesetzlichen Vorschriften zur Bestellungspflicht sind jedoch umfangreich und auch nicht nur von einer Norm abhängig. In nicht eindeutigen Fällen sollte folglich fachkundiger Rat eingeholt werden, gerne auch beim TLfDI. Um ein Bußgeld zu vermeiden, müssen Unternehmen spätestens einen Monat nach Aufnahme Ihrer Tätigkeit

einen Datenschutzbeauftragten bestellt haben, sofern das Gesetz ihnen dies vorschreibt.

3.24 Der Anwalt, nicht immer dein Freund und Helfer – von fragwürdigen Praktiken dubioser Verbraucherschützer und Rechtsanwaltskanzleien

Kommt Ihnen der nachfolgende Sachverhalt vielleicht bekannt vor? Sie waren bis vor kurzem Kunde einer Bank, die nun insolvent ist. Allein das ist meistens schon ein Umstand, der mit nicht wenig Bürokratie und vielen Terminen für Sie verbunden ist. Zu allem Überfluss bekommen Sie dann aber noch ein wenig später Post von einem eingetragenen Verein, der sich, wie sein Name suggeriert, den Verbraucherschutz auf die Fahnen geschrieben hat. Dieser Verein teilt Ihnen mit, dass Sie Kunde der insolventen Bank gewesen sind und er, der Verein, gern bereit ist, nicht nur Ihre Interessen, sondern die Belange vieler weiterer Kunden zu vertreten. Nur gemeinsam sei man stark, um viel versprechende Schadensersatzklagen gemeinsam zu meistern. Ihr gesunder Menschenverstand schaltet sich ein und Sie stellen sich die nahe liegende Frage: Woher haben die meine personenbezogenen Daten? Ihr darauf folgender Anruf bei dem freundlichen Verein bringt immerhin insoweit Klarheit, als dass eine Datenspeicherung lediglich bei dem Auftraggeber des Vereins, einer Rechtsanwaltskanzlei erfolgte. Auf Ihre darauf folgende E-Mail und Anfrage an die Rechtsanwaltskanzlei, woher diese denn bitteschön Ihre personenbezogenen Daten habe, erklärt man Ihnen von dort lapidar: Als Mandant würden Sie in der Rechtsanwaltskanzlei nicht geführt. Soweit im Rahmen der Mandatsbearbeitung zusätzliche Daten Dritter – also auch von Ihnen – gespeichert würden, entstammten diesen öffentlichen Registern bzw. den einsehbaren Unterlagen der Insolvenzgerichte. Eine Nutzung dieser Daten erfolge ausschließlich im Rahmen der Interessenwahrnehmung für Mandanten als geschädigte Kapitalanleger.
An dieser Stelle wird der Sachverhalt auch für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) interessant. Denn auch in Thüringen haben sich im Berichtszeitraum mehrere Kunden von Banken oder Beteiligungsfonds, die genau denselben Sachverhalt erlebt hatten, an den TLfDI gewandt und ihn gebeten, zu klären, woher die Rechtsanwaltskanzlei

bzw. der „dazwischengeschaltete“ Verein, die personenbezogenen Daten erhalten haben.
Der TLfDI hat mit den ihm zur Verfügung stehenden Mitteln versucht aufzuklären, auf welchem Wege die Rechtsanwaltskanzlei die personenbezogenen Daten erhalten hat. Oftmals waren ihm im Ergebnis aber die Hände aus folgenden Gründen gebunden: Dem TLfDI steht im Ergebnis kein Auskunftsanspruch aus § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) gegenüber einer Rechtsanwaltskanzlei zu. Dies ergibt sich aus § 1 Abs. 3 Satz 2 BDSG, der bestimmt, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vom BDSG unberührt bleiben. Genau eine solche Verschwiegenheitspflicht hat das Kammergericht Berlin (Entscheidung vom 20. August 2010 – Aktenzeichen 1 Ws (B) 51/07 – 2 Ss 23/07) aus § 43 a Abs. 2 Satz 1 und 2 der Bundesrechtsanwaltsordnung (BRAO) jedoch abgeleitet. Diese Regelungen lauten: „Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist.“
Diese Regelung, die grundsätzlich ihre Berechtigung hat, weil der Rechtsanwalt ein Organ der Rechtspflege ist (§ 1 BRAO), hatte in den konkreten Fällen aber zur Folge, dass dem TLfDI nach Abschluss seiner Recherchen nur die Möglichkeit blieb, die betreffenden Bürgerinnen und Bürger an die Rechtsanwaltskammer Thüringen zu verweisen, um dort noch einmal ihren Sachverhalt vorzutragen. Denn die Rechtsanwaltskammern sind für die Einhaltung des Standesrechts der Rechtsanwälte und die Kontrolle der anwaltlichen Schweigepflicht zuständig.
Abschließend sei noch einmal festgehalten: Es ist nicht die Absicht des TLfDI, an dieser Stelle „einen Stab“ über die redlichen Thüringer Rechtsanwälte zu brechen. Allerdings sind die wenigen „schwarzen Schafe“ unter den Rechtsanwälten in akuter Erklärungsnot, wenn Sie im Rahmen von Akteneinsichten bei Gerichten und Staatsanwaltschaften die kompletten Listen von Bankkunden oder Investoren finden, diese dann zur Akquise neuer Mandanten verwenden und zwecks Ablenkung darüber einen Verein „zwischenschalten“.
Dem TLfDI bleibt es natürlich unbenommen, Rechtsanwaltskanzleien einer datenschutzrechtlichen Kontrolle zu unterziehen.

Wenn Sie auch Post von einem Verbraucherschutzverein erhalten, der Sie als geprellten Bankkunden oder Gesellschafter eines Fonds bei der Wahrnehmung Ihrer rechtlichen Interessen unterstützen will, dann seien Sie auf der Hut. Fragen Sie schriftlich bei dem Verein an, woher dieser Ihre personenbezogenen Daten generiert hat. Verweist der Verein Sie darauf hin an eine Rechtsanwaltskanzlei, so wenden Sie sich in Thüringen an die Rechtsanwaltskammer Thüringen, Bahnhofstraße 46, 99084 Erfurt, damit diese Ihren Fall standesrechtlich überprüfen kann.

3.25 Patientendaten – ab in die blaue Tonne?

Aufgrund einer Beschwerde wurde eine Arztpraxis in Hinblick auf die Einhaltung datenschutzrechtlicher Vorschriften gerade in Bezug auf die ordnungsgemäße Entsorgung und Vernichtung von Dokumenten mit Patientendaten kontrolliert. Angeblich hätten sich in der im Hof frei zugänglichen Papiertonne Patientendaten befunden. Dieser Vorwurf hat sich bei der Kontrolle nicht bestätigt.
Trotzdem soll an dieser Stelle darauf hingewiesen werden, dass bei hochsensiblen Patientendaten, die aufgrund ihrer Schutzbedürftigkeit einem sehr hohen Vertraulichkeitsgrad unterfallen, strenge Anforderungen an die Entsorgung zu stellen sind. Daten auf Papier, welche Rückschlüsse auf bestimmte oder zumindest bestimmbare Personen zulassen, dürfen keinesfalls nach dem Motto: "zerreißen und ab in den Papierkorb" entsorgt werden. Bei Arztpraxen gilt dies insbesondere für Altakten, vertippte Briefe mit bereits ausgefülltem Adresskopf, nicht brauchbare Kopien, fehlerhaft ausgefüllte Rezepte und Überweisungsträger. Es ist notwendig, dass diese Dokumente stets so geschreddert werden, dass eine Wiederherstellung des Inhaltes dauerhaft unmöglich gemacht wird und die einzelnen Papierstücke in keinen Zusammenhang mehr gebracht werden können. Bei der Auswahl des Gerätes ist der erhöhte Vertraulichkeitsgrad der Dokumente ausschlaggebend. Es ist daher notwendig, dass in Arztpraxen Aktenvernichtungsgeräte verwendet werden, die nach der alten DIN-Norm 32757 mindestens die Sicherheitsstufe 4 oder nach der neuen DIN 66399-1 mindestens die Sicherheitsstufe P-5 aufweisen. Erst nach einer solchen Vernichtung ist eine Entsorgung der verbleibenden Papierstücke in der blauen Tonne möglich. Zu beachten ist auch, dass das Sammeln von zu vernichtendem Datenmaterial immer in Behältern erfolgen soll, die vor unbefugtem Zugriff geschützt sind.

Zudem sollte eine schriftliche Dienstanweisung an alle Arbeitnehmer erfolgen, in welcher alle Maßnahmen für eine ordnungsgemäße Entsorgung festgelegt werden. Weitergehend sollte auch deren Einhaltung in regelmäßigen Abständen durch die Ärzte kontrolliert werden. Sollten sowohl größere Datenmengen oder auch nur einzelne Dokumente mit personenbezogenen Daten nicht ordnungsgemäß vernichtet worden sein, so können Ärzten neben Sanktionen nach dem Bundesdatenschutzgesetz, auch die strafrechtliche Verfolgung nach § 203 Strafgesetzbuch (StGB) i. V. m. § 9 der Berufsordnung der Landesärztekammer Thüringen auch ein Berufsverbot gemäß § 70 StGB drohen. Sollte seitens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit ein solcher Verstoß bei einem Arzt oder Krankenhaus festgestellt werden, wird dieser grundsätzlich der zuständigen Staatsanwaltschaft weitergeleitet.

An eine ordnungsgemäße Vernichtung und Entsorgung von Patientendaten sind besonders strenge Anforderungen zu stellen. Es ist notwendig, dass Dokumente stets so geschreddert werden, dass eine Wiederherstellung dauerhaft unmöglich gemacht wird. In Arztpraxen müssen Aktenvernichtungsgeräte mit mindestens der Sicherheitsstufe 4 der alten DIN-Norm 32757 oder nach der neuen DIN 66399-1 mindestens die Sicherheitsstufe 5 verwendet werden.

3.26 Patientenarmbänder

Nachdem in der örtlichen Presse darüber berichtet wurde, dass in einem Krankenhaus ab sofort alle Patienten mit einem Patientenarmband versehen werden sollen, ging der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) der Sache nach. Zwar ist ein solches Patientenarmband für das Krankenhaus durchaus praktisch. So kann beispielsweise jederzeit festgestellt werden, um welchen Patienten von welcher Station es sich handelt. Dies kann in Fällen, in denen der Patient nicht selbst kommunizieren kann, äußerst wichtig sein. Allerdings ist der Einsatz von Patientenarmbändern aus datenschutzrechtlicher Sicht kritisch zu prüfen, denn die Angaben, die auf dem Patientenarmband gemacht werden, sind grundsätzlich für alle Personen im Krankenhaus, also auch die Mitpatienten und die Besucher, sichtbar. Es ist daher unzulässig, medizinische Informationen, beispielsweise die Zugehörigkeit zu einer bestimmten Station, offen sichtbar auf dem Patientenarmband fest-

zuhalten. Nach § 27 Abs. 3 Satz 1 Thüringer Krankenhausgesetz dürfen Patientendaten nur genutzt werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses erforderlich ist. Die Mitteilung medizinischer Informationen mittels eines Patientenarmbands ist hierzu nicht erforderlich. Auch zur Identifikation ist ein solches Patientenarmband in aller Regel nicht erforderlich, denn die Patienten können im Normalfall selbst die nötigen Angaben machen. Auf Nachfrage teilte das Krankenhaus mit, dass das Tragen des Armbandes freiwillig sei. Der Patient müsse vorab einwilligen. Diese Einwilligung könne auch jederzeit widerrufen werden. Auf dem Armband selbst befinden sich lediglich der Name des Patienten sowie sein Geburtsdatum und ein Strichcode, der der eindeutigen Identifizierung des Patienten dient. Aufgrund der Freiwilligkeit des Angebots und der Tatsache, dass keine medizinischen Informationen aus den auf dem Armband befindlichen Angaben ersichtlich sind, war das Vorhaben aus datenschutzrechtlicher Sicht nicht zu bemängeln.

Patientenarmbänder dienen der Sicherheit der Patienten und dem reibungslosen Ablauf im Krankenhaus. Der Einsatz ist aber nur zulässig, wenn er datenschutzgerecht gestaltet ist und insbesondere keine Gesundheitsdaten auf dem Patientenarmband preisgegeben werden.

3.27 Dashcam – Trashcam: Videogaga 11

Auto, Fahrrad, LKW;
die Dashcam ist dabei – oje.
davor, dahinter, nebendran,
Personen, Unfall, Autobahn,
Dashcam zeichnet's auf – ein Wahn.

Tatsächlich, und da herrscht Einigkeit,
verfehlt sie die Datenschutz-Zulässigkeit.
Zwar sind schon von Gesetzes wegen
Ausnahmetatbestände vorgegeben,
das Filmen in Familienkreisen
sowie auch von privaten Reisen,
dem Bundesdatenschutz entreißen.

Dashcams muss man,
das sollte man wissen,
nach dem BDSG besser doch missen.
Das Filmen von Unfällen, eigenen - fremden,
um das dann vor Gericht zu verwenden,
ist keine persönliche Tätigkeit,
die vom Anwendungsbereich befreit.

Vom Filmen von öffentlichen Räumen,
darf der Einzelne nur träumen,
es sei denn, man hat das Hausrecht inne
und dieses dabei auch im Sinne.
Ebenfalls, so die Gesetze,
kann aus berechtigtem Interesse
dann aber nur zu bestimmtem Zwecke
die Kamera an des Hauses Ecke.

Darüber hinaus, man glaubt es kaum,
sind schutzwürdige Interessen im Raum.
Erst wenn keine Punkte vorliegen,
dass diese Interessen nicht überwiegen,
wird es mit der Filmerei
mehr als nur `ne Träumerei.

Beim Autofahren, so sei bedacht,
ist die Kamera damit nicht angedacht,
so liegt es nach Natur der Dinge,
auf der Straße wird’s mit dem Hausrecht dünne.
Zwar sind fürs Filmen die eig‘nen Interessen
des Autofahrers nicht sogleich vermessen,
doch beim Aufnehmen anderer im Verkehr,
ist für jeden erkennbar gar nicht schwer,
dass Anhaltspunkte sind vorhanden
für‘s Überwiegen der Interessen der and‘ren,
nämlich gerade auch der Passanten.

Wegen des hier Erreimten sei dem Bürger gesacht,
dass der Datenschützer über den Datenschutz wacht.
Der Verstoß, wie grade berichtet,

wird gern mit Bußgeldern gerichtet.
Daher hier noch ein letzter Satz:
Lieber Besitzer einer Dashcam,
diese gehört ganz schnell in die Trashcan!

Jetzt mal ohne Flachs: Das Betreiben von Autokameras, auch bekannt als Dashcams, insbesondere zum Zwecke der Beweissicherung im Falle eines Unfalls, fällt nicht in den Ausnahmetatbestand der persönlichen oder familiären Tätigkeit, § 1 Abs. 2, Nr. 3 Bundesdatenschutzgesetz (BDSG). Damit ist das BDSG anwendbar und solche Kameras sind nur nach Maßgabe des § 6 b BDSG zulässig. Dessen Voraussetzungen sind jedoch unter keinem Gesichtspunkt erfüllt, da zumindest immer Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen, was absolutes Ausschlusskriterium für die Beobachtung öffentlich zugänglicher Räume ist.
Damit handelt es sich bei solchen Aufnahmen um ein unerlaubtes Erheben und Speichern von personenbezogenen Daten, was als Ordnungswidrigkeit mit einem Bußgeld von bis zu 300.000 € geahndet werden kann.

3.28 Feuermelder mit Augen: Videogaga 12

Über einen anonymen Hinweisgeber wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) der Tipp gegeben, dass ein Arbeitgeber in der Umkleidekabine mit angeschlossenem Duschraum seines Unternehmens eine verdeckte Videoüberwachung – getarnt als Rauchmelder – durchführen würde.
Am Folgetag hat der TLfDI eine vor Ort Kontrolle durchgeführt. Nachdem man die Arbeitnehmer des TLfDI widerwillig auf das Betriebsgelände ließ, musste allerdings festgestellt werden, dass der entsprechende Umkleideraum über Nacht umfassend renoviert wurde. Es roch sogar noch nach Farbe.
Im darauf folgenden Verwaltungsverfahren konnte festgestellt werden, dass der Arbeitgeber mit der Videokamera Einbrüche in die Spinde seiner Arbeitnehmer aufklären wollte. Die Kamera wurde nach einem dokumentierten Einbruch installiert. Es handelte sich dabei um ein sogenanntes Blackbox-System. Die Kamera zeichnete auf eine angeschlossene Festplatte auf, nach 48 Stunden wurde der Speicherinhalt überschrieben, an einen anderen Ort wurden die auf-

genommenen Bilder nicht übermittelt. Insgesamt wurde die Kamera etwa zwei Wochen betrieben. In diesem Zeitraum kam es erneut zu einem Einbruch, die Festplatte wurde ausgebaut, durch ein Fachunternehmen ausgewertet, der Täter ermittelt und ihm gekündigt. Nach dem Vorfall wurde die Festplatte bis jetzt nicht wieder eingebaut. Was vorbildlich klingen mag, ist es leider manchmal nicht, so auch in diesem Fall. Auch wenn aus Sicht des Arbeitgebers alles wunderbar geklappt hat, sind auch im Bereich des Arbeitsverhältnisses datenschutzrechtliche Vorschriften zu beachten. Nicht alles, was zweckmäßig erscheint, ist auch zulässig.
Zwar sieht § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz explizit die Datenerhebung zu Zwecken der Aufklärung von Straftaten im Beschäftigungsverhältnis vor, jedoch sind diese auch nur unter besonderen Voraussetzungen zulässig. Dabei fließt auch mit ein, dass eine Videoüberwachung in einem Umkleideraum anders zu bewerten ist, als eine Videoüberwachung in einem Kassenbereich.
So darf eine heimliche Videoüberwachung nur dann durchgeführt werden, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Bereits der letzte Punkt ist in dieser Konstellation nicht gegeben. Eine verdeckte Videoüberwachung in einem Umkleideraum, der für eine Komplettentkleidung vorgesehen ist, ist fast immer unverhältnismäßig, da hier in einem Maße in die Intim- und damit Persönlichkeitssphäre der Betroffenen eingegriffen wird, die eine Abwägung zu Gunsten der Interessen des Überwachenden fast unmöglich macht. Darüber hinaus wurden in diesem Fall jedenfalls nicht alle anderen Mittel zur Aufklärung ausgeschöpft. Ein Ordnungswidrigkeitenverfahren wurde eingeleitet.

Die (verdeckte) Überwachung von Arbeitnehmern ist nur unter bestimmten Aspekten zulässig und Arbeitgeber müssen beachten, dass die Anforderungen hierfür hoch sind und weiter steigen, je mehr sie in den Intimbereich Ihrer Arbeitnehmer eingreifen. Empfohlen wird, vor der Installation von Videoanlagen den TLfDI um eine Stellungnahme zu bitten.

3.29 Seniorenwohnheim – datenschutzrechtlich keine Idylle

Anlässlich eines Fundes von in einer Plastiktüte verstauten Gesundheitsdaten über Bewohner eines Seniorenheimes unterzog der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das in Frage kommende Heim einer datenschutzrechtlichen Kontrolle. Hierbei offenbarten sich mehrere datenschutzrechtliche Verstöße: Zum einen mangelte es an einem Datenschutzbeauftragten (§ 4 f Bundesdatenschutzgesetz [BDSG]); zum anderen wurden sämtliche (!) Daten des Seniorenwohnheims an den Mutterkonzern übermittelt, obwohl ein Vertrag zur Auftragsdatenverarbeitung (§ 11 BDSG) nicht existierte. Ein solcher Vertrag existierte ebenfalls nicht hinsichtlich der Inanspruchnahme einer Firma zur Abwicklung von Zahlungsvorgängen. Schließlich mangelte es in erheblichem Umfang an der Festlegung technisch-organisatorischer Maßnahmen (§ 9 BDSG) zur Gewährleistung der Ausführung der Vorschriften des BDSG. Die Leitung des Seniorenwohnheims wurde gebeten, die datenschutzrechtlichen Mängel abzustellen. Der Träger des Seniorenwohnheims hat sich Beistand bei einem Rechtsanwalt gesucht.

Auch Seniorenwohnheime – sofern als nicht-öffentliche Stelle betrieben – unterliegen den Anforderungen des BDSG. Regelungen des BDSG unter anderem zu technisch-organisatorischen Maßnahmen (§ 9 BDSG), zur Auftragsdatenverarbeitung (§ 11 BDSG) und zur Bestellung eines Datenschutzbeauftragten (§ 4 f BDSG) sind einzuhalten.
Datenschutzrechtliche Ordnungswidrigkeits- oder Strafverfahren sind auch hier nicht ausgeschlossen.

3.30 Veröffentlichung personenbezogener Daten auf Gegnerliste durch Kanzlei

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage, inwieweit eine Rechtsanwaltskanzlei berechtigt sei, Firmennamen auf einer Gegnerliste zu veröffentlichen.
Eine Gesellschaft bürgerlichen Rechts (GbR) begehrte bei einer Rechtsanwaltskanzlei die Löschung des GbR-Namens von der Inter-

netpräsenz der Kanzlei. Die GbR war zuvor in die Liste der Gegner der Rechtsanwaltskanzlei auf deren Internetseite mit ihrem Firmennamen namentlich aufgenommen worden. Die Mitglieder der GbR befürchteten berufliche und private Nachteile durch die Nennung auf der Internetseite.
Insoweit wurde der TLfDI um datenschutzrechtliche Prüfung sowie Auskunft zur Rechtslage ersucht.
Das Bundesverfassungsgericht (BVerfG) hat in der Entscheidung vom 12. Dezember 2007 (1 BvR 1625/06) die Frage der Werbung mit Gegnerlisten behandelt und die sachliche und unkommentierte Benennung von Unternehmen in Gegnerlisten zu Werbezwecken erlaubt.
Darüber hinaus wurde klargestellt, das allgemeine Persönlichkeitsrecht etwaiger betroffener Firmen werde durch eine solche Nennung nicht verletzt. Das BVerfG hat in seiner Entscheidung anerkannt, dass ein berechtigtes Informationsinteresse potentieller Mandanten zu der Frage, über welche Erfahrung eine Kanzlei bzw. ein Rechtsanwalt verfügt, besteht. Schließlich begründet das BVerfG seine Entscheidung mit dem Grundrecht der Berufsfreiheit, das auch die freie Entscheidung über die Art und Weise der beruflichen Außendarstellung schütze.
Die Gegnerliste auf der Homepage der Rechtsanwaltskanzlei enthielt keine Wertungen dahingehend, dass eventuell ausgesprochene Abmahnungen oder Forderungen an die Fima sowie an die anderen in der Liste genannten Gegner berechtigt oder unberechtigt waren. Dies wurde auch ausdrücklich in der Kopfzeile der Gegnerliste klargestellt. Unter dem Link war lediglich eine – nicht abschließende – Liste von Gegnern veröffentlicht. Dabei ging es um urheber- und medienrechtliche Angelegenheiten. Nach außen sollte diese Liste darstellen, gegen welche Gegner eine Beratung, eine außergerichtliche oder auch gerichtliche Vertretung der Mandantschaft erfolgt war und damit die Erfahrungen der Rechtsanwälte auf diesem Rechtsgebiet widerspiegeln.
Eine solche Nutzung wurde durch das BVerfG als zulässig erachtet.
Aus datenschutzrechtlicher Sicht konnte daher keine Löschung des Firmennamens von der Gegnerliste der Rechtsanwaltskanzlei erwirkt werden.

Das Bundesverfassungsgericht hält (Aktenzeichen 1 BvR 1625/06) die wertungsfreie Nutzung von Firmennamen auf sogenannten Gegnerlisten von Rechtsanwälten für zulässig.
Das Namensrecht als Teil des allgemeinen Persönlichkeitsrechts ist hier im Rahmen der konkreten Bewertung von untergeordneter Bedeutung, da gerade juristische Personen und Personengesellschaften (beispielsweise auch die GbR) sich über einen öffentlichen Auftritt im Geschäftsleben (beispielsweise über Internetseiten) definieren. Insoweit gilt der Grundsatz über die Selbstbestimmung einer Nutzung des Namens (Zeit, Ort und Medium) nur eingeschränkt.

3.31 Ein Autohaus in den Fängen des Autokonzerns: Videogaga 13

Bei der Kontrolle des Autohauses kamen vielschichtige Datenschutzprobleme zum Vorschein. Es wurde festgestellt, dass eine Videokamera existiert, die allerdings nicht in Betrieb war. Die Firma wurde darauf hingewiesen, dass beim Einsatz von Attrappen zwar keine Verarbeitung personenbezogener Daten und damit auch keine Beobachtung im Sinne von § 6 b Bundesdatenschutzgesetz stattfindet. Eine für echt gehaltene Attrappe wird jedoch von den betroffenen Bürgern ebenso als Grundrechtseingriff empfunden wie eine tatsächlich funktionierende Kamera. Da die Videobeobachtung an der Stelle, an der sich die Kamera befand, nicht zulässig gewesen wäre, wurde der Inhaber gebeten, die Kamera zu entfernen.
Die Verwaltung der Kundendaten im Autohaus war datenschutzgerecht. Ein Problem bestand allerdings darin, dass in dem Autohaus vornehmlich Kraftfahrzeuge eines bestimmten Herstellers veräußert wurden. Dieser Hersteller, der seinen Sitz nicht in Thüringen hat, verlangte von dem Autohaus, dass die Daten der Arbeitnehmer bei dem Autokonzern gespeichert werden. Auch die Werbeansprache der Kunden des Autohauses erfolgte durch den Autokonzern, bei dem alle Kundendaten gespeichert waren. Entsprechende Verträge des Autohauses mit dem Konzern zur Auftragsdatenverarbeitung konnten allerdings nicht vorgelegt werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat den am Sitz des Autokonzerns zuständigen Landesdatenschutzbeauftragten mit der Angelegenheit befasst.
Weiterhin betreibt das Autohaus einen Autoverleih in Form eines Franchisings. Der Kunde muss vor der Ausleihe eines Fahrzeugs den Personalausweis und den Führerschein vorlegen. Die Dokumente

werden kopiert und die Kopien zu den Akten genommen. Nach § 14 Nr. 2 des Personalausweisgesetzes (PAuswG) darf die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises durch nichtöffentliche Stellen nur nach §§ 18 bis 20 PAuswG erfolgen. Danach ist das Anfertigen von Kopien datenschutzrechtlich nicht zulässig, es sei denn, sie ist durch eine spezielle gesetzliche Ermächtigung erlaubt (siehe hierzu genauer Punkt 3.48). Zum Nachweis der Identität eines Kunden ist es ausreichend, sich den Personalausweis vorlegen zu lassen und hierüber einen Vermerk zu machen, der allein die notwendigen Identitätsdaten enthält. Da der Franchisegeber aber die Anfertigung der Kopien verlangt, steht der TLfDI weiterhin im Dialog mit den Beteiligten. Bereits mehrfach fanden zur datenschutzrechtlichen Bewertung der Einzelprobleme Termine statt, an der auch Vertreter der Handwerkskammer teilnahmen. Hier ist noch einige Überzeugungsarbeit zu leisten.

Ein rechtlich selbständiger Betrieb ist die für die Datenverarbeitung verantwortliche Stelle. Auch wenn er Beziehungen zu einem größeren Konzern hat, darf er seine Daten nicht ohne einen den gesetzlichen Anforderungen entsprechenden Auftragsdatenverarbeitungsvertrag übermitteln.
Das Erstellen von Personalausweiskopien ist zum Nachweis der Identität einer Person nicht erforderlich, wenn der Personalausweis eingesehen werden kann. Kopien sind damit unzulässig.

3.32 Finger von der Wurst: Videogaga 14

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte sich mit einem Bauern auseinanderzusetzen, der in seinen Verkaufsstellen für landwirtschaftliche Produkte eine umfangreiche und nahezu flächendeckende Videoüberwachung durchführte. In einer Filiale war gar der einzige unbeobachtete Ort die Arbeitnehmertoilette. Auf Nachfrage meinte der Betreiber, die Videoüberwachung sei notwendig, weil er vermutet, dass immer mal eine Scheibe Wurst fehle. Mit dem Bundesdatenschutzgesetz (BDSG) ist eine solche Videoüberwachung von Arbeitnehmern und Kunden selbstverständlich nicht zu vereinbaren. Zwar sieht das BDSG die Möglichkeit der Datenerhebung zu Aufklärung von Straftaten im Arbeitsverhältnis vor, jedoch nur in sehr engen Grenzen und

vor allem in verhältnismäßigem Rahmen. Jedenfalls muss eine solche Videoüberwachung das allerletzte Mittel sein. Vorher muss z. B. bei Diebstahlverdacht eine Taschenkontrolle unter Heranziehung der örtlichen Polizei erfolgen. Die Kameras waren jedenfalls zu entfernen.
In diesem Fall musste der TLfDI die Einhaltung des BDSG nicht mit Hilfe einer Anordnung durchsetzen. Der Betreiber der Läden hat einen Rechtsanwalt hinzugezogen, der seinen Mandanten davon überzeugen konnte, der Aufforderung des TLfDI Folge zu leisten.

Eine Arbeitnehmerüberwachung zur Aufdeckung von Straftaten ist nur dann zulässig, wenn diese Überwachung das letzte zur Verfügung stehende Mittel ist und alle anderen Möglichkeiten erfolglos durchgeführt worden sind. Außerdem muss die Überwachung in Hinblick auf die vermeintliche Straftat verhältnismäßig sein. Wegen des Diebstahls einer Wurstscheibe ist eine Videoüberwachung in jedem Fall unzulässig.

3.33 … bis zur Bahre: Patientenakten am Ende

Nach der Insolvenz eines Arztes oder einer Einrichtung zur ambulanten medizinischen Versorgung stellt sich immer die Frage, was mit den Patientenakten passiert. Bei Patientenakten handelt es sich nach § 3 Abs. 9 des Bundesdatenschutzgesetzes (BDSG) um besondere Arten von personenbezogenen Daten, da sie Angaben über die Gesundheit enthalten. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 und Abs. 7 BDSG nur unter den dort genannten Voraussetzungen zulässig. In einem vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu untersuchenden Fall hatte sich ein Nachfolger für die Arztpraxis gefunden. Aufgrund einer Eingabe war zu untersuchen, wie bei der Übernahme durch den neuen Praxisinhaber mit den Patientendaten des bisherigen Arztes verfahren wurde. Im Rahmen einer Vor-Ort-Kontrolle wurde geprüft, wie Patientendaten aufbewahrt werden. Dort konnte festgestellt werden, dass es im Hinblick auf die elektronischen Patientendaten eine Trennung gab. Die Patientendaten der übernehmenden Praxis waren auf dem dortigen Server gespeichert. Die elektronischen Patientendaten der übernommenen Praxis waren separat auf einer USB-Platte gesichert. Die Papierakten der übernommenen

Praxis wurden in einem von der übrigen Praxis getrennten abgeschlossenen Raum aufbewahrt. Grundsätzlich unterliegen diese Patientendaten (der übernommenen Praxis) nicht dem Zugriff des neuen Inhabers. Diese werden nur im Falle der Einwilligung des Patienten für die neue Praxis aktiviert. Eine Übernahme der elektronischen Akten ist nicht möglich. Sofern Befunde benötigt werden, werden diese ausgedruckt und zu den Akten der übernehmenden Praxis genommen. Zugriff auf die Patientendaten des übernommenen Arztes, die sich in Akten befinden, wird nur genommen, wenn der Patient hiermit einverstanden ist. Dieses Verfahren war datenschutzrechtlich nicht zu beanstanden.
Beim Praxisverkauf oder bei der Praxisübernahme ist zu beachten, dass der übernehmende Arzt nicht automatisch ein Zugriffsrecht auf die Patientendaten der übernommenen Praxis hat. Gemäß § 203 Abs. 1 Satz 1 Strafgesetzbuch wird derjenige mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, der unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis offenbart, welches ihm als Arzt anvertraut wurde. Der Verkauf einer Praxis oder die Insolvenz stellt dabei keine Befugnis dar, die anvertrauten Geheimnisse einem anderen Arzt zu offenbaren. Für die Übernahme der Patientenakten muss es daher eine Einwilligungserklärung aller Patienten geben. Diese kann im Rahmen der laufenden Behandlung mündlich erfolgen, alle anderen Patienten müssen schriftlich befragt werden. Bei der Praxisübernahme wird daher oft auf das so genannte Zwei-Schrank-Modell zurückgegriffen. Dabei werden die übernommenen Patientenakten zunächst separat im ersten Schrank aufbewahrt. Sobald das Einverständnis erteilt worden ist, werden die Akten dann im laufenden System der übernehmenden Praxis eingefügt (zweiter Schrank).

Die Verpflichtung zur ärztlichen Schweigepflicht besteht auch bei der Übernahme einer Praxis an einen anderen Arzt. Sämtliche Patienten müssen um ihr Einverständnis zur Weitergabe ihrer Gesundheitsdaten gebeten werden.

3.34 Argusaugen wachen über Material…oder vielleicht doch über die Arbeitnehmer?: Videogaga 15

Aufgrund der Vorgaben des europäischen Rechts zur Schaffung unabhängiger Aufsichtsbehörden für den Datenschutz auch im nicht-

öffentlichen Bereich, was der Europäische Gerichtshof in seinem Urteil vom 9. März 2010 Az. C-518/07 Kommission ./. Bundesrepublik Deutschland unterstrichen hat, ging der Zuständigkeitsbereich für den nicht-öffentlichen Bereich vom Thüringer Landesverwaltungsamt (TLVwA) auf den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über. Mit Übernahme der Zuständigkeit des nicht-öffentlichen Bereiches hat der TLfDI verschiedene Verfahren vom TLVwA übernommen. So auch einen besonders krassen Fall von Arbeitnehmerüberwachung. Unter dem Deckmantel des Verarbeitens besonders wertvoller Materialien betreibt das Unternehmen sechzehn Kameras, von denen eine Vielzahl direkt auf die Arbeitsplätze der Arbeitnehmer ausgerichtet sind, sodass auf den betroffenen Arbeitnehmer ein massiver Überwachungsdruck ausgeübt wird. Besonders intensiv ist die Videoüberwachung in einem Büro gestaltet. Dort werden zwei Computerarbeitsplätze aus nächster Nähe videoüberwacht. Begründet wird dies damit, dass es sich um die Entwicklungsabteilung handele und die Daten höchster Geheimhaltung unterlägen. Darauf kommt es allerdings nicht an. Das informationelle Selbstbestimmungsrecht der Arbeitnehmer überwiegt das Interesse des Arbeitgebers in einem solchen Fall nahezu immer. In jedem Fall war die Speicherdauer aller Kameras mit mehreren Wochen unabhängig von deren Zulässigkeit zu lang gewählt. Auch rechtmäßig erhobene Daten dürfen nur so lange vorgehalten werden, wie dies nach deren Zweck notwendig ist. Zur Aufklärung eventueller Verstößen sind hierfür in der Regel 48 Stunden und über das Wochenende (Freitag - Montag) 72 Stunden ausreichend.

Mit Übernahme des Verfahrens hat der TLfDI eine Kontrolle durchgeführt, durch die oben genannte Umstände erst festgestellt werden konnten. Dem Unternehmen wurde mitgeteilt, dass die Art und Weise der durchgeführten Videoüberwachung unzulässig ist, was das Unternehmen dazu veranlasste, einen Rechtsanwalt einzuschalten. Der Geschäftsführer möchte gern an der Videoüberwachung seiner Arbeitnehmer festhalten.

Nach langwieriger und aufwendiger Korrespondenz mit der Interessenvertretung des Unternehmens ist der TLfDI nunmehr zur Erkenntnis gelangt, dass hier auf ein Einsehen und Einhalten der datenschutzrechtlichen Regelungen nicht zu hoffen ist. Es ist eine Anordnung in Vorbereitung, die die Deinstallation der meisten Kameras verlangen wird. Mit einem langjährigen und aufwendigen verwal-

tungsgerichtlichen Verfahren ist zu rechnen. Wie in allen Fällen der unzulässigen Videoüberwachung ist hier die Einleitung eines Ordnungswidrigkeitenverfahrens naheliegend.

§ 32 Bundesdatenschutzgesetz regelt, dass das Erheben und Verarbeiten von Arbeitnehmerdaten nur dann zulässig ist, wenn dies für die Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Bei einer Videoüberwachung ist dies in aller Regel nicht der Fall. Daher gilt: Jede Videokamera, die auf Arbeitsplätze oder sonstige Orte gerichtet ist, an denen sich Arbeitnehmer regelmäßig aufhalten, ist unzulässig. Lediglich zur Aufklärung von Straftaten hat der Gesetzgeber unter engen Voraussetzungen das Erheben und Verarbeiten von Arbeitnehmerdaten zugelassen. Dabei darf es sich allerdings nur um das allerletzte Mittel handeln und es müssen vorher dokumentierte Vorfälle vorgelegen haben. Außerdem bedarf es einer umfangreichen Verhältnismäßigkeitsprüfung.

3.35 Einkauf unter Beobachtung: Videogaga 16

Aufgrund einer Beschwerde erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis, dass in einem Lebensmittelladen großflächig eine Videoüberwachung betrieben wird. Eine Kontrolle vor Ort bestätigte dies. In dem Geschäft wurden insgesamt zahlreiche Domekameras eingesetzt, die sämtlich an der Decke des Marktes installiert waren. Die Aufnahmen der im angegliederten Getränkemarkt befindlichen Kameras wurden nicht aufgezeichnet. Die übrigen Kameras waren vorzugsweise in den Gängen zu den Regalen angebracht. Eine direkte Überwachung fest eingerichteter Arbeitsplätze konnte nicht festgestellt werden. Diese Aufnahmen wurden über 24 Stunden gespeichert und dann überschrieben. Der Festplattenrecorder und die Bildschirme zu den Kameras befanden sich in einem separaten Büro der Geschäftsleitung, zu dem nur der Geschäftsleiter und sein Stellvertreter Zutritt hatte. Der Anzeige- und Beobachtungsbildschirm sind beide abschaltbar sowie durch ein Passwort und einen besonderen Schalter mit einem Sicherheitsschlüssel, über den nur die Geschäftsleitung und eine Sicherheitsfirma verfügt, gesichert. Die Anlage wird rund um die Uhr betrieben, allerdings sind die Bildschirme nur in

Betrieb, wenn sich entweder die Geschäftsstellenleitung oder ein Sicherheitsmann im Büro aufhalten.
Der TLfDI stellte fest, dass der Markt zunächst seiner Hinweispflicht nach § 6 b Abs. 2 Bundesdatenschutzgesetz (BDSG) nicht hinreichend nachgekommen war. Zwar existierten Schilder. Diese waren jedoch so angebracht, dass die von der Videoüberwachung Betroffenen den Umstand der Videoüberwachung nicht ohne weiteres erkennen konnten. Auf Aufforderung des TLfDI hin wurde dies geändert.
Zum Zweck der Videoüberwachung gab der Geschäftsstellenleiter glaubhaft an, dass es in der Vergangenheit im verstärkten Maße zu Diebstählen gekommen war. Die Kameras sollen dazu dienen, Diebstähle verfolgen zu können und sollen auch eine abschreckende Wirkung erzielen.
Bei dem Lebensmittelladen handelt es sich um einen öffentlich zugänglichen Raum. Daher ist nach § 6 b Abs. 1 BDSG die Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Geschäftsstellenleitung konnte glaubhaft machen, dass die Videoüberwachung zur Wahrnehmung des Hausrechts bzw. zur Wahrnehmung berechtigter Interessen erforderlich ist. In den ersten Monaten nach der Kamerainstallation wurden zahlreiche Diebstähle registriert, diese hatten sich nachweislich bis zum Kontrollzeitpunkt signifikant reduziert. Allerding bestanden aufgrund der Vielzahl der angebrachten Kameras Anhaltspunkte dafür, dass schutzwürdige Interessen der Betroffenen überwogen. Bis auf den Kassenbereich wurde der Markt nahezu komplett videoüberwacht. Hier musste eine Abwägung erfolgen zwischen den durch die Zwecke der Videoüberwachung grundrechtlich geschützten Positionen des Geschäftsinhabers und dem Grundrecht auf informationelle Selbstbestimmung derjenigen, die Objekt der Videoüberwachung sind. Die permanente lückenlose Überwachung mit Aufzeichnung eines bestimmten Raumes, der sich der Betroffene nicht entziehen kann, stellt einen sehr weitreichenden Grundrechtseingriff dar. Der im Markt einkaufende Kunde sowie auch der dort beschäftigte Arbeitnehmer hat keine Möglichkeit, sich der Videoüberwachung zu entziehen. Der Kunde ist nahezu während des gesamten Einkaufs und der Arbeitnehmer während der gesamten Arbeitszeit unter Beobachtung. Der TLfDI unterzog daher sämtliche Kameras einer eigenen datenschutzrechtlichen Bewertung und kam

mit dem Inhaber des Lebensmittelmarkes überein, dass ein Drittel der Kameras abzuschalten ist. Es wurde außerdem im Datenschutzkonzept schriftlich festgelegt, unter welchen konkreten Voraussetzungen die Auswertung der Bilddaten möglich ist.

Videoüberwachung kann im Einzelhandel zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen zulässig sein. Allerdings darf keine permanente und lückenlose Überwachung stattfinden, der sich Kunden oder Arbeitnehmer nicht entziehen können. Zur Auswertung von Videomaterial müssen konkrete schriftliche Festlegungen getroffen werden.

3.36 Weniger ist mehr: Reduzierung von Videokameras in einer Einkaufsgalerie: Videogaga 17

Im Düsseldorfer Kreis – einem Arbeitskreis derjenigen Landesdatenschutzbeauftragten und des Bayerischen Landesamtes für Datenschutzaufsicht, die auch für den nicht-öffentlichen Bereich zuständig sind[a] – wurde die Zulässigkeit des Einsatzes von Videoüberwachung in den Einkaufszentren eines europaweit agierenden Unternehmens, das auch in Deutschland Einkaufszentren betreibt, diskutiert. Zu diesem Zweck wurden die datenschutzrechtlichen Aufsichtsbehörden um Vorort-Besichtigungen in den Einkaufszentren im jeweiligen Zuständigkeitsbereich gebeten. Ziel der Kontrollen war nicht die Videoüberwachung in den einzelnen Geschäftslokalen, sondern in der Einkaufspassage selbst. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte diese Aufgabe vom vormals zuständigen Thüringer Landesverwaltungsamt übernommen. Dieses hatte festgestellt, dass in der Einkaufspassage 16 Kameras installiert waren. Die Kontrollen der Aufsichtsbehörden zeigten offensichtlich Wirkung, sodass sich das Unternehmen zu einem bundesweiten Abbau von Kameras in seinen Einrichtungen entschloss. Zum Zeitpunkt der Vorort-Kontrolle durch den TLfDI gab es im Einkaufszentrum noch lediglich drei Kameras, deren Betrieb einer datenschutzrechtlichen Beurteilung unterzogen wurde. Das Management konnte schlüssig darlegen, dass die von den verbliebenen Kameras überwachten Bereiche zur Verhinderung und Verfolgung von Straftaten (Aufbrüche, Warendiebstähle, Drogende-

[a] Siehe Punkt 2

likte) und hohen Sachschäden (durch unachtsames Rangieren von LKWs) zur Wahrnehmung des Hausrechts erforderlich sind. Kritik übte der TLfDI an den nicht ausreichend angebrachten Hinweisen auf die Videoüberwachung sowie die Beobachtung einer benachbarten, nicht zum Einkaufzentrum gehörenden Einfahrt. Die festgestellten Mängel wurden durch das Einkaufszentrum kurzfristig beseitigt.

Oftmals wird durch die Reduzierung der Anzahl von Videokameras der gesetzlich zugelassene Zweck ebenfalls erreicht und gleichzeitig schutzwürdige Interessen der Betroffenen werden nicht überwiegend beeinträchtigt.

3.37 Hotel California: Videogaga 18

In diesem bekannten Lied wird ein Hotel besungen, das, einmal betreten, zwar wieder verlassen werden kann, es richtig hinter sich zu lassen, ist jedoch unmöglich. So ähnlich ist das auch mit einem Thüringer Hotel, wobei es hier weniger um Sehnsüchte als mehr um Videokameras geht. Wollten Sie schon immer mal wissen, mit wem Ihr Partner in diesem Hotel am Frühstücktisch saß? In diesem Hotel bislang kein Problem, sofern der Geschäftsführer Sie an die Videodaten lässt.
Sämtliche Gemeinschaftsbereiche des Hotels sind videoüberwacht. Dies beginnt beim Frühstücksraum und endet beim Billardraum. „Selbstverständlich“ zeichnen alle Kameras auf, das ist ja auch Stand der Technik. Aufgefallen ist das Hotel aber seltsamerweise nicht, weil sich Gäste beschwert haben, sondern weil auch der Außenbereich des Hotels überwacht wird und sich Dritte zu Recht gestört fühlen.
Tatsächlich ist es nicht so, dass Videoüberwachung in einem Hotel per se unzulässig ist. Allerdings sind die Hürden hierfür sehr hoch anzusetzen. Was jedoch vollkommen unzulässig ist, ist die Überwachung von Räumen, die der Erholung und Freizeitgestaltung dienen.
Videoaufnahmen von Personen stellen personenbezogene Daten dar. Der Umgang mit diesen, also das Erheben, Verarbeiten und Nutzen, ist nur dann zulässig, wenn das Bundesdatenschutzgesetz (BDSG) oder ein anderes Gesetz hierfür eine Erlaubnisvorschrift bereithält oder der einzelne Betroffene in den Umgang mit diesen Daten eingewilligt hat, § 4 Abs. 1 BDSG. Es handelt sich um ein so genanntes Verbot mit Erlaubnisvorbehalt.

Für öffentlich zugängliche Räume, und um solche handelt es sich bei Hotelräumen, die für alle Hotelgäste zugänglich sind, hat der Gesetzgeber die Zulässigkeit von Videobeobachtung und Speicherung dieser Daten abschließend geregelt. Diese in § 6 b BDSG getroffene Regelung verfügt über einen abgestuften Voraussetzungskatalog, der zur Unzulässigkeit der Beobachtung und/oder Speicherung führt, wenn einer der Punkte nicht erfüllt wird.
So ist eine Videobeobachtung öffentlich zugänglicher Räume nur dann zulässig, wenn diese zur Durchsetzung des Hausrechts oder für berechtigte Interessen zu konkret festgelegten Zwecken erforderlich ist. Darüber hinaus dürfen keine Anhaltspunkte dafür vorhanden sein, dass schutzwürdige Interessen der Betroffenen überwiegen.
Ähnlich wie bei der Überwachung von Gasträumen in Gaststätten ist die Videoüberwachung von Aufenthalts- und Essensräumen in Hotels immer unzulässig, da hier immer Anhaltspunkte dafür vorhanden sind, dass die schutzwürdigen Interessen Betroffener die des Überwachenden überwiegen. Diese Räume stehen den Gästen zur Verfügung, um einer ungestörten Entfaltung der Persönlichkeit im Rahmen der Freizeitgestaltung nachzugehen. In dieser Entfaltung der Persönlichkeit könnten sich einzelne Personen durch die Videoüberwachung gehemmt fühlen. Zum Beispiel in der Frage, mit wem man sich an einen Frühstückstisch setzt.
Die bei der Kontrolle auch geprüfte Videoüberwachung im Außenbereich war in Teilen ebenfalls unzulässig. Insbesondere eine Kamera, die Teile des Nachbargrundstücks erfasste, ist von Erlaubnistatbeständen des BDSG nicht mehr gedeckt bzw. überhaupt nicht vorgesehen. So ist in § 6 b BDSG die Beobachtung öffentlich zugänglicher Bereiche geregelt. Um solche handelt es sich bei einem privaten Nachbargrundstück aber in der Regel und auch hier nicht. Daneben käme noch § 28 BDSG in Betracht, welcher den Datenumgang zu eigenen Geschäftszwecken regelt. Allerdings handelt es sich bei der Beobachtung des Nachbargrundstücks nicht um die Erfüllung eigener Geschäftszwecke, weswegen auch diese Norm als Erlaubnistatbestand ausscheidet.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wird gegen das betroffene Hotel in Kürze eine Anordnung erlassen, die darauf abzielt, datenschutzrechtlich konforme Zustände durchzusetzen. Darunter fällt auch die Demontage einiger Kameras. Ein Bußgeldverfahren ist wahrscheinlich.

Videoüberwachung in Bereichen, die der Freizeitgestaltung dienen, ist unzulässig. Hierzu zählen auch die entsprechenden Räume in Hotels, die allen Gästen zugänglich sind. Sollten Sie eine solche Videoanlage bemerken, wenden Sie sich bitte an den TLfDI, damit dieser der Sache nachgehen kann.

3.38 Video *vor* dem Kaufhaus – zulässig?: Videogaga 19

Erfreulicherweise meldete sich wieder einmal ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und gab an, im Eingangsbereich eines Kaufhauses würden Videoaufnahmen gefertigt, die auch den öffentlichen Verkehrsraum erfassten; zudem fehle ein Hinweisschild zu den Videokameras.
§ 6 b Bundesdatenschutzgesetz (BDSG) erlaubt nicht-öffentlichen Stellen die Videoüberwachung zur Wahrnehmung des Hausrechts und berechtigter Interessen für konkret festgelegte Zwecke, soweit dies *erforderlich* ist *und schutzwürdige Interessen der Betroffenen nicht überwiegen.*
Selbst wenn – etwa aufgrund vorhergegangener Straftaten (z. B. Diebstahl, Sachbeschädigung, Graffiti) – eine Videoüberwachung eines Kaufhaus*eingangs*bereichs erforderlich erscheint, weil für die Betroffenen (Passanten) weniger belastende Maßnahmen nicht (mehr) in Betracht kommen, so scheitert eine Videoüberwachung gleichwohl an den überwiegenden Interessen der Passanten, wenn (auch) der öffentliche Verkehrsraum videografiert wird. Die Schutzbedürftigkeit dieser öffentlichen Räume ist hoch, da sich hier Menschen typischerweise länger aufhalten und untereinander kommunizieren. Der Videoüberwachung auszuweichen, etwa durch einen Wechsel der Straßenseite, wird infolge der zunehmenden Überwachungsdichte immer schwieriger nicht mehr in Betracht. Diese auch von der Rechtsprechung vertretenen Positionen kamen in dem von der Bürgerin beanstandeten Fall jedoch nicht zum Tragen, denn einerseits wurde der öffentliche Verkehrsraum nur in unerheblichem Maße videografiert – die Rechtsprechung lässt je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu 1 Meter aufgenommen wird. Diese richterrechtlichen Vorgaben waren in concreto eingehalten. Zum anderen existierte tatsächlich ein entsprechendes Hinweisschild (§ 6 b Abs. 2 BDSG). Bei dieser Gelegenheit: Ein Schild, das auf eine Videoüberwachung

hinweist, macht diese nicht rechtmäßig. Vielmehr ist auf eine rechtmäßige (!) Videoüberwachung mittels Schildes hinzuweisen! Dabei ist auch die für die Videoüberwachung zuständige Stelle zu benennen.

Die Videoüberwachung öffentlich zugänglicher Räumen durch nichtöffentliche Stellen richtet sich nach § 6 b BDSG.
Selbst wenn danach eine Videoüberwachung als erforderlich zu qualifizieren sein mag, überwiegt das nach dieser Norm zu berücksichtigende schutzwürdige Interesse der Betroffenen (Passanten) grundsätzlich, wenn der öffentliche Verkehrsraum videoüberwacht wird.
Die Videoüberwachung ist dann datenschutzrechtswidrig. Auch ein Schildchen, das auf die Videoüberwachung hinweist, hilft dann nicht mehr. Denn nicht das Schildchen macht die Videoüberwachung rechtmäßig, sondern auf eine rechtmäßige(!) Videoüberwachung muss das Schildchen hinweisen!

3.39 Datenschutz gerade auch in Frauenschutzeinrichtungen

Aufgrund einer Beschwerde brachte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in Erfahrung, dass in einem neu entworfenen Verfahren der Leistungsgewährung und Abrechnung von Frauenschutzeinrichtungen durch das Landratsamt des Unstrut-Hainich-Kreises eine datenschutzrechtlich unzulässige Forderung vorgesehen war. Nach dem Vertrag zwischen Landkreis und dem privaten Träger des Frauenhauses sollten personenbezogene Daten (Name, Wohnanschrift) der von Gewalt betroffenen Frauen und Kinder unverzüglich per Fax an das Landratsamt weitergeleitet werden.
Indem sich das Landratsamt diese Daten von betroffenen Frauen und Kindern zuleiten lässt, erhebt es Daten im Sinne des Thüringer Datenschutzgesetzes (ThürDSG). Dies ist nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist, § 19 Abs. 1 ThürDSG. Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben, § 19 Abs. 2 Satz 1 ThürDSG. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn entweder eine Rechtsvorschrift dies vorsieht oder die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen erforderlich macht oder die Erhebung

beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Allerdings ist die Erhebung bei Dritten in den beiden zuletzt genannten Fällen nur zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegend schutzwürdige Interessen des Betroffenen beeinträchtigt werden, § 19 Abs. 2 Satz 2 ThürDSG.
Nach Auffassung des TLfDI war eine Erforderlichkeit für die Übermittlung des Namens und der Wohnanschrift der von der Gewalt betroffenen Frau bzw. des Kindes in nicht anonymisierter Form nicht gegeben. Dem Landratsamt muss es zwar möglich sein, die zweckentsprechende Verwendung öffentlicher Gelder im Einzelfall nachprüfen zu können. Dazu reicht es jedoch aus, dass die jeweilige Einrichtung dem Landratsamt die Zahl der sich in dieser Einrichtung aufhaltenden Frauen und Kinder regelmäßig übermittelt. Die erforderliche Kontrolle durch das Landratsamt kann durch stichprobenartige Einsicht in die Belegungslisten gewährleistet werden. Im Hinblick darauf, dass die Arbeitnehmer des Landratsamtes der Amtsverschwiegenheit unterliegen, ist im Regelfall nicht davon auszugehen, dass gegen die Einsichtnahme bei Stichproben schutzwürdige Interessen des Betroffenen überwiegen. Treten jedoch besondere Konstellationen auf, wie z. B. die Unterbringung der Frau eines Bediensteten der entsprechenden Behörde des Landratsamtes, so können im Einzelfall durchaus schutzwürdige Interessen der Frauen am Ausschluss der Datenerhebung vorliegen.
Das Landratsamt nahm die Stellungnahme des TLfDI zum Anlass, den Vertrag zu überarbeiten. In der neu abzuschließenden Vereinbarung wurde ein Ablauf festgelegt, nach dem die Einrichtung Namen und Wohnanschrift der Betroffenen nicht standardmäßig erheben und übermitteln wird.

Es ist nicht zulässig, dass das Landratsamt personenbezogene Daten der von Gewalt betroffenen Frauen und Kinder von einer Frauenschutzeinrichtung erhebt. Stichprobenartige Kontrollen können zum Zweck der Leistungsprüfung im Einzelfall zulässig sein.

3.40 Vorsicht bei Gesundheitsdaten!

Aufgrund einer Nachfrage der Landesapothekerkammer erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) von einem geplanten sozialen Projekt Kenntnis. Von den Initiatoren des Projekts war geplant, Bedürftigen mithilfe

eines Sponsorenkontos bei verschreibungsfreien Medikamenten einen Sonderpreis in Höhe 50 % des Apothekenverkaufspreises einzuräumen. Zu diesem Zweck sollen die Bedürftigen zunächst eine Berechtigungskarte erhalten und sich dann von ihrem Arzt ein sogenanntes "Grünes Rezept" ausstellen lassen, welches dann zusammen mit dem Ausweis in der Apotheke vorgelegt werden sollte. Mit dem Grünen Rezept werden Medikamente verschrieben, die in der Regel nicht auf Kosten der gesetzlichen Krankenkassen verordnet werden können. Bei der Einlösung des Rezepts soll der Patient 50 % des Arzneimittelpreises bezahlen, während die anderen 50 % von einem Sponsorenkonto bezahlt werden sollen.

Gegen dieses Verfahren meldete der TLfDI datenschutzrechtliche Bedenken gegen die Übermittlung von Patientendaten durch Apotheken an eine private Verrechnungsstelle an. Bei Gesundheitsdaten handelt es sich um besondere Arten personenbezogener Daten, § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG). Für derartige Daten gelten nach BDSG besonders strenge Anforderungen. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten für eigene Geschäftszwecke ist nach § 28 Abs. 6 BDSG zulässig, soweit nicht der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat, wenn eine der in § 28 Abs. 6 Nummer 1 bis 4 BDSG genannten Voraussetzungen vorliegen. Da keine dieser Voraussetzungen vorlag, ist die Datenübermittlung nur mit der Einwilligung des Betroffenen möglich. Eine wirksame Einwilligung setzt nach § 4 a Abs. 1 BDSG voraus, dass sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Zudem ist, da besondere Arten personenbezogener Daten betroffen sind, die Einwilligung ausdrücklich auf diese Daten, das heißt auf die Übermittlung der Rezepte, zu beziehen.

Daher ist eine ausdrückliche schriftliche Einwilligungserklärung des Patienten in die Übermittlung der Rezepte an die private Abrechnungsstelle gegenüber der jeweils übermittelnden Apotheke erforderlich. Das sollte machbar sein. Hingewiesen wurde auch darauf, dass sich nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch strafbar macht, wer

unbefugt – in diesem Fall also ohne Einwilligung des Betroffenen – ein fremdes Geheimnis offenbart, das ihm als Apotheker anvertraut worden ist.
Da sich im Laufe des Verfahrens herausstellte, dass der Träger des Projektes eine kirchliche Einrichtung ist, wurde das Verfahren insoweit an den zuständigen kirchlichen Datenschutzbeauftragten abgegeben. Mit Blick auf das verfassungsrechtlich garantierte Selbstbestimmungsrecht von Religionsgemeinschaften gilt das Bundesdatenschutzgesetz im Bereich der Kirchen nicht.

Auch wenn ein guter Zweck verfolgt wird, sind die Anforderungen des Datenschutzrechts zu beachten. Eine Übermittlung von Gesundheitsdaten ist nur bei einer vorliegenden schriftlichen Einwilligung, die sich ausdrücklich auf diese Daten bezieht oder bei Vorliegen der Voraussetzungen des § 28 Abs. 6 BDSG zulässig. Für kirchliche Einrichtungen besteht keine Zuständigkeit des TLfDI.

3.41 Datenverkauf im Apothekenrechenzentrum?

Aus der Presse war zu entnehmen, dass die Verrechnungsstelle der süddeutschen Apotheken (VSA) Millionen von Patientendaten nur unzureichend verschlüsselt an den Gesundheitsdienstleister und Marktforscher IMS Health verkauft haben soll. Die Apothekenrechenzentren bieten für die Apotheken in Deutschland die Dienstleistung der Abrechnung mit den Kassen an. Dies ist nach § 300 Abs. 2 Satz 1 des Fünften Buches Sozialgesetzbuch (SGB V) zulässig. Danach dürfen die Apotheken zur Erfüllung ihrer Verpflichtungen Rechenzentren in Anspruch nehmen. § 300 Abs. 2 Satz 2 SGB V legt fest, dass die Rechenzentren diese Daten nur für diese Zwecke verarbeiten und nutzen dürfen, anonymisierte Daten allerdings dürfen auch für andere Zwecke verarbeitet und genutzt werden. Das bedeutet, dass die Daten, wenn sie anonymisiert sind, von den Rechenzentren auch an andere Dienstleister oder Pharmaunternehmen verkauft werden dürfen. Nach § 3 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Entscheidend für die datenschutzrechtli-

che Zulässigkeit der Tätigkeit der Apothekenrechenzentren ist beim Verkauf von Daten an Dritte, ob diese entsprechend den gesetzlichen Vorgaben anonymisiert sind. Laut den damaligen Pressemitteilungen war die Identität der Patienten lediglich durch einen 64-stelligen Code verschleiert, der sich leicht auf die tatsächliche Versichertennummer zurückrechnen ließ.
Es besteht ein großes wirtschaftliches Interesse an der Auswertung von Verordnungsdaten. Die Apothekenrechenzentren sind daher grundsätzlich bestrebt, eine Auswertung der Daten weitestgehend zu ermöglichen. Um die Tätigkeit der Apothekenrechenzentren bundesweit einheitlich zu bewerten, wurde die Unterarbeitsgruppe „Apothekenrechenzentren“ des Arbeitskreises „Gesundheit und Soziales“ der Datenschutzkonferenz eingerichtet. Diese Unterarbeitsgruppe kam unter Vorsitz des Bayerischen Landesamtes für Datenschutzaufsicht zweimal im Berichtszeitraum in Ansbach zusammen.
Von einer Anonymisierung kann dann nicht mehr gesprochen werden, wenn die Verordnungsdaten in einer Art und Weise an Dritte weitergegeben werden, dass diese zu einem Rezept die Versicherungsnummer des Patienten und die Arztnummer des verschreibenden Arztes, wenn auch mit einigem Aufwand, bestimmen können. Bei den Sitzungen der Unterarbeitsgruppe ging es vor allem darum festzulegen, wann von einer Anonymisierung der Daten gesprochen werden kann. Nach Auffassung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist eine absolute Anonymisierung die sicherste Methode, um die gesetzlichen Anforderungen zu erfüllen. Eine Anonymisierung kann jedenfalls dann nicht erreicht werden, wenn dasselbe Anonym für einzelne Ärzte, Versicherte und Apotheken über einen unbestimmten Zeitraum dauerhaft verwendet wird. Mit fortschreitender Zeit vergrößert sich die Gefahr, dass durch gezielte Abfragen, die immer wieder in anderer Weise miteinander verknüpft werden, die Anonyme personifiziert werden können. Daher ist zu fordern, dass die bei der Übermittlung verwendeten Schlüssel eine kurze Gültigkeit haben, dass Daten einzelner Ärzte nicht gezielt abgefragt werden, sondern Ärzte-Cluster größeren Umfangs zu bilden sind. Gleiches gilt für Patientendaten. Im Nachgang zu den Sitzungen der Unterarbeitsgruppe „Apothekenrechenzentren“, hat der TLfDI auch ein Apothekenrechenzentrum in Thüringen geprüft. Offensichtliche Anhaltspunkte für ein gesetzwidriges Verhalten gab es dabei nicht. Da die Verfah-

ren allerdings äußerst komplex sind, ist die Prüfung noch nicht abgeschlossen. Der TLfDI wird das Ergebnis der Prüfung im nächsten Tätigkeitsbericht darlegen.

Apothekenrechenzentren dürfen Rezeptdaten auch für andere Zwecke als die Abrechnung verwenden, wenn diese anonymisiert sind. An die Anonymisierung sind wegen der enthaltenen Sensibilität der Gesundheitsdaten hohe Anforderungen zu stellen.

3.42 Taxi - alles im Blick: Videogaga 20

Es ist bekannt, dass Taxifahrer Opfer einer Straftat werden können, entweder indem ein Fahrgast „das Bezahlen vergisst“ oder der Fahrer sogar überfallen und ausgeraubt wird. Da liegt es nahe, auch in diesem Bereich auf die Wirkung der Videoüberwachung zu setzen. Im Düsseldorfer Kreis (siehe oben Punkt 2) wurde darüber beraten, unter welchen Voraussetzungen aus datenschutzrechtlicher Sicht die Videoüberwachung des Taxiinnenraums zulässig ist. Dabei wurde festgestellt, dass grundsätzlich der Einsatz von Videokameras, z. B. im Armaturenbrett, im Dachhimmel usw. nicht ausgeschlossen ist. Hierbei müssen aber die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer Beachtung finden. Es sind daher die berechtigten Sicherheitsinteressen und die schutzwürdigen Interessen der Betroffenen gegeneinander abzuwägen und die Videoüberwachung auf das unbedingt erforderliche Maß zu beschränken. Die Zulässigkeit einer Videoüberwachung durch ein Taxi-Unternehmen bestimmt sich nach § 6 b Abs. 1 Nr. 3 Bundesdatenschutzgesetz (BDSG), wonach die Beobachtung und vorliegend auch die Aufzeichnung mittels Videokameras nur zulässig ist, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Düsseldorfer Kreis verweist dabei darauf, vorrangig alternative und weniger einschneidende Schutzmaßnahmen (z. B. anlassbezogene Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals) zu ergreifen. Eine Videoüberwachung kann außerdem nur in Orten als erforderlich angesehen werden, die eine hohe Kriminalitätsrate aufweisen. Falls eine Videoüberwachung danach als erforderlich anzusehen ist – wovon in Thüringen in aller Regel nicht auszugehen ist – dann sollte sich diese auf

das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen beschränken. Soweit eine Aufzeichnung erfolgt, ist diese ohne ein Vorkommnis unverzüglich zu löschen. Dem Transparenzgebot nach § 6 b Abs. 2 BDSG ist Rechnung zu tragen, indem an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung hingewiesen werden.
Da Taxis rund um die Uhr am Straßenverkehrsgeschehen teilnehmen, ist hier die Gefahr hoch, in einen Unfall verwickelt zu werden. Sowohl vermeintlich findige Versicherungsunternehmen als auch Taxibetriebe verfolgen deshalb die Idee, durch die Installation von Außenkameras, häufig in Form von so genannter „Dashboardkameras“, die auf dem Armaturenbrett (Dashboard) angebracht werden und das Verkehrsgeschehen durch die Windschutzscheibe aufzeichnen, im Falle eines Schadensereignisses vorsorglich Beweise zu sichern. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit geht davon aus, dass diese Form der Videoüberwachung nicht die gesetzlichen Anforderungen an eine zulässige Videoüberwachung erfüllt. Jeder Verkehrsteilnehmer kann sich im Verkehrsraum grundsätzlich darauf verlassen, nicht ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Ausdruck des Rechts auf informationelle Selbstbestimmung ist es, sich in der Öffentlichkeit, auch im Verkehrsraum, frei und ungezwungen bewegen zu können. Der Düsseldorfer Kreis hat deshalb den Beschluss gefasst, dass es eine Rechtsgrundlage für diese Form der Datenerhebung nicht gibt und die Ausstattung von Taxis mit Außenkameras, wie dies von Versicherungsunternehmen vorgeschlagen wird, unzulässig ist (Beschluss des Düsseldorfer Kreises am 26./27. Februar 2013, siehe Anlage 4).

Eine anlasslose Videoüberwachung in Taxis ist weder erforderlich noch angemessen. Zum einen hat der Taxifahrer ein Recht darauf, nicht durchgängig während seiner Arbeitsschicht beobachtet zu werden, zum anderen müssen auch unbescholtene Fahrgäste nicht damit rechnen, permanent während der Fahrt unter Videobeobachtung zu stehen.
Die Beobachtung des Verkehrsgeschehens durch Außenkameras bei Taxis ist grundsätzlich unzulässig.

3.43 Keine Beobachtung öffentlicher Straßen zur Zugangskontrolle: Videogaga 21

Auf polizeilichen Hinweis kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein Recyclingunternehmen in Thüringen, das über eine umfangreiche Videoüberwachung verfügte. Dabei wurde festgestellt, dass eine der Kameras auf die öffentliche Straße in Richtung des anliegenden Dorfes ausgerichtet war. Jeder im Dorf und jeder der die betroffene öffentliche Straße nutze, musste davon ausgehen, Gegenstand einer Videoüberwachung zu werden. Nach dem Bundesdatenschutzgesetz (BDSG) bedarf jedoch die Videoüberwachung öffentlich zugänglicher Bereichen wie Straßen grundsätzlich einer Rechtsgrundlage. Gemäß § 6 b BDSG ist die Videobeobachtung zum einen zulässig, sofern sie zu Zwecken der Ausübung des Hausrechts erforderlich ist. Außerdem darf sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke durchgeführt werden. In beiden Fällen darf kein Anhaltspunkt ersichtlich sein, dass schutzwürdige Interessen Betroffener überwiegen. Diese Voraussetzungen waren hier nicht gegeben. Darüber überwiegen in aller Regel die Interessen Dritter, wenn eine ganze Straße in den Bereich der Videoaufnahmen fällt. Bei der Beobachtung öffentlicher Straßen werden immer auch Personen „Opfer“ der Beobachtung, die die Straße benutzen müssen, von der Beobachtung nichts wissen und keinen Anlass für eine Beobachtung gegeben haben. Da das Unternehmen uneinsichtig war und immer neue Ausflüchte suchte, untersagte der TLfDI dem Unternehmen die in dieser Weise durchgeführte Videoüberwachung mit Hinweis auf den dadurch auf Passanten ausgeübten Überwachungsdruck. Dem Unternehmen wurde im Wege einer Anordnung unter Zwangsgeldandrohung aufgegeben, die Kamera wahlweise zu verhüllen oder in eine zulässige Position zu verdrehen.

Es ist unerlässlich, dass sich Unternehmen mit den Grenzen der Videoüberwachung vertraut machen. Dies gilt nicht nur, aber insbesondere für die Videoüberwachung in öffentlich zugänglichen Bereichen. In der Regel verstößt das Ausrichten einer Videokamera auf eine öffentliche Straße oder einen öffentlichen Fußweg gegen Datenschutzrecht.

3.44 Das "elektronische Auge" des Nachbarn: Videogaga 22

Gegenstand einer Beschwerde waren Videoaufnahmen von Bewohnern und Besuchern eines Grundstücks, die ein Nachbar mit seiner Videokamera aufgenommen und ohne Erlaubnis der Abgebildeten seinen Gästen zur Schau gestellt haben soll. Nach § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) sind Videoaufnahmen mit personenbezogenen Daten nur dann am BDSG zu messen, wenn ihre Erhebung, Verarbeitung und Nutzung nicht ausschließlich für persönliche oder familiäre Zwecke erfolgt.
Obwohl der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seiner Aufsichtstätigkeit kontrollieren kann, ob die Videoaufnahmen ausschließlich für persönliche oder familiäre Zwecke gefertigt werden, befriedigt ihn die oben dargelegte Rechtslage nicht, da sie ihn von Maßnahmen trotz etwaiger Datenerhebungen im unter Umständen sehr privaten Bereich (z. B. Video) abhält, wenn diese Datenerhebungen lediglich privaten oder familiären Zwecken dienen.
Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben eine gemeinsame Orientierungshilfe zur Videoüberwachung erarbeitet. In diesem Zusammenhang hat sich der TLfDI dafür eingesetzt, dass die Datenschutzaufsichtsbehörden im Falle einer durch Privatpersonen durchgeführten Videoüberwachung, die zugleich auch öffentliche Bereiche, wie z. B. öffentliche Parkplätzen, Gehwege und Straßen erfassen, zuständig sein sollen. Zum Thema private Videoüberwachung ist gegenwärtig eine Klage vor dem Europäischen Gerichtshof (EUGH, C-212/13) anhängig. Dieses Vorabentscheidungsersuchen betrifft die Frage, ob der Betrieb eines Kamerasystems, das an einem Einfamilienhaus zum Zwecke des Schutzes des Eigentums, der Gesundheit und des Lebens der Besitzer des Hauses angebracht ist, unter die Verarbeitung personenbezogener Daten, „die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird“ im Sinne des Art. 3 Abs. 2 der Richtlinie 95/46/EG gefasst werden kann, obschon dieses System auch öffentlichen Raum überwacht. Der Ausgang dieses Gerichtsverfahrens und sein Einfluss auf die künftige Rechtlage sind derzeit jedoch noch nicht abzusehen.
Im konkreten Fall wurde festgestellt, dass die Videoaufnahmen durch den Nachbarn einen privaten Bereich betrafen und zu aus-

schließlich privaten Zwecken erfolgten, weswegen eine Zuständigkeit des TLfDI nicht gegeben war.
Insofern wurde der Beschwerdeführer auf die Möglichkeit, über die ordentliche Gerichtsbarkeit auf zivilrechtlichem Wege (§ 823 BGB i. V. m. § 1004 BGB) gegen eine solche Videoüberwachung vorzugehen, hingewiesen. Nach § 22 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturheberrechtsgesetz [KunstUrhG]) dürfen Bildnisse nur mit Einwilligung der Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Nach § 33 KunstUrhG wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer entgegen §§ 22, 23 KunstUrhG ein Bildnis verbreitet oder öffentlich zur Schau stellt.

Gegen Videoaufnahmen mit personenbezogenen Daten, die einen privaten Bereich betreffen und zu ausschließlich privaten oder familiären Zwecken gefertigt werden, kann sich der Betroffene auf dem Zivilrechtsweg zur Wehr setzen.
Wer Bildnisse ohne Einwilligung der Abgebildeten verbreitet oder öffentlich zur Schau stellt, verstößt gegen das KunstUrhG. Dies kann eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe zur Folge haben.

3.45 Prüfungspflicht der Banken nach dem Geldwäschegesetz

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Anfrage eines Vorsitzenden eines nicht in das Vereinsregister eingetragen Vereins. Dieser Verein hatte bei einer Bank ein Konto eröffnet: Die Bank verlangte nun die Übermittlung von Namens-, Vornamens-, Geburts-, Geburtsorts-, Wohnanschrifts-, Wohnorts-, Staatsangehörigkeits- sowie Personalausweisnummerdaten nebst ausstellender Behörde zu jedem Vereinsmitglied. Begründet wurde diese Anforderung der Daten mit dem § 4 Abs. 5 Geldwäschegesetz (GWG).
Um die Zulässigkeit der Datenerhebung beurteilen zu können, wurde die Bank um Stellungnahme gebeten. Die Bank teilte mit, dass sie vor Eröffnung einer Geschäftsbeziehung den Geschäftspartner (wirtschaftlicher Berechtigter) nach § 4 GWG identifizieren müsse. Wirtschaftlich Berechtigter im Sinne von § 1 Abs. 6 Satz 1 GWG sei die natürliche Person, in deren Eigentum oder unter deren Kontrolle der Vertragspartner letztlich stehe oder die natürliche Person, auf deren

Veranlassung die Transaktion letztlich durchgeführt oder eine Geschäftsbeziehung begründet werde. Darunter sei nach § 1 Abs. 6 Nr. 2 d GWG insbesondere auch jede natürliche Person zu zählen, die auf sonstige Weise unmittelbar oder mittelbar beherrschenden Einfluss auf die Vermögensverwaltung oder Ertragsverteilung ausübe.
Da der Verein nicht im Vereinsregister eingetragen war, konnte die Bank den wirtschaftlich Berechtigten nicht mittels Auskunft aus dem Vereinsregister feststellen. Bei einem nicht rechtsfähigen Verein sind alle Vereinsmitglieder (im Außenverhältnis) als wirtschaftliche Berechtigte mit potenzieller Verfügungsmacht über das Vereinsvermögen anzusehen. Eine etwaige satzungsmäßige Übertragung von Verfügungsrechten auf einzelne Mitglieder wie Vorstandsmitglieder und Schatzmeister würde sich mangels einer entsprechenden Registereintragung nur in dessen Innenverhältnis auswirken. Die Bank ist verpflichtet, aufgrund der Vorschriften des GWG die Identifizierung des Kontoinhabers, Erfassung der Kontrollrechte und Abklärung des wirtschaftlichen Berechtigten zu erfragen. Bei Zweifelsfragen hat der Kontoinhaber nach § 4 Abs. 6 GWG mitzuwirken. Da der Verein seiner Mitwirkungspflicht nicht nachkam, hat die Bank letztendlich die Geschäftsverbindung gekündigt und das Konto gelöscht.
Da sich der Verein in dieser Angelegenheit auch an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) gewandt hatte, hat der TLfDI die BaFin mit Einverständnis des Vereins gebeten, das Prüfergebnis zu übersenden. Die BaFin sieht die Verfahrensweise der Bank in diesem Fall als vertretbar an.
Im Ergebnis ist daher die von der Bank geforderte Übermittlung personenbezogener Daten der Vereinsmitglieder zur Ermittlung wirtschaftlich Berechtigter im Sinne der spezialgesetzlichen Normen des GWG nicht als Verstoß gegen datenschutzrechtliche Bestimmungen anzusehen. Es wird jedoch angeraten, in ähnlichen Fällen künftig die erforderlichen Prüfungen bereits vor Aufnahme der Geschäftsbeziehung vorzunehmen.

Nach § 4 GWG muss die Bank vor Eröffnung einer Geschäftsbeziehung den Geschäftspartner (wirtschaftlicher Berechtigter) identifizieren. Bei einem Verein, der nicht im Vereinsregister eingetragen ist, oder bei einer Gesellschaft bürgerlichen Rechts kann die Bank den wirtschaftlich Berechtigten nicht mittels Auskunft aus einem öffentlichen Register feststellen. Bei Zweifelsfragen hat der Kontoinhaber

(Verein) daher mitzuwirken und die Daten der Vereinsmitglieder zu übersenden.

3.46 Immer wieder der Geburtstag

Manche Menschen werden gerne an ihrem Geburtstag gefeiert und empfinden es als Affront, wenn ihr Geburtstag vergessen wird. Andere werden am liebsten gar nicht daran erinnert, dass schon wieder ein Jahr vergangen ist. Vor diesem Konflikt stehen auch Kollegen, die in einem Betrieb zusammen arbeiten. Regelmäßig erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen, ob es in Unternehmen zulässig ist, einen Geburtstagskalender mit den Angaben zu den Arbeitnehmern (Name und Datum) zu führen. Da es sich bei den Geburtstagsdaten um Arbeitnehmerdaten handelt, ist § 32 Bundesdatenschutzgesetz (BDSG) anzuwenden. Danach dürfen personenbezogene Daten eines Arbeitnehmers für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Eine konkrete Erforderlichkeit für diese Zwecke besteht bei dem Führen eines Geburtstagskalenders jedoch nicht.
Ohne zu verkennen, dass es sich bei der Gratulation zum Geburtstag um einen Teil im Rahmen des sozialen Miteinanders auch im Beschäftigungsbereich handelt, wäre eine Nutzung des Geburtsdatums der Arbeitnehmer nur mit der Einwilligung der Betroffenen möglich, da nach § 4 Abs. 1 BDSG die Verarbeitung und Nutzung personenbezogener Daten alternativ auch auf Einwilligungsbasis zulässig ist, wenn eine konkrete Rechtsvorschrift diesbezüglich nicht vorhanden ist. Die Anforderungen an eine Einwilligung sind in § 4 a BDSG aufgelistet. Sie könnte bestenfalls bereits bei der Einstellung eines Betroffenen eingeholt werden, wobei konkret auf den vorgesehenen Zweck (Gratulation zum Geburtstag) hingewiesen wird. Dabei muss eine Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Aus einer Verweigerung dürfen keine Folgen entstehen. Damit liegt es in der freien Entscheidung eines jeden Arbeitnehmers, ob er in einer Geburtstagsliste aufgenommen werden möchte. Die Angabe des Geburtsjahres ohne Einwilligung des Betroffenen ist jedenfalls

nicht zulässig, da sie zum Zweck der Gratulation zum Geburtstag nicht erforderlich ist.

Das Führen einer Geburtstagsliste ist nur zulässig für die Arbeitnehmer, die in die Nennung Ihres Geburtsdatums eingewilligt haben. Das Geburtsjahr darf nicht genannt werden.

3.47 Meldepflicht nach Hackerangriff

Wie auch immer wieder in verschiedenen Printmedien zu lesen ist, häufen sich in letzter Zeit Angriffe auf IT-Anlagen von Unternehmern. Ziel dieser Angriffe sind meist solche Daten, die für den Angreifer unmittelbaren finanziellen Vorteil bieten. Bankdaten zum Beispiel. Aus diesem Grund hat der Gesetzgeber den Unternehmen in solchen Fällen umfangreiche Pflichten aufgegeben. § 42 a Bundesdatenschutzgesetz (BDSG) sieht vor, dass Unternehmen, denen besondere personenbezogene Daten abhanden gekommen oder von diesen solche Daten unrechtmäßig an Dritte übermittelt worden sind, weitreichenden Informations- und Meldepflichten unterliegen. Unter besonderen personenbezogenen Daten versteht man nach § 3 Abs. 9 BDSG „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben“. Denselben Pflichten unterliegen diese Unternehmen, wenn statt der besonderen personenbezogenen Daten, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, oder eben auch personenbezogene Daten zu Bank- oder Kreditkartenkonten betroffen sind.
Zunächst muss das Unternehmen prüfen, ob für die Betroffenen schwerwiegende Beeinträchtigungen ihrer Rechte drohen. Dabei handelt es sich um eine Einzelfallentscheidung. Zumindest aber bei Bank- oder Kreditkartendaten dürfte dies immer der Fall sein. Drohen solche Beeinträchtigungen, sind durch das Unternehmen der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sowie die einzelnen Betroffenen zu informieren. Diese Information hat unverzüglich zu erfolgen, das heißt ohne schuldhaftes Zögern, nachdem Maßnahmen zur Sicherung der entsprechenden Daten eingeleitet wurden. Einzige Ausnahme hierzu ist eine eventuelle Gefährdung strafrechtlicher Ermittlungen. Die Aufsichtsbehörde und die Betroffenen sind darüber zu unterrichten, in

welcher Art und Weise Dritte unrechtmäßig Kenntnis der personenbezogenen Daten nehmen konnten. Auch müssen Hinweise und Empfehlungen zu Maßnahmen enthalten sein, mit denen mögliche nachteilige Folgen gemindert werden können.
Aus Unternehmenssicht bietet es sich an, einen Notfallplan zu erarbeiten, der alle notwendigen Maßnahmen im Falle eines Abhandenkommens von Daten beschreibt, so eben auch die notwendigen Meldungen an die Betroffenen und den TLfDI. Diese „Checkliste“ ist zwar nicht gesetzlich vorgeschrieben, erleichtert jedoch das Vorgehen im Falle des Falles. Dies ist auch deswegen wichtig, weil eine vergessene, verspätete oder unzureichende Meldung nach § 42 a BDSG vom TLfDI mit einer Geldbuße von bis zu 300.000 Euro geahndet werden kann.
In Thüringen gab es für den Berichtszeitraum vier Meldungen, die beim TLfDI eingegangen sind und geprüft wurden.

Sobald ein Unternehmen feststellt, dass personenbezogene Daten, die in den Anwendungsbereich von § 42 a BDSG fallen, abhanden gekommen sind, ist der Aufsichtsbehörde und den Betroffenen unverzüglich eine dem § 42 a BDSG entsprechende Mitteilung zu machen. Andernfalls drohen empfindliche Geldbußen. Daher ist es sinnvoll, zumindest in Unternehmen, in denen ein meldepflichtiger Fall nicht unwahrscheinlich ist, für alle Fälle einen Notfallplan zu entwerfen.

3.48 Personalausweiskopie? Schrott!

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) liegen mehrere Eingaben vor, in denen sich Bürger darüber beschweren, dass Metall-Recycling-Firmen den angebotenen Metallschrott nur dann annehmen, wenn die Lieferanten der Erstellung einer Kopie ihres Personalausweises zustimmen. Eine solche Praxis hält der TLfDI für unzulässig.
Das betroffene Unternehmen gab an, dass die Bundesvereinigung Deutscher Stahl-Recycling- und Entsorgungsunternehmen e. V. in einem Rundschreiben das Kopieren von Personalausweisen empfiehlt. Im Schrotthandel gebe es einige „schwarze Schafe“. Die Finanzbehörden hätten deshalb die gesetzlichen Nachweis- und Dokumentationserfordernisse deutlich verschärft. Es sei in der Vergangenheit regelmäßig zur Nichtanerkennung von Betriebsausgaben

durch die Finanzbehörden gekommen, wenn der Ankäufer nicht den Empfänger der Zahlungen zweifelsfrei benennen konnte. Im Rahmen eines solchen Empfängerbenennungsverfahrens des Finanzamtes nach § 160 der Abgabenordnung sei es inzwischen häufiger vorgekommen, dass die Finanzbehörden die Benennung vordringlich mittels Vorlage einer Personalausweiskopie einforderten.
Der TLfDI wandte sich daraufhin an die Thüringer Landesfinanzdirektion. Diese teilte mit, dass seitens der Thüringer Finanzbehörden von den Schrott- bzw. Recyclingfirmen keine Kopien der Personalausweise der Lieferanten für steuerliche Zwecke verlangt würden. Damit besteht keine Erforderlichkeit des Kopierens des Personalausweises und auch keine Rechtsgrundlage für diese Datenerhebung. Die Anfertigung von Personalausweiskopien ist nicht nach § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich.
Die Unzulässigkeit der Anfertigung einer Kopie des gesamten Personalausweises ergibt sich insbesondere aus den §§ 14 ff des Personalausweisgesetzes (PAuswG). Nach § 14 Nr. 2 PAuswG darf die Erhebung und Verwendung personenbezogener Daten auf dem Ausweis oder mit Hilfe des Ausweises ausschließlich durch öffentliche und nicht-öffentliche Stellen nach Maßgabe der §§ 18 bis 20 PAuswG erfolgen. Die Vorlage eines Personalausweises dient primär der Erfüllung der gesetzlich vorgeschriebenen Ausweispflichten im öffentlichen Bereich. §§ 18 und 19 PAuswG regeln den elektronischen Identitätsnachweis. Darüber hinaus ist es nach § 20 Abs. 1 PAuswG auch zulässig, den Personalausweis als Ausweis- und Legitimationspapier zu verwenden. Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nicht-öffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden, § 20 Abs. 2 PAuswG. In der Gesetzesbegründung zu § 14 PAuswG heißt es: „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mit Hilfe des Ausweises künftig nur über die vorgesehenen Wege erfolgen darf. […] Weitere Verfahren z. B. über die optoelektronische Erfassung („Scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden.“ (BR-DRs 550/2008 Seite 69 f).
Der TLfDI beabsichtigt daher das Unternehmen unter Zwangsgeldandrohung aufzufordern, für die Zukunft keine Personalausweisko-

pien mehr anzufertigen. Zulässig ist allenfalls die Kopie des Personalausweises mittels einer Schablone, auf der die nicht-erforderlichen Daten, wie das Lichtbild und die Personalausweisnummer verdeckt sind. Ansonsten reicht es aus, wenn das Unternehmen vermerkt, dass sich eine betreffende Person mittels Personalausweis ausgewiesen hat. Das entsprechende Verwaltungsverfahren läuft derzeit noch.

Die Anfertigung von Personalausweiskopien durch nicht-öffentliche Stellen ist grundsätzlich unzulässig. In aller Regel ist die Anfertigung einer Kopie des Personalausweises zur Erfüllung eigener Geschäftszwecke oder zur Wahrnehmung berechtigter Interessen nicht erforderlich, weil die Identität des Betroffenen vor Ort selbst durch Vorlage des Personalausweises geklärt werden kann.

3.49 Video im Wind: Videogaga 23

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass – wahrscheinlich durch den Betreiber eines Windparks – in einer bestimmten Region öffentliche Wege in Thüringen videoüberwacht würden. Der TLfDI musste zunächst die verantwortliche datenverarbeitende Stelle ermitteln und schrieb das Unternehmen an, das in der betreffenden Region Windräder betreibt. Nach umfangreichen Aufklärungsarbeiten stellte sich heraus, dass das in Thüringen ansässige Unternehmen nicht der Betreiber der vorhandenen Videoüberwachung war. Das Thüringer Unternehmen liefert lediglich die Windenergieanlagen. Eine Firma, die in einem anderen Bundesland ansässig ist, war jedoch der Betreiber und hatte auch die Videoüberwachung vor Ort zu verantworten. Diese Firma hat zwischenzeitlich mitgeteilt, dass die Videoüberwachung eingestellt worden sei; damit war über die Frage der Zuständigkeit des TLfDI für den vorliegenden Sachverhalt nicht mehr zu entscheiden.
Grundsätzlich kommt es für die Zuständigkeit der Aufsichtsbehörde darauf an, in welchem Bundesland die datenverarbeitende Stelle ihren Sitz hat. Da weder das Bundesdatenschutzgesetz noch das Thüringer Datenschutzgesetz zur örtlichen Zuständigkeit der Aufsichtsbehörde Regelungen treffen, ist das Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) ergänzend heranzuziehen. Nach § 3 Abs. 1 Nr. 2 ThürVwVfG ist in Angelegenheiten, die sich auf

den Betrieb eines Unternehmens oder einer seiner Betriebsstätten beziehen, die Behörde örtlich zuständig, in deren Zuständigkeitsgebiet das Unternehmen oder die Betriebsstätte betrieben wird oder werden soll.

Für die örtliche Zuständigkeit der Aufsichtsbehörde ist grundsätzlich der Sitz der datenverarbeitenden Stelle entscheidend. Grundsätzlich ist die Aufsichtsbehörde zuständig, in deren Gebiet (Bundesland) sich der Sitz des Unternehmens befindet. Bei Betriebsstätten in anderen Bundesländern kann es zu abweichenden Zuständigkeiten kommen.

3.50 Pakete auf datenschutzrechtlichen Abwegen: Videogaga 24

Aufgrund einer Beschwere wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auf einen Missstand in einem Paketshop aufmerksam. Über zweierlei beschwerte sich der Bürger: Zum einen würden die zur Abholung bereitliegenden Pakete teilweise für jedermann sichtbar im Laden herumliegen, weswegen jeder, der wollte, Absender und Adressat erkennen könne, zum anderen könne man die Pakete nur gegen Vorzeigen des Personalausweises und Speicherung bestimmter darauf enthaltender Daten, wie zum Beispiel der Ausweisnummer, abholen. Bei der in der Folge durch den TLfDI durchgeführten Kontrolle wurden diese Umstände bestätigt und ein weiteres Problemfeld aufgetan.
Beide vom Bürger gerügten Aspekte sind datenschutzrechtlich relevant. Gemäß § 39 des Postgesetzes unterliegen alle näheren Umstände des Postverkehrs natürlicher wie auch juristischer Personen sowie der Inhalt der Postsendung dem Postgeheimnis. Zu den näheren Umständen des Postverkehrs gehören insbesondere alle Verbindungsdaten, die nicht den Inhalt der konkreten Sendung selbst betreffen, wie z. B. Name und Anschrift des Absenders und Empfängers, Ort und Zeit der Aufgabe der Postsendung, Art und Weise der Inanspruchnahme der Dienstleistung. Daher ist es erforderlich, dass Pakete und Briefsendungen so aufbewahrt werden müssen, dass Dritte nicht die Möglichkeit haben, auf diese Daten zuzugreifen. Damit ist es aus datenschutzrechtlicher Sicht unzulässig, Pakete auf eine Art zu lagern, die es unbeteiligten Dritten ermöglicht, Adressat und Absender zur Kenntnis zu nehmen.

Hinsichtlich der Abholung der Pakete stellt sich die Rechtslage ein wenig komplizierter dar. Gemäß § 8 Abs. 1 der Postdienste-Datenschutz-Verordnung (PDSV) können die Postdienstleister verlangen, dass sich die am Postverkehr beteiligte Person durch Vorlage eines gültigen Personalausweises oder Passes oder durch Vorlage sonstiger amtlicher Ausweispapiere ausweist, wenn dies erforderlich ist, um die ordnungsgemäße Ausführung des Postdienstes sicherzustellen. Gemäß § 8 Abs. 2 PDSV kann der Postdienstleister die Art des Ausweises, die ausstellende Behörde sowie die Nummer des Ausweises und das Ausstellungsdatum speichern, sofern ein besonderes Beweissicherungsinteresse dahingehend besteht, dass der jeweilige Postdienst ordnungsgemäß ausgeführt wurde. Dieses Beweissicherungsinteresse besteht bereits hinsichtlich des Zugangs von Paketen. Insoweit stellt das Speichern dieser Informationen kein datenschutzrechtliches Problem dar. Allerdings verlangte der Paketshop zwingend einen Pass oder Personalausweis. Unter den Begriff des amtlichen Dokuments fallen jedoch alle Dokumente, die von einer Behörde zum Zwecke des Ausweisens ausgegeben wurden, beispielsweise der Führerschein. Dies ist insoweit ein Problem, als dass das informationelle Selbstbestimmungsrecht, soweit der gesetzliche Rahmen dies zulässt, dem Einzelnen auch die Entscheidung überlässt, welche personenbezogenen Daten erhoben und gespeichert werden. Hierzu gehört auch die Entscheidung darüber, ob der Einzelne sich bei Abholung eines Pakets lieber per Ausweis oder zum Beispiel per Führerschein ausweisen möchte.
Im Rahmen der Kontrolle konnte die verantwortliche Stelle jedoch glaubhaft machen, dass ihr durch das entsprechende Paketunternehmen keine Wahl bei den Ausweisdokumenten eingeräumt wird. Das vom versendenden Unternehmen bereitgestellte Programm akzeptiert ausschließlich Pass- oder Personalausweisnummern, ansonsten ist das Austragen von Sendungen und deren Übergabe an den Kunden nicht möglich. Hinsichtlich dieser Problematik wird sich der TLfDI mit der für das Paketunternehmen zuständigen Aufsichtsbehörde in Verbindung setzen.
Ebenfalls wurde bei der durchgeführten Kontrolle festgestellt, dass in dem Unternehmen eine umfangreiche Videoüberwachung durchgeführt wurde. Nach rechtlicher Prüfung musste der TLfDI feststellen, dass diese nach § 6 b BDSG nicht erforderlich und damit unzulässig war. Auf einer Ladenfläche von ca. 7 qm wurden drei Videokameras aus verschiedenen Blickwinkeln betrieben. Zweck der

Überwachung sollte die Verfolgung von Diebstählen sein. Hierzu ist bei einer solch kleinen Ladenfläche jedoch keine Videoüberwachung erforderlich. Vielmehr kann die Verkaufsfläche hier ohne weiteres durch den Verkäufer überwacht werden.
Noch dazu übertrug das Unternehmen die Videoaufnahmen „live“ ins Internet und publizierte diese auf der Homepage des Unternehmens. Ein solches Vorgehen stellt selbstverständlich einen massiven Datenschutzverstoß dar, der unabhängig von der grundsätzlichen Zulässigkeit einer Videoüberwachungsanlage unzulässig ist, da diese Datenübermittlung nicht durch § 28 Abs. 1 BDSG gedeckt ist. Diese Norm regelt die Zulässigkeit des Umgangs mit personenbezogenen Daten zu eigenen Geschäftszwecken. Auf den Hinweis des TLFDI hin stellte das Unternehmen die Übertragung über das Internet unverzüglich ein.
Der TLfDI hat dem Unternehmen mitgeteilt, dass die Lagerung der Pakete so zu erfolgen hat, dass eine Einsichtnahme Dritter in Absender- oder Adressdaten nicht möglich ist. Sofern das Unternehmen dieser Aufforderung nicht nachkommt, wird der TLfDI eine entsprechende Anordnung erlassen, mit der das Unternehmen zu einer datenschutzgerechten Handhabung angehalten wird.
Wegen der durchgeführten unzulässigen Videoüberwachung und der Übertragung der Bilddaten auf die Unternehmenshomepage wird der TLfDI ein Ordnungswidrigkeitenverfahren gegen das Unternehmen oder dessen Geschäftsführer einleiten.

Pakete sind in Läden, die neben ihrem eigentlichen Kerngeschäft auch als Paketshop dienen, so aufzubewahren, dass Kunden die entsprechenden Adressaufkleber nicht einsehen können, da diese dem Postgeheimnis unterfallen.

3.51 „Livestream“ aus dem Friseursalon: Videogaga 25

Auf einen Hinweis hin erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass die Inhaberin eines Friseursalons auf der Homepage eine „Live-Ansicht“ ihres Geschäftes veröffentlicht habe, wodurch Arbeitnehmer und Kunden für jedermann jederzeit im Internet sichtbar wären.
Nach Recherchen des TLfDI war auf der Homepage des Friseursalons über einen Link tatsächlich eine „Live-Ansicht“ möglich, indem durch ein Anklicken auf den Spruch „Klicken Sie hier und schauen

Sie uns bei der Arbeit zu“ ein „Livestream“ aus dem Friseursalon einsehbar war. Die Aufnahmekamera war unmittelbar auf die Friseurstühle gerichtet, sodass Kunden und Arbeitnehmer vollständig gesehen werden konnten. Zum Zwecke der Beweiserhebung wurden mehrere Screenshots aufgenommen und der Akte beigefügt. Darauf zu sehen waren die Inhaberin des Friseursalons und ein männlicher Kunde, dem gerade die Haare geschnitten wurden sowie eine weitere Kundin, die für ein kurzes Gespräch das Geschäft betreten hatte.
Nachdem die Saloninhaberin vom TLfDI aufgefordert wurde, einen Fragenkatalog unter anderem zum Zweck der Videoüberwachung zu beantworteten und die angeforderten Nachweise, wie zum Beispiel den Grundriss des Salons, den Standort der Kamera und Screenshots beim TLfDI einzureichen, erläuterte der TLfDI den Sachverhalt wie folgt: Eine Videokamera ist eine Überwachungsanlage. Ihr bleibt nichts verborgen. Gerade am Arbeitsplatz kann eine Überwachung dazu führen, dass man sich ständig beobachtet und kontrolliert fühlt. Bei der Überwachung am Arbeitsplatz stoßen zudem die Interessen von Arbeitnehmer und Arbeitgeber aufeinander.
Die Aufzeichnung von Bildern stellt eine Datenerhebung dar, die nach § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig ist, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift sie erlaubt. Weder die Kunden noch die Arbeitnehmer hatten in die Videoüberwachung wirksam eingewilligt. Die Kunden waren sich zum einen der Überwachung oftmals nicht bewusst, zum anderen kann aufgrund des bloßen Verweilens in dem Geschäft nicht von einer wirksamen Einwilligung ausgegangen werden. Nach § 4 a Abs. 1 Satz 3 BDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Hiervon kann angesichts der Schwere des Eingriffs nicht ausgegangen werden. Eine wirksame Einwilligung setzt jedenfalls voraus, dass der Betroffene sich der Art und des Umfangs des Eingriffes bewusst ist. Dies war nicht der Fall. Bei Arbeitnehmern kann aufgrund des bestehenden Abhängigkeitsverhältnisses zum Arbeitgeber generell nicht von einer nach § 4 a Abs. 1 Satz 1 BDSG erforderlichen, „freien Entscheidung des Betroffenen“ ausgegangen werden.
Als mögliche gesetzliche Grundlage für eine Videoüberwachung kommt § 6 b BDSG in Betracht. Bei öffentlich zugänglichen Flächen und Arbeitsplätzen, wie in diesem Fall dem Friseursalon, ist die Videokontrolle gemäß § 6 b BDSG nur erlaubt, wenn sie zur Wahr-

nehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Die Inhaberin des Salons benannte als Zweck der Videoüberwachung und Übertragung ins Internet die Werbung für ihr Geschäft. Hierbei handelt es sich sicherlich um ein berechtigtes Interesse, für das die Videoüberwachung auch noch erforderlich sein mag. Jedenfalls aber überwiegen die schutzwürdigen Interessen der Kunden und Arbeitnehmer daran, bei dem Friseurbesuch oder bei der Arbeit nicht gefilmt zu werden sowie daran, dass diese Aufnahmen nicht der Weltöffentlichkeit zur Verfügung gestellt werden.
Die Saloninhaberin wurde vom TLfDI aufgefordert, die Videoüberwachung nach Erhalt des Schreibens unverzüglich zu beenden. Die Kamera war sofort zu entfernen. Des Weiteren war der Link „Klicken Sie hier und schauen Sie uns bei der Arbeit zu“ sowie der dazugehörige Hinweis: „Live Ansicht“ von der Homepage zu entfernen. Den entsprechen Nachweis hat die Saloninhaberin beim TLfDI erbracht.

Ein Livestream (aus dem Friseursalon) stellt immer einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Kundinnen und Kunden und der Arbeitnehmerinnen und Arbeitnehmer dar. Hier überwiegen in aller Regel die schutzwürdigen Interessen dieser Betroffenen das Interesse derjenigen Person, die die Aufnahmen ins Internet einstellt.

3.52 Peepshow im Wald: Videogaga 26

Die Presse berichtete wiederholt über die datenschutzrechtliche Problematik bei Tierbeobachtungskameras im Wald. Rechtlich stellt sich die Lage wie folgt dar:
Die Zulässigkeit von Tierbeobachtungskameras ist nach dem Bundesdatenschutzgesetz (BDSG) zu beurteilen. Nach § 6 b BDSG ist die Beobachtung öffentlich zugänglicher Bereiche zur Wahrnehmung berechtigter Interessen zulässig, wenn die damit verfolgten Zwecke vorher konkret festgelegt worden, die Beobachtung auch zur Erfüllung dieser Zwecke erforderlich ist und keine Anhaltspunkte für ein Überwiegen schutzwürdiger Interessen der Betroffenen erkennbar sind. Es ist daher im Einzelfall eine Abwägung zwischen den

Interessen des Kamerabetreibers, in aller Regel des Jägers, und den Interessen der Personen abzuwägen, die potenziell Gegenstand der Videobeobachtung im Wald werden können. Aufgrund des Grundrechts auf informationelle Selbstbestimmung nach Artikel (Art.) 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz bzw. Art. 6 Abs. 2 Thüringer Verfassung hat jeder Einzelne das Recht, sich in der Öffentlichkeit frei und ungezwungen aufhalten zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Jedermann darf sich im Wald generell frei bewegen und auch abseits der Wald- bzw. Wanderwege durch das Gelände streifen. Hierbei rechnet er keinesfalls damit, in den Aufnahmebereich einer Videokamera zu gelangen. Bei dem Aufenthalt im Wald stehen die Entspannung und der Rückzug der Persönlichkeit im Vordergrund. Daher besteht hier ein besonders hoher Schutzbedarf des Persönlichkeitsrechts des Betroffenen. Es ist daher davon auszugehen, dass in aller Regel die schutzwürdigen Interessen derjenigen überwiegen, die potenziell von der Videoüberwachung erfasst werden können. Jedenfalls sind aber Anhaltspunkte für ein solches Überwiegen vorhanden, weswegen die Kameras zur Wildbeobachtung in der Regel unzulässig sind.
Aus diesem Grund trat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an das Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz (TMLFUN) heran, und bat um Mitteilung, ob und gegebenenfalls an welchen Stellen es in Thüringen derartige Videoüberwachung durch Jäger im Wald gibt. Dieses teilte mit, dass es unter anderem zur Überwachung von Schwarzwildkirrungen oder zum Nachweis von Luchs oder Wildkatze über sogenannte Risse Fotofallen gäbe, die Jäger aus privaten Gründen betrieben. Angaben zu konkreten Standorten oder zu Videoüberwachung konnten nicht gemacht werden.
Der TLfDI kann nur tätig werden, wenn konkrete Hinweise auf eine bestimmte Videoüberwachung vorliegen. Es gab eine Beschwerde, bei der ein Beschwerdeführer lediglich Fotos von der Kamera einreichte, den genauen Standort der Videoüberwachung im Wald aber – auch auf Nachfrage hin – nicht näher bezeichnete. Daher konnte der Eingabe nicht nachgegangen werden. Der TLfDI steht allerdings mit dem Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt hinsichtlich der allgemeinen datenschutzrechtlichen Problematik mit Wildkameras in Kontakt.

In aller Regel überwiegen bei Tierbeobachtungskameras im Wald die schutzwürdigen Interessen der von der Videoüberwachung Betroffenen und die Videoüberwachung ist unzulässig. Der TLfDI kann allerdings nur bei konkreten Hinweisen tätig werden.

3.53 Offene Tür

Fast zufällig entdeckte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in den Betriebsräumen eines alten volkseigenen Betriebes eine Vielzahl an Arbeitnehmerakten, die mehr oder weniger zugänglich in den alten Betriebsräumen gelagert wurden. Die Akten befanden sich in einem Raum, der durch einen „leeren“ Türrahmen, das heißt ohne Tür, zugänglich war. Einzigen Schutz vor Zugriffen Dritter bot der nicht ganz einfach zu findende Weg durch das Gebäude selbst. Noch dazu war dieses teilweise an andere Unternehmen vermietet, die theoretisch dadurch einfach Zugang zu den Akten hatten.
Dies stellt selbstverständlich einen datenschutzrechtlich nicht hinnehmbaren Zustand dar. Datenschutzrechtliche Normen greifen nicht nur dann, wenn die verantwortliche Stelle personenbezogene Daten erheben, verarbeiten oder nutzen möchte. Vielmehr hat die verantwortliche Stelle auch so genannte technische und organisatorische Maßnahmen zu treffen, durch die sichergestellt ist, dass die Anforderungen des Bundesdatenschutzgesetzes (BDSG) gewährleistet werden, § 9 BDSG. Eine solche technische Maßnahme stellt in diesem Fall beispielsweise eine Tür mit Schloss und Schlüssel, eine organisatorische Maßnahme die dazugehörige Schlüsselregelung dar.
Da die nach BDSG verantwortliche Stelle nicht ohne weiteres feststellbar war, wurden die Akten unter zu Hilfenahme des örtlich zuständigen Ordnungsamtes zunächst gegen einen Zugriff Unbefugter gesichert. Inzwischen konnte der TLfDI aber die verantwortliche Stelle ermitteln. Auf Wirken des TLfDI hin wird eine ausreichend sichere Tür installiert, damit die Arbeitnehmerakten bis ans Ende ihrer Aufbewahrungsfrist sicher verwahrt werden können.

Arbeitnehmerakten müssen nach den Vorschriften des BDSG gelagert werden. Entweder gibt man diese dazu in die Hände eines seriösen Aktenverwahrunternehmens und schließt den hierzu notwendigen Auftragsdatenverarbeitungsvertrag ab oder man lagert die Akten selbst. In letzterem Fall ist allerdings ebenfalls mit derselben Sorgfalt

das Mindestmaß an Datenschutz, so wie es das BDSG beschreibt, einzuhalten.

4 Ordnungswidrigkeitenverfahren

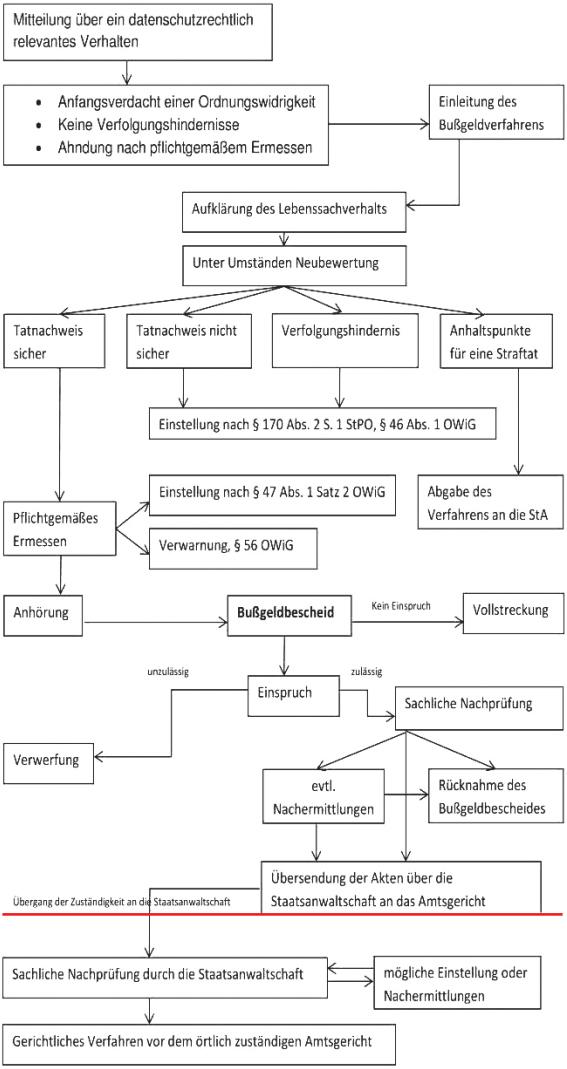
Mit Übertragung der Zuständigkeit für den Datenschutz im nicht-öffentlichen Bereich auf den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist dieser auch zuständige Behörde für Ordnungswidrigkeiten nach § 43 Bundesdatenschutzgesetz (BDSG) geworden. Das Verfahren musste auch behördenintern neu aufgebaut werden, da es sich um ein vom bisherigen Zuständigkeitsbereich völlig unterschiedliches Verfahren handelt. Das Ordnungswidrigkeitenverfahren bietet mit seinen großzügigen Verweisen in das Strafprozessrecht eine Vielzahl an neuen Ermittlungsansätzen, mit denen sich die Behörde zunächst vertraut machen musste. Es ist davon auszugehen, dass die Fallzahlen weiter stark ansteigen werden. Das Ordnungswidrigkeitenverfahren ist eine besondere Unterart des Verwaltungsverfahrens. Es ist streng von anderen Verfahren zu trennen. Im Unterschied zum grundsätzlich formfreien Verwaltungsverfahren handelt es sich um ein streng formalisiertes Verfahren mit vielen Parallelen zum strafrechtlichen Ermittlungsverfahren. Ziel des Verfahrens ist es, Verstöße gegen das Bundesdatenschutzgesetz zu ahnden und auf diesem Wege eine Änderung im Verhalten des Verstoßenden zu erreichen.
Im Wesentlichen teilt sich die Befugnis des TLfDI bei Ordnungswidrigkeiten wegen eines Verstoßes gegen Formalien des BDSG sowie gegen inhaltliche Vorgaben des BDSG auf. Erstere können mit einem Bußgeld bis zu 50.000 Euro, letztere mit bis zu 300.000 Euro geahndet werden. Dabei wird die Höhe der Geldbuße durch die Bedeutung der Ordnungswidrigkeit und den Vorwurf, der den Täter trifft, bestimmt. Es wird also die vorsätzliche Übermittlung von Gesundheitsdaten mit einem höheren Bußgeld geahndet als die versehentliche Herausgabe von Kundendaten eines Tabakgeschäftes, wobei die Herausgabe eines Datensatzes weniger schwer wiegt, als die Herausgabe vieler Datensätze. Letztlich ist die Höhe des Bußgeldes immer anhand des Einzelfalls und der damit einhergehenden Besonderheiten festzumachen. An die eben genannten Obergrenzen ist der TLfDI bei der Bemessung der Geldbuße allerdings dann nicht gebunden, wenn durch den zu ahndenden Verstoß ein wirtschaftlicher Vorteil über diesen Betrag hinaus entstanden ist. Diesen Vorteil soll die Geldbuße auf jeden Fall übersteigen. Verstöße gegen das BDSG können auch als Straftaten verfolgt werden. Stellt der TLfDI

im Rahmen seiner Ermittlungen oder seiner sonstigen Verwaltungstätigkeit fest, dass der Tatbestand einer Ordnungswidrigkeit gegen Entgelt, mit Bereicherungs- oder Schädigungsabsicht verwirklicht worden ist, gibt er das Verfahren zur Straftatverfolgung an die zuständige Staatsanwaltschaft ab. Der TLfDI verfügt über ein eigenes Strafantragsrecht.

Wegen der Sensibilität von Berichten über Datenschutzverstöße im nicht-öffentlichen Bereich im Allgemeinen und im Bereich der Ordnungswidrigkeiten im Speziellen kann über die Tätigkeit des TLfDI in diesem Bereich nur sehr allgemein berichtet werden. Seit der Übernahme dieses Bereiches durch den TLfDI sind die Fallzahlen von 2011 auf 2012 um 100 % angestiegen, von 2012 zu 2013 gar um 250 %. Die Tendenz ist weiterhin steigend.

Zur besseren Verständlichkeit und Übersicht ist das Bußgeldverfahren hier als Grafik dargestellt, in der man die jeweils möglichen Verfahrenswege und -möglichkeiten erkennen kann. Ab der roten Linie sieht das Ordnungswidrigkeitenrecht vor, dass das Verfahren aus der Zuständigkeit der Verwaltungsbehörde (TLfDI) als Ermittlungsbehörde in die Zuständigkeit der Staatsanwaltschaft übergeht.

Übersicht über den Ablauf eines Bußgeldverfahrens



Bei den bisher anhängigen Verfahren wird in den meisten Fällen wegen Verstößen gegen das unbefugte Erheben oder Übermitteln von personenbezogenen Daten ermittelt. Berichtet wird hier nur über Fälle, die bereits abgeschlossen sind.
Interessant war ein Verfahren gegen einen Auszubildenden einer Bank, der einem besonderen Berufsgeheimnis unterlag. Der Auszubildende gab Informationen über einen Kunden seiner Arbeitgeberin an Dritte weiter. Dies erfüllt den Bußgeldtatbestand nach § 43 Abs. 2 Nr. 1 BDSG. Hier wird mit Bußgeld bedroht, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Die Weitergabe der Informationen stellt eine Übermittlung dar, die in den Überbegriff der Verarbeitung fällt. Damit war der Tatbestand erfüllt und der TLfDI erließ einen Bußgeldbescheid gegen den Auszubildenden. Eingeräumt wurde, dass er den Bußgeldbetrag in zwei Raten begleicht.
In einem weiteren Fall wandte sich ein Arbeitnehmer an den TLfDI mit folgendem Hinweis: Er habe bei zwei verschiedenen Arbeitgebern gearbeitet. Sein „Hauptarbeitgeber“ verlangte im Rahmen einer arbeitsrechtlichen Streitigkeit wegen nicht genehmigter Nebentätigkeit vom anderen Arbeitgeber den Arbeitsvertrag heraus, den dieser dann auch an den Hauptarbeitgeber faxte. Eine Übermittlung personenbezogener Daten ist jedoch nur dann möglich, wenn das BDSG oder eine andere datenschutzrechtliche Vorschrift hierzu einen Erlaubnistatbestand bereithält oder der Betroffene in die Übermittlung eingewilligt hat. Eine Einwilligung lag hier nicht vor. Ebenfalls war ein Erlaubnistatbestand nicht gegeben. Im Rahmen des Arbeitsverhältnisses kommt allenfalls § 32 BDSG als Erlaubnistatbestand in Frage. Dieser genehmigt das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses, soweit diese für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich sind. Hier mangelte es schon an der Zweckbindung der Handlung. Die Übersendung eines Arbeitsvertrages an Dritte ging hier über den Zweck des Beschäftigungsverhältnisses hinaus. Damit stellte das Versenden des Arbeitsvertrages eine unerlaubte Übermittlung dar, § 43 Abs. 2 Nr. 1 BDSG. Der TLfDI erließ dementsprechend einen Bußgeldbescheid gegen den (Neben-)Arbeitgeber.
Ähnlich gelagert war ein Fall um einen Hotelier, der einem Ehemann auf dessen Anfrage hin Angaben machte, mit welchem anderen

Mann dessen Ehefrau im Hotel übernachtet hätte. Da das BDSG keinen Übermittlungstatbestand für die Bekanntgabe eventueller Seitensprüngen bereithält, handelte es sich auch hierbei um eine vorsätzliche unerlaubte Übermittlung nach § 43 Abs. 2 Nr. 1 BDSG. Der Hotelier ging gegen den vom TLfDI erlassenen Bußgeldbescheid mit dem Rechtsmittel des Einspruchs vor, unterlag damit allerdings vor Gericht.

Nicht alle Anzeigen von angeblichen Ordnungswidrigkeiten nach dem BDSG führen zu einem Bußgeldbescheid. Oftmals ist eine Ordnungswidrigkeit nach dem laienhaften Empfinden zu einem Vorgang oder Sachverhalt zwar gegeben, stellt nach rechtlicher Betrachtung aber keine solche dar. Die Einstellung des Verfahrens ist dann zwingende Folge. Es kommt auch vor, dass sich dem „Täter“ nicht mehr alle notwendigen Elemente der Tat nachweisen lassen. Denn, daran muss man immer denken: Der TLfDI muss dem, gegenüber dem er einen Bußgeldbescheid erlässt, die Ordnungswidrigkeit in allen Punkten nachweisen. Dies ist nicht immer möglich. In solchen Fällen gilt die Unschuldsvermutung, mit der Folge, dass das Verfahren eingestellt werden muss.

Einen weiteren, weit verbreiteten Bußgeldtatbestand stellt das nicht oder nicht vollständige Beantworten von Auskunftsersuchen des TLfDI seitens der verantwortlichen Stellen, in der Regel Unternehmen, dar. Dies ist überraschend, denn die Tatsache, dass die Angeschriebenen zur Antwort verpflichtet sind und ein Unterlassen mit einem Bußgeld geahndet werden kann, wird bereits im ersten Anschreiben mitgeteilt. Die Antwort bekommt der TLfDI immer, es wird irgendwann für die Betroffenen nur sehr teuer. Denn jedes erneute Auskunftsersuchen, das nicht beantwortet wird, stellt einen neuen Bußgeldtatbestand dar, der wiederum mit einem neuen Bußgeld geahndet werden kann.

So war der folgende Fall gelagert: Der TLfDI wandte sich mit einem Auskunftsersuchen unter Fristsetzung an einen Bürger. Es wurden Informationen über eine von dieser Person durchgeführte Videoüberwachung verlangt. Nachdem die Frist fruchtlos auslief, wurde eine Nachfrist gesetzt. Als innerhalb dieser Frist ebenfalls keine Antwort einging, erließ der TLfDI nach erfolgter Anhörung einen Bußgeldbescheid wegen vorsätzlichen Nichtantwortens auf ein Auskunftsersuchen des TLfDI nach § 38 Abs. 3 BDSG. Diese Ordnungswidrigkeit ist in § 43 Abs. 1 Nr. 10 BDSG geregelt.

Der größte Teil der Fälle, die der TLfDI im Berichtszeitraum bearbeitete, ist allerdings noch nicht abgeschlossen. Entweder dauern die Ermittlungen noch an oder die Bußgeldbescheide sind noch nicht rechtskräftig. Von den im Berichtszeitraum erlassenen Ordnungswidrigkeitsbescheiden ist bisher kein einziger durch ein Gericht aufgehoben worden.
In besonders schweren Fällen des Verstoßes gegen Vorschriften aus dem BDSG kann der TLfDI auch einen Strafantrag bei der zuständigen Staatsanwaltschaft stellen. Diese prüft dann in eigener Zuständigkeit das Vorliegen einer Straftat. Eine solche kommt dann in Betracht, wenn eine der in § 43 Abs. 2 BDSG bezeichneten Handlung vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, vorgenommen wird.
Im Berichtszeitraum hat der TLfDI einen Strafantrag gestellt. Dieser richtete sich gegen den ehemaligen Geschäftsführer und der-zeitigen Liquidator eines insolventen Aktenverwahrungsunternehmens.

Das Bußgeldverfahren wurde im Berichtszeitraum beim TLfDI erfolgreich aufgebaut. Es wird zunehmend an Bedeutung gewinnen, wie auch die steigenden Fallzahlen zeigen.

5 Veranstaltungen

Old man using a laptop with his grand son reading a newspaper
© Yuri Arcurs – Fotolia.com

5.1 TLfDI ist los!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) war im Berichtszeitraum auf zahlreichen Veranstaltungen vertreten bzw. führte selbst Veranstaltungen rund um das Thema Datenschutz durch:
So fand eine mehrtätige Fortbildungsveranstaltung zum Datenschutz im Sozialrecht im Jobcenter Jena statt. Die Arbeitnehmer hatten dem TLfDI zuvor Fragen zugesandt, die dann im Rahmen der Veranstaltung beantwortet wurden.
Für die Studierenden der Verwaltungsfachhochschule Gotha wurde eine Vorlesung zu den Grundlagen des in Thüringen geltenden Datenschutzrechts entwickelt. Die Studierenden wurden dann an zwei Tagen in das Datenschutzrecht eingeführt.
Zweimal fand ein Runder Tisch mit der Landeskrankenhausgesellschaft Thüringen und Vertretern der Landesärztekammer sowie Vertretern von Krankenhäusern zur Weiterentwicklung der Orientierungshilfe Krankenhausinformationssysteme statt (siehe 10. Tätigkeitsbericht für den öffentlichen Bereich Punkt 11.1).
Der TLfDI war in dem Jahr beim Tag der offenen Tür des Thüringer Landtags vertreten, sowie im Folgejahr beim Bürgerfest „Rund um die Verfassung“.
Gemeinsam mit der Verbraucherzentrale Thüringen e. V. und dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) führte der TLfDI eine Tagung „Soziale“ Netzwerke? Meine Daten! Mein Leben! – Dein Geschäft!“ durch. Bei dieser Veranstaltung sollten vor allem Schülern und Lehrern die Hintergründe Sozialer Netzwerke verdeutlicht und die damit verbundenen Probleme näher beleuchtet werden. Aufgrund der positiven

Resonanz, die der TLfDI wegen dieser Veranstaltung erhielt, führte er im Folgejahr wiederum gemeinsam mit der Verbraucherzentrale Erfurt e. V. eine Kooperationsveranstaltung zum Thema „Persönlichkeitsrechte – auch im Internet – keine Frage des Alters!“ durch, die sich speziell an Seniorinnen und Senioren richtete. Die Veranstaltung sollte den Teilnehmern in Vorträgen und Workshops ihre Rechte in der digitalen Welt aufzeigen. Der TLfDI war auch auf der Seniorenakademie der Stadt Gotha zum Thema „Der gläserne Bürger“ vertreten. Ebenfalls an Seniorinnen und Senioren richtete sich die Informationsveranstaltung der Eisenbahn- und Verkehrsgewerkschaft der Ortsverwaltung Erfurt, auf der der TLfDI zu Fragen des Datenschutzes zur Verfügung stand.

Mit der Evangelischen Akademie Thüringen und der Landesarbeitsgemeinschaft Kinder- und Jugendschutz e. V. veranstaltete der TLfDI eine Tagung zum Thema „Das Ende der Privatsphäre?“. Die Tagung befasste sich mit der Frage, wo heute die Grenzen zwischen Privatheit und Öffentlichkeit verlaufen und wie es gelingen kann, sinnvolle Regularien des digitalen Persönlichkeitsschutzes zu entwickeln.

Der TLfDI hat im Jahr 2013 in seiner Funktion als Landesbeauftragter für die Informationsfreiheit für ein Jahr den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland übernommen. In dieser Funktion richtete er zwei Sitzungen des Arbeitskreises der Informationsfreiheitsbeauftragten aus. Dieser Arbeitskreis bereitet die Sitzungen und Entschließungen der Konferenz der Informationsfreiheitsbeauftragten vor. Außerdem fanden am 27. Juni 2013 in Erfurt und am 28. November 2013 in Erfurt die 26. und 27. Konferenz der Informationsfreiheitsbeauftragten in Deutschland statt. Hierüber wird der TLfDI in seinem Tätigkeitsbericht als Informationsfreiheitsbeauftragter, der nächstes Jahr erscheinen wird, berichten.

Im Schulamt Nordthüringen führte der TLfDI eine Veranstaltung zum Thema Datenschutz und Internet als Fortbildungsveranstaltung für Lehrer durch. Ähnlich gelagerte Informationsveranstaltungen fanden am Friedrich-Schiller-Gymnasium Weimar, am Gustav-Freytag-Gymnasium Gotha und am Albert-Schweitzer-Gymnasium Ruhla für Lehrer statt.

Im Thüringer Landtag hielt der TLfDI für Bachelor-/Masterstudenten einen Vortrag über Maßnahmen zur Einhaltung bzw. Verbesserung des Datenschutzes in Thüringen speziell für

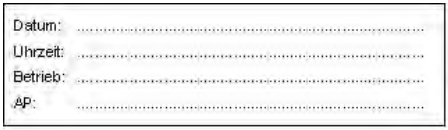
den Bereich Transport und Verkehr. Er nahm außerdem an der Podiumsdiskussion zum Thema „Die totale Überwachung - Gefahr im Netz für die Gesellschaft, für die Demokratie und für Medien?“ des Vereins zur Förderung der angewandten Informatik der Fachhochschule Erfurt teil.
Gegenüber dem Verband der Verwaltungsbeamten des höheren Dienstes in Thüringen e. V. stellte der TLfDI seine Behörde und ihr Aufgabengebiet vor. Dem gleichen Zweck diente die Teilnahme an der Konferenz der Datenschutzbeauftragten im Bereich der Katholischen Kirche Deutschlands am 19./20. Oktober 2013.
Der TLfDI war auch auf einigen Veranstaltungen der Industrie- und Handelskammern in Thüringen vertreten, hierzu wird auf den Beitrag unter Punkt 3.2 verwiesen. Im Berichtszeitraum nahm der TLfDI daneben an vier Sitzungen des ERFA-Kreises teil. Die Gesellschaft für Datenschutz und Datensicherheit e. V. hat zur Durchführung ihrer Aufgaben regionale Erfahrungsaustauschkreise (ERFA-Kreise) gebildet, die zum Ziel haben, die Arbeit der Teilnehmer in Fragen des Datenschutzes und der Datensicherheit zu unterstützen. Die ERFA-Kreise stehen grundsätzlich allen Interessierten offen, bedürfen jedoch der vorherigen Anmeldung. Eingeladen sind in erster Linie Datenschutzbeauftragte.
Die Fraktion „DIE LINKE“ initiierte eine Kryptoparty im Thüringer Landtag“, die der Information über Verschlüsselungstechniken diente. Der TLfDI nahm an der Podiumsdiskussion „Notwendigkeit (?) staatlicher Überwachung im Internet vs. Schutz der Privatsphäre“ teil. Zusammen mit der Friedrich-Ebert-Stiftung und der SPD-Fraktion führte er die Veranstaltung „Nach NSA: Kann die Verfassung uns noch vor den Geheimdiensten schützen?“ durch, die sich mit den Gefahren der ausufernden Überwachung auseinandersetzte. Anschließend gab es auch hier eine Kryptoparty.

Der TLfDI ist bestrebt, interessierten Stellen den Datenschutz auch im Wege des Dialogs nahezubringen. Zu diesem Zweck nahm er im Berichtszeitraum an zahlreichen Veranstaltungen teil und führte auch selbst Informations- und Fortbildungsveranstaltungen durch.

Anlagen

Anlage 1

Fragenkatalog für Kontrollen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit



Fragenkatalog für Kontrollen TLfDI
- nichtöffentlicher Bereich -

Allgemeine Fragen

1. Welche Arten von personenbezogenen Daten werden in Ihrem Unternehmen verarbeitet?

2. Personaldaten (Lohnabrechnung, Zeiterfassung)

3. Kunden- und/oder Lieferantendaten (Detailfragen ab Pkt. 29.)

4. Werden personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet?

5. Werden Daten in nicht automatisierten Dateien, die aus einer automatisierten Verarbeitung stammen verarbeitet?

Datenschutzbeauftragter

6. Wie viele Personen sind in Ihrem Unternehmen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt (incl. Geschäftsleitung)?

7. Haben Sie einen betrieblichen Datenschutzbeauftragten (bDSB) gemäß § 4f BDSG?
   Gibt es für den bDSB eine schriftliche Bestellung?

8. Über welche fachlichen Kenntnisse verfügt der bDSB?

9. Welche (schriftlichen) Richtlinien / Anweisungen gibt es im Unternehmen zur Einbeziehung des bDSB?

10. Welcher Zeitanteil steht dem bDSB für seine Aufgaben zur Verfügung?

11. Welche sonstigen Aufgaben hat der Datenschutzbeauftragte neben dieser Funktion im Unternehmen noch wahrzunehmen?

12. Gibt es ein eigenes Budget für den Datenschutzbeauftragten?

13. Wie ist der Datenschutzbeauftragte in das Unternehmen eingegliedert und wem ist er unterstellt?

14. Wer ist Ansprechpartner für betroffene Personen, die ihre Datenschutzrechte wahrnehmen wollen?

15. Wie werden Ihre Mitarbeiter, die mit personenbezogenen Daten arbeiten, auf das Datengeheimnis (§ 5 BDGS) verpflichtet?
Wer verpflichtet die Mitarbeiter?
Wann erfolgt die Verpflichtung?

Auftragsdatenverarbeitung § 11 BDSG

16. Welche Dienstleister werden mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt?
(Anmerkung: betrifft z.B. Verfahren der Lohn-/Gehaltsabrechnung, Kundenbindungsprogramme, Banküberweisungen, die das Unternehmen als Auftraggeber vertraglich durchführen lässt)

17. Welche Verträge wurden mit diesen Dienstleistern abgeschlossen?

In welcher Form sind die Verträge dokumentiert?

18. Nach welchen Kriterien werden die Dienstleistungsunternehmen ausgewählt und wie wird die ordnungsgemäße Auftragsabwicklung überwacht?

Technisch-organisatorischer Datenschutz

19. Welche allgemeinen technischen und organisatorischen Maßnahmen wurden in Ihren Unternehmen getroffen, um die Ausführung der Vorschriften des BDSG zu gewährleisen?

20. Wie sind diese Maßnahmen dokumentiert?

21. Gibt es ein Konzept über die Gesamtheit der Sicherheitsmaßnahmen (IT-Sicherheitskonzept)?

22. Wie sind der/die Server, die Rechner und das Netzwerk vor unbefugten Zugriffen von außen und innen geschützt?

23. Gibt es bzgl. der IT-Räume und der Datenverarbeitungsanlagen sowie der innerbetrieblichen Organisation Konzepte zur
    a. Zutrittskontrolle
    b. Zugangskontrolle
    c. Zugriffskontrolle

24. Wie erfolgt die Datensicherung? (Arbeitsanweisung, Workflow)

25. Werden mobile und andere Datenträger für personenbezogene Daten verwendet (USB-Sticks, CD-ROM; Laptop)?
    Sind diese sicher verschlüsselt?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

26. Was ist zur Sperrung bzw. Löschung von nicht mehr erforderlichen Daten in Ihrem Unternehmen festgelegt?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

27. Wie werden gesperrte Daten gekennzeichnet?
Welche (schriftlichen) Verfahrensanweisungen gibt es?

28. Wie wird bei der Abgabe von Altgeräten oder Altdatenträgern an Dritte in Bezug auf die auf ihnen befindlichen personenbezogenen Daten vorgegangen?
Auf welche Weise werden die Daten gelöscht?
Welches Verfahren wird für den Löschvorgang eingesetzt? (z. B. Entmagnetisierung bzw. Neuausrichtung, Überschreiben, wie oft?)
Welche (schriftlichen) Verfahrensanweisungen gibt es?

29. Auf welche Art und Weise wird Altpapier entsorgt?
Welche (schriftlichen) Verfahrensanweisungen gibt es?

30. Werden E-Mails mit personenbezogenen Daten versendet? (ja/nein)
Wenn ja, auf welche Art und Weise werden diese E-Mails versendet?
Gibt es in diesem Zusammenhang Konzepte zur Weitergabekontrolle, zur Eingabekontrolle, zur Auftragskontrolle und zur Verfügbarkeitskontrolle? (Arbeitsanweisungen, Workflow)

31. Gibt es einen Notfallplan für die Aufarbeitung einer eventuellen Datenpanne nach § 42 a BDSG?
Welche (schriftlichen) Verfahrensanweisungen gibt es?

Kundendaten/ Geschäftspartner

32. Wo sind Kunden- und/oder Lieferantendaten gespeichert?

33. Wer hat Zugriff auf die Kunden- und/oder Lieferantendaten?

34. Fordern Sie Einwilligungen von Ihren Kunden ein? Wenn ja: zu welchen Sachverhalten und in welcher Form?

35. Führen Sie adressierte Werbung durch? Wenn ja nach welchen Kriterien?

36. Wann und wie werden Kunden- und/oder Lieferantendaten gelöscht?

Arbeitnehmerdaten

37. Wo sind die Arbeitnehmerdaten gespeichert?

38. Wer hat Zugriff auf diese Daten?

39. Wie ist die Zeiterfassung in Ihrem Unternehmen geregelt?

40. Welche Festlegungen bestehen zur dienstlichen und privaten Nutzung von E-Mail, Internet und TK-Anlagen am Arbeitsplatz? Wann werden E-Mails gelöscht?

41. Was wird bei der Nutzung von E-Mail und Internet warum protokolliert?

42. Wann und durch wen werden die Protokolldateien ausgewertet und gelöscht?

43. Wie erfolgt eine evtl. Telefonabrechnung (Einzelverbindungsnachweis)?

44. Gibt es Bestimmungen zur Verwendung privater Geräte, wie bspw. Smartphones und Tablets, für dienstliche Zwecke (Bring Your Own Device – BYOD)?

45. Besteht in Ihrem Unternehmen ein Betriebsrat? Wenn ja, gibt es Betriebsvereinbarungen, die die oben genannten Bereiche oder anderen Umgang mit personenbezogenen Daten regeln?

46. Veröffentlichen Sie Arbeitnehmerdaten im Internet?

Internetseite

47. Betreiben Sie eine Internetseite? Wenn ja:

    - auf welchem Webserver?

    - Erfassen Sie Daten von Besuchern (bspw. mittels Tracking – Google-Analytics, Piwik…usw.)?

    - Betreiben Sie Foren und Blogs im Internet?

    - veröffentlichen Sie personenbezogene Daten?

48. Erfassen Sie auch Kundendaten über das Internet? Wenn ja über SSL/TLS?

Videoüberwachung

49. Findet Videoüberwachung innerhalb oder außerhalb des Firmengebäudes statt?

50. Wie viele Kameras sind an welchen Stellen im Unternehmen im Einsatz?

51. Für welche Zwecke erfolgt die Videoüberwachung und welche schriftlichen Festlegungen gibt es dazu?

52. Sind die Bilder bzw. Videosequenzen live zu beobachten?
    Wenn ja, wo und mit welchem Wiedergabemedium erfolgt die Beobachtung (PC-Bildschirm, mobiles Gerät)?

53. Erfolgt die Beobachtung permanent oder lediglich bei Bedarf (z. B. bei Vorkommnissen)?

54. Gibt es Zoommöglichkeiten und/oder ist/sind die Kamera/s schwenkbar?
    Wenn ja, bei welchen Kameras ist dies der Fall und zu welchem Zweck sind diese Funktionalitäten vorgesehen?

55. Gibt es in diesen Bildern bzw. Videosequenzen Schwärzungen?

56. Werden Bilder bzw. Videosequenzen aufgezeichnet?
Wenn ja, wie lange erfolgt die Speicherung?

57. Auf welchen Datenträgern werden Bilder/Videosequenzen aufgezeichnet?

58. Wird auf die Videoüberwachung hingewiesen? Wenn ja, auf welche Weise?

Anlage 2

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 17. Januar 2012)

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung[b]

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY1 daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z. B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (Krankenversicherung)2 benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache,

[b] Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5]
Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY *[Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird]* selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[7]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesund-

sdaten verfügen. Außerdem kann es zur Prüfung der Leistungs-
cht erforderlich sein, dass die Versicherung XY die Angaben
r Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur
ründung von Ansprüchen gemacht haben oder die sich aus einge-
hten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten)
r Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen
s Heilberufs ergeben.

se Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versi-
rung XY benötigt hierfür Ihre Einwilligung einschließlich einer
weigepflichtentbindung für sich sowie für diese Stellen, falls im
men dieser Abfragen Gesundheitsdaten oder weitere nach
3 Strafgesetzbuch geschützte Informationen weitergegeben
den müssen.

können diese Erklärungen bereits hier (I) oder später im Einzel-
(II) erteilen. Sie können Ihre Entscheidung jederzeit ändern.
e entscheiden Sie sich für eine der beiden nachfolgenden Mög-
keiten:

glichkeit I:

☐ Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung er-

ihrer Schweigepflicht. Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.[10]

glichkeit II:

☐ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

- in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder
der Prüfung der Leistungspflicht führen kann.

aben gemacht wurden und damit die Risikobeurteilung beeinst wurde. Auch dafür bedürfen wir einer Einwilligung und weigepflichtentbindung. Bitte entscheiden Sie sich für eine der en nachfolgenden Möglichkeiten:[13]

glichkeit I:

☐ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

glichkeit II:

☐ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten
entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XYGruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter (Internetadresse) eingesehen oder bei (Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die

Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt. Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt. Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.
Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.[25] Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.
Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.
Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet[26]

Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheits-

daten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, http://www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.[28] Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen
ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Infor-

mationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragenweiterer

Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres
Ort, Datum	Unterschrift des gesetzlichen Vertreters

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel - BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt

keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z. B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung ***dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.***

[1] Hier und im Folgenden kann anstelle von „die Versicherung XY“ der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY“) jeweils „wir“ eingefügt werden.
[2] Hier kann die konkrete Sparte genannt werden.
[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier

einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

[4] Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

[5] Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4 a Abs. 1 Satz 2 BDSG

[6] Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

[7] Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

[8] Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

[9] Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

[10] Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i. V. m. Abs. 4 VVG

[11] Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

[12] Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

[13] Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z. B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

[14] Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

[15] Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.
[16] Der Satzteil "für sich und" ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.
[17] Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.
[18] In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragsdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.
[19] Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.
[20] Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z. B. Krankentransporte.

[21] Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.
[22] Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.
[23] „und sonstige Stellen“ – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.
[24] Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.
[25] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.
[26] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.
[27] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht.
Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

[28] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.
[29] Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.
[30] Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt.
Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.
[31] Es zählt das Datum der Unterschrift im Antrag.
[32] Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/ Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

Anlage 3

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 18./19. September 2012)

Near Field Communication (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6 c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

Anlage 4

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 26./27. Februar 2013)

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6 b Bundesdatenschutzgesetz (BDSG). Gemäß § 6 b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6 b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6 b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6 b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kame-

ras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

Anlage 5

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 11./12. September 2013)

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z. B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4 c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

Abkürzungsverzeichnis

Abkürzung	Bedeutung
Abs.	Absatz
Art.	Artikel
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BRAO	Bundesrechtsanwaltsordnung
BVerfG	Bundesverfassungsgericht
ERFA-Kreis	regionaler Erfahrungsaustauschkreis der Gesellschaft für Datenschutz und Datensicherheit e.V.
EuGH	Europäischer Gerichtshof
GbR	Gesellschaft bürgerlichen Rechts
GWG	Geldwäschegesetz
HWK	Handwerkskammer
i. V. m.	in Verbindung mit
IHK	Industrie- und Handelskammer
KunstUrhG	Kunsturheberrechtsgesetz
OHA	Orientierungshilfe Aktenaufbewahrung
OWiG	Ordnungswidrigkeitengesetz
PAuswG	Personalausweisgesetz
PDSV	Postdienste-Datenschutz-Verordnung
SGB	Sozialgesetzbuch
StPO	Strafprozessordnung
ThILLM	Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien
ThürMeldeG	Thüringer Meldegesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLvWA	Thüringer Landesverwaltungsamt
TMBWK	Thüringer Ministerium für Bildung, Wissenschaft und Kultur
TMLFUN	Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz
VSA	Verrechnungsstelle der Süddeutschen Apotheken

Sachregister