Knittel – Akademie für Datenschutz & Compliance
Inhaber Patrick M. Knittel
Mescheder Weg 57·13507 Berlin ·Telefon (030) 43553308 · E-Mail: Knittel@knittel-compliance.de

Seminar: Aktuelles zum Datenschutz

Meine aktuellen Themen zum Seminar:

Begrüßung und Vorstellung

1) aus aktuellem Anlass:

- Schutz von Hinweisgebern bei Informationen an die Geschäftsführung

➔ Siehe dazu auch die Entscheidung des VG Bremen (Anhang 1)

- Streit um das (werbefreundliche) Meldegesetz

➔ Siehe dazu heise online (Anhang 2)

2) Datenschutz-Compliance / Reaktion der Aufsichtsbehörde

(unwirksame) Bestellung eines Datenschutzbeauftragten:

Reaktionsmöglichkeiten der Aufsichtsbehörde am Beispiel „Fall Unister“,

→ siehe dazu die aktualisierte Presseerklärung „ Der Sächsische Datenschutzbeauftragte vom 01.Februar 2013 (Anhang 3)

a) Rechte der Aufsichtsbehörde

aa) Auskunftsrechte (VG Dresden, Beschlüsse vom 03. u. 11.12.2012)

bb) So genannte Tiefenprüfung der Datenverarbeitung

cc) Informationspflicht des § 42 Satz 1 Nr. 4 a BDSG

b) (unwirksame) Bestellung eines Datenschutzbeauftragten

aa) gesetzliche Vorgaben zur Bestellung

bb) Erlass zur Anordnung eines (anderen) Datenschutzbeauftragten

3) Videoüberwachung

- Aktueller Bericht:

Ärger um Datenschutz beim DIHK:

Zwischen DIHK-Mitarbeitern und Hauptgeschäftsführer Wansleben gibt es Streit. Daten von Kameras und Chipkarten wurden wohl ohne Wissen der Mitarbeiter gespeichert. Datenschützer prüfen den Vorfall.

→ siehe „Die Welt" vom 16. Mär. 2013, Sie finden es online unter http://www.welt.de/114504491 (Anhang 4)

a) Grundzüge der Videoüberwachung

(Rechtsgrundlagen, Vorgabe an Videobeobachtung und -aufzeichnung, weitere Anforderungen des BDSG, Pflicht des Datenschutzbeauftragten zur Vorabkontrolle)

b) So genannte „offene" und „heimliche" Überwachung

c) Bedeutung des § 32 BDSG

d) neue Urteil des Bundesarbeitsgericht zur heimlichen Videoüberwachung

4) Besonderheiten zur Auftragsdatenverarbeitung

5) Abmahnung bei fehlendem Impressum auf der eigenen Webseite oder der Facebook-Seite

Anhang:

1) Vertrauliche Mitteilungen von Beschäftigten an die Datenschutz-Aufsichtsbehörden

Das VG Bremen hat in einer Entscheidung vom 30.03.2010 (Az.: 2 K 548/09) den Schutz von Informanten gestärkt: Wird in Unternehmen mit personenbezogenen Daten nachlässig umgegangen und wendet sich ein Beschäftigter vertraulich an die Datenschutz-Aufsichtsbehörde, hat der Arbeitgeber nach Ansicht des Gerichts keinen Anspruch auf die Preisgabe der Identität des Informanten gegenüber der Aufsichtsbehörde.

Der Sachverhalt

Der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen hatte von einem Beschäftigten des klagenden Unternehmens eine E-Mail mit dem Betreff „Videoüberwachung am Arbeitsplatz“ erhalten. Darin schilderte er, dass an seinem Arbeitsplatz eine ständige Überwachung mit zahlreichen Kameras erfolgte, ohne dass die Mitarbeiter darüber informiert worden wären. Eine akustische Überwachung und Aufzeichnung der Daten wollte er nicht ausschließen. Mit dem Hinweis, dass bislang aus Furcht vor Verlust des Arbeitsplatzes von niemandem etwas unternommen worden war und der Bitte, den Hinweis vertraulich zu behandeln, endete die Mitteilung.

Nachdem die Behörde das betreffende Unternehmen aufgefordert hatte, Auskunft zu den beschriebenen Vorgängen zu erteilen, verlangte dieses zunächst Akteneinsicht. Dem Verlangen kam die Aufsichtsbehörde nur teilweise nach. Die übersandten Unterlagen enthielten insbesondere keine Wiedergabe der E-Mail des Informanten. Außerdem war der Name des hinweisgebenden Beschäftigten in den übrigen Unterlagen geschwärzt. Beim Verwaltungsgericht Bremen wurde daraufhin durch das Unternehmen vollumfängliche Akteneinsicht bzw. Preisgabe des Namens des Informanten eingeklagt. Die Aufsichtsbehörde lehnte dies – aus Gründen des Informantenschutzes – ab und beantragte Klageabweisung.

Schutz von Informanten im Interesse des Datenschutzes

Dass mit Kenntniserlangung des Arbeitgebers von der Identität des Informanten negative Konsequenzen verbunden wären, liegt auf der Hand. Der Schutz von Informanten erfolgt aber nicht allein in deren Interesse, sondern auch um dem Datenschutzrecht zur Durchsetzung zu verhelfen. § 4 f Abs. 5 S. 2 BDSG sieht beispielsweise vor, dass sich jeder Betroffene an den unternehmenseigenen Datenschutzbeauftragten wenden kann. Gem. § 4 f Abs. 4 BDSG ist dieser dann zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

Mitteilung muss für den Betroffenen risikofrei sein

Die Mitteilung darf für den Betroffenen in jedem Fall nicht mit einem Risiko verbunden sein. Müssten betroffene Beschäftigte etwa um ihren Arbeitsplatz

fürchten, wenn sie sich an den Datenschutzbeauftragten oder die Aufsichtsbehörde wenden, blieben Missstände im Verborgenen.

Schutzbedürfnis besteht über die Dauer des Arbeitsverhältnisses hinaus
Besonders betont die Entscheidung, dass ein Schutzbedürfnis auch über die Dauer des Arbeitsverhältnisses hinaus bestehen kann. Selbst dann könne der Arbeitgeber noch Druck ausüben. Daneben droht natürlich gleichzeitig eine Rufschädigung, die sich insbesondere in kleinen Branchen sehr zum Nachteil des Betroffenen auswirken könnte.

Betroffene sind zu unterrichten
Neben der Identität des Informanten waren die Kläger auch daran interessiert, dass Dritte, insbesondere die von der Überwachungsmaßnahme betroffenen Beschäftigten, von der Überwachungsmaßnahme keine Kenntnis erlangen. Diesem Begehren stattzugeben sah sich das Gericht außer Stande, weil dies unvereinbar mit § 38 Abs. 1 S. 6 BDSG sei. Hiernach ist die Aufsichtsbehörde befugt, bei Feststellung eines Datenschutzrechtsverstoßes, die davon Betroffenen darüber zu unterrichten. Das Gericht teilte die Ansicht der hierüber im Eilverfahren vorab entscheidenden Kammer, dass Verstöße gegen datenschutzrechtliche Bestimmungen vorliegen würden.

Grenze für Schutzbedürftigkeit: strafbares Verhalten
Nur wer wider besseres Wissen und nur um seinem Arbeitgeber zu schaden, Datenschutzrechtsverstöße behauptet, muss grundsätzlich damit rechnen, dass diesem seine Identität mitgeteilt wird. Daneben ist auch der Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 UWG untersagt.

Entscheidung ist durchaus interessant für Arbeitgeber
Für Arbeitgeber ist die Entscheidung insofern interessant, als sie ausdrücklich auf die unternehmensrelevanten Vorschriften des BDSG hinweist. Angefangen von der Bestellung eines Datenschutzbeauftragten nach **§ 4 f BDSG** bis hin zur Meldepflicht für automatisierte Datenverarbeitungen nach §§ 4d, 4e BDSG hat es der Arbeitgeber selbst in der Hand für einen Betriebsablauf zu sorgen, der im Einklang mit dem Datenschutzrecht steht.

Fazit

Die Datenschutz-Aufsichtsbehörden haben die Identität von Informanten zu schützen. Arbeitgeber haben nach der Entscheidung grundsätzlich keinen Anspruch in Erfahrung zu bringen, welcher Beschäftigte sich vertraulich an die Aufsichtsbehörde gewandt hat. Eine Grenze bildet strafrechtlich relevantes Verhalten des Beschäftigten. Um derartige Streitigkeiten und die Konsequenzen aufsichtsrechtlichen Einschreitens zu vermeiden sollten Unternehmen nach Möglichkeit im Vorfeld für eine datenschutzkonforme Unternehmensorganisation sorgen.

2) Bundesrat macht Weg frei für neues Meldegesetz

Nach dem Bundestag hat am Freitag auch der Bundesrat dem Kompromissvorschlag zum neuen Melderecht aus dem Vermittlungsausschuss beider Gremien zugestimmt. Einwohnermeldeämter dürfen demnach persönliche Daten der Bürger nur dann an Firmen für Werbung und Adresshandel weitergeben, wenn die Betroffenen ausdrücklich eingewilligt haben. Die Bürger können generell gegenüber der Meldebehörde oder gesondert gegenüber Unternehmen zustimmen. Darin sehen Verbraucher- und Datenschützer ein Manko, da Firmen es mit dem Opt-in nicht so genau nehmen könnten.

Meldeämter sollen in Stichproben oder anlassbezogen prüfen, ob eine Einwilligungserklärung vorliegt. Zudem wird die Bundesregierung aufgefordert, die Bestimmungen "auf wissenschaftlicher Grundlage" vier Jahre nach Inkrafttreten des Bundesmeldegesetzes im Mai 2015 zu evaluieren und dem Parlament zu berichten.

Der Bundestag hatte mit dem Beschluss des ursprünglichen Textes während eines Halbfinalspiels der Fußball-WM nur ein lückenhaftes Widerspruchsrecht gegen den Transfer von Informationen wie Vor- und Familiennamen, akademischen Graden oder Anschriften an Marketingfirmen und Adresshändler verankern wollen.

Der Innenexperte der Grünen im Parlament, Konstantin von Notz, zeigte sich erleichtert, dass dieser "skandalöse Versuch" für ein großzügiges Geschenk an die Wirtschaft zu Lasten des Datenschutzes nun endgültig gescheitert sei.

Leider seien die von Schwarz-Gelb eingeführte Hotelmelde- und die Mitwirkungspflicht der Vermieter nicht Gegenstand des Vermittlungsverfahrens gewesen.

(*Stefan Krempl*) 01.03.2013 14:41, heise-online

http://www.heise.de/newsticker/meldung/Bundesrat-macht-Weg-frei-fuer-neues-Meldegesetz-1814903.html

3) „Unwirksame Bestellung des Datenschutzbeauftragten“

Der Sächsische Datenschutzbeauftragte in einer aktualisierten Presseerklärung vom 01. Februar 2013 zum Fall Unister

Presseerklärung zur aufsichtsbehördlichen Tätigkeit gegenüber Unternehmen der Unister-Unternehmensgruppe

1. Datenschutzrechtliche Auskünfte

Seit dem Sommer 2012 bemüht sich der Sächsische Datenschutzbeauftragte im Rahmen seiner Zuständigkeit als Datenschutzaufsichtsbehörde um eine Tiefenprüfung der Datenverarbeitung innerhalb der Unister-Unternehmensgruppe. Diese Tiefenprüfung kann derzeit nicht fortgesetzt werden, da Unister sich weigert, die zuletzt mit Heranziehungsbescheiden vom 14. August 2012 zwangsweise erbetenen Auskünfte zu erteilen, da sich das Unternehmen teils dem Grunde nach, teils dem Umfang nach, nicht dazu verpflichtet sieht.

Mit Beschlüssen vom 03. und 11. Dezember 2012 hat das Verwaltungsgericht Leipzig im einstweiligen Rechtsschutzverfahren Unisters Pflicht zur Auskunft bestätigt. Gegen die Entscheidungen hat Unister Beschwerde zum Oberverwaltungsgericht erhoben. Verstöße gegen die Auskunftspflicht können mit einem Bußgeld bis zu 50 000 Euro geahndet werden (§ 43 Abs. 1 Nr. 10 i. V. m. § 43 Abs. 3 Satz 1 Bundesdatenschutzgesetz – BDSG).

Wegen der nicht abgeschlossenen Tiefenprüfung können vom Sächsischen Datenschutzbeauftragten derzeit noch keine Aussagen zur Rechtmäßigkeit der Datenverarbeitung durch Unternehmen der Unister-Unternehmensgruppe getroffen werden.

2. Kein betrieblicher Datenschutzbeauftragter?

Der Sächsische Datenschutzbeauftragte ist der Auffassung, dass in den Unternehmen der Unister-Unternehmensgruppe entgegen der gesetzlichen Verpflichtung aus § 4f BDSG teils seit Jahren kein betrieblicher Datenschutzbeauftragter bestellt ist, da die Unternehmen einen wesentlichen Miteigentümer (Gesellschafter) mit dieser Funktion betraut haben.

Eine wirksame Bestellung liegt aber nur vor, wenn der bestellte Datenschutzbeauftragte nicht wegen eines anderen Interesses gehindert ist, seine Funktion zuverlässig und unabhängig auszuüben.

Im Fall der Unister-Unternehmensgruppe ist der (vermeintlich) Bestellte allerdings wegen seines eigenen finanziellen Interesses objektiv gehindert, die für die Aufgabe des betrieblichen Datenschutzbeauftragten notwendige Unabhängigkeit gegenüber dem wirtschaftlichen Interesse des auch ihm gehörenden Unternehmens aufzubringen, da es mit seinem finanziellen Interesse als Miteigentümer (bzw. Mitinhaber) identisch ist.

Der Sächsische Datenschutzbeauftragte hat daher gegen mehrere Unternehmen der Unister-Gruppe die Anordnung erlassen, einen (anderen) betrieblichen

Datenschutzbeauftragten zu bestellen. Gegen diese Anordnungen wehrt sich Unister derzeit vor dem Verwaltungsgericht Leipzig – eine Entscheidung des Gerichts steht derzeit noch aus. Eine (auch fahrlässig erfolgte) unwirksame Bestellung eines betrieblichen Datenschutzbeauftragten kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden (§ 43 Abs. 1 Nr. 2 i. V. m. § 43 Abs. 3 Satz 1 BDSG).

3. Anhaltspunkte für eine Verletzung der Informationspflicht

Im Dezember 2012 erhielt der Sächsische Datenschutzbeauftragte durch Medienberichte Hinweise darauf, Kreditkartendaten der Kunden von Unister könnten (auch mehrfach) wegen unzureichenden Sicherheitsvorkehrungen im Zahlungsverkehr unbefugt Dritten zur Kenntnis gelangt sein.

Gelangen Kreditkartendaten unrechtmäßig Dritten zur Kenntnis, sind darüber gemäß § 42a Satz 1 Nr. 4 BDSG unverzüglich die zuständige Datenschutzaufsichtsbehörde und die betroffenen Kunden zu informieren. Verstöße gegen die Mitteilungspflicht können mit einem Bußgeld bis zu 300 000 Euro geahndet werden (§ 43 Abs. 2 Nr. 7 i. V. m. § 43 Abs. 1 Satz 1 BDSG). Der Sächsische Datenschutzbeauftragte hat wegen des Sachverhaltes bußrechtliche Ermittlungen aufgenommen. Der Ausgang des Verfahrens ist offen.

4. Datenleck bei Flugbuchungen über www.urlaubstours.de

Der Sächsische Datenschutzbeauftragte hat nach dem öffentlichen Bekanntwerden einer Sicherheitslücke im Zusammenhang mit Ryanair-Flugbuchungen gegenüber der Unister-Tochter Urlaubstours GmbH am 4. Januar 2013 die unverzügliche Schließung der Sicherheitslücke angeordnet.

Dieser Anordnung hat Urlaubstours bisher nur teilweise nachkommen können, denn nach Angaben des Unternehmens ist eine anderweitige Zuordnung der Datensätze jedenfalls bei Kunden, deren Flugreise in der Vergangenheit liegt, allenfalls unter Mitwirkung von Ryanair möglich.

Der Sächsische Datenschutzbeauftragte steht daher mit beiden Unternehmen wegen einer kundenfreundlichen Lösung des Problems im Kontakt. Die unbefugte (auch fahrlässige) Übermittlung personenbezogener Daten ist ordnungswidrig und kann mit einem Bußgeld bis zu 300 000 Euro geahndet werden (§ 43 Abs. 2 Nr. 1 i. V. m. § 43 Abs. 1 Satz 1 BDSG).

4) Ärger um Datenschutz beim DIHK

Zwischen DIHK-Mitarbeitern und Hauptgeschäftsführer Wansleben gibt es Streit. Daten von Kameras und Chipkarten wurden wohl ohne Wissen der Mitarbeiter gespeichert. Datenschützer prüfen den Vorfall**.** Von Hans Evert

In einem der wichtigsten deutschen Wirtschaftsverbände gibt es Unruhe in Teilen der Belegschaft. Mitarbeiter und der Hauptgeschäftsführer des Deutschen Industrie- und Handelskammertages (DIHK), Martin Wansleben, liegen im Streit. Wanslebens Führungsstil gilt intern als nicht unumstritten. Nun sorgt eine fehlende Betriebsvereinbarung für zusätzlichen Ärger. Konkret geht es um Schutz von Mitarbeiterdaten.

Wie heutzutage in vielen Unternehmen üblich, haben die mehr als 200 DIHK-Mitarbeiter Chipkarten. Damit öffnet sich die Eingangsschranke zum Haus der Wirtschaft, die Zeiterfassung wird dadurch aktiviert, Beträge fürs Kantinenessen abgebucht. Beim DIHK öffnen sich zudem die Türen zu einzelnen Etagen im Bürohaus, Tiefgarage sowie Konferenzzentrum nur mit Hilfe der Karte.

Was Mitarbeiter bis vor kurzem nicht wussten: Die Daten – wer öffnet wann und wo eine Tür im Haus – werden für jeden Mitarbeiter sechs Monate lang gespeichert. Zwei Wochen lang bleiben Aufnahmen der Überwachungskameras erhalten, die sich an vielen Stellen im DIHK befinden.

Zudem sollen diese Mitarbeiterdaten bei einem externen Unternehmen gespeichert sein, dass Gebäude- und Sicherheitsdienstleistungen im Haus der Deutschen Wirtschaft erbringt.

In dem Haus an der Breiten Straße in Mitte sitzen zudem der Bundesverband der Deutschen Industrie (BDI) und die Bundesvereinigung der DEutschen Arbeitgeberverbände (BDA).

Bei Rechtsstreit kam Datensammlung ans Licht

Intern bekannt wurde das Thema auf einer DIHK-Betriebsversammlung am 20. Dezember vergangenen Jahres. Dort kam unter anderem ein Rechtsstreit mit einer früheren Mitarbeiterin zur Sprache. Der Frau war wegen Arbeitszeitbetrug gekündigt wurde.

Im Zuge dieses Rechtsstreits wurde offenbar, wie umfangreich die Datenerfassung beim DIHK ist. Teilnehmern zufolge wurde es auf der Betriebsversammlung "sehr lebhaft", als das Thema zur Sprache kam. Befragt nach dem Grund der Kamera- und Sicherheitssysteme habe Wansleben sinngemäß geantwortet: Damit seine Frau im Falle eines Anschlags auf ihn erfahre, wer der Täter sei.

Warum die Daten so detailliert sind, warum sie sechs Monate lange gespeichert werden und wer eigentlich Zugriff darauf – diese Fragen lässt DIHK-Geschäftsführer Wansleben unbeantwortet. Auch auf Nachfrage der "Berliner Morgenpost". Ein DIHK-Sprecher: "Die Sicherheitseinbauten dienen allein dem Schutz der Mitarbeiterinnen und Mitarbeiter, der Gäste sowie des gesamten Gebäudes. Bewegungsprofile wurden und werden im DIHK nicht erstellt."

Zudem sollen diese Mitarbeiterdaten bei einem externen Unternehmen gespeichert sein, dass Gebäude- und Sicherheitsdienstleistungen im Haus der Deutschen Wirtschaft erbringt.

In dem Haus an der Breiten Straße in Mitte sitzen zudem der Bundesverband der Deutschen Industrie (BDI) und die Bundesvereinigung der DEutschen Arbeitgeberverbände (BDA).

Bei Rechtsstreit kam Datensammlung ans Licht

Intern bekannt wurde das Thema auf einer DIHK-Betriebsversammlung am 20. Dezember vergangenen Jahres. Dort kam unter anderem ein Rechtsstreit mit einer früheren Mitarbeiterin zur Sprache. Der Frau war wegen Arbeitszeitbetrug gekündigt wurde.

Im Zuge dieses Rechtsstreits wurde offenbar, wie umfangreich die Datenerfassung beim DIHK ist. Teilnehmern zufolge wurde es auf der Betriebsversammlung "sehr lebhaft", als das Thema zur Sprache kam. Befragt nach dem Grund der Kamera- und Sicherheitssysteme habe Wansleben sinngemäß geantwortet: Damit seine Frau im Falle eines Anschlags auf ihn erfahre, wer der Täter sei.

Warum die Daten so detailliert sind, warum sie sechs Monate lange gespeichert werden und wer eigentlich Zugriff darauf – diese Fragen lässt DIHK-Geschäftsführer Wansleben unbeantwortet. Auch auf Nachfrage der "Berliner Morgenpost". Ein DIHK-Sprecher: "Die Sicherheitseinbauten dienen allein dem Schutz der Mitarbeiterinnen und Mitarbeiter, der Gäste sowie des gesamten Gebäudes. Bewegungsprofile wurden und werden im DIHK nicht erstellt."

Ab 2004 nahm der DIHK "Sicherheitseinbauten" vor

Die veränderte Sicherheitslage führt der DIHK als Grund dafür an, dass in den Jahren 2004 und 2006 "Sicherheitseinbauten" vorgenommen wurden. Die Mitarbeiter seien über die Umbauten informiert worden. Was mit den Daten geschieht, wurde nicht erwähnt. Genau das hätte nach dem Betriebsverfassungsgesetz (Paragraf 87 Absatz 1 Nr. 6) seit mindestens neun Jahren passieren müssen.

Eine entsprechende Vereinbarung will der DIHK nun mit den Belegschaftsvertretern nachträglich abschließen. Beim Berliner Datenschutzbeauftragten interessiert man sich bereits dafür, was beim DIHK los ist. "

17. Mär. 2013, 18:34

Diesen Artikel finden Sie online unter

http://www.welt.de/114504491

Zulässigkeit der verdeckten Videoüberwachung von Mitarbeitern

Das Bundesarbeitsgericht (BAG) hat festgestellt, dass die verdeckte Videoüberwachung von Mitarbeitern durch den Arbeitgeber in öffentlichen Betriebsräumen trotz eines Verstoßes der Regelung in § 6b Abs. 2 BDSG zulässig sein kann (Urteil vom 21.06.2012 – Aktz.: 2 AZR 153/11).

Eines der am häufigsten diskutierten Themen des Beschäftigtendatenschutzes ist die Zulässigkeit der Videoüberwachung von Mitarbeitern durch den Arbeitgeber. Der Einsatz von Videoüberwachung kann vielfältig sein, so bspw. zur Prävention oder Aufklärung von Straftaten, zu bloßen Überwachungszwecken der Belegschaft oder der Wahrung des Hausrechts des Arbeitsgebers. Eine spezialgesetzliche Regelung für die Videoüberwachung gibt es bisher nicht. Die Zulässigkeit der Videoüberwachung beurteilt sich nach den einschlägigen Normen des Bundesdatenschutzgesetzes (BDSG) insbesondere den §§ 4 Abs. 1, 6b, 32 BDSG.

Generell wird unterschieden zwischen der offenen und der verdeckten Videoüberwachung sowie ob die Überwachung in öffentlich zugänglichen Räumen stattfindet oder in Räumlichkeiten, die nur einem beschränkten Personenkreis zugänglich sind.

Das BAG hatte zu entscheiden, ob eine verdeckte Videoüberwachung in öffentlich zugänglichen Räumen des Betriebs des Arbeitgebers zulässig ist, obwohl der Arbeitgeber das in § 6b Abs. 2 BDSG geregelte Gebot bei Videoaufzeichnungen öffentlich zugänglicher Räume den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen kenntlich zu machen, missachtet hat.

Der Arbeitgeber, ein Einzelhandelsunternehmen, hatte in dem der Entscheidung zu Grunde liegenden Fall seine öffentlichen Verkaufsräume mit einer heimlichen Videoüberwachung ausgestattet. Nach Auswertung des Filmmaterials kündigte der Arbeitgeber einer Mitarbeiterin mit dem Vorwurf, sie habe sich unrechtmäßig Zigaretten angeeignet.

Nach der herrschenden Rechtsprechung hat das BAG zunächst festgestellt, dass die heimliche Videoüberwachung eines Arbeitnehmers zulässig ist, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zulasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit praktisch das einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.

Der Verdacht muss in Bezug auf eine **konkrete strafbare Handlung oder andere schwere Verfehlungen** zulasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern bestehen. Er darf sich *nicht auf allgemeine Mutmaßungen* beschränken, es könnten Straftaten begangen werden. Der Verdacht muss sich jedoch nicht notwendig nur gegen einen einzelnen, bestimmten Arbeitnehmer richten. Weniger einschneidende Mittel als eine verdeckte Videoüberwachung müssen zuvor ausgeschöpft worden sein.

Vorliegend hatte der beklagte Arbeitgeber bei der Installation des Überwachungssystems in seinen Geschäftsräumen § 6b Abs. 2 BDSG, den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen, nicht beachtet. Daraus folgt aber nicht automatisch, so das BAG, dass die Videoüberwachung gänzlich unzulässig sei. Das BAG hat sich nicht derjenigen Rechtsauffassung angeschlossen, dass eine verdeckte Videoüberwachung in öffentlich zugänglichen Räumen ausnahmslos unzulässig sei, wenn die Voraussetzungen des § 6b Abs. 2 BDSG nicht eingehalten sind.

Die Kammer führt in diesem Zusammenhang aus, dass für den Fall, dass die verdeckte Videoüberwachung das **einzige Mittel zur Überführung von Arbeitnehmern** ist, die der Begehung von Straftaten konkret verdächtig sind, auch eine heimliche Videoaufzeichnung in öffentlich zugänglichen Räumen nach § 6b Abs. 1 Nr. 3 BDSG zulässig sein kann.

Das Kennzeichnungsgebot nach § 6b Abs. 2 BDSG ist weder in § 6b Abs. 1 BDSG noch in § 6b Abs. 3 BDSG als Voraussetzung für die Zulässigkeit einer Verarbeitung oder Nutzung von nach § 6b Abs. 1 BDSG erhobenen Daten aufgeführt. Ebenso wenig ergibt sich aus der Gesetzesbegründung zu § 6b BDSG, dass die Einhaltung des Gebots nach § 6b Abs. 2 BDSG Voraussetzung für die materiell-rechtliche Zulässigkeit der Maßnahme wäre. Ein vollständiges Verbot der verdeckten Videoüberwachung öffentlich zugänglicher Verkaufsräume würde verfassungsrechtlichen Bedenken begegnen, so die entscheidende Kammer des BAG.

Die Voraussetzungen für die Zulässigkeit der verdeckten Videoüberwachung in öffentlich zugänglichen Räumen sind hoch. Das BAG hat die strengen Voraussetzungen für eine verdeckte Überwachung dahingehend bestätigt, dass diese „notwehrähnlich“ den Notstandsvoraussetzungen der §§ 34 StGB bzw. 228 BGB entsprechen müssen.

Fazit:

In der Entscheidung bestätigt das BAG erstmalig, dass die verdeckte, heimliche Videoüberwachung in öffentlich zugänglichen Räumen des Betriebs des Arbeitgebers zulässig sein kann.

Das Urteil beseitigt daher eine bisher strittige Rechtsfrage. Die Voraussetzungen für diese Form der Videoüberwachung sind freilich hoch. Bleibt aber diese Form der Überwachung das einzige Mittel des Arbeitgebers, den Beweis für eine strafbare Handlung von Mitarbeitern zu führen, so ist die Überwachung zulässig, wenn die jederzeit vorzunehmende Interessenabwägung der durch das Grundgesetz geschützten Interessen der Arbeitsvertragsparteien zu Gunsten des Arbeitgebers zu entscheiden ist.

Berlin, 11. Oktober 2012

Von RA Christian Willert, Kanzlei Härting

Auszug aus dem Telemediengesetz (TMG):

Abschnitt 1 Allgemeine Bestimmungen

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

(2) Dieses Gesetz gilt nicht für den Bereich der Besteuerung.

(3) Das Telekommunikationsgesetz und die Pressegesetze bleiben unberührt.

(4) Die an die Inhalte von Telemedien zu richtenden besonderen Anforderungen ergeben sich aus dem Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag).

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert,
2. ist niedergelassener Diensteanbieter jeder Anbieter, der mittels einer festen Einrichtung auf unbestimmte Zeit Telemedien geschäftsmäßig anbietet oder erbringt; der Standort der technischen Einrichtung allein begründet keine Niederlassung des Anbieters,
3. ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen,
4. sind Verteildienste Telemedien, die im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Anzahl von Nutzern erbracht werden,
5. ist kommerzielle Kommunikation jede Form der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dient, die eine Tätigkeit im Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt; die

Übermittlung der folgenden Angaben stellt als solche keine Form der kommerziellen Kommunikation dar:

a) Angaben, die unmittelbaren Zugang zur Tätigkeit des Unternehmens oder der Organisation oder Person ermöglichen, wie insbesondere ein Domain-Name oder eine Adresse der elektronischen Post,

b) Angaben in Bezug auf Waren und Dienstleistungen oder das Erscheinungsbild eines Unternehmens, einer Organisation oder Person, die unabhängig und insbesondere ohne finanzielle Gegenleistung gemacht werden.

6. sind „audiovisuelle Mediendienste auf Abruf" Telemedien mit Inhalten, die nach Form und Inhalt fernsehähnlich sind und die von einem Diensteanbieter zum individuellen Abruf zu einem vom Nutzer gewählten Zeitpunkt und aus einem vom Diensteanbieter festgelegten Inhaltekatalog bereitgestellt werden.

Einer juristischen Person steht eine Personengesellschaft gleich, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

§ 2a Europäisches Sitzland

(1) Innerhalb des Geltungsbereichs der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (ABl. EG Nr. L 178 vom 17.7.2000, S. 1) bestimmt sich das Sitzland des Diensteanbieters danach, wo dieser seine Geschäftstätigkeit tatsächlich ausübt. Dies ist der Ort, an dem sich der Mittelpunkt der Tätigkeiten des Diensteanbieters im Hinblick auf ein bestimmtes Telemedienangebot befindet.

(…)

§ 3 Herkunftslandprinzip

(1) In der Bundesrepublik Deutschland nach § 2a niedergelassene Diensteanbieter und ihre Telemedien unterliegen den Anforderungen des deutschen Rechts auch dann, wenn die Telemedien in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG geschäftsmäßig angeboten oder erbracht werden.

(2) Der freie Dienstleistungsverkehr von Telemedien, die in der Bundesrepublik Deutschland von Diensteanbietern geschäftsmäßig angeboten oder erbracht werden, die in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG niedergelassen sind, wird nicht eingeschränkt. Absatz 5 bleibt unberührt.

(3)… (5)

Abschnitt 2 Zulassungsfreiheit und Informationspflichten

§ 4 Zulassungsfreiheit

Telemedien sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 5 Allgemeine Informationspflichten

(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,
2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,
3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,
4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,
5. soweit der Dienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25, 1995 Nr. L 17 S. 20), zuletzt geändert durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. L 184 S. 31), angeboten oder erbracht wird, Angaben über

a) die Kammer, welcher die Diensteanbieter angehören,

b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,

c) die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,

6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,
7. bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, die Angabe hierüber.

(2) Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt.

§ 6 Besondere Informationspflichten bei kommerziellen Kommunikationen

(1) Diensteanbieter haben bei kommerziellen Kommunikationen, die Telemedien oder Bestandteile von Telemedien sind, mindestens die folgenden Voraussetzungen zu beachten:

1. Kommerzielle Kommunikationen müssen klar als solche zu erkennen sein.
2. Die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen, muss klar identifizierbar sein.
3. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke müssen klar als solche erkennbar sein, und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.
4. Preisausschreiben oder Gewinnspiele mit Werbecharakter müssen klar als solche erkennbar und die Teilnahmebedingungen leicht zugänglich sein sowie klar und unzweideutig angegeben werden.

(2) Werden kommerzielle Kommunikationen per elektronischer Post versandt, darf in der Kopf- und Betreffzeile weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

(3) Die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb bleiben unberührt.

Abschnitt 3 Verantwortlichkeit

§ 7 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.