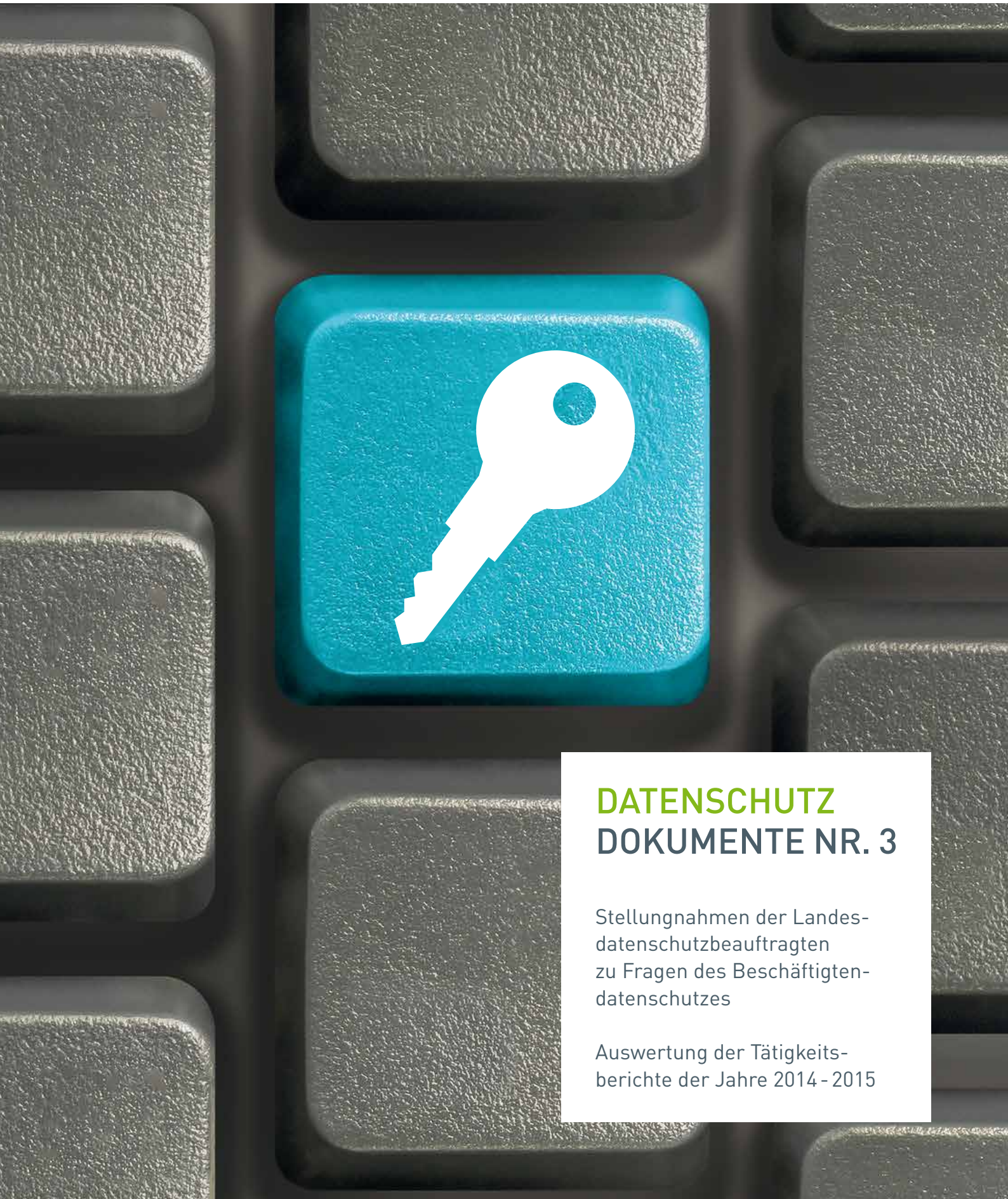
UNIVERSITY OF APPLIED SCIENCES

THM
TECHNISCHE HOCHSCHULE MITTELHESSEN



DATENSCHUTZ
DOKUMENTE NR. 3

Stellungnahmen der Landesdatenschutzbeauftragten zu Fragen des Beschäftigtendatenschutzes

Auswertung der Tätigkeitsberichte der Jahre 2014 - 2015

Vorwort

Datenschutzverstöße am Arbeitsplatz können weitreichende Folgen haben. Diese Erfahrung musste jüngst eine Mitarbeiterin einer Berliner Einwohnermeldebehörde machen. In 561 Fällen hatte sie unberechtigt auf Meldedaten zugegriffen. Die Folgen: Das Landesarbeitsgericht Berlin-Brandenburg bestätigte die fristlose Kündigung und das Amtsgerichts Tiergarten verhängte eine Geldstrafe von 4.950 €. Die beiden Urteile zeigen exemplarisch: Verstöße gegen Datenschutzbestimmungen und Datensicherheitsmaßnahmen werden von Gerichten, egal ob Arbeits- oder Strafgerichte, nicht als „Kavaliersdelikte" eingestuft.

Dabei haben Datenschutzverstöße in Behörden und Unternehmen, egal ob durch Arbeitnehmer und Arbeitgeber begangen, nicht immer solch dramatische Folgen wie in dem beschriebenen Berliner Fall. Aber sie kommen offensichtlich öfter vor. Zu diesem Eindruck kann man bei der Lektüre der Tätigkeitsberichte der Landesdatenschutzbeauftragten gelangen. Kein Bericht, in dem nicht über Datenschutzverstöße und –pannen am Arbeitsplatz berichtet wird. Dabei wird anhand von Beispielen aus der Behörden- und Unternehmenspraxis nicht nur beschrieben, was alles schief gehen kann, sondern es werden hilfreiche Hinweise und Tipps für die praktische Umsetzung des Datenschutzes gegeben.

Die vorliegende Broschüre dokumentiert Stellungnahmen der Datenschutzbehörden zu Fragen des Beschäftigtendatenschutzes aus den Tätigkeitsberichten der Aufsichtsbehörden für die Jahre 2014 und 2015.

Ich hoffe, mit dieser Broschüre nicht nur den Datenschutzbeauftragten an den Hochschulen eine kleine Hilfeleistung bei ihrer nicht immer einfachen Arbeit zu bieten. Sicher sind die gesammelten Texte auch für Mitarbeiterinnen und Mitarbeiter in den Fachbereichen und der Hochschulverwaltung eine interessante Lektüre und können Anregungen geben für eine gesetzeskonforme Datenschutzpraxis. Und sicher werden auch Arbeitgeber sowie Personal- und Betriebsräte hilfreiche Tipps für Ihre Arbeit finden. Auch in Lehrveranstaltungen zum Thema Datenschutz dürften die abgedruckten Texte auf studentisches Interesse stoßen.

Soweit einzelne Texte wegen der Fülle der Fälle nicht abgedruckt werden konnten (siehe Übersicht Seite 40), alle seit 1971 erschienen Tätigkeitsberichte können über www.zaftda.de abgerufen werden.

Ich wünsche eine lehrreiche Lektüre.

Hajo Köppen

Inhalt

zaftda.de – ein Blick lohnt sich

Seit 2009 stellt die Technische Hochschule Mittelhessen mit dem digitalen „Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz – ZAfTDa" alle seit 1971 erschienenen Tätigkeitsberichte (TB) der Datenschutzbehörden der Öffentlichkeit zur Verfügung.

Über die Seite www.zaftda.de sind abrufbar
- die Tätigkeitsberichte des Bundesdatenschutzbeauftragten
- die Tätigkeitsberichte der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz
- die Berichte des Europäischen Datenschutzbeauftragten
- die Berichte der Artikel 29-Gruppe
- Meldungen zu neu erschienenen Tätigkeitsberichten
- eine Übersicht mit den Fundstellennachweisen aller Berichte
- die Erscheinungstermine der TB im jeweils kommenden Jahr
- Links zu den Parlamentsdatenbanken der Länder

Das Online-Archiv ZAfTDa bietet damit für alle, die sich mit dem Thema Datenschutz und -sicherheit befassen, eine wahre Fundgrube. Die Tätigkeitsberichte sind lohnende, Hilfestellung gebende Nachschlagewerke für behördliche und betriebliche Datenschutzbeauftragte, für Personal- und Betriebsräte sowie für Behörden- und Unternehmensleitungen. Und natürlich auch für Mitarbeiterinnen und Mitarbeiter. Und, last but not least, auch für Bürgerinnen und Bürger.

Landesbeauftragter für den Datenschutz Baden-Württemberg

32. Tätigkeitsbericht (2014/2015)

9.1 Mindestlohngesetz und Datenschutz

Zum 1. Januar 2015 ist das Mindestlohngesetz in Kraft getreten, das nicht zuletzt durch den Streit über die damit verbundenen Dokumentationspflichten für Arbeitgeber immer wieder im Fokus der politischen und medialen Aufmerksamkeit stand. Das Bundesgesetz wirft auch eine Reihe von datenschutzrechtlichen Problemen auf.

Nach § 13 des Mindestlohngesetzes (MiLoG) i. V. mit § 14 des Arbeitnehmerentsendegesetzes haftet ein auftraggebendes Unternehmen wie ein Bürge dafür, wenn der Auftragnehmer seinen Beschäftigten nicht den gesetzlichen Mindestlohn zahlt; diese Haftung erstreckt sich ggf. auch auf weitere Subunternehmer und deren Arbeitnehmer, wobei sich der Betroffene aussuchen kann, gegen welchen übergeordneten Auftraggeber er vorgehen will. Weiterhin steht ein Bußgeld im Raum, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass der Subunternehmer nicht den Mindestlohn zahlt (§§ 20, 21 Absatz 2 MiLoG). Wie die Überprüfung, ob ein Auftragnehmer den Mindestlohn tatsächlich zahlt, konkret zu erfolgen hat, wird im Mindestlohngesetz jedoch nicht näher bestimmt. Die Industrie- und Handelskammern berichten von einer erheblichen Verunsicherung bei Unternehmen, die mittlerweile versuchen würden, sich durch entsprechende Verpflichtungserklärungen ihrer Subunternehmer abzusichern. Dabei würden z.T. auch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf Beschäftigtendaten beim Auftragnehmer (Lohnlisten, Verdienstbescheinigungen usw.) eingefordert.

Aus Sicht des Datenschutzes geht es angesichts dieser Problemlage darum, Wege aufzuzeigen, wie Unternehmen ihren gesetzlich vorgeschriebenen Prüfpflichten bezüglich der Einhaltung der Mindestlohnvorgaben durch ihre Subunternehmer nachkommen können, ohne - oder zumindest nur so wenig wie möglich - personenbezogene Daten der Beschäftigten ihrer Subunternehmer erheben zu müssen. Grundsätzlich muss der Auftraggeber zunächst eine gewisse Sorgfalt bei der Auswahl seiner Geschäftspartner walten lassen, beispielsweise also unrealistisch billige Angebote von Subunternehmen eingehend prüfen. Im Übrigen ist er nicht daran gehindert, das mit dem Mindestlohn- bzw. Arbeitnehmerentsendegesetz verbundene Haftungsrisiko auf den neuen Vertragspartner abzuwälzen. Hierzu bieten sich vorrangig zivilrechtliche Vereinbarungen zwischen dem Unternehmen und seinen Subunternehmern an, in denen die Subunternehmer versichern, die Voraussetzungen des Mindestlohngesetzes einzuhalten, und für den Fall von Zuwiderhandlungen Vertragsstrafen vereinbart werden; ergänzend sollten Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer vorgesehen werden. Darüber hinaus kann ggf. die Überlassung anonymisierter Lohnabrechnungsdaten vereinbart werden. Schließlich können sich Unternehmen die Bestätigung eines vom Subunternehmer eingeschalteten Steuerberaters oder Wirtschaftsprüfers vorlegen lassen, wonach der Subunternehmer die Mindestlohnvorgaben beachtet („Testatlösung"). Lediglich dann, wenn eine solche Bestätigung nicht vorgelegt werden kann und im Einzelfall konkrete Anhaltspunkte dafür bestehen, dass ein Subunternehmer seinen Arbeitnehmern nicht den gesetzlichen Mindestlohn auszahlt, kann es zulässig sein, dass ein vom Unternehmen beauftragter Wirtschaftsprüfer oder Steuerberater Einblick in die Lohnabrechnungsdaten des Subunternehmers nimmt. Darüber hinaus ist die Erhebung personenbezogener Beschäftigtendaten durch Unternehmen zur Kontrolle der Einhaltung der Mindestlohnvorgaben durch ihre Subunternehmer weder geboten noch erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung vom 18./19. März 2015 in diesem Sinne zu der Thematik geäußert (vgl. Anhang 20); etwaige Beratungen meiner Dienststelle erfolgen auf dieser Grundlage.

> Zur Kontrolle der Einhaltung der Vorgaben des Mindestlohngesetzes bei Subunternehmern durch ihre Auftraggeber ist im Regelfall keine Übermittlung personenbezogener Daten der Beschäftigten des Subunternehmers an seinen Auftraggeber erforderlich. Solche Übermittlungen sind daher grundsätzlich unzulässig. Daran ändern auch entsprechende vertragliche Vereinbarungen zwischen Auftraggeber und Subunternehmer nichts.

9.3 Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern: Die Ausnahme muss wieder zur Regel werden

Diesen Text aus der automatisierten Begrüßungsansprache eines Call-Centers kennen wir alle: „Aus Gründen der Qualitätssicherung und für Schulungszwecke werden einzelne Gespräche aufgezeichnet." Das Aufzeichnen und Abhören von Telefongesprächen ist aber strafbar, soweit dies unbefugt im Sinne des § 201 Absatz 1 StGB erfolgt. Danach wird das unbefugte Aufnehmen des nicht-öffentlich gesprochenen Wortes eines anderen auf einem Tonträger mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe geahndet. Die Betreiber von Call-Centern müssen daher rechtlich Einiges beachten, damit diese Form der Datenverarbeitung auch rechtmäßig durchgeführt werden kann.

Man gewinnt fast den Eindruck, dass das Aufzeichnen und Mithören von Telefongesprächen in Call-Centern inzwischen die Regel ist. Auch der Grundsatz der Datensparsamkeit scheint hier bedauerlicherweise keine Rolle zu spielen. Den Betreibern der Call-Center scheinen dabei die rechtlichen Grenzen des Aufzeichnens und Mithörens oft nicht bewusst zu sein.

Die als Begründung genannten Schulungs- und Qualitätssicherungsmaßnahmen werden in der Regel in folgenden Varianten durchgeführt:

- das vom Beschäftigten und vom Kunden gesprochene Wort wird durch eine Kontrollperson direkt am Arbeitsplatz im Call-Center unter Nutzung eines Kopfhörers offen mitgehört,
- das vom Beschäftigten und vom Kunden gesprochene Wort wird ohne direkte Anwesenheit einer Kontrollperson am Arbeitsplatz durch Aufschalten mitgehört oder
- das Gespräch wird aufgezeichnet und später ausgewertet.

Datenschutzrechtlich ist zwischen den Rechten des Kunden und denen der Beschäftigen zu unterscheiden.

9.3.1 Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern aus Sicht des Kunden

Jedem Kunden steht das Recht am gesprochenen Wort als Ausfluss des grundrechtlich geschützten allgemeinen Persönlichkeitsrechts des Artikels 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes zu. Jedermann soll - sowohl im privaten als auch im geschäftlichen Bereich - grundsätzlich selbst entscheiden können, ob seine Worte allein dem Gesprächspartner oder auch Dritten zugänglich sein sollen oder ob diese gar auf Tonträger aufgenommen werden dürfen.

Gem. § 4 Absatz 1 BDSG ist die Erhebung und Verarbeitung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Als mögliche Rechtsgrundlagen für das Mithören und Aufzeichnen von Telefongesprächen könnten § 28 Absatz 1 Satz Nr. 1 und Nr. 2 BDSG in Betracht kommen. Diese sind aber im Regelfall im Rahmen der Abwägung zwischen den berechtigten Geschäftsinteressen des Unternehmens und den schutzwürdigen Interessen der Kunden und Mitarbeiter abzulehnen, weil

- das Recht am gesprochenen Wort wirtschaftlichen oder geschäftlichen Interessen grundsätzlich vorgeht und
- die Gespräche umfangreicher sein können, als es für die Erfüllung des Geschäftszwecks erforderlich ist.

Daraus folgt, dass die heimliche Aufzeichnung bzw. das Abhören von Telefongesprächen grundsätzlich verboten ist und gem. § 201 StGB sogar mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden kann.

Ein solches Aufzeichnen oder Mithören ist demnach nur zulässig, wenn der Kunde

- vor Beginn des Aufzeichnens oder Mithörens hierüber informiert wird und
- nach seiner ausdrücklichen Einwilligung im Sinne von § 4a BDSG gefragt wird.

Ebenso müssen die Kunden über die Identität der verantwortlichen Stelle und den Zweck der Erhebung und Verarbeitung aufgeklärt werden, § 4 Abs. 3 Satz. 1 BDSG.

Nur wenn der Kunde anschließend ausdrücklich mit einem „Ja" in das Aufzeichnen oder Mithören einwilligt, ist dies zulässig und erlaubt. Ein Schweigen des Kunden genügt hierfür nicht. Erst nach dieser Entscheidung des Kunden darf die Aufzeichnung oder das Mithören beginnen.w

Eine reine Widerspruchslösung („Wenn Sie mit einer Gesprächsaufzeichnung nicht einverstanden sind, geben Sie bitte zu Beginn des Gesprächs unserem Kundenberater Bescheid.") reicht keinesfalls aus, da diese eine konkludente Einwilligung unterstellt, die aber keine Einwilligung im Sinne der §§ 4 Absatz 1 und 4a Absatz 1 BDSG darstellt. Erforderlich ist vielmehr die Erkundigung zu Beginn des Gesprächs, ob der betroffene Kunde einverstanden ist oder nicht.

Der Kunde kann seine erteilte Einwilligung natürlich auch während des Telefongesprächs jederzeit ohne Angabe von Gründen widerrufen. Die bisherige Aufzeichnung muss dann gelöscht bzw. das Mithören umgehend beendet werden. Sowohl die Einwilligung als auch der Widerruf der Einwilligung sind vom Unternehmen zu dokumentieren.

Auch die Aufzeichnung von Telefongesprächen im Arbeitsspeicher der Rechner ist ein Speichern im Sinne von § 3 Absatz 4 Nr. 1 BDSG und somit eine automatisierte Datenverarbeitung, die das vorherige Erheben der Daten nach § 3 Absatz 3 BDSG voraussetzt. Selbst wenn die Gespräche nur für Sekunden oder Minuten im (flüchtigen) Arbeitsspeicher gespeichert werden, liegt tatbestandlich ein Erheben und physikalisches Speichern vor. Die Aufzeichnungen sind erst dann gelöscht im Sinne von § 35 Absatz 2 BDSG, wenn die entsprechenden Bereiche des Arbeitsspeichers überschrieben werden. Es kommt auch nicht darauf an, ob ein Zugriff auf diese Daten erfolgt.

Ein Aufzeichnen von Telefongesprächen kann schließlich auch gegen den Grundsatz der Datenvermeidung und Datensparsamkeit aus § 3a BDSG verstoßen. Soweit andere Möglichkeiten vorhanden sind, um eine Aufnahme von Telefonaten zu vermeiden, sollten diese auch wahrgenommen werden.

9.3.2 Aufzeichnung von Telefongesprächen in Call-Centern aus Sicht der Mitarbeiter

Auch im Hinblick auf die Rechte der Beschäftigten in den Call-Centern bestehen für das Aufzeichnen und Mithören von Telefongesprächen klare Grenzen.

§ 32i des Gesetzentwurfs der Bundesregierung zu einem Gesetz zur Regelung des Beschäftigtendatenschutzes vom Dezember 2010 (BT-Drs. 17/4230) sah in diesem Zusammenhang Folgendes vor:

§ 32i Nutzung von Telekommunikationsdiensten (1) Soweit dem Beschäftigten die Nutzung von Telekommunikationsdiensten ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubt ist, darf der Arbeitgeber bei dieser Nutzung anfallende Daten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist zur Gewährleistung des ordnungsgemäßen Betriebs von Telekommunikationsnetzen oder Tele-

kommunikationsdiensten, einschließlich der Datensicherheit, zu Abrechnungszwecken oder zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskontrolle und soweit keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Beschäftigten an einem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegen. Werden nach Satz 1 Nummer 3 erhobene Daten einem bestimmten Beschäftigten zugeordnet, ist dieser über eine Verarbeitung und Nutzung zu unterrichten, sobald der Zweck der Verarbeitung oder Nutzung durch die Unterrichtung nicht mehr gefährdet wird. (2) Inhalte einer ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubten Nutzung von Telefondiensten darf der Arbeitgeber nur erheben, verarbeiten und nutzen, soweit dies zur Wahrung seiner berechtigten Interessen erforderlich ist und der Beschäftigte und seine Kommunikationspartner im Einzelfall vorher darüber informiert worden sind und darin eingewilligt haben. Ist die ausschließlich zu beruflichen oder dienstlichen Zwecken erbrachte telefonische Dienstleistung wesentlicher Inhalt der geschuldeten Arbeitsleistung, darf der Arbeitgeber Inhalte dieser Nutzung ohne Kenntnis des Beschäftigten im Einzelfall zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskontrolle erheben, verarbeiten und nutzen, wenn der Beschäftigte in geeigneter Weise vorab darüber informiert worden ist, dass er in einem eingegrenzten Zeitraum mit einer Kontrolle zu rechnen hat, und die Kommunikationspartner des Beschäftigten über die Möglichkeit der Erhebung, Verarbeitung und Nutzung informiert worden sind und darin eingewilligt haben. Der Arbeitgeber hat den Beschäftigten unverzüglich über die Erhebung, Verarbeitung und Nutzung der Inhaltsdaten nach Satz 2 zu unterrichten.

Diese Vorschrift ist zwar nicht in Kraft getreten65; sie gibt jedoch den aktuellen Stand der arbeits- und datenschutzrechtlichen Rechtsprechung und Literatur zur Auslegung des § 32 BDSG im Zusammenhang mit der Aufzeichnung dienstlicher Telefongespräche wieder.

Das bedeutet, dass ein Aufzeichnen und eine spätere Auswertung bzw. ein Abhören der aufgezeichneten Gespräche zum Zweck einer Verhaltens- und Leistungskontrolle zum einen zulässig ist

- während der Anlernphase von Mitarbeitern und danach

- nur stichprobenartig oder anlassbezogen, d. h. im Fall konkreter Kundenbeschwerden oder bei Anhaltspunkten für offensichtliche Qualitätsmängel bei einzelnen Mitarbeitern in einem eingegrenzten Zeitraum.
  Im Fall stichprobenartiger Kontrollen sind von der verantwortlichen Stelle konkrete Zahlenobergrenzen hierfür festzulegen (z.B. 3 % aller geführten Gespräche oder 30 Gespräche im Monat).

Darüber hinaus ist ein berechtigtes Interesse des Arbeitgebers anzuerkennen, Telefongespräche zum Zwecke der Gewinnung von Schulungsmaterial aufzuzeichnen oder auszuwerten. Aufzeichnungen zu diesem Zweck sind jedoch nur so lange zulässig, bis der Arbeitgeber genügend Schulungsmaterial zusammengestellt hat und können daher keine unbegrenzte und unbefristete Aufzeichnung von Telefongesprächen rechtfertigen. Die Aufzeichnung von Telefongesprächen muss zudem offen geschehen, d. h. die Arbeitnehmer sind grundsätzlich im Einzelfall vor jeder Aufzeichnung hierüber zu informieren. Ausnahmsweise kann (entsprechend der Regelung in § 32i Absatz 2 Satz 2 des o. g. Entwurfs) eine Vorabinformation des Arbeitgebers, dass der Arbeitnehmer in einem eingegrenzten Zeitraum mit Kontrollen zu rechnen hat, genügen. Auch dies gilt jedoch nur im Fall stichprobenartiger oder anlassbezogener Leistungs- oder Verhaltenskontrollen.

Ausnahmsweise können Beweisinteressen der verantwortlichen Stelle ein dauerhaftes Aufzeichnen von Telefongesprächen rechtfertigen. Dies setzt jedoch voraus, dass ein überwiegendes Beweisinteresse des Arbeitgebers besteht, welches nur dann anzuerkennen ist, wenn telefonisch etwa ausschließlich oder weit überwiegend zivilrechtliche Verträge von nicht unerheblicher finanzieller Bedeutung abgeschlossen werden, über die es nachträglich erfahrungsgemäß häufig zu Streit kommt (etwa Telefonbanking).

Die Vereinbarung von Terminen mit Kunden, deren Beratung oder sonstiger telefonischer Kundenservice begründet grundsätzlich kein entsprechendes überwiegendes Beweisinteresse des Arbeitgebers. Außerdem besteht in solchen (Ausnahme-) Fällen grundsätzlich eine Zweckbindung, d.h. die Gespräche dürfen nur soweit abgehört und ausgewertet werden, wie das Beweisinteresse des Arbeitgebers - etwa zur Geltendmachung zivilrechtlicher Ansprüche gegenüber Kunden - dies unabweisbar erfordert. Nutzungen der Aufzeichnungen zu anderen Zwecken - etwa dem einer Verhaltens- und Leistungskontrolle der Mitarbeiter - sind nur unter den oben dargelegten Voraussetzungen, d.h. insbesondere nur stichprobenartig oder anlassbezogen, d. h. im Fall konkreter Beschwerden im Einzelfall, zulässig.

Der Umfang der Aufzeichnung und Auswertung von Telefongesprächen sowie der oder die damit verfolgte(n) Zweck(e) und die Speicher- und Löschungsfristen für Aufzeichnungen sind stets vorab schriftlich festzulegen.

Einwilligungen der betroffenen Arbeitnehmer in das Mithören oder Aufzeichnen in einem darüber hinausgehenden Umfang können eine entsprechende Datenerhebung nicht rechtfertigen. Dies folgt bereits aus der zumeist fehlenden Freiwilligkeit von Einwilligungen, die Arbeitnehmer im Arbeitsverhältnis abgeben.

Das Aufzeichnen und Mithören von Telefongesprächen in Call-Centern nimmt leider überhand - auf Kosten der Kunden und Beschäftigten der Call-Center. Ich werde daher die Kontrollen in diesem Bereich ausweiten. Denn es wäre meines Erachtens eher ein Ausdruck des Service- und Qualitätsgedankens eines Unternehmens, das Aufzeichnen und Mithören von Telefongesprächen auf ein datenschutzrechtlich gebotenes Mindestmaß zu reduzieren.

Berliner Beauftragter für Datenschutz und Informationsfreiheit

Bericht 2015

9.1 Bonitätsauskünfte im Bewerbungsverfahren

In mehreren Fällen haben Unternehmen vor oder während eines Bewerbungsgespräches eine Bonitätsabfrage getätigt, um die Zuverlässigkeit der Bewerberinnen und Bewerber zu überprüfen. In einem Fall war die Bewerberin für das Telefonmarketing eines Unternehmens vorgesehen. Nach Auffassung des Unternehmens sei eine gute Bonität eine Voraussetzung, um nicht in die Gefahr der Bestechlichkeit zu kommen.

Die Vermögensverhältnisse gehören grundsätzlich zur Privatsphäre und müssen daher für die Geschäftsleitung ohne Interesse sein. Nur in Ausnahmefällen haben Unternehmen ein berechtigtes Interesse an Informationen über die finanzielle Situation ihrer Beschäftigten, das eine Übermittlung von Bonitätsdaten durch eine Auskunftei rechtfertigt.

Ein Fragerecht der Unternehmen kommt nur dann in Betracht, wenn die Beschäftigten eine Position ausfüllen sollen, in der Seriosität und Vertrauenswürdigkeit in finanziellen Fragen bedeutsam sind (z. B. Finanzberatung). Gleiches gilt aber auch für Beschäftigte, bei denen finanzielle Zuverlässigkeit gefordert ist (z. B. Kassiererinnen oder Kassierer).

Eine etwaige Bestechlichkeit kann nicht als Argument herangezogen werden, um eine umfassende Bonitätsauskunft einzuholen. Bewerber sollten nicht aufgrund privater finanzieller Probleme stigmatisiert und als kriminalitätsanfällig angesehen werden. Die Bonitätsabfrage, bei der das Unternehmen gegenüber der Auskunftei einen falschen Anfragegrund angegeben hatte, war rechtswidrig.

> Standardisierte Bonitätsauskünfte enthalten auch Informationen, die Aufschluss über die privaten Lebensumstände und über Geld- und Warenkreditverträge der Betroffenen geben. Die Einholung einer solchen Auskunft ist in der Regel unzulässig, da diese über das für die Einstellungsentscheidung erforderliche Informationsinteresse hinausgeht und in das Persönlichkeitsrecht der Bewerberinnen und Bewerber eingreift.

9.3 Big Boss is watching you – Videoüberwachung im Beschäftigungsverhältnis

Immer mehr Beschäftigte aus verschiedenen Tätigkeitsbereichen wenden sich an uns, um auf die Videoüberwachung in ihrem Arbeitsumfeld aufmerksam zu machen. Dabei kommen sowohl offene als auch versteckte Kameras zum Einsatz. Einige Beschäftigte berichteten von Verhaltens- und Leistungskontrollen bzw. von der Nutzung des Videomaterials ohne ihr Einverständnis für interne Schulungen oder Fortbildungen. Die Unternehmen trugen zumeist vor, dass diese Kameras der Abschreckung und der Verhinderung von Diebstählen dienen. Es wurde auch angegeben, dass durch die Kameras eine Kommunikation mit den Beschäftigten bei Abwesenheit der Geschäftsleitung oder die Analyse des Kundenstroms intendiert sei.

Durch den Einsatz von Videokameras sind schutzwürdige Interessen der Beschäftigten berührt. Bei den Beschäftigten kann ein ständiger Überwachungsdruck entstehen, da durch die Kameras eine permanente und lückenlose Kontrolle möglich ist. Das Unternehmen ist nur zu Überwachungsmaßnahmen befugt, wenn diese für den durch das Unternehmen angegebenen Verwendungszweck erforderlich sind. Sofern die Kameras aufgrund einer potenziellen Diebstahlgefahr installiert wurden, rechtfertigen allgemeine, nicht näher beschriebene Vorfälle eine Videoüberwachung nicht. Die teilweise von den Unternehmen angeführten Argumente der Kundenstromanalyse oder die Kommunikation der Leitung mit den Beschäftigten können die Videoüberwachung nicht legitimieren, da diese Ziele durch mildere Mittel erreicht werden können.

Der Eingriff in das Persönlichkeitsrecht der Beschäftigten ist dann besonders gravierend, wenn die Überwachung kontinuierlich erfolgt und sie ihr nicht ausweichen können. Es müssen daher stets Maßnahmen getroffen werden, die die schutzwürdigen Interessen der Beschäftigten berücksichtigen, wie z. B. die Reduzierung des Erfassungsbereichs oder die Verpixelung der Gesichter. Ferner sollte im Arbeitsvertrag selbst oder in einer entsprechenden Geschäftsrichtlinie klargestellt werden, dass etwaige Videoaufzeichnungen nicht für Verhaltens- und Leistungskontrollen der Beschäftigten herangezogen werden. Eine Nutzung dieser Aufnahmen für interne Schulungen oder Fortbildungen ist grundsätzlich nicht zulässig.

> Durch die Videoüberwachung sind schutzwürdige Interessen der Beschäftigten berührt. Diese darf nicht zu einer unzumutbaren Drucksituation führen. Eine Interessenabwägung muss daher für einen Ausgleich der widerstreitenden Interessen der Geschäftsleitung und der Beschäftigten sorgen.

9.4 GPS-Tracking im Beschäftigungsverhältnis

Mehrere Beschäftigte von Handwerksunternehmen erfragten bei uns die rechtliche Zulässigkeit von GPS-Ortungssystemen in ihren Dienstfahrzeugen. Die Beschäftigten gaben teilweise an, dass sie aufgrund der permanenten Überwachung auch psychischen Druck erleiden. Die Unternehmen machten vor allem geltend, dass die GPS-Ortung zur flexibleren Terminierung bei anfallenden Störeinsätzen im Tagesgeschäft diene.

Die Erhebung und Verarbeitung der Ortungsdaten ist zulässig, wenn dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Dabei ist eine permanente Ortung der Beschäftigten nicht notwendig. Im Allgemeinen ist eine

Datenverarbeitung aus betrieblichen Gründen nur zur Sicherheit oder zur Koordinierung des Einsatzes der Beschäftigten zulässig. Es ist immer zu prüfen, ob eine Aufenthaltsbestimmung der Handwerker in einem Havariefall durch ein milderes Mittel erreicht werden kann. Eine Ortung kommt dann nicht in Betracht, wenn dem Unternehmen aufgrund der Tagesplanung der Beschäftigten klar ist, wo sich diese im Zeitpunkt des Störeinsatzes gerade befinden.

Im Ergebnis sollte gewährleistet sein, dass das Ortungssystem nur in absoluten Ausnahmefällen (z. B. bei Störeinsätzen) genutzt und anderenfalls deaktiviert wird. Ferner muss eine Verhaltens- und Leistungskontrolle der Beschäftigten ausgeschlossen sein. Sofern das GPS-System auch für Zwecke des Diebstahlschutzes genutzt werden soll, ist es ausreichend, wenn die Ortung durch das System technisch etwa erst nach einem Kfz-Diebstahl eingesetzt wird. Darüber hinaus ist die Verarbeitung der Daten zum Zwecke der Dokumentation der Einsatzzeiten gegenüber dem Kunden nicht erforderlich, da in vielen Fällen ohnehin eine Pauschale berechnet wird bzw. dieser Zweck auch hier durch den Einsatz milderer Mittel erreicht werden kann, etwa durch das bereits zum jetzigen Zeitpunkt vorgeschriebene Führen von Fahrten- und Stundenbüchern.

Bei unseren Prüfungen konnten wir ferner feststellen, dass in den Unternehmen kein betrieblicher Datenschutzbeauftragter bestellt wurde. Unabhängig von der Anzahl der mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigten Personen besteht eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, wenn eine Vorabkontrolle erforderlich ist. Diese ist bei einem geplanten Einsatz eines Ortungssystems vorzunehmen, da die Verarbeitung der Positionsdaten dazu bestimmt werden kann, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Im Ergebnis hat ein Unternehmen auf unsere Forderung hin das GPS-System aus dem Fahrzeug eines Mitarbeiters, für dessen Einsatz im Unternehmen das GPS-Gerät nachweislich nicht erforderlich war, ausgebaut. Ferner wurde der Dienstleister angewiesen, die Positionsdaten nur für den aktuellen und nicht für den nachträglichen Abruf zu speichern, sodass das Risiko einer potenziellen Verhaltens- und Leistungskontrolle verringert wurde.

> Der Einsatz eines Ortungssystems bei Beschäftigten ist streng am Erforderlichkeitsgrundsatz zu messen und sollte nur in Ausnahmen zulässig sein. Eine Speicherung der Positionsdaten ist über den Zweck der Einsatzkoordinierung hinaus nicht notwendig. Diese sind daher nach Erfüllung des Zweckes zu löschen.

9.5 Daten von Bediensteten im Internet

Wir beschäftigten uns in verschiedenen Zusammenhängen mit der Frage, ob personenbezogene Daten von Behördenbeschäftigten, d. h. dienstliche Kontaktdaten und behördliche Schreiben, E Mails und Entscheidungen, durch Private in das Internet eingestellt werden dürfen. So erreichte uns z. B. die Beschwerde einer bayerischen Verwaltungsmitarbeiterin, deren Antwort-E-Mail auf eine Bürgeranfrage samt ihrer dienstlichen Kontaktdaten auf einer Berliner Webseite veröffentlicht wurden. Auch Beschäftigte unserer Behörde waren davon betroffen, dass ihre Schreiben eingescannt und ins Internet eingestellt wurden. Darüber hinaus erhielten wir eine Reihe von Anfragen, die die Veröffentlichung von Behördenkommunikation betrafen.

Die Zulässigkeit solcher Veröffentlichungen muss im Einzelfall geprüft werden. Sofern die Informationen durch einen rechtmäßigen Informationszugang nach dem Berliner Informationsfreiheitsgesetz (IFG) erlangt wurden, sind die Daten der Betroffenen nicht schutzwürdig. Da die nach dem IFG erlangten Informationen keinen Verwendungsbeschränkungen unterliegen, spricht nichts gegen eine Veröffentlichung im Internet. Handelt es sich um Informationen, die nicht auf der Grundlage des IFG erlangt wurden, stellt sich gleichwohl die Frage, ob die Informationen bei einem IFG-Antrag freizugeben wären. Wenn ja, dürfen die Angaben veröffentlicht werden.

In jedem Fall müssen Betroffene nach der Rechtsprechung des Bundesverfassungsgerichts keine falschen Zitierungen hinnehmen, d. h. wenn ihnen Äußerungen in den Mund gelegt werden, die von ihnen nicht getätigt wurden und die ihren Geltungsanspruch beeinträchtigen. Zudem sind die Betroffenen dann schutzwürdig, wenn die Informationen in einen Kontext gestellt werden, durch den die Grenze zur Schmähkritik, Formalbeleidigung oder Diffamierung überschritten ist und die Gefahr der Stigmatisierung besteht.

Im Fall der bayerischen Verwaltungsmitarbeiterin bestand die Besonderheit, dass die Zulässigkeit der Veröffentlichung nicht an den Wertungen eines Informationsfreiheitsgesetzes hätte gemessen werden können, da ein solches in Bayern bisher nicht existiert. Im Ergebnis spielte dies jedoch keine Rolle, da die Betreiber der Webseite die Angaben zu der Mitarbeiterin auf unsere Anfrage durch nicht sprechende Kürzel ersetzten und sich das Anliegen der Betroffenen damit erledigte.

Auch Behördenbeschäftigte bleiben bei der Wahrnehmung öffentlich-rechtlicher Aufgaben und somit in ihrer Eigenschaft als Amtswalter Trägerinnen und Träger von Grundrechten. Das bedeutet, dass ihre personenbezogenen Daten gegenüber den Veröffentlichungsbedürfnissen Dritter schutzwürdig sein können. Gleichwohl müssen in Berlin auch die Wertungen des IFG berücksichtigt werden. Das IFG ermöglicht grundsätzlich einen voraussetzungslosen Anspruch zu behördlichen Informationen.

9.6 Wenn der Arbeitgeber den Facharzt kennt – Umgang mit Arbeitsunfähigkeitsbescheinigungen

Der Personalrat eines Kita-Eigenbetriebes wandte sich an uns, da die Kita-Leitung einer Einrichtung die Beschäftigten angewiesen hat, die Arbeitsunfähigkeitsbescheinigung ausschließlich bei der örtlichen Kita-Leitung und nicht auch alternativ beim Personalservice abzugeben.

Aus der Angabe des Fachgebietes der Ärztin bzw. des Arztes kann die Führungskraft ohne Weiteres Rückschlüsse auf die Art der Erkrankung ziehen, die die Betroffenen in ihren schutzwürdigen Belangen nicht unerheblich beeinträchtigen können. So kann z. B. die Fachbezeichnung „Onkologie" auf

eine bestehende Krebserkrankung, der Zusatz „Drogenambulanz" auf etwaige Alkohol- oder Drogenprobleme oder der „Fachbereich Psychiatrie" auf psychische Erkrankungen hindeuten.

Gemäß Entgeltfortzahlungsgesetz (EntgFG) haben die Beschäftigten eine ärztliche Bescheinigung über das Bestehen der Arbeitsunfähigkeit, sofern sie länger als drei Kalendertage andauert, spätestens an dem darauffolgenden Arbeitstag beim Arbeitgeber vorzulegen. Dabei ist der Begriff des Arbeitgebers allerdings nicht gleichzusetzen mit dem Begriff des direkten Vorgesetzten. Zwar hat die Kita-Leitung ein nachvollziehbares Interesse an der Kenntnis der Arbeitsunfähigkeitsbescheinigung bei der Dienstplanung, die Einreichung der Arbeitsunfähigkeitsbescheinigung beim Personalservice stellt aber im Rahmen der Prüfung der Verhältnismäßigkeit ein milderes Mittel dar, das die Interessen der Betroffenen weniger beeinträchtigt.

Wir haben daher die Geschäftsleitung des Eigenbetriebes aufgefordert, es den Betroffenen weiterhin freizustellen, ob sie Arbeitsunfähigkeitsbescheinigungen bei der Personalstelle oder bei der örtlichen Kita-Leitung abgeben.

> Die verpflichtende Abgabe der Arbeitsunfähigkeitsbescheinigung bei der direkten Führungskraft ist nicht erforderlich. Den gesetzlichen Vorgaben kann entsprochen werden, wenn den Betroffenen freisteht, selbst über den Adressaten ihrer Arbeitsunfähigkeitsbescheinigung (Führungskraft oder Personalservice) zu entscheiden.

Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

18. Tätigkeitsbericht (2014/2015)

5.1 Betriebliches Eingliederungsmanagement – Teilnahme einer Vertrauensperson aus dem privaten Umfeld?

Eine Dienststelle des Landes Brandenburg war sich unsicher, ob sie dem Wunsch des Betroffenen Rechnung tragen darf, eine Vertrauensperson aus seinem privaten Umfeld für die Durchführung des Betrieblichen Eingliederungsmanagements hinzuzuziehen.

Arbeitgeber (ebenso Dienstherren) sind nach § 84 Abs. 2 Neuntes Buch Sozialgesetzbuch zur Durchführung des Betrieblichen Eingliederungsmanagements (BEM) verpflichtet, sobald ein Arbeitnehmer (oder Beamter) innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig ist. Bei der Durchführung dieses Verfahrens hat der Arbeitgeber bzw. der mit der Durchführung des Verfahrens betraute BEM-Beauftragte ein Höchstmaß an Vertraulichkeit bei der Verarbeitung personenbezogener Daten des Betroffenen zu gewährleisten.

Die an uns gerichtete Anfrage zielte nicht, wie sonst üblich, auf den Schutz personenbezogener Daten des BEM-Betroffenen ab. Vielmehr hatte der Arbeitgeber Sorge, dass einer hinzugezogenen Vertrauensperson dienstliche Belange (auch Daten anderer Kollegen) bekannt werden könnten.

Ein Betroffener hat immer das Recht, im Rahmen der Durchführung des BEM-Verfahrens eine Vertrauensperson zu benennen. Im angefragten Fall schlug die Dienststelle hierfür ein Mitglied des Personalrats, den Betriebsarzt, einen Vertreter der Arbeitssicherheit, die Gleichstellungsbeauftragte, einen Vertreter der Krankenkasse oder der Rentenversicherung vor. Der Betroffene lehnte den vorgenannten Personenkreis ab und wünschte die Hinzuziehung einer ihm bekannten Privatperson, die in keinem Verhältnis zum Arbeitgeber stand und auch sonst keiner Verschwiegenheitspflicht unterlag. Der Arbeitgeber hatte in Anbetracht dieses Vorschlags und unter Berücksichtigung der im BEM-Gespräch zu erörternden möglichen Eingliederungsmaßnahmen, die dienstliche Belange (auch die anderer Kollegen) berühren könnten, Sorge, mit der Einbeziehung der gewünschten Privatperson gegen den Datenschutz zu verstoßen.

Wir haben den Arbeitgeber dahingehend beraten, dem Wunsch des Betroffenen Rechnung zu tragen. Dem lagen folgende Überlegungen zugrunde:

- Es ist einem BEM-Betroffenen immer erlaubt, eine Person seines Vertrauens hinzuzuziehen. Dies kann ein Kollege oder eine Person aus dem privaten Umfeld sein.
- Ein Datenschutzproblem besteht deshalb nicht, weil bei einem Gespräch in Gegenwart einer Person des Vertrauens immer die gleichen datenschutzrechtlichen Maßstäbe zugrunde zu legen sind, wie für ein Gespräch mit dem Betroffenen allein.
- Der mit der Durchführung des Verfahrens betraute BEM-Beauftragte darf im Gespräch zu keiner Zeit Personalaktendaten oder gar BEM-Daten eines Kollegen offenbaren.
- Das BEM-Gespräch behandelt einzig und allein den Fall des Betroffenen. Der Betroffene entscheidet, was er selbst offenbaren möchte und setzt damit den BEM-Beauftragten und die Person des Vertrauens freiwillig über seine Situation in Kenntnis.
- Soweit Eingliederungsmaßnahmen als Konsequenz des BEM-Gesprächs abzuleiten sind und diese unmittelbar oder mittelbar andere Kollegen betreffen (etwa Änderungen der Arbeitsorganisation), sollten diese nicht bereits im BEM-Gespräch personenbezogen besprochen werden.

Arbeitnehmer dürfen als Vertrauensperson auch solche aus ihrem privaten Umfeld hinzuziehen. Der Arbeitgeber bzw. BEM-Beauftragte muss allerdings dieselben datenschutzrechtlichen Maßstäbe zugrunde legen wie für ein Gespräch mit dem Betroffenen allein.

5.2 Betriebliches Eingliederungsmanagement – unerlaubte Datenübermittlung

Ein Bediensteter einer Fachhochschule beschwerte sich darüber, dass personenbezogene Daten aus seinem Verfahren zum Betrieblichen Eingliederungsmanagement (BEM-Verfahren) nach § 84 Abs. 2 Neuntes Buch Sozialgesetzbuch unerlaubt an nicht am Verfahren beteiligte Dritte übermittelt wurden.

Der Arbeitgeber hatte einem Langzeiterkrankten ein BEM-Verfahren angeboten, welches dieser im Vertrauen auf die Einhaltung der auch in der Dienstvereinbarung geregelten datenschutzrechtlichen Vorgaben annahm. In einem Gespräch informierte der Betroffene die Leiterin des BEM-Teams u. a. über sein zurzeit ruhendes Mobbingverfahren, welches nicht im Rahmen des BEM-Verfahrens geführt wurde. Er willigte ein, dass die BEM-Teamleiterin die Dienststellenleitung kontaktiert, um das Mobbingverfahren wieder aufzunehmen. Er übersandte ihr per E-Mail seine Aufzeichnungen und Unterlagen, die das Mobbing belegen würden (Mobbingtagebuch), zur Kenntnis und Bearbeitung. Daraufhin sah sich die Empfängerin der Unterlagen veranlasst, diese, ohne die weitere Einwilligung des Betroffenen einzuholen, sofort an die Leiterin der Personalabteilung weiterzuleiten. Letztere wiederum stellte die Unterlagen sodann der Dienststellenleitung zur Verfügung. Die BEM-Team-Leiterin glaubte, mit der Übermittlung in seinem Sinne gehandelt zu haben, der Petent jedoch fühlte sich in seinem Recht auf informationelle Selbstbestimmung verletzt.

Die Landesbeauftragte hat nach Prüfung der Sach- und Rechtslage festgestellt, dass die Datenübermittlung aus dem BEM-Verfahren des Betroffenen wegen des Verstoßes gegen § 29 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) rechtswidrig war. Diesen Verstoß hat sie auf der Grundlage von § 25 Abs. 1 BbgDSG beanstandet.

Nach § 4 Abs. 1 BbgDSG dürfen personenbezogene Daten nur mit freiwilliger und ausdrücklicher Zustimmung (Einwilligung) des Betroffenen oder aufgrund einer Rechtsvorschrift verarbeitet werden. Die Übermittlung der personenbezogenen Daten des Petenten im Mobbingtagebuch konnte weder auf eine Einwilligung gestützt werden, noch erlaubte eine Rechtsvorschrift die Datenverarbeitung.

Eine ausdrückliche Einwilligung zur Weiterleitung des Mobbingtagebuchs an die Dienststelle zu Zwecken der Prüfung der Wiederaufnahme des Mobbingverfahrens lag seitens des Betroffenen nicht vor. Es war lediglich schriftlich dokumentiert, dass eine Kontaktaufnahme der BEM Team Leiterin mit der Dienststellenleitung erfolgen sollte mit dem Ziel, dass das Mobbingverfahren wieder aufgenommen wird. Diese Willenserklärung ist eindeutig und impliziert nicht, dass Dokumente, die das BEM-Team im BEM-Verfahren vom Betroffenen erhält, ohne dessen ausdrückliches Einverständnis an nicht am Verfahren Beteiligte übermittelt werden dürfen.

Auch aus der E-Mail, die der Petent zusammen mit seinen Mobbingunterlagen an die BEM Team Leiterin sandte, war keine Einwilligung für eine Weiterleitung des Tagebuchs ersichtlich. Er schrieb: „… anbei … zur Kenntnis für Ihre Bearbeitung." Eine Datenverarbeitung darf die BEM-Team-Leiterin aber nur für das BEM-Verfahren vornehmen, etwa um festzustellen, dass sie die Aufnahme des Mobbingverfahrens für (dringend) geboten hält. Nur dieses Ergebnis hätte sie letztlich der Dienststellenleitung gegenüber kommunizieren dürfen.

Die Datenübermittlung entbehrte auch einer entsprechenden Erlaubnisnorm. Da der Petent das Mobbingtagebuch in das BEM-Verfahren eingebracht hatte, handelte es sich um Personaldaten, für deren Übermittlung in Ermangelung einer entsprechenden Vorschrift im Landesbeamtengesetz (im Gegensatz zu Personalaktendaten) § 29 Abs. 1 BbgDSG Anwendung findet. Danach dürfen Personaldaten u. a. dann übermittelt werden, wenn eine Dienstvereinbarung dies erlaubt. Die Fachhochschule hatte mit dem Personalrat eine Dienstvereinbarung zum Betrieblichen Eingliederungsmanagement abgeschlossen. Diese regelt neben der Verschwiegenheitspflicht der Mitglieder des BEM-Teams explizit den vertraulichen Umgang mit erlangten Informationen. Übermittlungsbefugnisse an Nichtverfahrensbeteiligte stützen sich nach der Dienstvereinbarung ausschließlich auf die vorherige Zustimmung des Betroffenen.

Die Beanstandung wurde anerkannt und die Dienstvereinbarung deutlicher gefasst, um Missverständnissen vorzubeugen.

Die mit einem BEM-Verfahren Beauftragten müssen vor einer Datenübermittlung aus dem Verfahren genauestens prüfen, ob die Betroffenen der jeweiligen Übermittlung zugestimmt haben oder ob eine Rechtsgrundlage diese erlaubt. Mutmaßliche Einwilligungen sind hier absolut fehl am Platz.

5.4 Entgeltabrechnungen und Arbeitgeberbescheinigungen online

Eine Beschäftigte informierte uns, dass ihr Arbeitgeber die monatlichen Entgeltabrechnungen nur noch in elektronischer Form über ein Online-Mitarbeiterportal zum Abrufen und Ausdrucken bereitstellt. Gleiches sollte für Bescheinigungen zur Vorlage beim Finanzamt und der Sozialversicherung gelten. Da am Arbeitsplatz unserer Petentin jedoch kein Drucker verfügbar war, verwies der Arbeitgeber sie darauf, Drucker am Arbeitsplatz der Vorgesetzten bzw. an öffentlich zugänglichen PCs im Foyer des Unternehmens zu nutzen.

Arbeitgeber sind gem. § 108 Abs. 1 Gewerbeordnung verpflichtet, Arbeitnehmern bei Zahlung des Arbeitsentgelts eine Abrechnung in Textform zu erteilen. Ob hierfür die Papierform mit postalischer Übermittlung oder die elektronische Form per Online-Abruf oder per E-Mail-Versand genutzt wird, kann der Arbeitgeber selbst festlegen. Er ist bei der elektronischen Variante allerdings verpflichtet, die Anforde-

rungen des Bundes- bzw. Landesdatenschutzgesetzes insbesondere zur Wahrung der Vertraulichkeit und Integrität der Daten einzuhalten. Durch die Umsetzung technischer und organisatorischer Maßnahmen ist zu gewährleisten, dass die personenbezogenen Daten der Entgeltabrechnung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Gleiches gilt für andere Bescheinigungen, die der Arbeitgeber Arbeitnehmern z. B. zur Vorlage bei Finanz- oder Sozialbehörden ausstellt.

Im konkreten Fall hatte das Unternehmen bereits eine Reihe von Maßnahmen realisiert, die den Zugriff Unbefugter auf Entgeltabrechnungen und andere Dokumente, die über das Mitarbeiterportal bereitgestellt werden, verhindern sollten: die Datenübertragung wurde verschlüsselt, der Abruf erst durch Eingabe eines starken Passworts möglich und der Benutzer nach einer gewissen Zeit der Inaktivität beim Portal automatisch abgemeldet. Der Vorschlag, den Ausdruck der Abrechnungen oder Bescheinigungen unbeaufsichtigt und auf einem räumlich vom Arbeitsplatz entfernten Drucker (z. B. bei Vorgesetzten) durchzuführen, war jedoch untauglich, da so nicht ausgeschlossen werden konnte, dass Dritte sensitive personenbezogene Daten der Beschäftigten zur Kenntnis nehmen. Dies ließe sich z. B. durch eine sogenannte Follow-Me-Funktion am Drucker verhindern, bei der der eigentliche Druck erst dann erfolgt, wenn der Beschäftigte am Gerät steht und dort eine personengebundene PIN oder Chipkarte zum Start des Druckvorgangs eingibt.

Auch die Nutzung von PCs und Druckern in öffentlich zugänglichen Bereichen des Unternehmens verbietet sich für die genannten Zwecke, da diese missbräuchlich verwendet werden können, wenn nicht entsprechende Vorkehrungen getroffen werden. Die Möglichkeiten für Angreifer reichen von der Einschleusung von Schadsoftware oder -hardware (z. B. Keylogger zur Protokollierung von Tastatureingaben) bis hin zur Anbringung von Miniaturkameras im Raum, die Bildschirminhalte fotografieren. Stattdessen wäre die Bereitstellung von Selbstbedienungsterminals, die in nicht öffentlich zugänglichen Bereichen des Unternehmens aufgestellt werden und unter administrativer Kontrolle der IT-Abteilung stehen, eine Alternative.

Da das Unternehmen bereits in ausgewählten Abteilungen Drucker mit Follow-Me-Funktion einsetzte, sagte es zu, die Beschäftigten auf die Nutzung dieser Geräte zum Druck der Entgeltabrechnungen oder Arbeitgeberbescheinigungen zu verweisen. Parallel sollte geprüft werden, bei Ersatzbeschaffungen von Druckern und Multifunktionsgeräten diese Funktion verbindlich vorzuschreiben. Weiterhin zog das Unternehmen auch die Installation von Selbstbedienungsterminals in nicht öffentlich zugänglichen Bereichen in Erwägung.

Bei der Überprüfung der Verschlüsselungslösung für die elektronische Übertragung der Beschäftigtendaten aus dem Mitarbeiterportal stellten wir fest, dass das verwendete Zertifikat, mit dem sich der Server des Unternehmens gegenüber einem Client-PC ausweist, Schwächen aufwies. Diese führten zu einer Warnung, die in ähnlicher Form auch bei Angriffen auf die Verschlüsselung auftreten würde und Unsicherheiten bei den Beschäftigten hätte hervorrufen können: Sie mussten die Kenntnisnahme der Warnung explizit bestätigen, um weiter zum Abruf der Entgeltabrechnungen oder der Arbeitgeberbescheinigungen zu gelangen. Das Unternehmen sagte eine Änderung der Serverkonfiguration zu.

Ergänzend forderten wir, dass der Fingerabdruck zur Prüfung der Korrektheit des Zertifikats auf mehreren verschiedenen Informationskanälen an die Beschäftigten weiterzugeben ist. So kann verhindert werden, dass Dritte durch Manipulieren der elektronischen Kommunikation sowohl das Zertifikat selbst als auch dessen Fingerabdruck verändern und verschlüsselte Inhalte anschließend im Klartext zur Kenntnis nehmen können. Das Unternehmen sagte zu, diese Forderung zu erfüllen.

> Entgeltabrechnungen und Arbeitgeberbescheinigungen z. B. zur Vorlage bei Finanz- oder Sozialbehörden enthalten sensitive Daten von Beschäftigten. Stellt der Arbeitgeber die Dokumente nur in elektronischer Form zur Verfügung, muss er durch geeignete und angemessene technische und organisatorische Maßnahmen ausschließen, dass die Daten Dritten zur Kenntnis gelangen.

1.7.2 „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4 a BDSG rechtmäßig erfolgen.

- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4 a Abs. 3 BDSG, entspricht.

- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.

- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.

- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen

38. Tätigkeitsbericht (2015)

11.1 Einholung einer SCHUFA-Auskunft über Bewerber

Ein Autohaus holte über einen Bewerber eine SCHUFA-Auskunft ein mit der Begründung, der Bewerber habe darin eingewilligt. Dies bestritt der Bewerber und führte an, durch die Einholung der Auskunft sinke sein Scorewert und somit seine Kreditwürdigkeit. Das Autohaus erklärte auf unsere Anfrage, es habe wohl ein Missverständnis wegen der Einwilligung vorgelegen. Grund für die Einholung der Auskunft bei der Auskunftei sei gewesen, dass der Bewerber als Autoverkäufer mit sehr viel Geld bei der Abwicklung eines Autoverkaufs in Kontakt hätte kommen können. In diesem Zusammenhang fragte das Autohaus, ob unseren Bedenken begegnet würde, wenn nur zwei Personen der Personalabteilung Einsicht in die SCHUFA-Auskunft bekämen und der Geschäftsleitung nur das Gesamtergebnis nennen würden.

Hierzu erklärten wir, dass eine Einwilligung in die Einholung von Auskünften bei Auskunfteien im Bewerbungsverfahren wegen des Abhängigkeitsverhältnisses regelmäßig nicht wirksam ist, weil sie nicht auf der freien Entscheidung der Betroffenen beruht. Verweigern sie die Auskunft, droht ihnen die Nichteinstellung. Außerdem ist eine derartige Auskunft regelmäßig weder geeignet noch erforderlich. Einerseits enthalten diese Auskünfte erheblich mehr Daten über den Bewerber als für die Entscheidung über den zu besetzenden Arbeitsplatz erforderlich sind. Andererseits sind Daten zur Kreditwürdigkeit häufig falsch und sollen nach einem Spiegel-Online-Artikel aus dem Jahre 2009 in fast 50 Prozent der Fälle auf fehlerhaften Daten beruhen (www.spiegel.de/wirtschaft/Service/0,1518,druck-643778,00.html).

Soweit an Bewerberinnen und Bewerber besondere Anforderungen zu stellen sind, reicht es aus, im Wege der Direkterhebung bei den Betroffenen nach Verurteilungen wegen Straftaten im Zusammenhang mit Vermögensdelikten in den letzten fünf Jahren zu fragen. Daher ist die Einholung von Auskünften über Bewerberinnen und Bewerber bei Auskunfteien nicht zulässig, sodass entsprechend gespeicherte Daten zu löschen sind.

Daraufhin erklärte das Autohaus, zukünftig im Rahmen des Bewerbungsverfahrens auf die Einholung von Auskünften bei Auskunfteien oder sonstigen Dritten zu verzichten.

11.2 Kopien von Führerscheinen durch den Arbeitgeber

Ein Unternehmen nutzt ein Formular „Führerscheinkontrolle Nachweisbogen". Darin sind die wesentlichen Führerscheindaten der Beschäftigten aufgeführt, die Fahrzeuge des Unternehmens benutzen. Zugleich ist dort vorgesehen, Kopien der Führerscheine zu erstellen und zu den Vorgängen zu nehmen. Bei jeder Führerscheinkontrolle wurde der Führerschein mit der Kopie verglichen.

Wir halten die Anfertigung von Kopien der Führerscheine nicht für erforderlich. Es reicht aus, sich bei jeder Kontrolle davon zu überzeugen, ob die oder der Beschäftige einen gültigen Führerschein besitzt. Zudem stellt die Anfertigung von Kopien der Führerscheine eine Doppelspeicherung dar, die gegen den gesetzlichen Grundsatz der Datensparsamkeit verstößt.

Das Unternehmen verzichtet nunmehr auf die Anfertigung von Kopien der Führerscheine und vernichtete auf unsere Veranlassung sämtliche noch bestehenden Kopien.

11.3 Aushang der Ergebnisse von Leistungskontrollen

Laut einer bei uns eingegangenen Eingabe hängte ein großes Logistikunternehmen täglich vor jeder Schicht personenbezogene Daten über Leistungskontrollen der Beschäftigten aus. Dadurch waren die Beschäftigten einem unzumutbaren Leistungsdruck ausgesetzt. Wir wiesen das Unternehmen auf diesen Sachverhalt hin und verlangten Auskunft darüber, für welche konkreten Zwecke es diese Maßnahme für erforderlich halte.

Daraufhin erklärte das Unternehmen, es habe geprüft, in welchem Unternehmensbereich diese Praxis durchgeführt worden sein könnte. Dabei sei es auf einen Bereich aufmerksam geworden, in dem Leistungsdaten mit der mitarbeiterbezogenen Bearbeitungsnummer ausgehängt worden seien. Die Zuordnung der Bearbeitungsnummer zum Namen des Beschäftigten sei jedoch nicht veröffentlicht worden. Nach Bekanntwerden sei diese Praxis zeitnah eingestellt worden, sodass nunmehr generell auf den Aushang verzichtet werde. Hierzu ist aus datenschutzrechtlicher Sicht anzufügen, dass die Veröffentlichung der mitarbeiterbezogenen Bearbeitungsnummern ein personenbeziehbares Datum ist, das wie der Name der Beschäftigen selbst vom Grundrecht auf informationelle Selbstbestimmung geschützt ist. Auch die Veröffentlichung der Leistungsdaten mit Bearbeitungsnummern war daher rechtswidrig.

12.7 Videoüberwachung und Tonüberwachung der Beschäftigten in einem Restaurant

In einem Restaurant wurden Beschäftigte per Videokameras mit integrierten Mikrofonen mindestens in der Küche überwacht; am Tresen sowie im mittleren Teil des Restaurants galt dies auch für die Gäste. Der Geschäftsführer des Restaurants erklärte uns, die Videoüberwachungsanlage und Tonüberwachungsanlage diene ausschließlich der Einbruchsdiebstahlvorsorge, da er bereits mehrfach nachweislich Schäden durch Einbruchsdiebstahl habe hinnehmen müssen. Die Anlage würde erst nach Geschäftsschluss eingeschaltet.

Wir erklärten ihm, dass es nach unseren Erfahrungen zur Einbruchsvorsorge ausreicht, nur die Haupteingänge und Nebeneingänge per außen angebrachten Videokameras zu überwachen, die zudem weder schwenkbar noch zoombar sein dürfen. Daher verlangten wir, die Kameras innerhalb der Räumlichkeiten des Restaurants zu entfernen, auch weil die Betroffenen keine Gewähr hatten, ob die Videokameras im Tresenbereich, in der Küche und im mittleren Teil des Restaurants tatsächlich nur außerhalb der Geschäftszeiten aktiviert waren.

Eine Tonüberwachung ist für die Einbruchsvorsorge nicht erforderlich, weil hierzu die Videoüberwachung ausreicht. Zudem ist Tonüberwachung generell nicht zulässig, weil hierfür keine Rechtsgrundlage besteht, die dies ausdrücklich erlaubt. Außerdem wiesen wir darauf hin, dass sich alle strafbar machen, die das nicht öffentlich gesprochene Wort anderer unbefugt auf einen Tonträger aufnehmen. Wir verlangten daher, auf die Tonaufzeichnung beziehungsweise Tonüberwachung zu verzichten, und diese Funktion unverzüglich programmtechnisch zu deaktivieren. Sofern eine Deaktivierung nicht möglich ist, sind die Videokameras an den Haupteingängen und Nebeneingängen unverzüglich durch Kameras zu ersetzen, die Tonaufnahmen technisch ausschließen.

Daraufhin erklärte der Geschäftsführer, er habe die Videoüberwachungsanlage und Tonüberwachungsanlage abmontiert.

Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit

25. Tätigkeitsbericht (2013/2014)

1.1 Mitarbeiterüberwachung – Einsatz von Ortungssystemen

Der Einsatz von Ortungssystemen durch Arbeitgeber darf nicht zu permanenter Überwachung der Beschäftigten führen.

Uns erreichen häufig Anfragen zur Zulässigkeit der Ausrüstung von Firmenfahrzeugen mit GPS Empfängern oder anderer Ortungsmöglichkeiten, beispielsweise über das dienstliche Smartphone. Dabei ist für die Beschäftigten von Interesse zu erfahren, ob der Arbeitgeber mit einem solchen System den Arbeitsplatz überwachen darf und ob Ortungsdaten beispielsweise bei privater Verwendung des Fahrzeugs erhoben, verarbeitet oder genutzt werden dürfen, wie etwa

in Pausen oder nach Feierabend. Befürchtet wird eine mehr oder weniger lückenlose Überwachung.

Vielfach sind die Beschäftigten gar nicht oder unzureichend über den Einsatz solcher Ortungsmöglichkeiten und deren Einsatzzwecke informiert. Vorabkontrollen nach § 4 d Abs. 5 BDSG wurden oftmals mit dem Argument nicht durchgeführt, weil keine personenbezogenen Beschäftigtendaten verarbeitet würden. Mit der Zusammenführung beispielsweise der Personaleinsatzpläne und der Ortungsdaten der Fahrzeuge ist ein Personenbezug ohne besonderen Aufwand möglich.

Bei unseren Prüfungen stand für die Unternehmen üblicherweise die Personaleinsatzplanung der Außendienstmitarbeiter oder deren Zeiterfassung im Vordergrund.

Nach § 32 Abs. 1 S. 1 BDSG dürfen personenbezogene Beschäftigtendaten erhoben, verarbeitet oder genutzt werden, wenn sie für die Durchführung des Beschäftigungsverhältnisses erforderlich sind. Im Rahmen unserer Prüfungen stellen wir den Unternehmen folgende Fragen:

1. Sind alle Dienstfahrzeuge/Smartphones o.ä. mit GPS-Ortungssystemen ausgestattet? Wenn nicht alle Fahrzeuge/Geräte damit ausgerüstet bzw. die Systeme aktiviert wurden, um wie viele Fahrzeuge/Geräte handelt es sich?

2. Welche Daten werden mit den eingesetzten GPS-Ortungssystemen erhoben?

3. Werden neben Standort und Route bei Fahrzeugen weitere technische Angaben über die Fahrzeugnutzung erhoben (z. B. über den Betriebszustand des Motors, die Drehzahlbereiche oder das Bremsverhalten)?

4. Zu welchen konkreten Zwecken werden die Daten über die GPS-Ortungssysteme erhoben?

5. Werden die Daten beim Unternehmen gespeichert?

5.1. Wenn nein, welcher Dienstleister wurde damit beauftragt?

5.2. Werden die Anforderungen zur Auftragsdatenverarbeitung nach § 11 Abs. 2 BDSG eingehalten?

6. Über welchen Zeitraum werden die Daten gespeichert?

7. Gibt es ein Konzept zur Löschung der Daten?

7.1. Wenn ja, unter welchen Voraussetzungen werden die Daten gelöscht?

7.2. Wenn nein, wie lange bleiben die Daten personenbeziehbar gespeichert?

8. In welcher Form werden die Daten ausgewertet?

9. Findet über die Auswertung der GPS-Daten auch eine Leistungs- und Verhaltenskontrolle der Mitarbeiter statt?

10. Erfolgt eine langfristige Speicherung der Daten zu statistischen Zwecken? Werden die Daten vorab aggregiert?

11. Werden die mit GPS ausgestatteten Fahrzeuge/Geräte von den Mitarbeitern auch außerhalb der Dienstzeiten, etwa zum Zweck der An- und Abfahrt zum Arbeitsplatz oder für private Telefonate genutzt?

12. Besteht eine Möglichkeit, die GPS-Ortung im Falle einer privaten Nutzung auszuschalten bzw. zu deaktivieren?

13. Gibt es in Ihrem Betrieb einen Betriebsrat?

13.1. Wenn ja, ist der Einsatz der GPS-Systeme in einer Betriebsvereinbarung geregelt?

13.2. Wenn nein, existiert zum Einsatz der GPS-Ortung eine Arbeitsanweisung?

14. Wie wurden die Mitarbeiter über den Einsatz von Ortungssystemen informiert?

15. Auf welche Art und Weise werden Personaleinsätze geplant und dokumentiert?

Unter engen Voraussetzungen kann der Einsatz von GPS in Firmenwagen für die Personaleinsatzplanung und bei Smartphones für die Zeiterfassung erlaubt sein. Eine Überwachung in Pausen oder nach Feierabend ist unzulässig.

1.3 Arbeitgeberzeitschrift AKTIV

Private Anschriften der Beschäftigten dürfen vom Arbeitgeber nicht genutzt werden, um eine von Arbeitgeber- und Unternehmensverbänden herausgegebene Zeitschrift zu versenden.

Die Zeitschrift AKTIV wird seit 1972 von der IW Medien bzw. ihren Vorgängerunternehmen herausgegeben und erscheint in der Regel 14-tägig bis monatlich. Die IW Medien betreut die redaktionellen und publizistischen Aktivitäten des Instituts der deutschen Wirtschaft Köln e.V. Hierbei handelt es sich um ein von Arbeitgeber- und Unternehmerverbänden finanzierte, beratend tätige Institution. Die Zeitschrift AKTIV ist ein Erzeugnis der IW Medien, welches dazu bestimmt ist, Arbeitnehmer in Unternehmen über branchenspezifisch relevante politische, wirtschaftliche und gesellschaftliche Entwicklungen zu informieren sowie insbesondere Verständnis für branchen- und betriebsrelevante sowie gestaltende, politische sowie wirtschaftliche Ansichten der Arbeitgeber bei den Arbeitnehmern hervorzurufen.

Arbeitgeber abonnieren die Zeitschrift und stellen der IW Medien die privaten Postanschriften ihrer Arbeitnehmer zur Verfügung, so dass ein Direktversand der Zeitschrift von IW Medien an die einzelnen Arbeitnehmer erfolgen kann. Bei der erstmaligen Zusendung eines Exemplars wird dem Empfänger unter Beilegung eines entsprechenden Vordrucks die Möglichkeit gegeben, der weiteren Zusendung von AKTIV unmittelbar gegenüber IW Medien zu widersprechen. Dort werden die Daten der widersprechenden Arbeitnehmer in einer „Robinsonliste" zusammengetragen und mit der

entsprechenden vom jeweiligen Arbeitgeber überlassenen Auflistung der Arbeitnehmerdaten abgeglichen. Eine bloße Auslegung der AKTIV im Unternehmen im Gegensatz zur Versendung an die Privatadressen der Arbeitnehmer wird von Arbeitgeberseite als weniger geeignet betrachtet, da durch ein bloßes Auslegen der Zeitung nicht sämtliche Arbeitnehmer, wie etwa Außendienstler, erreicht werden könnten. Vor diesem Hintergrund wird die unmittelbare Versendung an die Privatanschriften der Arbeitnehmer für erforderlich erachtet. Die IW Medien handele im Hinblick auf die Versendungstätigkeit als Auftragsdatenverarbeiter i.S.d. § 11 BDSG, mithin als Dienstleister der Arbeitgeber.

Bereits 2007 haben die Aufsichtsbehörden für den Datenschutz mehrheitlich die Auffassung vertreten, dass die Nutzung der Privatadresse des Arbeitnehmers zum Zwecke der Versendung einer Zeitschrift eines Arbeitgeberverbandes unzulässig ist. Im Januar 2015 haben sich die Aufsichtsbehörden für den Datenschutz erneut mit diesem Thema beschäftigt, weil ein neues Gutachten vorgestellt wurde, das die Nutzung für zulässig erachtet.

Eine Rechtfertigung der Datennutzung durch § 32 Abs. 1 S. 1 BDSG scheidet aus. Zutreffend ist, dass den Arbeitgeber eine Vielzahl an Informations- und Aufklärungspflichten im Verhältnis gegenüber den Arbeitnehmern trifft. Zur Erfüllung dieser Pflichten kann er sich Informationsmaterials aus fremden Quellen bedienen. Zutreffend ist ebenfalls, dass der Arbeitgeber für die Erfüllung ihn treffender Verpflichtungen aus dem Arbeitsverhältnis hierfür grundsätzlich die personenbezogenen Daten der Arbeitnehmer verwenden kann. Eine Datennutzung ist jedoch lediglich dann zulässig, sofern sie für die Erfüllung der Pflicht erforderlich ist. Insofern ist zu prüfen, ob der verfolgte Zweck auch ohne die jeweils intendierte Datennutzung zu erreichen ist.

Ein Direktversand unter Verwendung der Privatanschriften der Arbeitnehmer ist zur Erfüllung der hier in Rede stehenden Pflichten nicht erforderlich. Die Zeitschrift AKTIV enthält lediglich allgemeine, abstrakte Informationen, die nicht für die Erfüllung der Aufklärungspflichten des Arbeitgebers gegenüber den jeweiligen Arbeitnehmern in seinem Betrieb relevant sind. Insbesondere lässt sich hieraus nicht die Erforderlichkeit ableiten, die Zeitschrift durch Verwendung der Privatadressen der Arbeitnehmer zu versenden. Das Auslegen der Zeitschrift reicht hier völlig aus und ist möglich, ohne dass die Anschriftendaten der Arbeitnehmer genutzt werden.

Diese Auffassung wird mehrheitlich von den Aufsichtsbehörden für den Datenschutz vertreten.

Hessischer Datenschutzbeauftragte

44. Tätigkeitsbericht (2015)

4.10.1 Datenschutzrechtliche Einwilligungen von Beschäftigten im Rahmen des Abschlusses von Arbeitsverträgen

Ist die Übermittlung von Beschäftigtendaten von einer gesetzlichen Rechtsgrundlage gedeckt, besteht keine Notwendigkeit für die Einholung einer Einwilligung. Sie wirkt in solchen Konstellationen irreführend und ist daher zu vermeiden. Aufgrund ihrer freien Widerruflichkeit ist die Einwilligung keine taugliche Basis für Standardverfahren.

4.10.1.1 Beschwerdegegenstand

Der Betriebsrat eines Konzerns wandte sich mit der Frage an mich, ob es zulässig sei, Übermittlungen von Beschäftigtendaten an die Konzernmutter durch Einwilligungen zu legitimieren.

Das Unternehmen hatte bei Abschluss von Arbeitsverträgen diesen eine „Datenschutzerklärung" beigefügt, in welcher die Beschäftigten ihre Einwilligung dafür zu erklären hatten, dass ihre Personaldaten an eine Zentraldatenbank der Konzernmutter übermittelt und dort verarbeitet und genutzt werden dürfen.

4.10.1.2 Rechtliche Bewertung

Das deutsche Datenschutzrecht kennt kein Konzernprivileg. Handelt es sich bei einer Datenverarbeitung weder um eine Verarbeitung innerhalb des Unternehmens, bei dem der Arbeitnehmer beschäftigt ist, noch um eine Auftragsdatenverarbeitung, ist von einer Übermittlung nach § 3 Abs. 8 BDSG auszugehen. Diese bedarf gemäß § 4 Abs. 1 BDSG einer Rechtsgrundlage oder der Einwilligung des Betroffenen.

Als Rechtsgrundlage für die Übermittlung von Beschäftigtendaten kommt zunächst § 32 Abs. 1 Satz 1 BDSG in Betracht. Diese Bestimmung setzt voraus, dass die Verarbeitung – hier also die Übermittlung der Daten der Beschäftigten eines Konzernunternehmens an die Konzernmutter – für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.

Von der Erforderlichkeit einer Datenübermittlung im Konzern wird auszugehen sein, „sofern der Arbeitsvertrag einen bei Vertragsabschluss für den Betroffenen erkennbaren Konzernbezug aufweist, wenn er also ein Tätigwerden des Arbeitnehmers auch in anderen Konzernunternehmen vorsieht" (Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" vom 11.01.2005, 3; https://www.datenschutz.hessen.de/ftkonzerndatenschutz.htm). Ein Konzernbezug, der eine Übermittlung rechtfertigt, wäre ferner auch dann gegeben, wenn bei der Einstellung des Arbeitnehmers deutlich erkennbar ist, dass die Personaldatenverarbeitung in einem anderen Konzernunternehmen zentralisiert ist (Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" vom 11.01.2005, 3; https://www.datenschutz.hessen.de/ft-konzerndatenschutz.htm).

Auch eine Einwilligung gemäß § 4a BDSG kann Grundlage für die Übermittlung von Daten sein. Aufgrund des wirtschaftlichen Ungleichgewichts und der existentiellen Bedeutung des Beschäftigungsverhältnisses wird im Allgemeinen jedoch bezweifelt, dass auf Seiten der Beschäftigten die Einwilligung freiwillig erteilt werden kann. Dies gilt erst recht, wenn sie Voraussetzung für den Abschluss des jeweiligen Arbeitsvertrags ist.

Darüber hinaus gilt es zu bedenken, dass die Einwilligung jederzeit widerruflich ist und sie daher nur ausnahmsweise einen praktikablen Weg darstellt. Widerruft der Betroffene seine Einwilligung, hat nämlich mit dem Widerruf eine Übermittlung zu unterbleiben. Ist also die Einwilligung die einzige Rechtfertigung der Übermittlung, muss die Möglichkeit eines Widerrufs berücksichtigt und organisatorisch umgesetzt werden. Dies ist für Verfahren wie etwa die zentrale Gehaltsabrechnung wohl keine Option.

Im konkreten Fall teilte das Unternehmen mit, dass bereits im Zuge des Bewerbungsverfahrens die künftigen Mitarbeiter dahingehend informiert werden, dass die Personaldatenverarbeitung beim Mutterkonzern erfolge. Auch ergebe sich der Konzernbezug bereits aus der Organisationsstruktur des Unternehmens. Dies wurde näher ausgeführt. Die Übermittlung konnte daher auf § 32 Abs. 1 Satz 1 BDSG gestützt werden.

Da eine dennoch von den Beschäftigten eingeholte Einwilligung zu der Übermittlung ihrer Daten irreführend wäre und den Beschäftigten den unrichtigen Eindruck vermittelt, sie hätten es selbst in der Hand, ob ihre Daten an eine andere Konzerngesellschaft übermittelt werden, habe ich von einer solchen Einholung von Einwilligungen „auf Vorrat" dringend abgeraten. Ob eine solche Einwilligung überhaupt wirksam wäre, kann bezweifelt werden, da Widerruf praktisch nicht möglich ist (Artikel 29-Datenschutzgruppe WP 187 Stellungnahme 15/2011 zur Definition von Einwilligungen, III.A.1., S. 16; http://ec.europa.eu/justice/dataprotection/article 29/documentation/opinion recommendation/files/2011/wp187_de.pdf). Geht man weiter davon aus, dass im vorliegenden Fall gemäß § 4 Abs. 1 BDSG auch auf die Folgen der Verweigerung der Einwilligung hinzuweisen ist, wären die Betroffenen auch darüber zu informieren, dass die Nichterteilung ihrer Einwilligung folgenlos bliebe. Die Datenübermittlung an die Konzernmutter würde dann auf § 32 Abs. 1 Satz 1 BDSG gestützt trotzdem rechtlich zulässig stattfinden. Spätestens diese Information macht deutlich, dass die Einholung einer Einwilligung „auf Vorrat" in einer solchen Konstellation keinen zusätzlichen Nutzen bringt.

Die Information der Beschäftigten gemäß § 4 Abs. 3 BDSG über die Identität der verantwortlichen Stelle, die Zwecke der Verarbeitung sowie die Kategorien der Empfänger der Daten ist hier notwendig, aber auch ausreichend. Folgerichtig hat das Unternehmen im Ergebnis darauf verzichtet, für die Übermittlung von Beschäftigtendaten Einwilligungen einzuholen. Vielmehr werden die Beschäftigten künftig in geeigneter Weise gemäß § 4 Abs. 3 BDSG über die beabsichtigte Datenübermittlung auf der Grundlage von § 32 Abs. 1 Satz 1 BDSG informiert.

Landesbeauftragte für den Datenschutz Niedersachsen

22. Tätigkeitsbericht (2014/2015)

Überwachung durch GPS-Sender am Fahrzeug

Mehrfach hatte ich mit Vorfällen im Zusammenhang mit einer Überwachung von Personen durch Anbringen eines GPS-Senders an einem Fahrzeug zu tun. Wenn auf diese Weise Mitarbeiter im Betrieb durch Vorgesetzte kontrolliert werden, handelt es sich regelmäßig um einen Verstoß gegen das informationelle Selbstbestimmungsrecht und eine Ordnungswidrigkeit. Entsprechend habe ich erstmals im Berichtszeitraum in zwei Fällen ein Bußgeld wegen einer solchen Überwachung festgesetzt.

Zugenommen haben Anzeigen wegen Ausspionierens von Personen mittels Überwachung ihrer Fahrzeuge durch ihre privaten Ex-Partner. Nach meiner Auffassung unterliegen diese Taten jedoch nicht dem Anwendungsbereich des Bundesdatenschutzgesetzes, da es sich um ein Geschehen innerhalb des privaten Lebensbereiches handelt, welches das Datenschutzrecht nicht durch Regelungen ausfüllen will.

Wiederholungsfälle

Im Berichtszeitraum ist aufgefallen, dass viele Unternehmen und Personen trotz bereits erfolgter „Bestrafung" durch eine Bußgeldfestsetzung zu einem späteren Zeitpunkt die geahndete Handlung wiederholen. In diesen Fällen habe ich erneute Bußgeldverfahren durchgeführt und die Höhe des Bußgeldes verdoppelt. Viele der Betroffenen zahlen das Bußgeld nicht freiwillig, und es müssen Vollstreckungsverfahren eingeleitet werden. Ich werde dennoch auch künftig Nachlässigkeiten und eine Missachtung des Datenschutzes nicht hinnehmen und Datenschutzverstöße weiterhin mit Bußgeldern ahnden.

Biometrisches Zugangssystem: Fingerabdruckscanner in Fensterfirma unzulässig

Zum Stichwort Fingerabdruckscanner erreichte mich eine Anfrage einer Firma, die im Internet mit Holzfenstern handelt. Das Unternehmen hat ungefähr 50 Mitarbeiter. In der Firma wurde der Einsatz eines biometrischen Zugangssystems mittels Fingerabdruck geplant. Ich wurde gebeten, die rechtliche Zulässigkeit zu beurteilen.

Ob Mitarbeiterdaten erhoben werden dürfen, richtet sich nach § 32 Bundesdatenschutzgesetz (BDSG). Hiernach ist relevant, ob die Erfassung des Fingerabdrucks erforderlich ist zur Durchführung des jeweiligen Beschäftigungsverhält-

nisses. Auf Details zu den Erhebungsdaten (wird zum Beispiel im Ergebnis nur ein mathematischer Wert abgeglichen oder werden tatsächlich biometrische Merkmale der Beschäftigten dauerhaft gespeichert?) kam es in diesem konkreten Einzelfall nicht entscheidend an. Vielmehr war entscheidend, ob ein solches System selbst bei geringer Eingriffstiefe erforderlich ist. Für die Erfassung derart sensibler Daten ist die Erforderlichkeit nur dann zu bejahen, wenn es sich um Branchen handelt, bei denen Sicherheitsaspekte eine große Rolle spielen, insbesondere bezogen auf Leib und Leben wie in einem Hochsicherheitslabor oder auf besonders hohe Wertbeträge wie im Tresorbereich.

Zweck auch mit Chipkarte oder Passwort erreichbar

Die anfragende Firma, die im Internet handelsübliche Fenster verkauft, hatte dagegen kein sicherheitsrelevantes Tätigkeitsgebiet; es bestand kein Unterschied zu anderen, „normalen" Firmen. Der beabsichtigte Zweck (Zugangskontrolle) konnte daher auch mit einer Chipkarte oder einem Passwort sichergestellt werden, zumal sich die rund 50 Mitarbeiter jeweils persönlich kennen dürften. Auch das vorgebrachte Argument, dass eine Chipkarte vergessen werden könne, war nicht stichhaltig: Bei Vergessen der Chipkarte kann der jeweilige Mitarbeiter zum Beispiel mit einer Besucherchipkarte ausgestattet werden.

Ich konnte der Firma daher die Antwort mitteilen, dass für eine Erhebung biometrischer Daten keine Erforderlichkeit besteht; eine solche Datenerhebung wäre daher rechtswidrig. Auch bei Firmen mit erhöhter Sicherheitsrelevanz sind allerdings immer noch Zwischenlösungen möglich. Beispielsweise kann ein Schutz vor Spionage auch sichergestellt werden durch die Kombination von Chipkarte und zusätzlichem Passwort. Alternativ wäre denkbar, nur sensible Bereiche wie Entwicklungsabteilungen für die dort Beschäftigten mit einem Fingerabdrucksystem auszustatten. Eine pauschale Anwendung auf alle Beschäftigten wäre jedoch auch in solchen Fällen nicht erforderlich.

Konto beim Arbeitgeber: Bank darf nicht Mitarbeiterkonten einsehen

Ein Arbeitgeber darf grundsätzlich keine Kontodaten seiner Mitarbeiter erheben. Was aber ist, wenn die kontoführende Bank des Kunden gleichzeitig dessen Arbeitgeber ist?

Um diese Konstellation ging es bei einer Rechtsberatung. Ein Mitarbeiter eines Bankhauses, der bei dieser Bank zugleich sein Konto führte, wurde von einem Leitenden Angestellten auf regelmäßige Geldeingänge auf seinem Konto angesprochen. Vom Rechenzentrum der Bank sei ein Einblick in die Konten der Mitarbeiter möglich; Hintergrund der Frage seien Aspekte der Bestechlichkeit bzw. einer unerlaubten Nebentätigkeit. Der Petent war über diese Anfrage des Leitenden Angestellten erstaunt und suchte rechtliche Beratung. Ich teilte dem Petenten mit, dass ein solcher Zugriff auf die Kontoübersichten der Mitarbeiter durch die Arbeitgeber-Bank rechtswidrig sei. Eine Rechtsgrundlage für eine solche Datenerhebung besteht nicht. Vielmehr sind die zwei verschiedenen Vertragsverhältnisse (Arbeitsverhältnis einerseits/Kontoführungsverhältnis andererseits) strikt zu trennen. Die Bank hat somit keine weitergehenden Rechte als andere Arbeitgeber.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

25. Tätigkeitsbericht (2014/15)

3.1.2 Online-Zugriff des Personalrats auf Zeiterfassungsdaten

Zwischen Dienststelle und Personalrat kann es zu Konflikten kommen, wenn die Unterrichtung des Personalrats unter namentlicher Nennung von Beschäftigten im Raum steht. Im Berichtszeitraum musste sich der LfDI mit der Frage beschäftigen, ob der Personalrat auf die Daten der elektronischen Zeiterfassung zugreifen darf.

Datenschutzrechtlich handelt es sich bei Datenweitergaben innerhalb einer verantwortlichen Stelle um eine Nutzung, deren Zulässigkeit sich nach §§ 31 Abs. 1, 13 LDSG beurteilt. Hiernach ist die Weitergabe personenbezogener Personaldaten an den Personalrat zulässig, wenn dies entweder eine Rechtsvorschrift ausdrücklich vorsieht oder zur Aufgabenerfüllung des Personalrats erforderlich ist.

Das Landespersonalvertretungsgesetz selbst enthält keine Verpflichtung der Dienststelle, dem Personalrat personenbezogene Daten in Bezug auf die elektronische Zeiterfassung zur Verfügung zu stellen. Es kommt daher entscheidend darauf an, ob die Weitergabe mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit zu vereinbaren ist. Die Anwendung des Erforderlichkeitsgrundsatzes beinhaltet eine Prüfung dahingehend, ob es für die Aufgabenerfüllung der Personalvertretung ausreichend ist, lediglich anonymisierte bzw. pseudonymisierte Daten zu erhalten. Wenn diese Frage zu bejahen ist, scheidet die Weitergabe personenbezogener Mitarbeiterdaten aus.

Das Bundesverwaltungsgericht hat die Frage, ob der Personalrat verlangen kann, dass ihm die in der elektronischen Arbeitszeiterfassung gespeicherten Daten unter Namensnennung der Beschäftigten zur Verfügung gestellt werden, konsequent nach dem datenschutzrechtlichen Grundsatz der Erforderlichkeit entschieden (Beschluss des Bundesverwaltungsgerichts vom 19. März 2014, Az. 6 P 1/13):

Die Auflistung anonymisierter Daten zur Kontrolle der Arbeitszeiten – so das Bundesverwaltungsgericht – sei für den Personalrat ausreichend; eines eigenen unmittelbaren Zugriffs auf die Datenbank bedürfe es daher nicht.

Wörtlich führt das Bundesverwaltungsgericht hierzu aus:

> „Den vorstehenden Ausführungen ist zu entnehmen, dass der Auskunftsanspruch des Antragstellers zunächst auf die Überlassung der Arbeitszeitlisten ohne Namensnennung beschränkt ist. Dies entspricht dem Grundsatz der Erforderlichkeit nach § 68 Abs. 2 Satz 1 und 2 BPersVG. Damit wird zugleich dem Grundrecht der Beschäftigten auf informationelle Selbstbestimmung Rechnung getragen (vgl. Beschluss vom 4. September 2012 a.a.O. Rn. 28). Zwar sind die Angaben über die Arbeitszeiten der Beschäftigten sowie die dabei zu bewertenden Fallgestaltungen (Dienstreisen, Urlaub, Gleittage) grundsätzlich nicht als sensibel einzustufen. Doch verbietet es der Grundsatz der Verhältnismäßigkeit, dass der Personalrat diese Angaben einer bestimmten Person zuordnen kann, ohne dass dies für die Wahrnehmung seiner Kontrollaufgabe erforderlich ist. Hinzu kommt, dass aus den Arbeitszeitlisten auch die Fehlzeiten wegen Erkrankung ersichtlich sind (vgl. Nr. 3.5 Satz 1 und Nr. 4.6.1 Satz 4 DV). Diese Angaben sind in besonderer Weise schützenswert (vgl. § 3 Abs. 9 BDSG). Aus alledem ergibt sich, dass die Überwachungsaufgabe des Antragstellers wegen der Einhaltung arbeitszeitrechtlicher Bestimmungen in einem zweistufigen Verfahren stattfindet. Auf der ersten Stufe muss sich der Antragsteller mit der Vorlage anonymisierter Arbeitszeitlisten begnügen. Soweit die Überprüfung der Listen Unstimmigkeiten zu erkennen gibt, hat der Antragsteller auf einer zweiten Stufe Anspruch auf Erläuterungen, welche auch zur Aufdeckung der Identität des betroffenen Beschäftigten führen kann, wenn anders eine Klärung der Angelegenheit nicht möglich ist. Entsprechendes gilt, wenn die Listen Hinweise auf besondere Fallgestaltungen enthalten, welche ein Tätigwerden des Antragstellers zum Schutz des betroffenen Beschäftigten gebieten."

3.1.3 Online-Bewerbungen

Die klassische Bewerbungsmappe auf Papier wird zunehmend zum Auslaufmodell. Nur noch rund jedes vierte Unternehmen (27 Prozent) wünscht sich von Jobinteressentinnen und -interessenten schriftliche Bewerbungsunterlagen. Mehr als doppelt so viele Personalverantwortliche (58 Prozent) bevorzugen dagegen eine Bewerbung per Internet. Das hat eine Umfrage im Auftrag des Digitalverbands BIT-KOM unter 408 Personalverantwortlichen aus allen Branchen im Frühjahr 2015 ergeben.

Online-Bewerbungen sind auf zwei Wegen möglich. Entweder erfolgt die Zusendung der Unterlagen per E-Mail oder über ein eigenes Online-Bewerbungsportal, bei denen die Interessentinnen und Interessenten ein Formular mit persönlichen Angaben ausfüllen und eingescannte Dokumente wie Zeugnisse und Zertifikate hochladen können.

Bei der Übersendung per E-Mail ist Folgendes zu beachten: Normalerweise erfolgt die Übertragung von E-Mails im Internet ohne besondere Absicherung, d.h. die an der Übertragung beteiligten Stellen (z.B. Internetzugangsprovider, E-Mail-Dienstleister etc.) sind grundsätzlich in der Lage, neben den für die Zustellung erforderlichen Verbindungsdaten (E-Mail-Adressen) auch die Inhalte der Nachrichten zur Kenntnis zu nehmen und diese sogar zu verändern. Um sowohl die Vertraulichkeit der Übertragung als auch die Integrität der übermittelten Daten und Authentizität der Kommunikationspartner zu gewährleisten, sind zusätzliche Sicherungsmaßnahmen zu treffen, wie z.B. die Nutzung kryptografischer Verfahren zur Verschlüsselung und der Einsatz elektronischer Signaturen.

In der täglichen Praxis haben sich darüber hinaus Lösungen entwickelt, mit denen auch ohne entsprechende Infrastrukturen eine hinreichend sichere Kommunikation möglich ist. Beispiele hierfür sind die Nutzung von verschlüsselten Containerformaten (z.B. ZIP-Dateien), die die eigentlichen Dokumente enthalten und zu deren Öffnung ein Passwort erforderlich ist. Die Containerdatei kann den Empfangenden per E-Mail zugesandt werden, das zum Öffnen erforderliche Passwort sollte auf einem anderen Übertragungsweg (z.B. telefonisch) übermittelt werden.

Sofern lediglich unveränderbare Text- oder Grafikinformationen übermittelt werden sollen, bieten sich offene Austauschformate wie z.B. PDF-Dateien an, die ebenfalls durch Passwortschutz gegen unbefugtes Öffnen geschützt werden können. In jedem Fall sollte mit den Bewerberinnen und Bewerbern vorab abgestimmt werden, welche Sicherungsmaßnahme unterstützt wird.

Kommt ein Online-Portal zum Einsatz, gelten folgende technische Anforderungen:

- Noch vor dem Aufrufen und Ausfüllen von Masken sollten Hinweise zum Verfahren und zur Datenverarbeitung erfolgen; diese beinhalten ebenfalls eine Aussage darüber, ob eine Bewerbung auch auf dem herkömmlichen Postweg möglich ist sowie dazu, ob die Daten von der einstellenden Stelle selbst verarbeitet werden oder ob externe Dienstleister im Wege einer Auftragsdatenverarbeitung zum Einsatz kommen.
- Für die Nutzung des Portals sollte eine Registrierung und Anmeldung mit Benutzername und Passwort vorgesehen sein.
- Für den Fall, dass das Passwort vergessen wurde, sollten Sicherheitsfragen hinterlegt sein.
- Die Betroffenen sollten eine Bestätigung über die erfolgte Übermittlung ihrer Daten erhalten (z.B. über eine Bestätigung-E-Mail).
- Übertragungsweg und Speicherung müssen gegen unbefugte Zugriffe abgesichert sein (z.B. durch eine verschlüsselte HTTPS-Verbindung).
- Die Speicherung in der Online-Datenbank sollte sechs Monate nicht übersteigen.
- Für die Kommunikation mit den Bewerberinnen und Bewerbern sollten eigene Funktionsadressen eingerichtet werden.

3.2 Datenschutz im privaten Bereich

3.2.1 Rechtsprechung des Bundesarbeitsgerichts stärkt den Datenschutz

Der Datenschutz gewinnt in der Arbeitswelt weiter an Bedeutung. § 32 BDSG regelt, unter welchen Voraussetzungen Arbeitgeberinnen und Arbeitgeber personenbezogene Daten ihrer Arbeitnehmerinnen und Arbeitnehmer erheben oder verwenden dürfen. Allerdings ist diese Vorschrift zu Recht als unscharf und schwer verständlich kritisiert worden. Umso wichtiger sind Vorgaben der Rechtsprechung. Das Bundesarbeitsgericht hat mittlerweile in einer Reihe von Entscheidungen klargestellt, welche Anforderungen die Arbeitgeberschaft beim Beschäftigtendatenschutz berücksichtigen muss. Letzthin hat das Bundesarbeitsgericht in einer durchaus als spektakulär zu bezeichnenden Entscheidung klargestellt, wie § 32 BDSG auszulegen ist – und hat bei Verstößen gegen den Beschäftigtendatenschutz sogar ein Beweisverwertungsverbot angenommen.

Die Arbeitsgerichte haben seit der Einführung von § 32 BDSG zum 1. September 2009 bereits in einer Reihe von Entscheidungen wichtige Vorgaben zum Beschäftigtendatenschutz gemacht. Neben dem Bundesarbeitsgericht haben auch andere Gerichte Entscheidungen mit erheblichen Auswirkungen auf die Datenschutzpraxis gefällt. Zuletzt verurteilte etwa der Bundesgerichtshof zwei Privatermittler wegen unzulässiger Überwachungsmaßnahmen zu Haftstrafen (vgl. Bundesgerichtshof ZD 2013, Seite 502 ff.; Urteil vom 4. Juni 2013 – 1 StR 32/13) Die Gerichte nehmen den Datenschutz jetzt erkennbar sehr ernst, mit drastischen Folgen vor allem für Unternehmen. Verletzungen der informationellen Selbstbestimmung werden zunehmend härter und konsequenter geahndet. Zugleich wählen die Gerichte als Anknüpfungspunkt nicht mehr allein das Allgemeine Persönlichkeitsrecht, sondern – systematisch richtig – das Bundesdatenschutzgesetz, insbesondere § 32 BDSG.

Mit einem Urteil zur Verwertbarkeit datenschutzwidrig erhobener Beweise (Bundesarbeitsgericht ZD 2014, Seite 260; Urteil vom 20. Juni 2013 – 2 AZR 546/12) schafft der 2. Senat nun weitere Klarheit. Anlässlich einer rechtswidrigen weil gegen Datenschutzrecht verstoßenden Spindkontrolle durch den Arbeitgeber stellt das Bundesarbeitsgericht fest, dass es sich bei der in Rede stehenden Schrankkontrolle tatbestandlich um eine Datenerhebung im Sinne des Bundesdatenschutzgesetzes handelt. Der hier einschlägige § 32 BDSG setze keinerlei technische Datenverarbeitung voraus, etwa dass die Datenerhebung zum Zwecke ihrer Nutzung und Verarbeitung in automatisierten Dateien erfolge. Die Vorschrift erfasse damit sowohl nach ihrem Wortlaut als auch nach ihrem Regelungszweck die Datenerhebung durch rein tatsächliche Handlungen – wie etwa eine Spinddurchsuchung.

Gleichzeitig bewertet das Bundesarbeitsgericht das Vorgehen des Arbeitgebers als datenschutzrechtlich unzulässig. Der persönliche Schrank eines Arbeitnehmers und dessen Inhalt seien Teil seiner Privatsphäre, in die nur nach Maßgabe des Verhältnismäßigkeitsgrundsatzes eingegriffen werden darf. Vorliegend beanstandet das Bundesarbeitsgericht, dass der Arbeitgeber den Eingriff nicht nach Information und in Anwesenheit des Arbeitnehmers durchführte, was ein milderer Eingriff gewesen wäre, sondern ohne dessen Beteiligung, also heimlich.

Da es im vorliegenden Fall an einer Rechtfertigung der Spinddurchsuchung nach § 32 BDSG fehle, seien die Erkenntnisse aus der Durchsuchung des Spinds auch nicht prozessual verwertbar. Zwar kenne die Zivilprozessordnung kein generelles prozessuales Verwendungs- bzw. Verwertungsverbot für rechtswidrig erlangte Informationen oder Beweismittel. Die Verwertung von Beweismitteln, die der Arbeitgeber rechtswidrig erlangt habe, scheide jedoch dann aus, wenn sich deren prozessuale Verwertung als erneuter bzw. fortgesetzter Eingriff in das allgemeine Persönlichkeitsrecht des Klägers darstelle, der nicht durch überwiegende Interessen des Arbeitgebers gerechtfertigt sei. Damit dürfte die gerichtliche Verwertung von datenschutzwidrig gesammelten Kündigungsgründen in der Praxis künftig in vielen Fällen ausscheiden.

Das Bundesarbeitsgericht stellt damit in seiner Entscheidung hohe Anforderungen an den Umgang mit Beschäftigtendaten. Gerade für Compliance-Kontrollen und interne Ermittlungen hat das Urteil erhebliche Folgen. Letztlich verpflichten die Richter den Arbeitgeber, bei kritischen Datenerhebungen oder der weiteren Verwendung von Daten genau darauf zu achten, aus den zur Verfügung stehenden, gleich effektiven Maßnahmen stets das mildeste Mittel mit der geringsten Eingriffstiefe auszuwählen. Dabei stellt das Bundesarbeitsgericht mit großer Klarheit heraus, dass heimliche Überwachungsmaßnahmen einen wesentlich massiveren Grundrechtseingriff darstellen als offene.

Das Urteil betrifft insbesondere auch Fallkonstellationen, in denen die Arbeitgeberseite den Beschäftigten Betriebsmittel zur Nutzung überlässt, die private Informationen betreffen; hier den Spind. Eine Übertragung dieser Grundaussagen des Bundesarbeitsgerichts auf vergleichbare Konstellationen – wie etwa die Kontrolle des (auch) zur privaten Nutzung überlassenen E Mail Zugangs der Beschäftigten – liegt dabei auf der Hand.

Der LfDI begrüßt die neue Richtung, welche die Rechtsprechung der Arbeitsgerichte damit eingeschlagen hat und sieht sich in seiner Beurteilung der Grenzen der Kontrollbefugnisse des Arbeitgebers und der Folgen von Datenschutzverstößen bestärkt. Diese Maßstäbe wird der LfDI auch seiner zukünftigen Tätigkeit im wichtigen Bereich des Beschäftigtendatenschutzes zugrunde legen.

3.2.2 IT-Nutzung am Arbeitsplatz (Orientierungshilfe)

Viele Beschäftigte haben heute an ihrem Arbeitsplatz neben Telefon und Faxgerät auch Zugang zum Internet und damit die Möglichkeit, per E-Mail, Chat oder VoIP zu kommunizieren. Arbeitgeberinnen und Arbeitgeber, deren Beschäftigte Informations- und Kommunikationstechnik (IuK) zu betrieblichen oder privaten Zwecken nutzen, erheben und verarbeiten dabei personenbezogene Daten der Beschäftigten selbst sowie ihrer inner- und außerbetrieblichen Kommunikationspartnerinnen und -partner und weiterer Betroffener (etwa in einer E-Mail erwähnter Dritter); insoweit haben die Arbeitgeberinnen und Arbeitgeber datenschutzrechtliche Anfor-

derungen zu beachten, die sich je nach Kommunikationszweck, -partner und -mittel unterscheiden und auch davon abhängen, ob den Beschäftigten neben der betrieblichen auch die private Nutzung der betrieblichen IuK ganz oder teilweise am Arbeitsplatz gestattet ist. Entsprechend differenziert sind die Anforderungen an die datenschutzgerechte Verwendung dieser Daten, insbesondere an Kontrollmaßnahmen der Arbeitgeberinnen und Arbeitgeber.

In der Praxis herrscht aufgrund der angesprochenen Vielfältigkeit der Nutzungs- und Überwachungsmöglichkeiten einerseits und der Differenziertheit der Rechtslage andererseits erhebliche Unsicherheit. Die Aufsichtsbehörde für den Datenschutz trifft regelmäßig auf Unternehmen, die trotz ihres Bemühens um faire und akzeptable Nutzungsbedingungen für die betriebliche IuK gravierende, teilweise sogar strafrechtlich relevante Fehler begehen. Andererseits kennen viele Beschäftigte häufig nicht die Grenzen zulässiger Nutzungen und fühlen sich unsicher, weil sie vermuten, dass ihnen die Arbeitgeberin oder der Arbeitgeber oder die EDV bei der IuK Nutzung am Arbeitsplatz „über die Schulter guckt" oder gar ihre private Kommunikation ausspäht. Betriebsräte schließlich suchen immer häufiger den Rat der Aufsichtsbehörde, weil sie zur IuK-Nutzung Betriebsvereinbarungen abschließen oder bestehende prüfen lassen wollen. In allen diesen Fällen kann eine Orientierungshilfe der Aufsichtsbehörde dabei helfen, bestehende Rechtsunsicherheiten durch klare Vorgaben zu beseitigen.

Der LfDI hat im Mai 2015 eine solche Orientierungshilfe erarbeitet (http://www.datenschutz.rlp.de/downloads/oh/oh_iuk_arbeitsplatz.pdf), sie stellt überblicksartig die bei der Nutzung der IuK geltenden datenschutzrechtlichen Anforderungen dar. Sie richtet sich an private Arbeitgeberinnen und Arbeitgeber, ihre Beschäftigten und Interessenvertretungen, ist aber grundsätzlich auch für den öffentlichen Dienst von Interesse, wobei dort zusätzlich landesspezifische Vorschriften etwa im Landesdatenschutzgesetz zu beachten sind. Die Orientierungshilfe bezieht nicht nur die aktuelle Rechtslage, insbesondere die Regelungen des § 32 BDSG, sondern auch arbeitsrechtliche Grundsätze mit ein, da sich der Erforderlichkeitsmaßstab des Bundesdatenschutzgesetzes auch am Arbeitsrecht orientiert.

3.2.3 Betriebsvereinbarungen als Erlaubnis zum Umgang mit Arbeitnehmerdaten

Das Bundesdatenschutzgesetz konkretisiert das Recht auf informationelle Selbstbestimmung und regelt, in welchem Umfang Eingriffe in dieses Recht zulässig sind. Fehlt es an einer Ermächtigungsgrundlage i.S.v. § 4 Abs. 1 BDSG, so ist das Erheben, Verarbeiten oder Nutzen personenbezogener Daten verboten. In Arbeitsverhältnissen kommt – neben gesetzlichen Ermächtigungsgrundlagen und der regelmäßig unpraktikablen Einwilligung – auch eine zwischen Arbeitgeberseite und Betriebsrat abgeschlossene Betriebsvereinbarung als Rechtsgrundlage für die Verwendung von Beschäftigtendaten in Betracht.

In einer Entscheidung aus dem Jahre 2013 (Bundesarbeitsgericht, NZA 2013, S. 1433; Beschluss vom 9. Juli 2013 – 1 ABR 2/13 (A)) bestätigte der 1. Senat des Bundesarbeitsgerichts, dass sorgfältig und angemessen gestaltete Betriebsvereinbarungen Gewähr für die Einhaltung der Vorgaben des Datenschutzes und des Betriebsverfassungsrechts bieten können. Betriebsvereinbarungen sind „sonstige Rechtsvorschriften" i.S.v. § 4 Abs. 1 BDSG. Im Ergebnis verschärft das Bundesarbeitsgericht mit dieser Entscheidung seine bisherige Rechtsprechung zum Umgang mit Arbeitnehmerdaten auf der Grundlage von Kollektivvereinbarungen.

Der LfDI sieht seine Rechts- und Beratungspraxis auch insoweit von der arbeitsgerichtlichen Rechtsprechung bestätigt, er hat auch im Berichtszeitraum auf Ansuchen von Arbeitgeber- wie auch von Arbeitnehmer- bzw. Betriebsratsseite abgeschlossene Betriebsvereinbarungen auf ihre Vereinbarkeit mit dem Bundesdatenschutzgesetz geprüft und Hinweise zur optimalen Umsetzung datenschutzrechtlicher Vorgaben in Kollektivvereinbarungen gegeben. Darüber hinaus hat er Verhandlungen zum Abschluss von Betriebsvereinbarungen in rheinlandpfälzischen Betrieben unterstützt und so dazu beigetragen, passgenaue datenschutzrechtliche Vereinbarungen auf Betriebsebene zu erstellen und umzusetzen.

Unabhängiges Datenschutzzentrum Saarland

25. Tätigkeitsbericht (2013/2014)

17.2.1 Arbeitnehmerüberwachung in einem Gastronomiebetrieb

Ein Mitarbeiter eines Gastronomiebetriebes hatte sich an die Dienststelle gewandt und behauptet, die Mitarbeiter in der Küche würden videografiert und permanent durch ihren Vorgesetzten überwacht. Die Kontrolle vor Ort ergab, dass die eingesetzte Dome-Kamera tatsächlich den nicht-öffentlich zugänglichen Arbeitsbereich der Mitarbeiter überwachte. Der Zugriff zur Kamera erfolgte über einen passwortgeschützten Remotezugang, der jederzeit vom Arbeitgeber abgerufen werden konnte.

Der Vorgesetzte wurde im Gespräch ausführlich über die Voraussetzungen einer zulässigen Videoüberwachungsmaßnahme, die den Anforderungen des BDSG entspricht und die dazu ergangene Rechtsprechung 100 Unabhängiges Datenschutzzentrum Saarland, 25. Tätigkeitsbericht des Bundesarbeitsgerichts informiert. Demnach dürfen Beschäftigte, außer in speziellen Einzelfällen, nicht permanent von einer Videoüberwachung erfasst werden. Da der Fokus der Kamera auf der Überwachung der Leistung und des Verhaltens der Mitarbeiter lag, die somit einem permanenten Überwachungsdruck durch ihren Arbeitgeber ausgesetzt waren, wurde die Kameraeinstellung für unzulässig erklärt.

Der Verantwortliche zeigte sich zunächst einsichtig und übermittelte uns eine Mail, in der er bestätigte, die Videokamera vom Netz genommen und keine Zugriffsmöglichkeiten mehr zu haben.

In einer Nachkontrolle mussten wir leider feststellen, dass die Kamera nach wie vor einsatzbereit und angeschlossen für Zugriffe zur Verfügung stand.

Das hierzu ergangene Ordnungswidrigkeitsverfahren wird unter Kapitel 18.2 des Tätigkeitsberichts beschrieben.

17.2.2 Telefonische Kontaktaufnahme zu ausgeschiedenen Mitarbeitern

Ein Petent, der sein Arbeitsverhältnis gekündigt hatte, beschwerte sich bei unserer Dienststelle über seinen ehemaligen Arbeitgeber.

Dieser hatte ein Callcenter damit beauftragt, Mitarbeiter, die ihr Arbeitsverhältnis gekündigt hatten, nach den Gründen zu befragen und dem Callcenter zu diesem Zweck Namen und Telefonnummern der betreffenden Personen übergeben. Ziel der Befragungsaktion sollte nach Aussage des Unternehmens sein, Ansatzpunkte für Verbesserungen im Unternehmen zu ermitteln.

Wir haben die beschriebene Datennutzung als Verstoß gegen § 32 Bundesdatenschutzgesetz (BDSG), der die Voraussetzungen einer zulässigen Datenverarbeitung von Beschäftigten regelt, bewertet. Eine Interessenabwägung zwischen dem Interesse des Unternehmens an einer Verbesserung der Arbeitsbedingungen mit den schutzwürdigen Belangen der ausgeschiedenen Mitarbeiter lässt die Maßnahme als unverhältnismäßig erscheinen.

Das Unternehmen hat dies auf unsere Nachfrage hin auch eingeräumt und als Alternative vorgeschlagen, künftig auf die Einschaltung eines Callcenters zu verzichten.

Da das Unternehmen die Aktion sofort eingestellt hat, haben wir auf die Einleitung eines Bußgeldverfahrens verzichtet.

19.2 Videoüberwachung im Beschäftigungsverhältnis

Immer wieder werden die Aufsichtsbehörden für den Datenschutz in Deutschland mit Fällen konfrontiert, in denen Beschäftigte eines Unternehmens per Videoüberwachung kontrolliert werden. So hat auch das Unabhängige Datenschutzzentrum des Saarlandes im Berichtszeitraum mehrere Eingaben zu dieser Thematik erhalten und musste die datenschutzrechtliche Zulässigkeit der Videoüberwachung beurteilen.

Generell ist dazu anzumerken, dass bereits im Jahr 2004 das Bundesarbeitsgericht festgestellt hat, dass eine permanente Videoüberwachung am Arbeitsplatz und der damit einhergehende permanente Überwachungsdruck in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht der Arbeitnehmer eingreift. Eine „Rund-um-die-UhrÜberwachung" von Mitarbeitern ist aufgrund dieses schwerwiegenden Eingriffs in die Persönlichkeitsrechte der Beschäftigten unzulässig (BAG Beschluss vom 14. Dezember 2004 AZ: 1 ARB 34/03).

Nur in ganz besonderen Ausnahmefällen kann eine solche Maßnahme gerechtfertigt sein. Eine permanente Videoüberwachung der Beschäftigten ist beispielsweise denkbar, wenn der Beschäftigte in einem besonders gefahrträchtigen Arbeitsbereich tätig ist und der Arbeitgeber seiner Schutzpflicht nachkommen muss. In der Regel fällt die Abwägung zwischen den Interessen eines Arbeitgebers an einer Videoüberwachung und den schutzwürdigen Belangen der Beschäftigten jedoch zugunsten der Beschäftigten aus. Die Zulässigkeit ist im Einzelfall zu überprüfen.

In der Abwägung zwischen den berechtigten Interessen der Arbeitgeber und der Beschäftigten an der Durchführung einer Videoüberwachung ist insbesondere zu gewichten, ob dem Beschäftigten überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich zur Verfügung steht. Generell unzulässig ist eine Videoüberwachung in sensiblen Bereichen wie Umkleidekabinen, sanitäre Einrichtungen und Aufenthaltsräume. Auch eine Videoüberwachung zur reinen Leistungs- und Verhaltenskontrolle der Beschäftigten ist unzulässig.

Da eine Videoüberwachung dazu geeignet ist, das Verhalten und die Leistung der Beschäftigten zu dokumentieren, ist die Installation einer Videoüberwachung im Betrieb mitbestimmungspflichtig, soweit ein Betriebsrat im Unternehmen existiert. Bei der Installation einer Videoüberwachung im Betrieb empfehlen wir daher den Abschluss einer Betriebsvereinbarung, die eine Auswertung der Videosequenzen zur Verhaltens- und Leistungskontrolle der Belegschaft ausschließt.

Der Düsseldorfer Kreis hat aufgrund der vermehrten Eingaben zur Thematik am 26. Februar 2014 eine Orientierungshilfe zur Videoüberwachung durch nicht-öffentliche Stellen veröffentlicht. Darin wird unter anderem unter Punkt 4 auch explizit auf die Videoüberwachung von Beschäftigten eingegangen. Die Orientierungshilfe ist in unserem Internetangebot zu finden und gibt eine umfassende Hilfestellung zur Zulässigkeitsprüfung von Videoüberwachungsmaßnahmen.

Sächsischer Datenschutzbeauftragter

17. Tätigkeitsbericht (2013/2015)

5.1.3 Beschäftigtendatenverarbeitung zur Prüfung der Eignung von Bediensteten

Im letzten Berichtszeitraum wandten sich Bedienstete einer JVA an meine Behörde. Gegenstand war ein Schreiben des SMJus an die Anstaltsleitung, das Vorkehrungen seitens der Einrichtung vorsah, um möglichen „Grenzverletzungen" zwischen Bediensteten des allgemeinen Vollzugs-

dienstes und Gefangenen vorzubeugen bzw. in diesen Fällen Maßnahmen ergreifen zu können. Hintergrund waren in der Vergangenheit vorgekommene Beziehungen und Verhältnisse zwischen Vollzugsbediensteten und Gefangenen gewesen. Z. T. war eine mediale Resonanz zu Vorkommnissen dieser Art zu verzeichnen.

Mit dem ministeriellen Schreiben wurde der Anstalt ein Maßnahmenbündel auferlegt, eine „Risikoanalyse und Prüfung der Eignung von Bediensteten", eine „regelmäßige Analyse der sozialen Beziehungen von Bediensteten und Gefangenen im Stationsbereich (Frühwarnsystem)" und eine „Fortbildung, kollegiale Beratung und Supervision für die Bediensteten der JVA..." zu verfolgen. Ich teilte dem Ministerium mit, dass eine Beschäftigtendatenverarbeitung gemäß § 37 SächsDSG bzw. bei Beamten gemäß den personalaktenrechtlichen Bestimmungen des Sächsischen Beamtengesetzes zulässig sei. Daneben enthält das Beamtengesetz Festlegungen zu Fragen der Eignung und Befähigung, die durch einschlägige Verordnungen ergänzt werden. Ich betonte dem Ministerium gegenüber, dass eine Verarbeitung der Daten der Bediensteten in geregelten Verfahren zu erfolgen habe.

Bedenken erhob ich zum einen, da mir unklar erschien, wie die Risikoanalyse und Prüfung der Eignung von Bediensteten anhand einer von der obersten Dienstbehörde vorgegebenen Checkliste vonstattengehen sollte, wie die erhobenen Daten verwendet und ob und wie die erhobenen Daten in der Personalakte verarbeitet werden können sollten. Ebenso hatte ich Zweifel an einer Verarbeitung außerhalb der Personalakte. Ein Problem schienen mir auch die relativ ungeregelten und - aus datenschutzrechtlicher Sicht - problematischen kaum zu umreißenden gefühlsbezogenen Einschätzungen im Beziehungsbereich zu sein, die nach den ministeriellen Ausführungen ausdrücklich im Hinblick auf die Analyse der sozialen Beziehungen im Stationsbereich eine Rolle spielen sollten. Auch sollten Informationen der Gefangenen zu Bediensteten genutzt werden, wogegen ich wegen der planmäßigen und verdeckten Datenerhebung über Bedienstete bei Dritten Bedenken geltend machte.

In einem Gespräch und in einer ersten Stellungnahme teilte mir das Ministerium mit, dass die besagte Checkliste zur „Risikoanalyse und Prüfung der Eignung von Bediensteten" ausschließlich als Gedankenstütze für den verantwortlichen Vorgesetzten anzusehen und von diesem zu verwenden sei. Zur Wahrung der datenschutzrechtlichen Bestimmungen sollten die in der Checkliste aufgeführten Fragen grundsätzlich ohne Aufzeichnung von personenbezogenen Daten ausgewertet werden.

Auch wurde mir zugesichert, dass die vorgesehene Analyse der sozialen Beziehungen von Bediensteten und Gefangenen- stationsbereich ausschließlich dem fachlichen Austausch im „Team" dienen solle, keinesfalls aber einer Bewertung oder gar dienstrechtlichen Beurteilung einzelner Bediensteter. Auch dabei sollte - so stellt es das Ministerium gegenüber der Anstalt klar - auf die Erhebung personenbezogener Daten verzichtet werden. Soweit personenbezogene Daten in der Besprechung anfallen sollten, sollten diese nach deren jeweiligem Ende unverzüglich auf datenschutzkonforme Weise gelöscht werden.

Die oberste Dienstbehörde verhielt sich bedacht. Aufgrund eines weiteren klarstellenden Schreibens des Ministeriums an die Anstalt mit den Stellungnahmen und Versicherungen mir gegenüber entsprechenden Inhalts konnte ich den Vorgang abschließen.

Landesbeauftragter für den Datenschutz Sachsen-Anhalt

12. Tätigkeitsbericht (2013/2015)

12.4 Personaldatenverarbeitung mittels WhatsApp

Im Berichtszeitraum hat der Landesbeauftragte erfahren, dass Polizisten mit privaten Handys Fotos von Dienstplänen per WhatsApp an Gruppenmitglieder versenden. Eine dienstliche Weisung oder einen Zwang zur Anmeldung bei WhatsApp habe es nach Mitteilung der Dienststellenleitung nicht gegeben. Der Landesbeauftragte erläuterte, dass derzeit eine datenschutzkonforme Nutzung von WhatsApp nicht möglich sei (siehe oben, Nr. 5.10). Die grundsätzlichen Bedenken zum Einsatz von WhatsApp bestehen seitens des Landesbeauftragten aber auch und gerade bei einer Nutzung zur Übermittlung dienstlicher Informationen der Polizei des Landes Sachsen-Anhalt. Aufgrund der datenschutzrechtlichen Probleme, die sich mit der Nutzung von WhatsApp ergeben, insbesondere auch der fehlenden Einflussmöglichkeit des Dienstherrn, wurden das Personal und insbesondere die Führungskräfte durch das Ministerium belehrt, die Übermittlung von Personaldaten und Dienstplänen mittels WhatsApp zu unterlassen.

15.2.10 Videoüberwachung der Beschäftigten

Bereits im XI. Tätigkeitsbericht (Nr. 4.17.3) ist ausgeführt, unter welch engen Voraussetzungen eine Videoüberwachung im Unternehmen zulässig ist, wenn von ihr auch Beschäftigte betroffen sind. Auch im hiesigen Berichtszeitraum war wieder eine erhebliche Zahl an Eingaben von (ehemaligen) Beschäftigten zu bearbeiten, die an ihrem Arbeitsplatz einer Videoüberwachung ausgesetzt sind oder waren.

Dabei ist auffällig, dass der klassische Anwendungsfall nicht der des § 32 BDSG ist, denn eine Videoüberwachung wird nur in den seltensten Fällen zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sein, und auch der konkrete Verdacht einer Straftat, wegen derer eine Videoüberwachung zur Aufklärung unvermeidbar war, lag in der Regel nicht vor. Vielmehr sind es häufig Gründe, die nicht in den Beschäftigten selbst liegen, die die Arbeitgeber zu einer Videoüberwachung veranlassen. So geht

es z. B. häufig um die Überwachung oder Verbesserung von Betriebsabläufen, um die Abwehr von Gefahren, die von außen befürchtet werden, etwa durch Einbruch oder Diebstahl durch Firmenexterne, oder auch um Beweissicherung, um damit eigene Schadensersatzansprüche zu unterlegen oder unberechtigte Haftungsansprüche Dritter abzuwehren.

In diesen Fällen werden die Beschäftigten, auch wenn dies vordergründig nicht bezweckt ist, gleichwohl zu Betroffenen. Befindet sich dann auch noch ein Dauerarbeitsplatz von Beschäftigten im Erfassungsbereich einer Videokamera, ist eine besonders intensive Prüfung erforderlich, ob hier nicht schutzwürdige Interessen der Betroffenen gegenüber den berechtigten Interessen der Arbeitgeber überwiegen (vgl. §§ 6b Abs. 1, 28 Abs. 1 BDSG). Denn an ihren Arbeitsplätzen können Beschäftigte einer Videoüberwachung häufig nicht ausweichen. Und auch an der Wirksamkeit einer Einwilligung der Beschäftigten in die Datenverarbeitung sind häufig Zweifel angebracht, da es angesichts des Abhängigkeitsverhältnisses gegenüber dem Arbeitgeber an der Freiwilligkeit mangeln dürfte (§ 4a Abs. 1 Satz 1 BDSG).

Nach der ständigen Rechtsprechung des Bundesarbeitsgerichtes ist bei der Überwachung von Beschäftigten ein besonders strenger Maßstab anzuwenden (vgl. bereits Urteil vom 7. Oktober 1987, Az. 5 AZR 116/86, NZA 1988, 92; zuletzt auch Urteil vom 21. November 2013, Az. 2 AZR 797/11, BAGE 146, 303). Eine dauerhafte Mitarbeiterüberwachung darf wegen des ständigen Überwachungsdrucks wenn überhaupt dann nur äußerst restriktiv eingesetzt werden. Denkbar ist dies etwa im Einzelhandel, in dem eine Videoüberwachung zur Senkung einer signifikanten Diebstahlsquote in den Verkaufsräumen im Einzelfall als arbeitsplatzimmanent einzustufen sein kann. Generell unzulässig ist es, die Bereiche zu überwachen, die Beschäftigte in ihren Pausen zur Entspannung und Kommunikation nutzen oder die der persönlichen Intimsphäre zuzurechnen sind; das sind insbesondere Aufenthalts-, Umkleide- und Sanitärräume. Eine Verhaltens- und Leistungskontrolle durch Videoüberwachung ist ebenso, auch in Verkaufsräumen, unzulässig.

Der Landesbeauftragte hat in den im Berichtszeitraum bearbeiteten Einzelfällen zunächst erörtert, ob es mildere Mittel gibt, mit denen die Arbeitgeber ihre Ziele erreichen können. Eine Überprüfung von Betriebsabläufen sollte in erster Linie durch eine reine Sichtkontrolle des Ablaufes oder des Endproduktes ohne technische Hilfsmittel oder durch die Analyse von Unternehmenskennzahlen möglich sein. Der Einbruchs- oder Diebstahlsgefahr kann ggf. bereits durch andere Sicherungsmaßnahmen begegnet werden, wie Umzäunungen, Sicherheitspersonal, einbruchhemmende Fenster und Türen, Sicherheitsschlösser, Zugangssicherungen.

Ferner hat der Landesbeauftragte untersucht, ob im Sinne der Datensparsamkeit zunächst eine Einschränkung der Überwachungsmaßnahme möglich ist, ohne die berechtigten Interessen der Arbeitgeber zu gefährden. In dem Fall eines Autohauses etwa fand u. a. eine Live-Beobachtung der gesamten Werkstatt mit den Hebebühnen durch den Geschäftsführer statt. Hier konnte der Landesbeauftragte erreichen, dass die Bildbereiche von Dauerarbeitsplätzen oder üblichen Arbeitsbereichen unkenntlich gemacht wurden.

Des Weiteren war an eine Neuausrichtung der Kameraeinstellung zu denken, z. B. in einem vom Landesbeauftragten behandelten Fall eines Produktionsbetriebes. In diesem sollten mit der Videoüberwachung u. a. mögliche Störungen auf einem Transportband frühzeitig erkannt werden. Das Unternehmen arbeitet derzeit daran, die Kamera sehr eingeschränkt nur auf dieses Transportband auszurichten, sodass von den dort Beschäftigten allenfalls die (behandschuhten) Hände erfasst werden.

Sofern sich die Einbruchs- und Diebstahlsgefahr etwa besonders auf die Zeitfenster außerhalb der üblichen Geschäftszeiten beschränkte, wirkte der Landesbeauftragte stets darauf hin, die Videokameras während des Geschäftsbetriebes zu deaktivieren.

Nicht zuletzt sollte auch bedacht werden, dass sich aus der Verletzung von Persönlichkeitsrechten auch zivil- und arbeitsrechtliche Abwehr- und Entschädigungsansprüche ergeben können. Für den Fall der nahezu stets unzulässigen heimlichen Videoüberwachung von Beschäftigten etwa hat das Bundesarbeitsgericht jüngst seine entsprechende Rechtsprechung fortgesetzt. Es bestätigte einen Geldentschädigungsanspruch (hier: Schmerzensgeld) einer Beschäftigten, die im Krankheitsfall durch Detektive im Auftrag ihres Arbeitgebers videoüberwacht worden war, um die Umstände der Krankheit zu überprüfen (Urteil vom 19. Februar 2015, Az. 8 AZR 1007/13, juris).

Neben den materiellen Fragen durfte die Prüfung des Landesbeauftragten auch Fragen der Organisation und des Verfahrens nicht außer Acht lassen. Längst nicht jedes Unternehmen führte das gesetzlich vorgeschriebene Verfahrensverzeichnis (vgl. § 4g Abs. 2 und 2a BDSG), in dem die verantwortliche Stelle die Zwecke und Ausgestaltung der Videoüberwachung konkret festzulegen hat und das auf Antrag jedermann zur Verfügung zu stellen ist.

Besonders bei umfangreichen Videoüberwachungsmaßnahmen ist zu prüfen, ob sie besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Dann nämlich ist eine besondere Prüfung vor Beginn der Videoüberwachung durchzuführen und zu dokumentieren, die sog. Vorabkontrolle (§ 4d Abs. 5 BDSG). Auf diese wirkte der Landesbeauftragte insbesondere bei umfassenden Videoüberwachungsanlagen hin, etwa in einer Spielbank (vgl. Nr. 15.2.5) oder im Einzelhandel (vgl. Nr. 15.2.3). Die Vorabkontrolle führt der betriebliche Beauftragte für den Datenschutz durch, der in diesen Fällen zwingend zu bestellen ist (§§ 4d Abs. 6, 4f Abs. 1 Satz 6 BDSG).

Letztlich hat – sofern vorhanden – die Arbeitnehmervertretung mitzubestimmen, wenn es um Einführung und Anwendung von technischen Einrichtungen geht, die es ermöglichen, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG in der Auslegung des Bundesarbeitsgerichtes, vgl. bereits Beschluss vom 6. Dezember 1983, Az. 1 ABR 43/81, BAGE 44, 285 und daran anschließende Entscheidungen; vgl. auch §§ 32 Abs. 3 BDSG, 75 Abs. 2 BetrVG).

Der Thüringer Landesbeauftragte für den Datenschutz und Informationsfreiheit

11.Tätigkeitsbericht öffentlicher Bereich (2014/2015)

6.1 Datenleck bei Betriebsratswahl

In einem Eigenbetrieb eines Landkreises hatten Betriebsratswahlen stattgefunden. Die Unterlagen hierzu wurden im Auftrag des Wahlvorstands unter Verschluss genommen und versiegelt und unter Versicherung, dass keine Kopien hiervon existierten, dem neuen Betriebsrat entsprechend der Vorschriften des Betriebsverfassungsgesetzes übergeben. Zum öffentlichen Kammertermin zur Wahlanfechtung vor dem Arbeitsgericht staunte der neue Betriebsrat, der den versiegelten Packen Unterlagen dabei hatte, allerdings darüber, dass das Gericht und alle Arbeitgebervertreter mit Kopien eben dieser Wahlunterlagen ausgestattet waren. Da diese Unterlagen personenbezogene Daten enthielten, wandte sich der Betriebsrat und Wahlvorstand an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem er bereits Strafantrag wegen der Veröffentlichung vertraulicher Unterlagen gestellt hatte.

Die Wahl war letztendlich vom Gericht als nichtig erklärt worden, wobei man festgestellt hatte, dass ein Mitglied des Wahlvorstands regelwidrig Wahlvorschläge entgegengenommen und kurzerhand für unzulässig erklärt hatte.

Der TLfDI konnte wegen der Dringlichkeit der Angelegenheit zunächst nur eine vorläufige Einschätzung vornehmen. Wahlunterlagen enthalten personenbezogen Daten und dienen dazu, den Nachweis der ordnungsgemäßen Durchführung zu erbringen. Zum Zweck der Wahlanfechtung kann Einblick genommen werden. Auch Unterstützungsunterschriften können zum Zweck der Einschätzung der Wirksamkeit überprüft werden, selbst wenn der Wahlvorstand ursprünglich irrtümlich gegenüber den unterzeichneten Unterstützern die Versicherung abgegeben hatte, dass die Unternehmensleitung davon nichts erfahre.

Der Betriebsrat bat den TLfDI, datenschutzrechtliche Maßnahmen einzuleiten. Der Eigenbetrieb war privatrechtlich organisiert, unterlag jedoch aufgrund der Beteiligung des Landkreises dem Thüringer Datenschutzgesetz (ThürDSG), § 1 Abs. 2 Satz 1 ThürDSG. Ein Betriebsrat ist der Stelle zuzuordnen, auch wenn er die gesonderte Aufgabe hat, die Beschäftigteninteressen gegenüber der Unternehmensleitung zu vertreten. Nach der Aufgabenwahrnehmung des Eigenbetriebs war er als Wettbewerbsunternehmen einzuordnen, sodass nach § 26 ThürDSG nur der Fünfte Abschnitt des ThürDSG anzuwenden war, im Übrigen die Bestimmungen des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts und des § 38.

Daher war zu prüfen, ob ein Ordnungswidrigkeitenverfahren gegen ein Mitglied des Wahlvorstands eingeleitet werden konnte, das nach Auffassung der Beschwerdeführer der Unternehmensleitung bewusst die Unterlagen unzulässigerweise zugespielt hatte. Da aber bereits ein entsprechender Strafantrag bei der zuständigen Staatsanwaltschaft gestellt war, ist zunächst der Ausgang des Strafverfahrens abzuwarten. Unter Umständen kann danach ein Ordnungswidrigkeitsverfahren eingeleitet werden, wenn ersteres Verfahren eingestellt werden sollte.

> Unterlagen mit personenbezogenen Daten sind gegen unbefugte Kenntnis zu schützen. Die besten technischen und organisatorischen Maßnahmen gehen ins Leere, wenn eine befugte Person die Unterlagen bewusst pflichtwidrig anderen Personen zugänglich macht. Das unbefugte Zugänglichmachen kann als Straftat oder Ordnungswidrigkeit geahndet werden. Die Einleitung eines Ordnungswidrigkeitenverfahrens durch den TLfDI entfällt, wenn bereits ein Strafverfahren eingeleitet wurde.

6.2 Darf der behördeninterne Datenschutzbeauftragte den Personalrat kontrollieren?

Ein Mitglied eines Personalrats bei einer Thüringer Behörde wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob der behördliche Datenschutzbeauftragte der Dienststelle denn befugt sei, den Personalrat zu überprüfen. Die geschilderte Situation gestaltete sich so, dass der Personalrat keinen eigenen Raum für die Personalratsarbeit zur Verfügung hatte. Den Vorsitzenden und den Stellvertreter hatte man einfach in einem Büroraum untergebracht, wo jeder zur Hälfte seiner jeweiligen Arbeitszeit sowohl Personalratsarbeit als auch behördliche Verwaltungstätigkeit verrichten sollte. Ein verschließbarer Schrank stand zur Verfügung, in dem die Unterlagen, die zur Personalratsarbeit benötigt werden, eingeschlossen werden konnten, um unbefugte Kenntnis während der „normalen Dienstzeiten" mit Publikumsverkehr zu verhindern. Auch erhielt der Personalrat eine Sekretärin, die mit einem nicht unwesentlichen Teil ihrer Arbeitszeit, aber auch einem Fachdienst- und Amtsleiter zur Verfügung zu stehen hatte. Die Arbeit für den Personalrat erledigte sie auf einem Notebook, das sie zum Schutz vor unbefugter Einsicht jeweils zuklappen konnte, wenn ihr jemand über die Schulter schauen konnte oder wollte.

Datenschutzrechtlich ist der Personalrat einer Dienststelle als Teil dieser Dienststelle zu bewerten. Die Pflicht zur Sicherstellung der Einhaltung der datenschutzrechtlichen Vorschriften trifft jedoch die verantwortliche Stelle nach § 34 Thüringer Datenschutzgesetz (ThürDSG), also die Dienststelle. Auch beim Personalrat müssen die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten, die im Rahmen seiner Aufga-

benerfüllung verarbeitet werden, getroffen sein. Werden Mängel festgestellt, ist die Dienststelle aufgerufen, geeignete Maßnahmen zu treffen, damit die Mängel behoben werden. Hierfür sind dem Personalrat von der Dienststelle auch die Mittel zur Verfügung zu stellen, damit die datenschutzrechtlichen Vorschriften eingehalten werden können.

Unter den in der betroffenen Dienststelle herrschenden Umständen fällt es nicht leicht, die an den Personalrat von den Beschäftigten herangetragenen Anliegen vertraulich zu behandeln und die erforderlichen Maßnahmen zum Schutz personenbezogener Daten der Beschäftigten (oftmals Personalaktendaten), die im Rahmen der Mitbestimmung dem Personalrat von der Dienststelle übermittelt werden müssen, einzuhalten.

Nun hatte der Dienststellenleiter den behördlichen Datenschutzbeauftragten (bDSB) mit einer datenschutzrechtlichen Überprüfung des Personalrats beauftragt und der Personalrat vermutete dahinter keine guten Absichten. Etwas Würze bekam die Sache dadurch, weil es sich beim behördlichen Datenschutzbeauftragten um den ehemaligen Personalratsvorsitzenden handelte, der möglicherweise Freude oder Genugtuung über aufgespürte Fehler seiner Nachfolger haben könnte.

Hierzu hat der TLfDI Folgendes ausgeführt: Die Zuständigkeit und die Befugnisse des Beauftragten für den Datenschutz sind in § 10a ThürDSG festgelegt. Zwar hat das Bundesarbeitsgericht (BAG) in seinem Beschluss vom 11. November 1997 entschieden, dass eine Kontrollbefugnis des betrieblichen Datenschutzbeauftragten für Betriebsräte nicht besteht. Gleichzeitig hat es allerdings dargelegt, dass das Bundesverwaltungsgericht die Frage der Kontrollbefugnis des betrieblichen Datenschutzbeauftragten in Bezug auf die Personalverwaltung im öffentlichen Dienst ausdrücklich offen gelassen hat (BAG, Beschluss vom 11. November 1997, Az.: 1 ABR 21/97, Rn. 31).

Nach § 10a Abs. 2 ThürDSG hat der Beauftragte für den Datenschutz die Aufgabe, die Daten verarbeitende Stelle bei den Ausführungen der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken. Dies gilt grundsätzlich auch für den Personalrat, der als Teil der Dienststelle, die für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist, hiervon nicht grundsätzlich ausgenommen ist. Auch das Thüringer Personalvertretungsgesetz enthält keine Ausnahmeregelung. Eine Ausnahme besteht aber im Hinblick auf personenbezogene Daten in oder aus Personalakten, die nur mit Einwilligung der Betroffenen durch den Beauftragten für den Datenschutz einsehbar sind (§ 10a Abs. 4 Satz 1 ThürDSG). Zudem besteht ein besonderes Amtsgeheimnis der Personalratsmitglieder hinsichtlich der personenbezogenen Daten, die ihnen in ihrer Aufgabenwahrnehmung bekannt geworden sind. Soweit also Personalaktendaten und einem besonderen Amtsgeheimnis unterliegende personenbezogene Daten beim Personalrat vorhanden sind, dürfen diese vom Beauftragten für den Datenschutz in seiner Aufgabenwahrnehmung nicht ohne Einwilligung des einzelnen Betroffenen eingesehen werden.

Im Falle einer Prüfung durch den behördlichen Datenschutzbeauftragten ist darüber hinaus auch die Sensibilität der Personalratstätigkeit zu beachten. Mitarbeiter dürfen sich vertrauensvoll an den Personalrat wenden, ohne dass die Dienststellenleitung davon über eine Kontrolle des Datenschutzbeauftragten Kenntnis erhalten könnte. Andererseits kann eine Prüfung durch den behördlichen Datenschutzbeauftragten in partnerschaftlicher Zusammenarbeit mit dem Personalrat auch Missstände, wie sie im vorliegenden Fall vorlagen, z. B. die ungeeigneten Räumlichkeiten, Mängel bei der Möglichkeit für Mitarbeiter, sich ungehindert an den Personalrat wenden zu können, ohne dass dies anderen Personen als den berechtigten Personalratsmitgliedern zur Kenntnis gelangt, aufzeigen und dazu beitragen, datenschutzgerechte Lösungen zu finden.

Der TLfDI beschränkte sich bis jetzt auf beratende Unterstützung, behält sich aber eine Kontrolle vor Ort vor.

> Eine Prüfung der Einhaltung der datenschutzrechtlichen Vorgaben beim Personalrat durch den behördlichen Datenschutzbeauftragten ist nicht vollständig ausgeschlossen. Im Falle einer Prüfung dürfen jedoch vom behördlichen Datenschutzbeauftragten grundsätzlich keine personenbezogenen Daten der Beschäftigten zur Kenntnis genommen werden, die dem Personalrat zur Aufgabenerfüllung vorliegen. Die datenschutzrechtliche Prüfung hat sich daher auf das Vorliegen geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten zu beschränken. Die Dienststelle hat dem Personalrat die erforderlichen Mittel zur Verfügung zu stellen, damit durch den Personalrat selbst geeignete Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften getroffen werden können.

6.4 Mitarbeiter: Bitte lächeln!

Der Beauftragte für den Datenschutz einer Thüringer Kommune bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung zu dem Vorhaben, Bilder von Beschäftigten in eigenen Prospekten, Flyern oder der Tageszeitung zu veröffentlichen. Ohne weitere Hintergrundinformationen, beispielsweise zu welchem Zweck welche konkreten Bilder von Beschäftigten veröffentlicht werden sollen, hat der TLfDI im Rahmen seiner Beratungsaufgabe nach § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hierzu allgemein ausgeführt:

Fotografien von Mitarbeitern der Stadtverwaltung sind personenbezogene Daten von Beschäftigten, die gemäß § 33 Abs. 1 ThürDSG nach den dienstrechtlichen Vorschriften der §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) verarbeitet werden dürfen. Bei der Verwendung von Fotografien von Mitarbeitern handelt es sich regelmäßig nicht um eine Aufgabe der Personalverwaltung und - bewirtschaftung, sodass dies nur mit Einwilligung der Betroffenen geschehen kann. Es muss jedoch zur Einholung einer Einwilligung vorab geprüft werden, dass eine Erforderlichkeit zur Aufgabenerfüllung vorliegt. Eine öffentliche Stelle wie die Stadtverwaltung muss daher auch bei der Veröffentlichung von Mitarbeiterbildern an die Erforderlichkeit zur Aufgabenerfüllung anknüpfen.

Handelt es sich um Bilder des Bürgermeisters oder der

Beigeordneten, die in Wahrnehmung von öffentlichen Veranstaltungen und Terminen entstanden sind, bedarf es aufgrund deren Stellung sozusagen als Personen der Zeitgeschichte keiner Einwilligung zur Veröffentlichung von Bildern.

Die Einwilligungserklärung zum Abdruck in Druckerzeugnissen (stadteigenen Prospekten und Flyern) ist an die formellen Voraussetzungen des § 4 Abs. 3 ThürDSG gebunden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Die Beschäftigten müssen auf den Zweck und den Umfang der beabsichtigten Veröffentlichung hingewiesen werden. Weiterhin muss die Einwilligung auf Freiwilligkeit beruhen. Sollte die Stadtverwaltung Aufnahmen von Mitarbeitern an die Tageszeitung zur Veröffentlichung geben, gilt dies ebenso. Sofern daran gedacht wird, dass die Prospekte und Flyer auch im Internet Veröffentlichung finden, ist § 23 ThürDSG zu beachten. Bei der Veröffentlichung von Daten im Internet handelt es sich um eine Übermittlung personenbezogener Daten an öffentliche und nichtöffentliche Stellen außerhalb des Geltungsbereiches des Grundgesetzes. Eine solche Übermittlung ist nur unter den Voraussetzungen des §°23 ThürDSG zulässig. Da nicht ausgeschlossen werden kann, dass bei einer weltweiten Veröffentlichung die Daten auch in Staaten übermittelt werden, in denen kein angemessenes Datenschutzniveau gewährleistet ist, müssen die Voraussetzungen des § 23 Abs. 2 ThürDSG gegeben sein. Von diesen Voraussetzungen kommt allenfalls die Nr. 1 in Betracht, nach der eine zweifelsfreie Einwilligung des Betroffenen vorliegen muss.

Die Einwilligung ist nach § 4 Abs. 2 ThürDSG die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seinen personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen. Sofern der Betroffene, dessen Daten veröffentlicht werden, in einem Arbeitsverhältnis mit der Daten übermittelnden Stelle steht, bestehen bereits große Zweifel an der Freiwilligkeit der Einwilligung. Freiwilligkeit ist nur dann gegeben, wenn für die Mitarbeiter keinerlei Druck besteht und im Falle einer Ablehnung auch keine Nachteile entstehen. Diesen Grundsatz hat auch das Bundesarbeitsgericht insbesondere zur Einwilligung im Sinne des § 22 Kunsturhebergesetz in jüngster Zeit ausgeführt (Vgl. BAG Urteil vom 19. Februar 2015 – 8 AZR 1011/13). Die Einwilligung kann jederzeit zurückgenommen werden. Wird die Einwilligung zurückgenommen, muss die Datenübermittlung für die Zukunft unterbleiben. In diesem Fall ist auch die Speicherung des Fotos auf dem Server unzulässig und der Betroffene hat einen Anspruch auf Löschung nach § 16 Abs. 1 Nr. 1 ThürDSG.

> Grundsätzlich ist es nicht Aufgabe einer öffentlichen Stelle, Mitarbeiterfotos zu veröffentlichen. Eine Veröffentlichung ohne besonderen Darstellungsgrund ist daher unzulässig. Sollen Beschäftigtenfotos durch öffentliche Stellen auf der Grundlage des Kunsturhebergesetzes veröffentlicht werden, sind hierzu zweifelsfrei freiwilllige Einwilligungen der Betroffenen erforderlich. Den Beschäftigten darf insbesondere bei Verweigerung der Einwilligung keinerlei Nachteil entstehen.

6.5 Bewerberunterlagen: Einsicht für alle Personalratsmitglieder?

Der Personalratsvorsitzende in einem Landratsamt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob denn nur der Personalratsvorsitzende oder auch andere Personalratsmitglieder Einsicht in Bewerberunterlagen nehmen dürften. Hintergrund war folgender: Dem Personalrat steht bei Einstellungen gemäß § 68 Abs. 2 Satz 4 Thüringer Personalvertretungsgesetz (ThürPersVG) das Recht zur Einsichtnahme in die Bewerbungsunterlagen aller Mitbewerber zu, um Benachteiligungen jeglicher Art auszuschließen. Dementsprechend ist die Dienststelle zur Vorlage der Bewerbungsunterlagen an den Personalrat verpflichtet. Die Dienststelle wollte das Einsichtsrecht mit Hinweis auf den besonderen Schutz von Bewerberdaten auf den Personalratsvorsitzenden beschränken.

Im Rahmen der Aufgabenverteilung unter den Personalratsmitgliedern wurde aber die Zuständigkeit der einzelnen Mitglieder auf verschiedene Ämter aufgegliedert. Das jeweils zuständige Mitglied nimmt folglich auch an den Bewerbergesprächen teil. Wenn die Einsicht in die entsprechenden Bewerberunterlagen auf den Personalratsvorsitzenden beschränkt bliebe, wäre das für das entsprechende Bewerbungsverfahren zuständige Personalratsmitglied auf die Weitergabe der entsprechenden Informationen vom Vorsitzenden angewiesen.

Zur Beantwortung der Frage führte der TLfDI aus, dass aus den datenschutzrechtlichen Grundsätzen die Dienststellenleitung verpflichtet ist, nur die für eine Personalmaßnahme erforderlichen personenbezogenen Daten dem Personalrat zugänglich zu machen. Bei der Einstellung eines Bewerbers sind die Unterlagen des Bewerbers sowie seiner Mitbewerber für die Entscheidung des Personalrats erforderlich. Auch wenn Bewerberdaten eine besondere Sensibilität zukommt, muss dem Personalrat zur Gewährleistung seiner Handlungsfähigkeit Kenntnis der erforderlichen Daten gewährt werden. Aufgrund der Sensibilität der personenbezogenen Daten der Bewerber ist es hingegen nicht erforderlich, dem gesamten Personalrat, also allen seinen Mitgliedern, den Zugang zu den personenbezogenen Daten zu gewähren. Wird jedoch, wie vorliegend geschildert, im Rahmen der Aufgabenverteilung unter den Personalratsmitgliedern die Zuständigkeit der einzelnen Personalratsmitglieder auf verschiedene Ämter aufgegliedert, müssen für das jeweils zuständige Personalratsmitglied, das an den Bewerbungsgesprächen teilnimmt, auch die für die Aufgabenwahrnehmung erforderlichen personenbezogenen Daten der Bewerber zugänglich sein.

Aus datenschutzrechtlicher Sicht sah der TLfDI daher keine Gründe, diesem zuständigen Personalratsmitglied die Einsicht in die zu seiner Aufgabe erforderlichen entsprechenden Bewerbungsunterlagen zu verweigern und diese nur dem Personalratsvorsitzenden zu gewähren, der das Mitglied entsprechend informieren müsste. Soweit aber dem zuständigen Personalratsmitglied die Daten zugänglich gemacht werden, ist darüber hinaus eine Vorlage an den Personalratsvorsitzenden oder andere Mitglieder des Personalrats grundsätzlich nicht mehr erforderlich.

Dem Personalrat müssen die zu seiner Aufgabenerfüllung erforderlichen Bewerberdaten von der Dienststelle zugänglich gemacht werden. Die Einsicht ist in die Unterlagen zu gewähren, soweit sie für die Aufgabenerfüllung des Personalrats erforderlich ist. Hat der Personalrat einzelne Aufgaben auf einzelne Personalratsmitglieder delegiert, reicht es aus, nur diesen Zugang zu den zur Aufgabenerfüllung erforderlichen personenbezogenen Daten von Bewerbern zu gewähren.

6.6 „Pranger 2.0" – Amtsleiter stellt sensible Daten von Mitarbeiterin ins Intranet

Eine Mitarbeiterin einer Stadtverwaltung teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Folgendes mit: Der Leiter eines städtischen Amtes habe ein Schreiben des Haupt- und Personalamtes mit sensiblen Daten zu ihrer Person aus einem Verfahren zur Vermeidung und Bekämpfung von Mobbing anderen Mitarbeitern der Stadtverwaltung über das Intranet zur Kenntnis gegeben. Eine Einwilligung der Mitarbeiterin der Stadtverwaltung zu dieser Datenübermittlung lag natürlich nicht vor.

Der TLfDI stellte schnell fest, dass die interne Veröffentlichung sensibler personenbezogener Daten aus einem Verfahren zur Dienstvereinbarung Mobbing an nicht am Verfahren beteiligte Personen im konkreten Fall unzulässig erfolgte und dies einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften darstellte. Daher hat der TLfDI die datenschutzrechtlichen Mängel in Form einer nach § 21 Thüringer Datenschutzgesetz (ThürDSG) unzulässigen Übermittlung personenbezogener Daten gemäß § 39 Abs. 1 Satz 1 ThürDSG beanstandet. Der TLfDI forderte die Stadtverwaltung auf, dafür Sorge zu tragen, dass künftig in ähnlichen Fällen die Datenübermittlung auf den Kreis der Berechtigten beschränkt wird. Die betroffene Stadtverwaltung hat zu der Angelegenheit ein Ordnungswidrigkeitenverfahren eingeleitet.

Dem Personalrat müssen die zu seiner Aufgabenerfüllung erforderlichen Bewerberdaten von der Dienststelle zugänglich gemacht werden. Die Einsicht ist in die Unterlagen zu gewähren, soweit sie für die Aufgabenerfüllung des Personalrats erforderlich ist. Hat der Personalrat einzelne Aufgaben auf einzelne Personalratsmitglieder delegiert, reicht es aus, nur diesen Zugang zu den zur Aufgabenerfüllung erforderlichen personenbezogenen Daten von Bewerbern zu gewähren.

6.7 Mitarbeiter im GPS-Dauer-Fokus

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass in Fahrzeugen eines Zweckverbands zur Wasser- und Abwasserversorgung GPS Technik eingesetzt werde. Diese Technik ist dazu geeignet, jederzeit den Standort eines Fahrzeugs festzustellen und eine Leistungs und Verhaltenskontrolle der Mitarbeiter durchzuführen. Der Zweck des GPS-Einsatzes in den Fahrzeugen war nicht bekannt, da sich die Mitarbeiter nicht ausreichend informiert sahen. Festlegungen zum Umgang mit mittels GPS erhobenen personenbezogenen Daten der Kraftfahrzeugnutzer sowie Regelungen zum Zugriff und zur Nutzung der Fahrzeuge gab es nicht.

Auf Anfrage des TLfDI gab der Zweckverband an, dass die Fahrzeuge tatsächlich mit GPS Geräten ausgestattet seien, um den Standort dieser Fahrzeuge schnell lokalisieren zu können. Dies sei für die Koordinierung der täglichen Einsätze insbesondere im Havariefall vorteilhaft, um Ausfallzeiten in der Wasserversorgung zu minimieren. Einen positiven Nebeneffekt sah man darin, dass die Fahrzeuge im Falle des Diebstahls wieder aufgefunden werden könnten, zumal in den letzten Jahren bereits Fahrzeuge gestohlen worden waren.

Die durch GPS übermittelten Daten zu den Fahrzeugen wurden auf einem externen Server für 90 Tage vorgehalten. Dort ist eine Zusammenführung mit den Fahrerdaten nicht möglich. Die Mitarbeiter seien über die Gründe und den Einsatz der Geräte mündlich informiert worden. Schriftliche detaillierte Informationen sollten jedoch erst nach Abschluss einer Testphase erfolgen bzw. wurden zum damaligen Zeitpunkt erarbeitet. Zur eingehenden datenschutzrechtlichen Prüfung waren diese Angaben selbstverständlich nicht ausreichend.

Durch GPS erhobene Standortdaten oder Bewegungsprofile von Fahrzeugen sind personenbeziehbare und damit personenbezogene Daten, wenn sie einem konkreten Fahrer zugeordnet worden sind. Damit verbunden ist, dass der jeweilige Beschäftigte einer Leistungs- und Verhaltenskontrolle unterzogen werden kann, die nach § 33 Abs. 4 Thüringer Datenschutzgesetz (ThürDSG) unzulässig ist. Nach § 19 Abs. 2 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Zu dem angegebenen Zweck der Standortlokalisierung zur Koordinierung der täglichen Einsätze ist eine Erforderlichkeit zur Erfassung der Position während der Fahrt gegeben. Eine Erforderlichkeit zur Erfassung z. B. der gefahrenen Geschwindigkeit ist nicht ersichtlich und damit unzulässig.

Nach § 20 Abs. 1 ThürDSG ist die Speicherung der Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Zur Feststellung der Position für Einsatzzwecke ist eine aktuelle Positionsbestimmung ausreichend. Hierfür bedarf es keiner über das Tagesende hinaus andauernden Speicherung. Aus der Feststellung der Fahrzeugposition im Fall eines Diebstahls ist eine Echtzeitfeststellung ausreichend. Die Speicherung der Fahrzeugdaten für 90 Tage war daher nicht begründbar und mangels Erforderlichkeit unzulässig. Der TLfDI forderte daher, dass mangels Rechtsgrundlage die Geschwindigkeitserfassung zu deaktivieren ist und die gespeicherten Daten zu löschen sind.

Die im Nachgang erarbeitete Dienstanweisung enthält nunmehr eine Auflistung der erfassten Daten, konkrete Festlegungen zur Zweckbindung und der Zugriffs- und Nutzungsrechte. Die Nutzung der erfassten Fahrzeugdaten zur Verhaltens- und Leistungskontrolle der Fahrzeugführer ist ausgeschlossen. Die Dauer der Speicherung wurde auf 72 Stunden verkürzt. Diese Speicherungsdauer kann ausnahmsweise damit begründet werden, dass unter Umständen ein

zulässiger Zugriff am Montag auf den vorhergehenden Freitag erforderlich sein kann.

> Wird in Fahrzeugen GPS eingesetzt, bedarf es konkreter Festlegungen in einer Dienstvereinbarung beziehungsweise einer Dienstanweisung. In dieser sind der konkrete Zweck der Fahrzeugdatenerfassung, die zu erfassenden Daten sowie die Dauer der Speicherung festzulegen und es ist zu bestimmen, zu welchem Zweck die Daten ausgewertet werden dürfen. Eine Verhaltens- und Leistungskontrolle der Fahrzeugführer ist auszuschließen (§ 33 Abs. 4 ThürDSG).

6.8 Übermittlungsbefugnis des Amtsarztes – keine Generalvollmacht!

Auch in diesem Berichtszeitraum zeigte sich, dass der Umfang der Offenbarungsbefugnis des Amtsarztes gegenüber der anfordernden Behörde nicht immer eingehalten wird (vgl. zuletzt 9. TB Punkt 6.2). Der Umfang der Offenbarungsbefugnis des mit der Untersuchung beauftragten Amtsarztes gegenüber der anfordernden Behörde wurde neu geregelt. Sie richtet sich seit 1. Januar 2015 nach § 33 Abs. 3 und 4 Thüringer Beamtengesetz (ThürBG). Danach teilt der Arzt der zuständigen Behörde die tragenden Feststellungen und Gründe des Ergebnisses der ärztlichen Untersuchung mit, soweit deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist. Ferner berichtet er über die infrage kommenden Maßnahmen zur Wiederherstellung der Dienstfähigkeit und die Möglichkeit einer anderen Verwendung. Als technische und organisatorische Maßnahmen zum Schutz dieser sensiblen Angaben ist weiterhin gesetzlich bestimmt, dass die Mitteilung des Arztes über die Untersuchungsergebnisse in einem gesonderten, verschlossenen und versiegelten Umschlag zu übersenden ist. Sie ist verschlossen zur Personalakte des Beamten zu nehmen. Weiterhin dürfen die an die Behörde übermittelten Daten nur für die im Einzelfall konkret zu treffende Entscheidung verarbeitet oder genutzt werden. Somit ist auch eine besondere Zweckbindung festgeschrieben.

Die Transparenz für die Betroffenen wurde ebenfalls berücksichtigt. Nach § 33 Abs. 2 ThürBG ist der Beamte zu Beginn der Untersuchung oder der Beobachtung auf deren Zweck und die Übermittlungsbefugnis an die Behörde hinzuweisen. Der Arzt übermittelt dem Beamten oder, soweit dem ärztliche Gründe entgegenstehen, dessen Bevollmächtigten eine Kopie der an die Behörde erteilten Auskünfte.

Eine in diesem Sinne betroffene Person wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem sie vom Amtsarzt keine Auskunft dazu erhielt, was denn nun an die personalverwaltende Dienststelle als Ergebnis einer Untersuchung gesandt worden war. Nachdem sie sich an ihre Personalverwaltung gewandt und Einsicht in die Unterlagen genommen hatte, fiel sie aus allen Wolken. Es waren alle erdenklichen Diagnosen aufgeführt, ob sie nun mit der Dienstfähigkeit in Verbindung standen oder nicht. Weiterhin machte die betroffene Person geltend, sie habe eine Schweigepflichtentbindungserklärung in pauschaler Form vorgelegt erhalten, die sie bereits vor der Untersuchung unterschreiben sollte, obwohl weder die zu entbindenden Ärzte noch der konkrete Zweck darin erkennbar waren.

Nachdem der TLfDI gegenüber dem Amtsarzt die Rechtslage dargelegt hatte, sagte dieser unverzüglich zu, zukünftig nur noch die für die Kenntnis der Behörde für die von ihr zu treffende Entscheidung erforderlichen Angaben zu übermitteln. Weiterhin werde zukünftig beachtet, dass auch die begutachteten Beamten einen Anspruch auf eine Kopie der an die Behörde erteilten Auskünfte haben. Die formularmäßige Entbindung von der Schweigepflicht für behandelnde andere Ärzte wurde überarbeitet und konkretisiert, sodass zukünftig wirksame Schweigepflichtentbindungen erteilt werden können.

Aufgrund der prompten Zusage zur Behebung der erheblichen datenschutzrechtlichen Verstöße hat der TLfDI unter Anwendung des § 39 Abs. 3 ThürDSG zunächst von einer Beanstandung nach § 39 Abs. 1 ThürDSG abgesehen. Nachdem sich aber die Beschwerdeführerin nach Ablauf einer angemessenen Frist wieder meldete, weil sie auf ihre Anfragen und Bemühungen immer noch keine Kopie des „neuen", den gesetzlichen Anforderungen entsprechenden Gutachtens erhalten habe, musste der TLfDI davon ausgehen, dass die Zusagen (noch) nicht umgesetzt wurden. Daher sprach er eine Beanstandung nach § 39 Abs. ThürDSG in Verbindung mit § 33 Abs. 3 und 5 ThürBG mit Fristsetzung zur Behebung der datenschutzrechtlichen Mängel aus.

> Es ist zu erwarten, dass den Amtsärzten in Wahrnehmung ihrer Aufgabe die gesetzlichen Vorschriften geläufig sind und damit die Übermittlung von Angaben bzw. Diagnosen unterbleibt, die nicht für die Entscheidung der Auftrag gebenden Behörde erforderlich sind.

6.10 Bewerbungen per E-Mail

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) führte eine stichprobenmäßige Durchsicht von Stellenausschreibungen der Landesregierung durch. Dabei hat sich ein gemischtes Bild ergeben. Während in den meisten Geschäftsbereichen Bewerbungen per E-Mail (teilweise aus datenschutzrechtlichen Gründen) nicht erwünscht waren oder keine Berücksichtigung finden sollten, wurden in anderen Geschäftsbereichen Bewerbungen durch die Angabe von E-Mail-Adressen zugelassen. Die Angabe der E-Mail-Adressen konnte von potentiellen Interessenten als Aufforderung zur Bewerbung per E-Mail verstanden werden.

Der TLfDI nahm dies zum Anlass, die obersten Landesbehörden auf die nachfolgenden datenschutzrechtlichen Aspekte hinzuweisen und bat darum, auch die nachgeordneten Bereiche hierüber zu informieren und bei zukünftigen Ausschreibungen zu beachten:

Kommt es aufgrund einer Bewerbung zu einer Beschäftigung, werden die von Bewerbern mit der Bewerbung eingereichten personenbezogenen Daten Bestandteil der Personalakten, für die die dienstrechtlichen Vorschriften der §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) gelten, die besondere

Schutzvorschriften und Zugangsregelungen enthalten. Diese Bestimmungen finden gemäß § 33 Thüringer Datenschutzgesetz (ThürDSG) für Angestellte, Arbeiter und Auszubildende im öffentlichen Dienst entsprechend Anwendung. Den von den Bewerbern zum Zweck der Eingehung eines Dienstverhältnisses eingereichten personenbezogenen Daten kommt somit ein besonderer Schutzbedarf zu. Zugang zu diesen Daten dürfen nur damit betraute Personen haben (vgl. § 80 Abs. 1 ThürBG). Ein allgemeiner Zugang zu Bewerberdaten ist daher in den Behörden auszuschließen.

Sollen von öffentlichen Stellen Bewerbungen per E-Mail zugelassen werden, sind besondere technische und organisatorische Maßnahmen zu treffen, die unbefugte Kenntnis der Bewerbungsunterlagen ausschließen. Für den unversehrten Zugang der personenbezogenen Daten muss daher eine Verschlüsselung und Entschlüsselung möglich sein.

Weiterhin kann nicht das allgemeine Postfach eines Hauses genutzt werden, da die allgemeine Poststelle und Registratur mangels konkreter Aufgabenerfüllung zu diesen personenbezogenen Daten der Bewerber keinen Zugang/Zugriff haben darf.

Wie im Nachgang festzustellen war, wurden die Ausführungen bei daraufhin folgenden Stellenausschreibungen berücksichtigt. Die meisten Ressorts verfügen offenbar nicht über die erforderlichen Vorrichtungen zur Sicherstellung gegen unbefugte Kenntnisnahme, denn es findet sich nunmehr meistens der Zusatz, dass E-Mail-Bewerbungen aus datenschutzrechtlichen Gründen nicht erwünscht sind.

> Bewerbungsunterlagen für Stellen im öffentlichen Dienst kommt ein besonderer Schutzbedarf zu. Stellenbewerber dürfen nur dann zur Einreichung von Bewerbungsunterlagen per E-Mail aufgefordert werden, wenn die Vertraulichkeit durch die öffentliche Stelle durch entsprechende technische und organisatorische Maßnahmen gewährleistet werden kann.

6.12 Fingerabdruckscanner zur Arbeitszeiterfassung?

Vereinzelt wenden sich Beschäftigte und Betriebsräte Hilfe suchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil in ihrem Betrieb im Zuge der fortschreitenden Technisierung ein Fingerabdruckscanner zur Arbeitszeiterfassung eingeführt werden soll. Mit solchen Geräten zur Erfassung von Fingerabdrücken sind bisweilen ungute Vorstellungen und Befürchtungen verbunden, da man mit der Abgabe von Fingerabdrücken oftmals polizeiliche Maßnahmen vor Augen hat. Fingerabdrücke müssen doch meist nur Verbrecher abgeben ...

Zur datenschutzrechtlichen Problematik des Einsatzes eines Fingerabdruckscanners bei der Arbeitszeiterfassung verweist der TLfDI auf die „Hinweise zur biometrischen Datenerfassung am Arbeitsplatz", die auf seiner Homepage unter Themen – Beschäftigtendatenschutz verfügbar sind. Folgendes ist zu beachten:

1. Die Erhebung, Speicherung, Übermittlung und Nutzung biometrischer Daten stellt grundsätzlich einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Arbeitnehmer dar. Er ist gemäß § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Biometrische Daten gelten dabei als besonders sensible Daten, die einer besonderen Schutzbedürftigkeit unterliegen.

2. Es existieren für die Arbeitnehmer weit weniger in das Recht auf informationelle Selbstbestimmung eingreifende und dem Grundsatz der Datensparsamkeit nach § 3a BDSG gerecht werdende technische wie organisatorische Möglichkeiten, die geeignet sind, die Arbeitszeit zu erfassen und dabei ohne die Verwendung biometrischer Daten auszukommen. Das sind beispielsweise Arbeitszeiterfassungssysteme, die mit einer Chipkarte oder einem Transponder zu bedienen sind. In manchen Betrieben reicht auch die handschriftliche Aufzeichnung aus.

3. Allein die geringere, aber auch nicht auszuschließende Betrugsanfälligkeit, Arbeitszeiten zu manipulieren, führt im Rahmen einer Verhältnismäßigkeitsprüfung nicht zu einer anzunehmenden Erforderlichkeit der Verwendung biometrischer Daten zur Arbeitszeiterfassung. Es kann regelmäßig nicht davon ausgegangen werden, dass Arbeitnehmer sich rechtswidrig verhalten. Im Falle festgestellter Falschangaben von Arbeitszeiten stehen dem Arbeitgeber genügend Mittel zur Vertretung eigener Interessen (z. B. strafrechtliche Verfolgung wegen Betruges gemäß § 263 StGB und außerordentliche Kündigung) zur Verfügung.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, auch biometrischer Daten, ist gemäß § 4 Abs. 1 BDSG unter anderem dann zulässig, wenn der von der Datenverarbeitung Betroffene einwilligt. Die Einwilligung ist aber nur unter den Voraussetzungen des § 4a BDSG wirksam, d. h., wenn diese schriftlich und tatsächlich freiwillig abgegeben und der Betroffene auf die Folgen einer verweigerten Einwilligung hingewiesen wird. Insbesondere in bestehenden Abhängigkeitsverhältnissen, wie im Rahmen arbeitsvertraglicher Beziehungen, ist die Frage der Freiwilligkeit regelmäßig kritisch zu hinterfragen. Hier müssen die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten umfassend informiert werden. Außerdem muss es eine tatsächliche Alternative zu der biometrischen Zeiterfassung geben, sodass der betroffene Arbeitnehmer ein Wahlrecht hat. Diese kann beispielsweise darin bestehen, dass neben der Zeiterfassung mittels Fingerabdruck die Erfassung über Transponder angeboten wird.

> Die mit dem Einsatz eines biometrischen Systems zur Arbeitszeiterfassung verbundene Problematik ist in den „Hinweisen zur biometrischen Datenerfassung am Arbeitsplatz" dargelegt und auf der Homepage des TLfDI abrufbar.

6.13 Fragebögen zur Mitarbeiterbefragung

Wie steht es mit der Zufriedenheit der Beschäftigten? Gibt es Missstände? Besteht Verbesserungsbedarf oder ist alles in

Ordnung? Qualitätsmanagement nimmt in der heutigen Zeit einen hohen Stellenwert ein. Und am Anfang steht meistens eine Befragung der Betroffenen, die möglichst eine ehrliche Einschätzung abgeben sollen, damit alles (noch) besser werden kann.

Für die Aussagekraft einer Befragung ist es wichtig, dass die Betroffenen wegen ihrer Offenheit keine Nachteile befürchten müssen. Das beste Mittel dafür ist die anonyme Befragung. Dabei reicht es nicht aus, dass lediglich auf die Angabe des Namens verzichtet wird. Sollen Geschlecht, Alter, Dauer der Betriebszugehörigkeit und konkreter Tätigkeitsbereich (Abteilung, Sachgebiet etc.) angegeben werden, bedarf es unter Umständen nur noch weniger weiterer Angaben und der Auskunftserteilende wird als Person zumindest bei interner Auswertung mit etwas Zusatzwissen wieder erkennbar, insbesondere, wenn in seinem Tätigkeitsbereich nur wenige Personen beschäftigt sind. Anonymität für die Betroffenen bedeutet, 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 (vgl. § 3 Abs. 9 Thüringer Datenschutzgesetz – ThürDSG). Kann ein einzelner Fragebogen unter den geschilderten Umständen einer Person zugeordnet werden, sind Maßnahmen zu treffen, dass diese Erkenntnisse nicht der Beschäftigungsstelle zur Kenntnis gelangen. Besonderes Augenmerk ist dann auf die Auswertung zu legen. Aus dem Gesamtergebnis der Befragung darf kein Rückschluss auf die einzelne Person mehr möglich sein. Dies wird in der Regel den Teilnehmern in einer Information versichert. Ob die Anonymität allerdings vollständig gewährleistet ist, wird bisweilen von den Teilnehmern bezweifelt. In solchen Fällen kann man sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wenden, wovon die Betroffenen im Berichtszeitraum regelmäßig Gebrauch machten.

Zu einer Mitarbeiterbefragung zur Arbeitszufriedenheit, der Arbeitsbelastung, zum Verhältnis zu Vorgesetzten und Kollegen und Ähnlichem in einer öffentlichen Stelle des Landes, die am Wettbewerb teilnimmt, und damit gemäß § 26 ThürDSG das Bundesdatenschutzgesetz (BDSG) Anwendung findet, hat der TLfDI auf eine Anfrage eines Betroffenen hin Folgendes ausgeführt:

Zwar blieb die Stellungnahme des Einzelnen in diesem Fall ohne Namen, gleichwohl konnte aber die Erhebung von personenbezogenen Daten aufgrund der Gestaltung des Fragebogens im Einzelfall bejaht werden. Insbesondere auf Seite 1 des Umfragebogens waren Angaben zu machen, welche sich auf die Abteilung, das Alter, Geschlecht und die Berufsgruppe des Befragten bezogen. Durch diese Einzelangaben über persönliche und sachliche Verhältnisse war der Befragte, auch ohne Angaben des Namens, zumindest bestimmbar i. S. v. § 3 Abs. 1 BDSG.

Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten 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. Die vorliegende Befragung sollte einer Zertifizierung nach DIN-Normen von Qualitätsmanagementsystemen dienen, auf deren Grundlage eine Leistungsverbesserung erreicht werden sollte. Dieser Zweck ist von der Erlaubnisnorm des § 32 BDSG gedeckt. Allerdings müssen bei der Befragung auch die schutzwürdigen Interessen der Beschäftigten beachtet werden. Eine Datenerhebung, -verarbeitung und –nutzung mittels einer Mitarbeiterbefragung ist daher grundsätzlich nur zulässig, wenn die nachfolgenden Voraussetzungen eingehalten werden:

Angaben und Ergebnis müssen hinreichend anonymisiert werden, sodass das Resultat der Befragung keinem konkreten Mitarbeiter mehr zugerechnet werden kann.

1. Die Teilnahme an der Befragung muss freiwillig sein.

2. Es dürfen den Mitarbeitern keine Sanktionen oder sonstigen Nachteile drohen, wenn keine Teilnahme an der Befragung erfolgt.

3. Der mittels der Umfrage verfolgte Zweck muss den Befragten im Fragebogen erläutert werden, und zudem darf das mittels Auswertung des Fragebogens gewonnene Resultat in Zukunft auch nur für diesen Zweck verwendet werden.

4. Die Befragten sind über den Ablauf und den Gegenstand der Befragung und darüber, durch wen und für wen die Daten erhoben und verarbeitet werden, zu informieren. Auch sollten die Beschäftigten darüber aufgeklärt werden, welche Auswertungen konkret vorgesehen sind.

5. Im Fragebogen selbst sind ausführliche Hinweise bezüglich der Einhaltung der in 1.–3. genannten Voraussetzungen zu machen. Die „Freiwilligkeit" ist insbesondere durch eine drucktechnische Hervorhebung kenntlich zu machen.

Diese Voraussetzungen für die Zulässigkeit der Mitarbeiterbefragung waren durch Gestaltung des Fragebogens weitgehend eingehalten. Es bedurfte jedoch noch der drucktechnischen Hervorhebung des Hinweises auf die Freiwilligkeit der Teilnahme, des Hinweises, dass bei Nichtteilnahme keine Nachteile drohen und negative Antworten sanktionslos bleiben. Wesentliche Bedeutung kommt einer vorherigen umfassenden Aufklärung und Information der Mitarbeiter zu. Es sollte daher noch ausdrücklich darauf hingewiesen werden, dass sich der Mitarbeiter der Umfrage ohne potentielle Nachteile entziehen kann. Ein solcher zusätzlicher Hinweis ist notwendig, um eine Freiwilligkeit der Teilnahme zu gewährleisten. Zudem war auch ein ausdrücklicher Hinweis im Fragebogen nicht enthalten, dass negative Beurteilungen des Vorgesetzten/des Unternehmens etc. ohne Konsequenzen für den Befragten bleiben. Dies ist erforderlich, um den Befragten nicht in einen Gewissenskonflikt zu bringen und unwahre positive Einschätzung als Antworten zu erzwingen. Zu guter Letzt bedurfte es eines Hinweises, dass Fragebögen nach Auswertung vernichtet werden, um nach Abschluss der Datenerfassung einen späteren Zugriff auf die Fragebögen sowie die damit verbundene Vorratsdatenspeicherung zu verhindern. Mithin wird somit auch sichergestellt, dass der einzelne Befragte auch weiterhin anonym bleibt.

Soll zum Zweck des Qualitätsmanagements eine Mitarbeiterbefragung durchgeführt werden, sind die Betroffenen vorab umfassend über das festgelegte Vorgehen zu informieren. Die Teilnahme muss freiwillig sein. Die Anonymität des Betroffenen ist sicherzustellen, nicht zuletzt auch, da nur anonyme Befragungen ein unverfälschtes Bild versprechen. Nach der Auswertung sind die Fragebögen zu vernichten.

6.18 Geheime Personalakten?

Ein Beschäftigter war zu einer Dienststelle im Geschäftsbereich einer obersten Landesbehörde zunächst abgeordnet und später übernommen worden. Nun befand er sich in Rechtstreitigkeiten wegen verschiedener Personalangelegenheiten mit seiner personalverwaltenden Stelle. Er stellte fest, dass dem Gericht weit mehr Unterlagen mit personenbezogenen Daten über ihn als Beschäftigten vorgelegt worden waren, als ihm im Rahmen der Einsicht in seine Personalakte bei der Beschäftigungsbehörde zuvor zur Verfügung standen. Daher wandte er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er nun davon ausging, dass über ihn neben der offiziellen Personalakte geheime Personalunterlagen geführt wurden und darüber hinaus aus seiner Sicht wesentliche Unterlagen in der Personalakte fehlten.

Der TLfDI führte daraufhin in der Beschäftigungsbehörde eine datenschutzrechtliche Kontrolle gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) durch und ließ sich sämtliche Personalunterlagen und Sachvorgänge, die personenbezogene Daten des Betroffenen als Beschäftigten enthielten, zur Einsicht vorlegen. Die Kontrolle wurde nicht vorher angekündigt, um jeglichen Manipulationsverdacht zu vermeiden. Der Überraschungseffekt einer unangekündigten Kontrolle hat den Vorteil, dass der Sachverhalt seitens der kontrollierten Stelle nicht vorbereitet werden kann. Der Stand der Aktenführung spiegelt dann im Regelfall das wider, was Beschwerdeführer vorgefunden hatten. Gleichzeitig besteht aber andererseits für die Kontrolle der Nachteil, dass auskunftsfähige Ansprechpartner eventuell nicht zur Verfügung stehen oder zwischenzeitliche Ereignisse die Verfügbarkeit der Unterlagen beeinträchtigen konnten. Bei dieser Kontrolle lagen aber keine derartigen Schwierigkeiten vor. Die Personalakte nebst eventueller Sachvorgänge war ausweislich der Anforderung durch das für die Rechtsstreitigkeiten zuständige Gericht abgefordert worden. Von den Unterlagen waren Kopien gefertigt worden, die dem TLfDI anstandslos vorgelegt wurden. Dabei stellte der TLfDI verschiedene Mängel hinsichtlich der Personalaktenführung fest.

Nach § 33 Abs. 1 ThürDSG gelten die §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) für das Verarbeiten oder Nutzen personenbezogener Daten über im öffentlichen Dienst beschäftigte Personen, die nicht verbeamtet sind, entsprechend, es sei denn besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor. Danach ist für jede Beamtin und jeden Beamten eine Personalakte zu führen. Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktenakten). Die Personalakte ist vertraulich zu behandeln. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein, wobei landesrechtlich hierzu Ausnahmen vorgesehen werden können.

Ergänzend zu den dienstrechtlichen Vorschriften kann die Personalaktenführungsrichtlinie (ThürStAnz 1998, S. 1812 ff.) sinngemäß herangezogen werden, auch wenn diese aufgrund der zum 1. Januar 2015 in Kraft getretenen Änderung der beamtenrechtlichen Vorschriften zu überarbeiten ist.

Neben der Personalakte können auch Sachvorgänge zu Bediensteten geführt werden, sofern die zugrundeliegenden Sachverhalte sachlich zu trennen sind. Dies betrifft insbesondere Vorgänge, die im Rahmen der Aufsicht oder zur Rechnungsprüfung angelegt werden, Prüfungs-, Sicherheits- und Kindergeldakten sowie Daten über ärztliche und psychologische Untersuchungen und Tests mit Ausnahme ihrer Ergebnisse (§ 81 Abs. 1 Satz 2 ThürBG). Prozessakten und Vorgänge zu Widerspruchsverfahren zählen ebenso zu derartigen Sachakten. Nach deren Abschluss ist zu prüfen, ob das Ergebnis unmittelbar Auswirkungen auf das Dienstverhältnis hat und damit zur Personalakte zu nehmen ist.

Zuoberst war in der Akte ein amtsärztliches Gutachten offen eingelegt. In der Akte befanden sich noch weitere ärztliche Gutachten. Auch wenn zum Zweck der Personalverwaltung eine Kopie der dem Gericht vorgelegten Personalakte gefertigt wird, ist mit amtsärztlichen Gutachten ebenso zu verfahren, als ob sie im Original vorhanden wären, sie sind nämlich in verschlossenen Umschlägen zur Personalakte zu nehmen. Darüber hinaus dürfen nur die Ergebnisse der Eignungsuntersuchung und dabei festgestellte Risikofaktoren zur Personalakte gelangen, nicht aber umfängliche Gutachten mit der ganzen Familiengeschichte (Daten Dritter) und sämtlichen festgestellten Diagnosen und erhobenen Gesundheitsdaten. Selbst wenn der Beschäftigte selbst ärztliche Gutachten zur Personalakte gibt, weil er damit möglicherweise einen Nachweis führen will, muss die personalverwaltende Stelle derartige Unterlagen mit zu vielen Gesundheitsdaten zurückweisen. In der Akte fanden sich weiterhin verschiedene Dokumente, deren Erforderlichkeit für die Aufgabenerfüllung nicht oder nicht auf den ersten Blick erkennbar war. Erschwerend kam hinzu, dass die Personalakte von einer anderen personalführenden Stelle des Landes übernommen worden war und man sich scheute, Unterlagen, die definitiv für die Aufgabenerfüllung der neuen personalführenden Stelle nicht (z. B. Unterlagen, die mit der Bewerbung eingereicht wurden, wie Exmatrikulationsbescheinigung oder Kündigungsschreiben an einen früheren privaten Arbeitgeber) oder nicht mehr (alter Personalbogen mit Angaben zu den Eltern) erforderlich waren, zu entfernen. Also hatte man lediglich, wie von der Personalaktenführungsrichtlinie vorgeschrieben, ein Trennblatt eingelegt und etwas ungeordnet aktuelle Unterlagen dahinter geheftet. Jedenfalls war die Personalakte anhand der vom TLfDI gegebenen Hinweise nach Rückgabe durch das Gericht zu überarbeiten.

Wie es dazu kam, dass der Beschwerdeführer weitere geheime Dokumente vermutete, war schnell geklärt. Das Gericht hatte nämlich nicht nur die Personalakte, sondern auch andere Vorgänge mit Beschäftigtendaten des Betroffenen abgefordert. Diese Unterlagen wurden nicht geheim geführt, denn auch in diese Akten oder Vorgänge hat ein Betroffener nach

§ 84 Abs. 4 ThürBG grundsätzlich ein Einsichtsrecht. Es gab einen Vorgang, der Unterlagen mit Notizen und Bemerkungen der unmittelbaren Vorgesetzten über den Beschwerdeführer enthielt. Diese Unterlagen waren über den nächsthöheren Vorgesetzten der Personalverwaltung zugeleitet worden, weil sich der Beschwerdeführer nicht nur mit der Personalverwaltung, sondern auch mit seinen Vorgesetzten und Kollegen kontrovers auseinandersetzte. Die Vorgesetzten sahen daher die Erforderlichkeit, sich über das dienstliche Verhalten und die Leistung des Beschwerdeführers Notizen zu machen, um sich abzusichern und gegebenenfalls rechtfertigen zu können.

Hierzu hat der TLfDI ausgeführt, dass grundsätzlich keine datenschutzrechtlichen Bedenken dagegen bestehen, soweit Dienstvorgesetzte sich zum Zweck der Beurteilung Notizen anfertigen und verschiedene Vorgänge als Gedankenstütze aufbewahren, um diese in die Beurteilung einzubeziehen. Für andere Zwecke dürfen die Notizen jedoch nicht genutzt werden. Eine Abbildung der Leistung und des Verhaltens des betreffenden Bediensteten entbehrt nach Erstellung einer Beurteilung der weiteren Erforderlichkeit zur Aufbewahrung. Somit sind die zum Zweck der Erstellung einer Beurteilung angefertigten Unterlagen zu löschen. Von Dienstvorgesetzten dürfen auch keine Kopien von Unterlagen, die sich auch in der Personalakte befinden, abgeheftet werden, weil dies eine unzulässige Führung einer Personalnebenakte darstellen würde. Werden Vermerke für die Personalverwaltung zum Zweck anstehender Personalmaßnahmen oder wegen anhängiger Rechtsstreitigkeiten gefertigt, können in einer Handakte hiervon grundsätzlich Entwürfe für einen kurzen Zeitraum aufbewahrt werden. Es ist jedoch darauf zu achten, dass sich daraus beim Dienstvorgesetzten kein Personalvorgang entwickelt, der das gesamte dienstliche Verhalten des Betroffenen dokumentiert. Die Führung eines solchen Vorgangs wäre nicht erforderlich und damit unzulässig.

Dem nächsthöheren Dienstvorgesetzten dürfen Dokumente und Schreiben über Bedienstete nur dann zugeleitet werden, wenn hierzu eine gesonderte Aufgabenstellung besteht. Werden Schreiben lediglich zur Personalverwaltung weitergeleitet, besteht keine Erforderlichkeit, dass die nächsthöheren Dienstvorgesetzten diese ebenfalls in Kopie aufbewahren.

Der TLfDI hat die Personalaktenführung nach § 39 ThürDSG beanstandet und die Dienststelle aufgefordert, nach Rückgabe der Unterlagen durch das Gericht die Personalakte anhand der gegebenen Hinweise zu überarbeiten. Dies hat die Stelle zugesagt. Zu gegebener Zeit wird der TLfDI dies überprüfen.

Zur Personalakte gehören alle Unterlagen, die einen Beschäftigten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Andere Unterlagen dürfen nicht zur Personalakte genommen werden. Die Personalakte kann in Grundakte und Teilakten gegliedert werden. Personalnebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur dann geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist. Neben der Personalakte können andere Akten (als Sachakten) existieren, die personenbezogene Daten über Beschäftigte enthalten, die für ihr Dienstverhältnis verarbeitet oder genutzt werden. Beschäftigte haben das Recht, in ihre Personalakte und grundsätzlich auch in die genannten anderen Akten Einsicht zu nehmen.

Der Thüringer Landesbeauftragte für den Datenschutz und Informationsfreiheit

2. Tätigkeitsbericht nicht-öffentlicher Bereich (2014/2015)

5.1 Mindestlohn versus Datenschutz?

Das Mindestlohngesetz (MiLoG) sieht vor, dass grundsätzlich alle Arbeitnehmer einen bestimmten Mindestlohn für ihre Arbeit erhalten sollen. Nach § 13 MiLoG haften die Handelsunternehmen dafür, dass auch Dienst- und Werkleister, die von ihnen beauftragt werden, ihren beschäftigten Mitarbeitern den Mindestlohn gewähren. Also haftet beispielsweise ein Unternehmen dafür, dass die von ihm beauftragte Spedition ihren Mitarbeitern und ggf. auch dort beschäftigten Leiharbeitern mindestens 8,50 Euro Lohn bezahlt. Mit dieser Regelung wollte der Gesetzgeber die Wirksamkeit des Mindestlohngesetzes stärken.

Das MiLoG enthält jedoch keine Regelung, wie diese Vorgaben überprüft werden können. Einige Firmen wollen daher am liebsten die Lohnzettel der Mitarbeiter der von ihnen beauftragten Unternehmen erhalten. Dies ist datenschutzrechtlich nicht zulässig, da eine Rechtsgrundlage für die Übermittlung von Beschäftigtenlohndaten aus Gehaltsabrechnungen durch den jeweiligen Arbeitgeber an den Auftraggeber fehlt. Auch eine vertragliche Vereinbarung zwischen Auftraggeber und Arbeitgeber ist kein Ausweg. Es würde dabei eine Regelung getroffen, die zu Lasten von Dritten, nämlich der Beschäftigten, geht.

Eine datenschutzgerechte Möglichkeit besteht darin, anonymisierte Zahlen zu übermitteln. Zulässig ist auch, vom jeweiligen Arbeitgeber eine Verpflichtungserklärung zur Tariftreue und Mindestentlohnung zu verlangen. Da dies jedoch nicht wirksam einen Haftungsausschluss begründen kann, haben die Datenschutzaufsichtsbehörden im Düsseldorfer Kreis (siehe hierzu unter Nummer 17) auf der Sitzung vom 4./5. März 2015 mehrheitlich ein Überprüfungsverfahren empfohlen, das sich wie folgt gestaltet:

1. Übermittlung anonymisierter Daten an Auftraggeber,

2. Festlegung vertraglicher Regelungen zwecks Prüfung, ob Auftragnehmer ihre Verpflichtungen zur Mindestlohngewährung einhalten (z. B. Vereinbarung von Vertragsstrafen),

3. Überprüfung der Mindestlohngewährung durch von Auftragnehmern im Wege der Datenverarbeitung im Auftrag als Vertrauensperson eingeschaltete Wirtschaftsprüfer oder Steuerberater (sog. „Testatlösung").

Die dritte Stufe sollte aber nach Ansicht des TLfDI erst dann zur Anwendung kommen, wenn sich Zweifel an der Entlohnung ergeben, da mit der Einschaltung der Vertrauenspersonen auch eine Datenübermittlung an Dritte verbunden ist, was einen weiteren schwerwiegenderen Einschnitt in das informationelle Selbstbestimmungsrecht der betroffenen Mitarbeiter darstellen würde.

Über die vom jeweiligen Unternehmen festgelegte Vorgehensweise sollten auch die betroffenen Mitarbeiter rechtzeitig und umfassend informiert werden.

> Der Gesetzgeber ist aufgerufen, eine Rechtsgrundlage für die Übermittlung von Beschäftigtendaten zur Überprüfung der Zahlung von Mindestlohn im MiLoG zu schaffen. Bis dahin bietet der Lösungsvorschlag des Düsseldorfer Kreises eine datenschutzgerechte Lösung für den nach dem MiLoG geforderten Nachweis.

5.3 Coaching und Mitarbeiterüberwachung

Der Betriebsrat eines Call-Centers wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Stellungnahme zu einer Betriebsvereinbarung zum Mitschnitt von Gesprächen zwecks Mitarbeitercoaching und Qualitätsüberwachung.

Bedenken meldete der TLfDI gegen eine vorgesehene von den Betroffenen zu unterzeichnende Einwilligungserklärung zur Durchführung des Mithörens der Telefonate zur Kundenzufriedenheitskontrolle an. Bezeichnend war, dass der Mitarbeiter nach der Bestimmung in der Betriebsvereinbarung seine Tätigkeit nicht ausführen konnte, ohne dass er die Einwilligungserklärung unterzeichnete. Das bedeutet, dass die Einwilligungserklärung nicht, wie nach § 4 a Bundesdatenschutzgesetz (BDSG) gefordert, auf der freiwilligen Entscheidung des Betroffenen beruhte. Die von dieser Vorschrift geforderte Freiwilligkeit ist im Beschäftigtenverhältnis grundsätzlich nicht gegeben. Nur dann, wenn dem Betroffenen eine echte Alternative zur Verfügung steht und ihm durch die Verweigerung der Einwilligung kein Nachteil entsteht, kann von einer rechtswirksamen freiwilligen Einwilligungserklärung ausgegangen werden. Ob im vorliegenden Fall geeignete Alternativen in Form der Beschäftigung an einer anderen Stelle ohne nachteilige Konsequenzen zur Verfügung standen, konnte der TLfDI nicht einschätzen. Bedingt die Einwilligungserklärung jedenfalls, dass der Mitarbeiter überhaupt eine Arbeit ausführen kann, ist nicht von der Freiwilligkeit auszugehen.

Aus den dem TLfDI zur Verfügung gestellten Unterlagen wurde nicht deutlich, ob die Kunden, deren Gespräche von der Zufriedenheits- und Qualitätskontrolle ebenfalls betroffen sind, hiervon erfahren und in welcher Form sie in diese Vorgehensweise einwilligen sollten. Weiteren erheblichen Bedenken begegneten auch das vorgesehene Bewertungs- und Analyseverfahren und in diesem Zusammenhang die Zugriffe durch Vorgesetzte oder andere hierzu berufene Personen auf die Bildschirmarbeit und die Telefontätigkeit. Falls die an einem bestimmten Datum aufgezeichneten Kontakte nicht dem normalen persönlichen Leistungsbild entsprachen, sollten die Beschäftigten nämlich die Möglichkeit haben, außergewöhnliche persönliche Belastungen oder gesundheitliche Gründe anzuführen, um sich zu rechtfertigen. Sofern dies dazu führen würde, dass die Beschäftigten aus Angst vor Maßnahmen oder Verlust des Arbeitsplatzes den Datenschutz über Bord werfen und sensible personenbezogene Daten aus dem Privatbereich oder zur Gesundheit offenlegen, entstünde für das Unternehmen ein großes Problem. Diese Daten sind nämlich aus Sicht des TLfDI für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich und könnten daher auch nicht auf der Rechtsgrundlage des § 32 Abs. 1 Satz 1 BDSG erhoben und verarbeitet werden. Auch ein von einem Beschäftigten zur Rechtfertigung seiner Arbeitsleistung zu einem bestimmten Zeitraum vorgelegtes ärztliches Attest dürfte keinesfalls eine Diagnose enthalten. Abgesehen davon, dass die wenigsten Personalverwaltungen über ärztlichen Sachverstand verfügen, wie sollten die Rechtfertigungen eines Beschäftigten für eine Leistung für einen zufällig bestimmten Zeitraum bewertet werden? An der Geeignetheit einer solchen Datenerhebung durch das Unternehmen bestehen daher darüber hinaus ebenfalls erhebliche Zweifel.

Ob die Hinweise des TLfDI letztendlich beim Unternehmen Gehör finden, ist noch offen und wird vom TLfDI beobachtet.

> Eine Einwilligungserklärung zur Überwachung und Auswertung von Kundengesprächen zur Zufriedenheitsfeststellung und zum Coaching ist nur auf freiwilliger Basis möglich. Besteht keine echte Alternative im Falle der Ablehnung für die Mitarbeiter, ist die Einwilligung rechtsunwirksam. Damit erfolgt eine Auswertung der Gespräche ohne Rechtsgrundlage. Ein Mitarbeiter kann nicht aufgefordert werden, seine Arbeitsleistung durch Offenbarung sensibler personenbezogener Daten aus seinem Privatbereich oder zu seinem Gesundheitszustand präventiv oder im Nachhinein zu rechtfertigen.

5.4 Fingerabdrücke im Beschäftigtenverhältnis?

Ein in einem Thüringer Unternehmen Beschäftigter bat um Rat im Zusammenhang mit der Arbeits- und Tätigkeitserfassung auf dem ihm vom Arbeitgeber überlassenen Handy, dass über Fingerprint zu aktivieren ist. Der Beschäftigte war an verschiedenen Einsatzorten eingesetzt und sollte seine Arbeitszeiten jeweils an den verschiedenen Standorten mit dem Handy erfassen. Die genaue Handhabung und was der Betroffene genau eingeben sollte, teilte er nicht mit. Ob das Gerät möglicherweise darüber hinaus (Bewegungs-)Daten erfasste, ist nicht bekannt. Weitere Informationen zu der eingesetzten Technik gab der Betroffene leider nicht preis.

Arbeitszeiten sind personenbezogene Daten eines Beschäftigten, die auf der Grundlage des § 32 Bundesdatenschutzgesetz (BDSG) für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen. Wie und in welcher Weise die Erfassung erfolgt, ist zunächst freigestellt. Dies kann handschriftlich erfolgen oder in automatisierter Form. Insbesondere bei der automatisierten Erfassung und dem Einsatz technischer Mittel ist die Zweckbindung der Verarbeitung und Nutzung zu beachten. Grundsätzlich gilt, dass eine vollständige Leistungs- und Verhaltenskontrolle mittels automatisierter Verfahren im Beschäftigungsverhältnis auszuschließen ist. Die Feststellung des Aufenthaltsortes des Beschäftigten wäre beispielsweise zulässig, wenn dies für einen Einsatz in Havarie- oder Notfällen notwendig ist. Eine andere Auswertung wäre jedoch auszuschließen.

Will ein Arbeitgeber ein derartiges System zur Arbeitszeiterfassung einsetzen, bedarf es konkreter Festlegungen in einer Betriebsvereinbarung oder einer Betriebsanweisung. Es müssen die Regelungen vorhanden sein, welche konkreten personenbezogenen Daten zu welchem Zweck erfasst werden und wie diese Daten zu welchem Zweck und durch wen ausgewertet werden dürfen. Selbstverständlich müssen die Festlegungen nach dem Grundsatz der Transparenz für die Betroffenen den Beschäftigten auch bekannt sein.

Von der Möglichkeit, dass der TLfDI als Aufsichtsbehörde den Vollzug der datenschutzrechtlichen Vorschriften bei seinem Arbeitgeber im Zusammenhang mit dem Einsatz von Handys zur Erfassung von Arbeitszeit und Standortdaten überprüft, machte er keinen Gebrauch, denn seinen Arbeitgeber nannte er nicht.

> Falls der Arbeitgeber beabsichtigt, die Arbeitszeit zukünftig per biometrischer Datenerfassung mittels Fingerabdruck- oder Irisscanner einzuführen, bieten die auf der Homepage des TLfDI veröffentlichten Hinweise zur biometrischen Datenerfassung am Arbeitsplatz weitergehende Informationen.

5.5 Alle Jahre wieder ... Geburtstagslisten

Wie in fast jedem Berichtszeitraum, wurde auch dieses Mal an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage herangetragen, ob Geburtstagslisten, diesmal in einem Verein, zulässig seien. Geplagt von Bedenken, wandte sich ein Vorstandsmitglied eines Vereins an den TLfDI, um argumentative Unterstützung in Hinsicht seiner uneinsichtigen Vorstandskollegen zu bekommen. Hierzu erklärte sich der TLfDI gerne bereit. Geburtstagslisten sind datenschutzrechtlich ein alter Hut. Egal, ob es sich um ein Unternehmen oder um einen Verein handelt, es gelten die gleichen Regeln. Geburtstage sind in Verbindung mit einem Namen ein personenbezogenes Datum. Der Umgang mit solchen personenbezogenen Daten wiederum ist nur erlaubt, wenn eine Rechtsvorschrift dies zulässt, dies anordnet oder wenn der Betroffene in den Umgang eingewilligt hat, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Eine Rechtsvorschrift, die eine Geburtstagsliste in einem Unternehmen oder einem Verein zulassen würde, gibt es nicht, weswegen hier nur mit einer Einwilligung gearbeitet werden kann. Dabei muss natürlich darauf geachtet werden, dass die formalen und materiellen Voraussetzungen der Einwilligung eingehalten werden. So muss diese – zumindest im Falle von Geburtstagslisten – schriftlich erfolgen, sie muss freiwillig erklärt werden und es muss sichergestellt sein, dass die einwilligenden Personen ausreichend über die geplante Datenverarbeitung aufgeklärt sind, § 4 a Abs. 1 BDSG.

> Geburtstagslisten können in Unternehmen etwas Angenehmes sein. Aber man sollte immer daran denken, dass nicht jeder seinen Geburtstag offen im Intranet oder am schwarzen Brett finden möchte. Solche Listen sind immer nur mit Einwilligung der aufgeführten Mitarbeiter zulässig. Erteilt jemand seine Einwilligung nicht, dann ist diese Person auf der Liste auch nicht zu führen.

5.6 Beratung und Unterstützung von Betriebsräten

Ein weiterer Hilferuf eines Betriebsrats einer Niederlassung eines Unternehmens in Thüringen erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu einer Betriebsvereinbarung, mit der unter anderem die Verarbeitung von Mitarbeiterdaten im Rahmen der Tätigkeit, aber auch die Führung von digitalen Personalakten und die digitale Abrechnung mitbestimmungspflichtig geregelt werden soll.

Die Besonderheit war in diesem Fall, dass die Betriebsvereinbarung zwischen dem Gesamtbetriebsrat und der Geschäftsleitung am Hauptsitz des Unternehmens in einem anderen Bundesland abgeschlossen werden sollte. Anschließend sollte die Betriebsvereinbarung auch für die Niederlassung in Thüringen umgesetzt werden. Ein eigener Datenschutzbeauftragter in der Betriebsstätte in Thüringen war nicht bestellt.

Selbstverständlich kann eine Beratung nur erfolgen, wenn hierfür auch eine Zuständigkeit des TLfDI als Aufsichtsbehörde gegeben ist. Der TLfDI hat nach § 3 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) zwar die Zuständigkeit für Betriebsstätten in Thüringen. Die fragliche Betriebsvereinbarung sollte jedoch in einem anderen Bundesland mit sich später auch entfaltender Wirkung für alle Standorte abgeschlossen werden. Insoweit ist zunächst die am Hauptsitz des Unternehmens zuständige Datenschutzaufsicht zuständig. Nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) berät und unterstützt die Aufsichtsbehörde

die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Im Einvernehmen mit dem Thüringer Betriebsrat wurde daher die Anfrage an die zuständige Datenschutzaufsicht in einem anderen Bundesland abgegeben. Diese hat den TLfDI zwischenzeitlich darüber informiert, von einer Überprüfung der Betriebsvereinbarung werde abgesehen, da der Betriebsrat ihrer Auffassung nach keine verantwortliche Stelle im Sinne des § 38 Abs. 1 Satz 2 BDSG sei und daher kein Anspruch auf Beratung durch die Aufsichtsbehörde bestehe. Gleichwohl ist es aus Sicht des TLfDI vorstellbar, soweit in einer beabsichtigten Betriebsvereinbarung offensichtliche datenschutzschutzrechtliche Mängel erkennbar sind, auch unaufgefordert das Unternehmen selbst zu beraten oder zu kontrollieren.

> Wird von einem Unternehmen mit Hauptsitz in einem anderen Bundesland eine Betriebsvereinbarung mit dem Gesamtbetriebsrat abgeschlossen, besteht für den TLfDI keine Zuständigkeit. Betriebsräte sind keine verantwortlichen Stellen im Sinne des § 38 Abs. 1 Satz 2 BDSG und haben daher grundsätzlich keinen Anspruch auf Beratung durch die Datenschutzaufsichtsbehörde. Sollten offensichtliche datenschutzrechtliche Mängel drohen, kann der TLfDI das Unternehmen als verantwortliche Stelle in seinem Zuständigkeitsbereich auch unaufgefordert beraten und kontrollieren.

5.7 Betriebsarzt übermittelt Gesundheitsdaten dem Arbeitgeber

Ein Industrieverband in Thüringen bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) um Beratung zu folgender Frage:

Aufgrund der Vielfältigkeit der Tätigkeitsbereiche werden seitens der Unternehmen so genannte Gefährdungsbeurteilungen für einzelne Arbeitsplätze formuliert. Arbeitnehmer, bei denen es einer gewissen medizinischen und körperlichen Eignung bedarf, werden daher regelmäßig betriebsärztlichen Eignungsuntersuchungen unterzogen, um ihnen gegebenenfalls einen anderen, besser geeigneten Arbeitsplatz zuzuweisen. Dafür müssten die Betriebsärzte den Arbeitgebern Gesundheitsdaten übermitteln. Dabei sollten allerdings keine Diagnosen weitergegeben, sondern nur die Tatsache übermittelt werden, dass der jeweilige Arbeitnehmer für die aktuell ausgeübte Tätigkeit aus medizinischen Gründen „geeignet" oder „nicht geeignet" ist. Der Verband wollte wissen, aufgrund welcher Rechtsgrundlage dies möglich sei.

Der TLfDI hat hierzu ausgeführt, dass es sich bei Angaben zu betriebsärztlichen Eignungsuntersuchungen um besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG handele, die einen gesteigerten Schutz genießen. Nach der europäischen Datenschutzrichtlinie ist ihre Verarbeitung nur zugelassen, wenn sie erforderlich ist, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von nationalem Recht, das angemessene Garantien vorsieht, zulässig ist.

Der Arbeitgeber kann nach § 2 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) Betriebsärzte bestellen, wenn dies erforderlich ist im Hinblick auf die Betriebsart und die damit für die Arbeitnehmer verbundenen Unfall- und Gesundheitsgefahren. Die Betriebsärzte haben nach § 3 ASiG Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten.

Hinsichtlich der Durchführung ärztlicher Untersuchungen gilt, dass der Arbeitnehmer aus der allgemeinen Treuepflicht nach § 242 Bürgerliches Gesetzbuch (BGB) verpflichtet sein kann, eine ärztliche Untersuchung seines Gesundheitszustandes zu dulden. Es müssen jedoch tatsächliche Anhaltspunkte dafür vorliegen, ob und welche Zweifel an der gesundheitlichen Tauglichkeit des Beschäftigten, den Anforderungen des Arbeitsplatzes dauerhaft gerecht zu werden, oder andere sachliche Gründe bestehen, welche die Durchführung einer ärztlichen Untersuchung rechtfertigen (z. B. Versetzung auf einen anderen Arbeitsplatz, für den gesteigerte gesundheitliche Anforderungen bestehen). Aufgrund der besonderen Sensibilität der Daten dürfen weder Diagnosen noch eine vom Arzt ermittelte Anamnese an den Arbeitgeber weitergegeben werden. Es darf lediglich ein allgemeines Urteil über die gesundheitliche Eignung des Mitarbeiters für die konkrete Tätigkeit abgegeben werden.

Die dargestellte beabsichtigte Datenweitergabe seitens des Betriebsarztes an den Arbeitgeber in der Form, ob der jeweilige untersuchte Arbeitnehmer für die aktuell ausgeübte Tätigkeit aus medizinischen Gründen „geeignet" oder „nicht geeignet" ist, begegnet keinen datenschutzrechtlichen Bedenken. Es handelt sich dabei um die Verarbeitung personenbezogener Daten des Mitarbeiters nach § 32 Abs. 1 S. 1 BDSG. Einer ausdrücklichen Einwilligung des Arbeitnehmers nach § 4 a Abs. 1 und 3 BDSG (die aufgrund der Freiwilligkeitsproblematik im Beschäftigtenbereich ohnehin problematisch wäre – siehe Nummer 9.10) oder einer entsprechenden Betriebsvereinbarung bedarf es nicht.

Arbeitnehmer können, wenn sie einen Arbeitsplatz innehaben, der eine gesundheitliche Eignung voraussetzt, betriebsärztlich untersucht werden. Der Betriebsarzt darf das Ergebnis der Untersuchung – „geeignet" oder „nicht geeignet" – dem Arbeitgeber mitteilen – mehr nicht! Einer Einwilligung des Arbeitnehmers oder einer entsprechenden verpflichtenden Betriebsvereinbarung bedarf es hierzu nicht.

5.8 Chefs mit Kontrollzwang oder Mitarbeiter mit Verfolgungswahn?

Immer wieder wenden sich Beschäftigte Thüringer Unternehmen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie sich intensiven Maßnahmen zur Leistungs- und Verhaltenskontrolle in den Unternehmen ausgesetzt sehen. Dies geht vom Einsatz von Videokameras über Mithören von Gesprächen oder Telefonaten bis hin zur Fahrzeugortung über GPS.

In einem besonders krassen Fall wurde der dringende Verdacht geäußert, dass alle Mitarbeiterbüros inklusive der Telefonzentrale sowie alle Diensttelefone und Dienstrechner

mit Mithörtechnik und/oder Minikameras ausgerüstet sind. Dieser Verdacht gründete sich insbesondere darauf, dass Gesprächsinhalte, die innerhalb des Büros des Betroffenen stattgefunden hatten, plötzlich Gesprächsthema beim Teamleiter waren, obwohl der an den „vertraulichen" Gesprächen überhaupt nicht teilgenommen hatte. Dass das Fahrzeug, das im Außendienst zu nutzen war, mit GPS-Technik oder einer Micro-Kamera mit Tonaufzeichnung ausgerüstet war, wurde ebenfalls vermutet. Die unerklärlichen Dinge gingen soweit, dass der Betroffene sich nach einem privaten Restaurantbesuch unangenehmen Ansprachen des Sicherheitspersonals ausgesetzt sah, er wolle wohl den Arbeitgeber wechseln. Der Beschwerdeführer wurde darauf hingewiesen, es existierten Videos von Geschäftsterminen, an denen auch Vertreter von Wettbewerbsunternehmen teilgenommen hätten.

Dass der Betroffene, wie üblich bei derartigen Nachfragen, anonym bleiben wollte, ist nachzuvollziehen. Der TLfDI kann den Arbeitgeber unter Wahrung der Anonymität des Hinweisgebers auffordern, zu den Vorwürfen der Überwachung der Betriebsstätte und der Fahrzeuge Stellung zu nehmen, um dies datenschutzrechtlich zu überprüfen. Die Wahrung der Anonymität funktioniert aber nur, wenn es sich um einen größeren Mitarbeiterkreis handelt und Einzelheiten keinen Rückschluss auf einen bestimmten Mitarbeiter zulassen. Im vorliegenden Fall informierte der TLfDI den Hinweisgeber wunschgemäß allgemein und wies darauf hin, dass das Mithören und das Aufzeichnen des nicht-öffentlichen gesprochen Wortes eine Straftat darstellen kann. Einem Betroffenen steht in einem derartigen Fall neben einer Beschwerde beim TLfDI auch die Möglichkeit einer Strafanzeige bei der Staatsanwaltschaft offen.

> Besteht der Verdacht, dass in einem Unternehmen das nichtöffentlich gesprochene Wort abgehört wird, kann der hiervon Betroffene auch wegen einer Straftat nach § 201 Strafgesetzbuch (StGB) bei der Staatsanwaltschaft oder der Polizei Strafantrag stellen.

5.10 Arbeitgeber will den Mutterpass sehen

Eine Arbeitnehmerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Unterstützung. Hintergrund war, dass sie ihren Arbeitgeber über ihre Schwangerschaft in Kenntnis gesetzt hatte. Gleichzeitig händigte sie dem Arbeitgeber ein ärztliches Schwangerschaftsattest mit allen relevanten Daten (voraussichtlicher Entbindungstermin, aktuelle Schwangerschaftswoche, letzter Arbeitstag vor dem Beschäftigungsverbot nach dem Mutterschutzgesetz) aus. Der Arbeitgeber wollte aber die Schwangerschaft nicht anerkennen, da die Betroffene nicht bereit war, ihren Mutterpass vorzulegen und kopieren zu lassen.

Der Betroffenen wurde folgende rechtliche Einschätzung des TLfDI mitgeteilt:

Das Erstellen einer Kopie des Mutterpasses erfüllt den Tatbestand des Erhebens personenbezogener Daten durch den Arbeitgeber. Dies ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da eine Einwilligung nicht vorlag und es im Übrigen wegen des bestehenden Beschäftigungsverhältnisses auch an deren Freiwilligkeit fehlen würde, muss eine Rechtsvorschrift das Erheben dieser Daten erlauben. Sofern eine spezielle Ermächtigungsgrundlage nicht existiert, ist das Erheben von Beschäftigtendaten nach § 32 BDSG nur zulässig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Nach § 5 des Mutterschutzgesetzes sollen werdende Mütter dem Arbeitgeber ihre Schwangerschaft und den mutmaßlichen Tag der Entbindung mitteilen, sobald ihnen ihr Zustand bekannt ist. Auf Verlangen des Arbeitgebers sollen sie das Zeugnis eines Arztes oder einer Hebamme vorlegen. Aufgrund der für Schwangere geltenden besonderen gesetzlichen Bestimmungen ist die Kenntnis von der Schwangerschaft und des voraussichtlichen Entbindungstermins für die Durchführung des Beschäftigungsverhältnisses für den Arbeitgeber in aller Regel erforderlich. Nicht erforderlich ist aber das Erheben der im Mutterpass zusätzlich zu diesen Angaben enthaltenen personenbezogenen Daten. Der Mutterpass enthält Informationen über die Gesundheit der Schwangeren, unter anderem Ergebnisse von Laboruntersuchungen, Angaben dazu, ob eine Rötelnerkrankung vorlag, ob die Schwangere mit Chlamydien – einer bestimmten Art von Bakterien – infiziert ist, ob eine HIV-Infektion besteht, ob eine Infektion mit Syphilis-Erregern nachgewiesen wurde, ob eine Erkrankung an Hepatitis B besteht und vieles mehr.

Der Arbeitgeber durfte daher im vorliegenden Fall die Vorlage des Mutterpasses nicht verlangen. Der Beschwerdeführerin wurde mitgeteilt, dass, sollte er gleichwohl eine Kopie des Mutterpasses fertigen, die Einleitung eines Ordnungswidrigkeitenverfahrens zu prüfen wäre. Nach § 43 Abs. 2 Nr. 1 BDSG handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt. Die Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 300.000 Euro geahndet werden. Der Betroffenen wurde geraten, dem Arbeitgeber das Schreiben des TLfDI zur Kenntnis vorlegen. Die Beschwerdeführerin hat sich daraufhin nicht mehr gemeldet.

> Die Kenntnis von der Schwangerschaft und des voraussichtlichen Entbindungstermins für die Durchführung des Beschäftigungsverhältnisses ist für den Arbeitgeber in aller Regel erforderlich. Nicht erforderlich und damit unzulässig ist aber das Erheben der im Mutterpass zusätzlich zu diesen Angaben enthaltenen personenbezogenen Daten.

5.14 Seminarteilnehmer per E-Mail anschreiben: Was ist zu beachten?

Der Mitarbeiter eines Unternehmens, das Fortbildungen anbot, fragte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob es denn rechtlich geregelt sei, ob er über die E-Mail-Adresse eines anderen Unternehmens Teilnehmer an Seminaren anschreiben dürfe. Nach seinem Dafürhalten übermittele er doch auf diese Weise keine personenbezogenen Daten der Teilnehmer.

Da die näheren Umstände vom Fragesteller trotz Rückfrage des TLfDI nicht dargelegt wurden (z. B.: Weshalb soll diese E-Mail-Adresse genutzt werden? Wurde die Fortbildung vom Unternehmen, das die E-Mail-Adresse besitzt, selbst veranlasst oder genehmigt oder ist der Fragesteller selbst in beiden Unternehmen tätig?), hat der TLfDI nur allgemein ausgeführt, eine konkrete gesetzliche Regelung hierzu gäbe es nicht.

Die Nutzung von E-Mail-Adressen eines Unternehmens wird üblicherweise durch eine Betriebsvereinbarung oder Anweisung in dem Betrieb, dem die E-Mail-Adresse zuzuordnen ist, geregelt. Es kommt darauf an, ob die E-Mail-Adresse des Unternehmens, auch wenn diese durch die Nennung des Mitarbeiters Personenbezug aufweist, nur für Unternehmenszwecke oder auch für andere Zwecke genutzt werden darf. Dem Unternehmen ist in der zugrundeliegenden Vereinbarung oder Anweisung in der Regel eine Kontrollbefugnis zu den ein- und ausgehenden E Mails eingeräumt. Selbst wenn nur der Header für Kontrollzwecke genutzt wird, käme dem Unternehmen bzw. der zur Kontrolle befugten Person zur Kenntnis, wer Seminarteilnehmer ist oder war. Je nachdem, ob dies gewollt ist oder vermieden werden soll, ist zu entscheiden, auf welchem Weg Seminarteilnehmer angeschrieben werden. Hat das in der E-Mail-Adresse bezeichnete Unternehmen mit dem Seminar selbst nichts zu tun, dürfen ihm auch die Seminarteilnehmer nicht zur Kenntnis gelangen, weil ihm keine eigenen Erhebungsbefugnisse nach § 28 Bundesdatenschutzgesetz (BDSG) bzw. bei eigenen Mitarbeitern nach § 32 BDSG zukommen.

Der Fragesteller bedankte sich beim TLfDI für die Ausführungen, die er für hilfreich erachtete.

> Bevor die E-Mail-Adresse eines Unternehmens genutzt wird, muss man sich kundig machen, welche Regelungen intern zur Nutzung getroffen sind. Bestehen Kontrollbefugnisse zu ein- und ausgehenden E-Mails, sollte der Versender von E-Mails darauf achten, dass dem Unternehmen keine personenbezogene Daten offenbart werden, die dieses nicht erheben darf.

5.16 Von Räuberpistolen – Datenschutz im Logistikunternehmen

Von A bis Z, von der Angel bis zur Zahnbürste, alles kann bei den großen Händlern im Internet bestellt werden und ist in der Regel schon am nächsten Tag bei einem zu Hause. Ein Komfort, der einen oft vergessen lässt, welch organisatorischer Aufwand hinter diesem Prozess steht, der diese Schnelligkeit bei gleichzeitiger Warenfülle gewährleistet. Wie geht das, fragen Sie sich? Nun, kurz und ohne Umschweife: Daten, Daten und nochmals Daten. Nicht alle personenbezogen, aber letztlich doch viele.

Die Lager der Händler sind in der Regel chaotisch sortiert. Darunter versteht man eine Lagerhaltung, die zwar sehr effektiv, aber ohne Computer nicht zu handhaben ist. Natürlich gibt es eine gewisse Grundordnung, letztlich werden aber einzulagernde Waren dort aufbewahrt, wo Platz ist und nicht unbedingt dort, wo ähnliche oder dazugehörige Teile gelagert werden. Wegen der vielen unterschiedlichen Formen der Waren müssen diese jedoch von Menschen einsortiert werden. Jede dieser Personen hat eine Scan-Pistole. Über diese wird der Einlagerungsprozess gesteuert und dokumentiert. Allerdings lässt sich über die damit erhobenen Daten nicht nur der Lagerort der Ware bestimmen, sondern auch recht genau die Arbeitsleistung des Pistoleros.

Ein solches Logistiklager hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum geprüft. Das Verfahren ist, auch wegen der umfangreichen IT des Unternehmens, noch nicht ganz abgeschlossen, befindet sich aber auf einem guten Weg. Aus Sicht das Datenschutzes, also aus Sicht des TLfDI ist problematisch, dass einerseits das Unternehmen die erhobenen Daten über die Waren- und Logistikprozesse unbedingt benötigt, andererseits aber irgendwie sichergestellt werden muss, dass dabei keine Arbeitnehmerdaten erhoben oder verarbeitet werden, die nicht hätten erhoben oder verarbeitet werden dürfen. Das Gesetz verlangt von der verantwortlichen Stelle hierfür technische und/oder organisatorische Maßnahmen (sog. Technische und organisatorische Maßnahmen oder kurz TOMs), die dies verhindern. Das Unternehmen arbeitet kooperativ mit dem TLfDI an einer Lösung.

> Verantwortliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um das Bundesdatenschutzgesetz umzusetzen.

5.19 Mitarbeiterüberwachung durch Handscanner?

Anlässlich der Durchführung einer datenschutzrechtlichen Kontrolle der Videoüberwachung in einem Logistikunternehmen wurde festgestellt, dass dort so genannte Handscanner genutzt werden. Diese Geräte erlauben die Speicherung von Mitarbeiterdaten dazu, wer wann welches Produkt wohin verbracht hat.

Das Handgerät verfügt über eine Windowsoberfläche und kann grundsätzlich alles, was ein PC auch kann. In dem Logistikunternehmen wird der Wareneingang und ausgang registriert. Somit ist jeweils nachvollziehbar, wann sich welches Warenteil wo befindet, aber auch, welcher Mitarbeiter zu welchem Zeitpunkt Waren scannt. Damit stellte sich die Frage nach der Möglichkeit und Zulässigkeit einer sekundengenauen Arbeitnehmerüberwachung.

Die Mitarbeiter müssen die Handscanner an einer Ausgabestation nach Registrierung abholen und dabei auch ihren Mitarbeiterausweis einscannen. Die Speicherung der Personalnummer ist nach Angaben der Ansprechpartner erforderlich, weil damit erst der Zugang zur Datenbank eröffnet wird und somit die Rechtezuordnung gewährleistet ist. Nach Erledigung der Aufträge wird der Handscanner zurückgegeben. Der Mitarbeiter loggt sich aus. Der Zeitpunkt der Rückgabe wird deshalb erfasst, weil in der Vergangenheit immer wieder derartige Handscannergeräte abhandengekommen waren. Die erfassten Daten werden in einer der Lagerverwaltung dienenden Datei gespeichert. Aus diesen Daten können so genannte Revisionslisten erzeugt werden, die im Falle von vermehrten Retoursendungen eine Überprüfung ermög-

lichen und damit zur Fehlervermeidung beitragen, weil gegebenenfalls Abläufe optimiert werden können. In einer Teilkonzernrahmenbetriebsvereinbarung, die in der Betriebsstätte umzusetzen ist, ist niedergelegt, dass eine Leistungs- und Verhaltenskontrolle grundsätzlich nicht zulässig ist. Die datenschutzrechtliche Prüfung und Bewertung aller in diesem Zusammenhang nachträglich durch die verantwortliche Stelle übermittelten Dokumente ist noch nicht abgeschlossen.

> Werden in einem Unternehmen Handscanner eingesetzt, mittels deren Speicherung der einzelnen Handlungen ein sekundengenaues Tätigkeitsprofil des Mitarbeiters erstellt werden kann, ist sicherzustellen, dass eine solche Leistungs- und Verhaltenskontrolle ausgeschlossen ist.

5.23 Kündigung – Zugriff des Arbeitgebers auf private Daten des Arbeitnehmers auf dem Arbeitsplatzrechner?

Eine private Fachhochschule bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung, wie mit einem Arbeitsplatz-PC bei Beendigung des Arbeitsverhältnisses umzugehen ist. In dem speziellen Fall sollten mit Ausscheiden eines Mitarbeiters dessen Zugriffsmöglichkeiten auf den PC unmittelbar entzogen werden. Der TLfDI stellte zunächst fest, dass dieses zulässig ist, da der PC grundsätzlich im Eigentum der Fachhochschule steht. Die Fachhochschule hat darüber hinaus nach § 9 Bundesdatenschutzgesetz (BDSG) sogar die Pflicht, Maßnahmen zu ergreifen, um eine Kenntnis von personenbezogenen Daten durch Unbefugte zu verhindern. Der weitere Zugang eines ausgeschiedenen Mitarbeiters auf dienstliche Unterlagen der Hochschule ist deshalb zu verhindern. Sind aber noch private Dateien des Mitarbeiters gespeichert, etwa private E-Mails oder Daten im Home-Verzeichnis der Festplatte des Rechners, darf die Hochschule diese privaten Dateien nicht ohne Weiteres öffnen oder löschen, sondern muss die Rechte des ausscheidenden Mitarbeiters beachten. Wenn die Hochschule ihren Beschäftigten die private Nutzung von E-Mail und Internet erlaubt, erbringt sie ihren Mitarbeitern gegenüber geschäftsmäßig Telekommunikationsdienste. Die Fachhochschule hat dann das Fernmeldegeheimnis zu wahren. Daher sind Zugriffe und Löschungen der privaten E Mails durch den Arbeitgeber nur mit ausdrücklich erteilter Einwilligung des Betroffenen gemäß § 4a Bundesdatenschutzgesetz zulässig. Auch wenn die Fachhochschule die private Nutzung des E-Mail-Verkehrs nicht ausdrücklich erlaubt oder verboten hat und die private Nutzung regelmäßig duldet, kommt ebenfalls das Telekommunikationsgesetz mit den o. g. Folgen zur Anwendung. War die E Mail Nutzung hingegen ausdrücklich nur zu betrieblichen Zwecken erlaubt, darf die Hochschule als Arbeitgeber allerdings in das E-Mail-Postfach des ausscheidenden Mitarbeiters Einsicht nehmen, da davon ausgegangen werden kann, dass nur dem Arbeitgeber zustehendes Schriftgut vorhanden ist. Sobald jedoch festgestellt wird, dass E-Mails privaten Charakter aufweisen, dürfen diese vom Arbeitgeber nicht weiter inhaltlich zur Kenntnis genommen werden. Hatte der Mitarbeiter bestimmte private Verzeichnisse auf der Festplatte des Rechners oder innerhalb des E-Mail-Accounts angelegt und sind diese klar gekennzeichnet, so hat dieser zwar gegen die betrieblichen Anweisungen der Hochschule verstoßen, aber auch hier darf aus datenschutzrechtlicher Sicht der Arbeitgeber in die Dateien keine Einsicht nehmen und die Dateien auch nicht einfach löschen. Vielmehr ist dem ausscheidenden Mitarbeiter die Gelegenheit zu geben, eingegangene E-Mails auf dem ihm zugewiesenen Account auf private Inhalte durchzusehen und diese zu löschen. Dies gilt ebenso für weitere private Dateien, die auf dem Rechner gespeichert sind. Um Konflikte zwischen Arbeitgeber und Arbeitnehmer von vornherein auszuschließen, sollte der Arbeitgeber die genaue Verfahrensweise beim Umgang mit privaten Dateien in einer Betriebsvereinbarung ausdrücklich regeln. Mit dieser Auskunft war die Hochschule zufrieden, sie hat sich nicht mehr gemeldet.

Wertvolle Hinweise zur Regelung und zum Abschluss einer entsprechenden Betriebsvereinbarung enthält die „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz", die jedoch erst nach Schluss des Berichtzeitraums beschlossen wurde und seit Februar 2016 auf der Internetseite des TLfDI verfügbar ist.

> Dem Arbeitgeber ist es nicht erlaubt, beim Ausscheiden von Mitarbeitern ohne Einwilligung der Betroffenen in private E-Mails Einblick zu nehmen oder diese zu löschen. Es wird empfohlen, den Umgang mit privaten E-Mails der Beschäftigten bei deren Ausscheiden in einer Betriebsvereinbarung zu regeln.

Landesbeauftragter für den Datenschutz Baden-Württemberg 32. Tätigkeitsbericht (2014/2015)	
Thema (Rot = nicht in der Broschüre abgedruckt)	Kapitel/Seite
Mindestlohngesetz und Datenschutz	9.1/145
Abgleich von Beschäftigtendaten mit Sanktionslisten der EU sowie sonstiger Drittstaaten	9.2/146
Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern: Die Ausnahme muss wieder zur Regel werden	9.3/147
Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern aus Sicht des Kunden	9.3.1/148
Aufzeichnung von Telefongesprächen in Call-Centern aus Sicht der Mitarbeiter	9.3.2/149

Berliner Beauftragter für Datenschutz und Informationsfreiheit 37. Tätigkeitsbericht (2015)	
Bonitätsauskünfte im Bewerbungsverfahren	9.1/113
Öffentliche Kommentierung von Personalangelegenheiten	9.2/114
Big Boss is watching you – Videoüberwachung im Beschäftigungsverhältnis	9.3/115
GPS-Tracking im Beschäftigungsverhältnis	9.4/117
Daten von Bediensteten im Internet	9.5/118
Wenn der Arbeitgeber den Facharzt kennt – Umgang mit Arbeitsunfähigkeitsbescheinigungen	9.6/120

Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg 18. Tätigkeitsbericht (2014/2015)	
Betriebliches Eingliederungsmanagement – Teilnahme einer Vertrauensperson aus dem privaten Umfeld?	5.1/73
Betriebliches Eingliederungsmanagement – unerlaubte Datenübermittlung	5.2/74
Akteneinsicht von Gemeindevertretern in Disziplinarvorgänge	5.3/76
Entgeltabrechnungen und Arbeitgeberbescheinigungen online	5.4/77
Beschäftigtendatenschutzgesetz jetzt!	1.7.1/238
„Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!"	1.7.2/239

Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen 38. Tätigkeitsbericht (2015)	
Einholung einer SCHUFA-Auskunft über Bewerber	11.1/51
Kopien von Führerscheinen durch den Arbeitgeber	11.2/52
Aushang der Ergebnisse von Leistungskontrollen	11.3/52
Übernahme der Gesundheitsakten der Beschäftigten ehemaliger Werften durch die Arbeitnehmerkammer	11.4/53
Videoüberwachung und Tonüberwachung der Beschäftigten in einem Restaurant	12.7/58
Verdeckte Überwachung der Beschäftigten bei Geld- und Werttransporten	12.8/59

Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit 25. Tätigkeitsbericht (2014/2015)	
Mitarbeiterüberwachung – Einsatz von Ortungssystemen	1.1/228
Mindestlohn	1.2/240
Arbeitgeberzeitschrift AKTIV	1.3/241
KoPers - Sachstand	2.1/243

Hessischer Datenschutzbeauftragte 44. Tätigkeitsbericht (2016)	
Datenschutzrechtliche Einwilligungen von Beschäftigten im Rahmen des Abschlusses von Arbeitsverträgen	4.10.1/195

Landesbeauftragte für den Datenschutz Niedersachsen 22. Tätigkeitsbericht (2013/2014)	
Beschäftigtendatenschutz: Das rechtliche Niveau muss gehalten werden	7/86
Weitergabe von Arbeitnehmerdaten: Datenübermittlung an Agrar Zertifizierungsstellen rechtswidrig	7/88
Biometrisches Zugangssystem: Fingerabdruckscanner in Fensterfirma unzulässig	7/90
Konto beim Arbeitgeber: Bank darf nicht Mitarbeiterkonten einsehen	7/91

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz 25. Tätigkeitsbericht (2014/15)	
Personaldatenschutz und Informationsfreiheit	3.1.1/53
Online-Zugriff des Personalrats auf Zeiterfassungsdaten	3.1.2/53
Online-Bewerbungen	3.1.3/54
Rechtsprechung des Bundesarbeitsgerichts stärkt den Datenschutz	3.2.1/55
IT-Nutzung am Arbeitsplatz (Orientierungshilfe)	3.2.2/56
Betriebsvereinbarungen als Erlaubnis zum Umgang mit Arbeitnehmerdaten	3.2.3/57

Unabhängiges Datenschutzzentrum Saarland 25. Tätigkeitsbericht (2013/2014)	
Auskunftssperren für besonders gefährdete Beamtengruppen	17.1.1/98
Weitergabe von Verwandtschaftsverhältnissen an die Presse	17.1.2/99
Arbeitnehmerüberwachung in einem Gastronomiebetrieb	17.2.1/99
Telefonische Kontaktaufnahme zu ausgeschiedenen Mitarbeitern	17.2.2/100
Videoüberwachung im Beschäftigungsverhältnis	19.2/105
Videoüberwachung in der industriellen Produktion	19.3/106
Videoüberwachung während einer Prüfung in der Universität des Saarlandes	19.4/107

Sächsischer Datenschutzbeauftragter 17. Tätigkeitsbericht (2013/2015)	
Personenbezogene Daten für das Rechnungsprüfungsamt	5.1.1/31
Ehegatteneinkünfte im Beihilfeverfahren	5.1.2/32
Beschäftigtendatenverarbeitung zur Prüfung der Eignung von Bediensteten	5.1.3/32
Grenzen der Auftragsdatenverarbeitung Vorgesehene Privatisierung im Beschaffungswesen	5.1.4/34
Videodatenverarbeitung im Beschäftigungsverhältnis	5.1.5/37

Landesbeauftragter für den Datenschutz Sachsen-Anhalt 12. Tätigkeitsbericht (2013/2014)	
Zeiterfassung mittels Fingerabdruck	12.3/135
Personaldatenverarbeitung mittels WhatsApp	12.4/136
Mindestlohngesetz	12.6/139
Videoüberwachung der Beschäftigten	15.2.10/179

Thüringer Landesbeauftragter für den Datenschutz und Informationsfreiheit 11.Tätigkeitsbericht öffentlicher Bereich (2014/2015)	
Datenleck bei Betriebsratswahl	6.1/172
Darf der behördeninterne Datenschutzbeauftragte den Personalrat kontrollieren?	6.2/174
Zeitungsnotiz zur „krankheitsbedingten" Schließung eines Amtes	6.3/177
Mitarbeiter: Bitte lächeln!	6.4/178
Bewerberunterlagen: Einsicht für alle Personalratsmitglieder?	6.5/180
„Pranger 2.0" – Amtsleiter stellt sensible Daten von Mitarbeiterin ins Intranet	6.6/182
Mitarbeiter im GPS-Dauer-Fokus	6.7/182
Übermittlungsbefugnis des Amtsarztes – keine Generalvollmacht!	6.8/184
GPS: nicht vom richtigen Weg abkommen	6.9/186
Bewerbungen per E-Mail	6.10/189
Elektronische Personalakte	6.11/191
Fingerabdruckscanner zur Arbeitszeiterfassung?	6.12/193
Fragebögen zur Mitarbeiterbefragung	6.13/194
Wenn sich Beschäftigte über andere Beschäftigte beschweren: ein Datenschutzproblem?	6.14/197
Schutz: Daten oder Kanzlerin? Datenübermittlung anlässlich des Besuchs der Bundeskanzlerin	6.15/199
Verfahren „Interamt" (Onlineverfahren mit Speicherung und Verarbeitung der Bewerberdaten)	6.16/202
Datenschutz im Stadtrat – was darf bei Disziplinarverfahren übermittelt werden?	6.17/204
Geheime Personalakten?	6.18/206
Lehrerdaten für die Schuljahresanalyse	6.19/210

Thüringer Landesbeauftragter für den Datenschutz und Informationsfreiheit 2. Tätigkeitsbericht nicht-öffentlicher Bereich (2014/2015)	
Mindestlohn versus Datenschutz?	5.1/264
Ausweispflicht gegenüber dem Arbeitgeber?	5.2/265
Coaching und Mitarbeiterüberwachung	5.3/267
Fingerabdrücke im Beschäftigtenverhältnis?	5.4/268
Alle Jahre wieder ... Geburtstagslisten	5.5/269
Beratung und Unterstützung von Betriebsräten	5.6/270
Betriebsarzt übermittelt Gesundheitsdaten dem Arbeitgeber	5.7/272
Chefs mit Kontrollzwang oder Mitarbeiter mit Verfolgungswahn?	5.8/273
Die Suche nach Personalakten	5.9/275
Arbeitgeber will den Mutterpass sehen	5.10/276
Nur weil's einer wissen darf, heißt es noch lange nicht, dass es ein anderer erzählen darf.	5.11/278
Unfallanzeige an die Berufsgenossenschaft	5.12/279
Wie heißt die Schwester? – Namensschilder im Krankenhaus	5.13/280
Seminarteilnehmer per E-Mail anschreiben: Was ist zu beachten?	5.14/282
Der gläserne Kraftfahrer	5.15/283
Von Räuberpistolen – Datenschutz im Logistikunternehmen	5.16/286
Bei Anruf Chef! – Nachprüfung der Dienstreisezeiten im Hotel	5.17/287
Bewerbung per E-Mail?	5.18/288
Mitarbeiterüberwachung durch Handscanner?	5.19/289
Fahrzeugvermittlung nur gegen Mitarbeiterdaten?	5.20/290
Handydaten auf Achse	5.21/291
Mitarbeiterüberwachung durch technische Vorrichtungen	5.22/293
Kündigung – Zugriff des Arbeitgebers auf private Daten des Arbeitnehmers auf dem Arbeitsplatzrechner?	5.23/295

Kontakt und Informationen

Technische Hochschule Mittelhessen
Wiesenstraße 14 | 35390 Gießen

Datenschutzbeauftragter der Hochschule

Hajo Köppen, Assessor jur.

Fon: 0641 309 -1030
Fax: 0641 309 - 2907
Gebäude B10 | Raum 1.02
Ostanlage 39
E-Mail: hajo.koeppen@verw.thm.de

Homepage des Datenschutzbeauftragten

www.thm.de/datenschutz

Recherche

Krispin Brandt

Download unter:
go.thm.de/dsdl

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C084253

Titelbild: © Nikolai Sorokin / fotolia.com

1. Auflage: März 2017