

Mit freundlicher Unterstützung von

BRENNECKE & PARTNER

RECHTSANWÄLTE



Mittelstand und Recht

Ausgabe 2/2011 · 7,90 € (Deutschland)

Im Urwald der Datenschutzregelungen: Was darf der Arbeitgeber?

Der Administrator hat alle Rechte – aber hat er auch das Recht?

Private E-Mail im Unternehmensnetzwerk – Archivierung verboten?

SCHUFA, Creditreform und Co. – Prüfen Sie ihre Daten!

Kostenlos ist nicht umsonst – Web-Analyse-Systeme im Vergleich.

Herausgeber:

DMA | Deutsche
Mittelstandsakademie

EDITORIAL

Datenerfassung und der Schutz von Daten sind der Schwerpunkt dieser Ausgabe. Bei der Planung für diese Ausgabe war mir gar nicht bewusst, wo es überall mögliche Probleme geben kann. Deshalb beschäftigt sich diese Ausgabe – anders als sonst – nahezu ausschließlich mit diesem Thema.

Ist Ihnen z. B. bewusst, welche Daten – auch ohne Ihr Wissen - von Schufa, Creditreform etc. erfasst und weitergegeben werden? Oder wie Institutionen wie Krankenkassen und Banken mit Daten umgehen? Welche Daten wie archiviert werden oder wie Sie Ihre Kundendaten vor Missbrauch durch Mitarbeiter schützen können?

Klaus Eppele ist unser aktueller Künstler. Ein Kurzporträt finden Sie auf Seite 31.

Ihre Dr. Maren Augustin, Chefredakteurin



INHALT

SCHLAGLICHT

Wissen ist Macht.

Von Harald Brennecke

3

RECHT FÜR UNTERNEHMER

Im Urwald der Datenschutzregelungen: Was darf der Arbeitgeber? Von Rechtsanwältin Dr. Maren Augustin, Hamburg

4

Arbeitnehmerdatenschutz – aktuelle Rechtslage und Ausblick in die Zukunft

Von Rechtsanwalt Christoph Lattreuter, Berlin

6

Kundendaten im Bankgeschäft- weshalb, warum, wofür?

Von Dirk Wittich, Hamburg

8

SCHUFA, Creditreform und Co. – Prüfen Sie ihre Daten!

Von Rechtsanwalt Andreas Albrecht, Hamburg

9

Der Administrator hat alle Rechte – aber hat er auch das Recht?

Rechtsanwalt Guido-Friedrich Weiler, Bonn

11

Private E-Mail im Unternehmensnetzwerk –

Archivierung verboten?

Von Rechtsanwalt Glenn D. Büllsfeld, Hamburg

13

Kundendaten – Schutz für den Schatz

Von Rechtsanwalt Harald Brennecke, Karlsruhe

14

Kompetenzmessinstrumente, Datenschutz und Betriebsvereinbarung. Von Rechtsanwalt Martin Kull, Baden Baden

18

Die Buchführung wird digital!

Von Klaus Buser, Karlsbad

19

Kostenlos ist nicht umsonst – Web Analyse Systeme im Vergleich

Von Christian Bennefeld, Hamburg

20

SERIEN

Der Modernisierungsbegriff im WEG-Recht –

einvernehmliche Übertragung

Von Rechtsanwalt Peter Hesse, Potsdam

22

RECHTSINFOS

„Compliance“ – braucht mein Unternehmen so etwas?

Von Rechtsanwältin Anja Uelhoff, Hamburg

23

Führung - ist nicht nur Chefsache, Führung ist auch Gehirnsache

Von Rechtsanwältin Friederike Matheis, Hamburg

25

Vereinsmitgliedschaft – in steuerrechtlicher Hinsicht

Von Rechtsanwalt Marc Y. Wandersleben, Hannover

27

Private Krankenversicherungen - (k)eine gute Wahl?

Von Rechtsanwältin Dr. Birgit Schröder, Hamburg

28

NEWS

30

KUNST IM MAGAZIN

Malerei von Klaus Eppele

31

IMPRESSUM

31



Wissen ist Macht. Marktwissen ist Marktmacht.

Wer heute genau weiß, wie sich die Märkte entwickeln und wo Nachfrage nach welchen Produkten besteht, hat einen großen Marktvorteil gegenüber der Konkurrenz. Wer früher als andere weiß, wie eine Börse auf der anderen Seite der Welt agiert, kann aus diesen Wissensvorsprung Millionen machen.

Die Infrastruktur zur Abwicklung von Börsengeschäften wird inzwischen technisch so optimiert, dass die Auswahl eines Rechenzentrums nach der optimal kurzen Laufzeit der Datenleitungen zwischen den Börsen gewählt wird: Hier zählen Mikrosekunden. Dasselbe Prinzip betrifft uns alle in unserem Alltag. Das Wissen über unsere Wünsche, unsere Sorgen, unsere Bedürfnisse und Interessen, ist Milliarden wert.

Inzwischen gibt es jemanden, der all das ganz genau weiß, genauer als jeder andere. Wir offenbaren unsere Gedanken, unsere Fragen, unsere Bedürfnisse täglich in Suchmaschinen ein – milliardenfach. Dieses Wissen wird gesammelt, aufbereitet, analysiert.

Jede Eingabe in eine Suchmaschine, jeder Klick auf einen bestimmten angezeigten Eintrag dazu, jeder Chat offenbart, was uns gerade beschäftigt. Selbst wenn dies nicht für eine einzelne Person gesammelt wird, sondern nur Personengruppen, beispielsweise aus einem Einzugsbereich eines Internetknotens, zusammengefasst werden, ist das so genau, dass Google besser als jede staatliche ärztliche Einrichtung feststellen kann, in welchem Ortsteil einer Stadt gerade eine Grippeepidemie beginnt.

Dass Google mit der Anzeige von Werbung neben Sucheinträgen Milliarden scheffelt, sei gegönnt. Wo-

vor ich wirklich Angst habe, ist dass Google aufgrund des Wissensvorsprungs, was wir Menschen gerade wo und in welcher Form suchen, genau weiß, wie sich Märkte entwickeln. Grob und dennoch richtig formuliert: Google kann sich damit die Welt kaufen.

Anstatt nun darüber zu lamentieren, dass dieses Wissen in der Welt ist, und darüber zu philosophieren, wie man dieses Wissen kontrollieren kann, so dass nicht ein einzelnes Unternehmen Vorteile aus diesem Wissen ziehen kann, hier ein radikal anderer Vorschlag:

Wie wäre es, wenn jedes Unternehmen, jeder Unternehmer und jeder Anbieter uneingeschränkter Zugriff darauf hätte, welche Suchbegriffe gerade wo und wie häufig eingegeben werden, und wie sich die Nachfrage nach bestimmten Suchbegriffen verändert? Jeder Anbieter könnte die Bedürfnisse der Nachfrageseite wesentlich besser erfassen. Wir hätten damit die Möglichkeit, die Produktion genauer auf Bedürfnisse der Menschen abzustimmen und Angebote von richtigen Dingen am falschen Ort deutlich zu verringern.

Eine grobe Vorstellung, wie so etwas aussehen könnte, gibt Google mit dem Tool „Trends“. Hier werden Suchbegriffe nach Häufigkeit angezeigt.

Die Nennung des Begriffs „Insolvenz“



in Deutschland hatte in 2009 durch die Finanzkrise eine deutliche Nachfragesteigerung um 50 % im Mittel und 100 % in den Spitzen. (Bild von Google Trends für den Begriff „Insolvenz“ in Deutschland).

Ich fände das charmant:

Mal etwas nicht verbieten und kontrollieren, sondern fruchtbar für alle nutzen. Marktwirtschaft funktioniert gesund, wenn alle dasselbe Recht und dieselbe Möglichkeit haben, auf dieses Wissen zuzugreifen. Gebt den Firmen eine Schnittstelle, mit der sie automatisch nach (Suchbegriff-) Nachfrageveränderungen suchen können.

Google bietet eingeloggten Usern heute bereits an, einzelne Begriffe mit fixen Skalierungen als Exceltabellen herunterladen. Danke Google. Trotzdem: Der potenzielle Wissensvorsprung bei systematischer Auswertung ist derart gigantisch, das Missbrauchsrisiko ist so immens, dass hier eine gesetzliche Regelung sinnvoll wäre. Diese Daten gehen uns alle an.

Was meinen Sie?

Neugierige Grüße,
Ihr Harald Brennecke
brennecke@brennecke-partner.de

Im Urwald der Datenschutzregelungen: Was darf der Arbeitgeber?

Ein Arbeitnehmer ist besonders schutzbedürftig. Dies ergibt sich aus den Besonderheiten des Arbeitsverhältnisses: Zwar stehen sich Arbeitgeber und Arbeitnehmer nach allgemeinem Verständnis als gleichwertige Partner gegenüber. Die Praxis zeigt jedoch, dass der Arbeitgeber zumeist wirtschaftlich und strukturell überlegen ist.

Der Arbeitgeber bestimmt die konkrete Ausgestaltung des Arbeitsvertrags und legt die Arbeitsbedingungen fest. Der Arbeitnehmer kann sich diesen Vorgaben in der Regel nicht entziehen. Diese Gegebenheiten müssen insbesondere in einem sensiblen Bereich wie dem Datenschutzrecht berücksichtigt werden. Das Recht des Arbeitnehmers, selbst darüber zu bestimmen, ob und welche seiner persönlichen Daten er anderen anvertraut, trifft auf das Weisungsrecht des Arbeitgebers. Der Arbeitnehmerdatenschutz versucht einen Ausgleich zwischen diesen unterschiedlichen Interessen zu finden. Letztendlich geht es um die Frage, welche Eingriffe des Arbeitgebers in das informationelle Selbstbestimmungsrecht und das Persönlichkeitsrecht des Arbeitnehmers zulässig sind.

Derzeit 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.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Die Erhebung, Verarbeitung oder Nutzung der Daten muss zur Aufdeckung der Straftat erforderlich sein. Dabei darf das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der

Erhebung, Verarbeitung oder Nutzung nicht überwiegen, insbesondere dürfen Art und Ausmaß der Datenerhebung im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Bei der Beurteilung der Zulässigkeit von Datenerhebungen ist auf zwei Tatbestandsmerkmale abzustellen: Verwendungszweck und Erforderlichkeit.

Zur Durchführung des Arbeitsverhältnisses bestimmt sind beispielsweise Daten, die der Arbeitgeber zur Erfüllung seiner Pflichten, aber auch zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt. Gestattet sind auch Maßnahmen zur Kontrolle, ob der Arbeitnehmer den geschuldeten Pflichten nachkommt. So darf der Arbeitgeber neben den Daten über die Person des Betroffenen (Name, Alter, Beruf etc.) auch solche über dessen Qualifikation und Einsatzfähigkeit speichern und nutzen. Es dürfen alle Stammdaten gespeichert werden, die für den zukünftigen Verlauf des Arbeitsverhältnisses von Bedeutung werden können (z. B. auch Familienstand für künftig notwendige Sozialauswahl).

Erforderlich sind Datenerhebungen, die für das Arbeitsverhältnis als geboten und nicht nur als „nützlich“ zu bewerten sind. Diese Voraussetzung ist nicht erfüllt, wenn von mehreren gleichermaßen wirksamen Maßnahmen die den Arbeitnehmer stärker belastende gewählt wird. Auch insoweit gilt das Gebot der Datensparsamkeit.

Immer wieder diskutiert wird das als „Fragerecht“ bezeichnete Datenerhebungsrecht des Arbeitgebers gegenüber Bewerbern und Arbeit-

nehmern. Maßgebend ist hier der Bezug zum konkreten Arbeitsverhältnis. So sind eventuelle Vorstrafen nur relevant, wenn sie Bezug zu der vom Arbeitnehmer zu übernehmenden Tätigkeit haben. Gleiches gilt für die Nachfrage nach gesundheitlichen Handicaps. Das zuletzt bezogene Gehalt hat den Arbeitgeber nur dann zu interessieren, wenn die Information für die Einstellungsentscheidung bzw. die auszuhandelnden vertraglichen Konditionen von Belang ist. Private Telefonnummern der Mitarbeiter sind in der Regel für das Arbeitsverhältnis nicht relevant und daher nur in solchen Fällen zu speichern, in denen dienstliche Interessen bestehen, z. B. bei Rufbereitschaft. Unzulässig ist die Erhebung oder Verwendung von Daten, die zu einer nach dem Allgemeinen Gleichbehandlungsgesetz untersagten Diskriminierung führen würde. Da die Schwangerschaft einer Bewerberin bei der Einstellungsentscheidung wegen der damit verbundenen unzulässigen geschlechtsbezogenen Diskriminierung keine Rolle spielen darf, ist auch das Erheben des Datums vor Abschluss des Arbeitsvertrages unzulässig. Gleiches muss für die Ableistung der Wehrpflicht gelten. In jedem Falle hat der Arbeitgeber kein berechtigtes Interesse zu erfahren, ob der Bewerber Wehr- oder Ersatzdienst geleistet hat. Aufgrund des Diskriminierungsverbots ist auch die Frage nach der Zugehörigkeit zu einer Gewerkschaft oder das Verlangen nach Bekanntgabe der Namen von Betriebsangehörigen Gewerkschaftsmitgliedern zum Nachweis des Zugangsrechts der Gewerkschaft unzulässig.

Erhoben werden dürfen Daten über Tatsachen, die die Verwirklichung des Vertragszwecks gefährden können.

ten, also auch tatsächliche oder vermeintliche Verletzungen der dem Vertragspartner obliegenden Verpflichtungen. So entspricht es z. B. dem berechtigten Interesse des Arbeitgebers, durch Erhebung von Daten über Krankentage festzustellen, inwieweit das Austauschverhältnis zwischen Arbeitsleistung gegen Lohnzahlung durch Krankheits- und Fehlzeiten gestört ist. Die erheblich intensiver in die Rechte des Arbeitnehmers eingreifende Krankenkontrolle, die ggf. unter Einsatz von Detektiven erfolgt, ist erst dann zulässig, wenn ein konkreter Verdacht für unberechtigtes Fehlen besteht.

In der Praxis bedeutsam ist auch die Frage, in welchem Umfang der Arbeitgeber das Arbeitsverhalten der Beschäftigten beim Einsatz von Medien am Arbeitsplatz kontrollieren darf. Bei der Telefondatenerfassung ist die Kosten- und Wirtschaftlichkeitskontrolle und der Schutz vor Missbrauch (z. B. unerlaubtes Führen von Privatgesprächen) als legitime Zweckbestimmung anerkannt. Eine darüber hinausgehende Zusammenführung der Daten zu „Profilen des Arbeitsverhaltens“ ist jedoch unzulässig. Die Kontrolle des dienstlichen E-Mail-Verkehrs, der grundsätzlich wie dienstlicher Briefverkehr behandelt werden kann, ist ebenfalls zulässig.

Aber Vorsicht: Gestattet der Arbeitgeber die Nutzung der betrieblichen Telekommunikation (Telefon, Email, Internet) auch für private Zwecke, unterliegt er insoweit den bereichsspezifischen Datenschutzregelungen des Telekommunikationsgesetzes bzw. des Telemediengesetzes (insbesondere Fernmeldegeheimnis).

Bei der Videoüberwachung von Arbeitnehmern ist das Kontrollinteresse des Arbeitgebers mit dem Persönlichkeitsrechtsschutz des Arbeitnehmers abzuwägen. Eine heimliche Überwachung ist jedenfalls nur zur Aufdeckung von Straftaten gerechtfertigt.

Eine besondere Problematik ergibt sich durch das Einstellen von Personaldaten in das Internet. Trotz der grundsätzlichen Vertraulichkeit von Personaldaten ist die Veröffentlichung von Mitarbeiterdaten in herkömmlicher Form (Briefbögen, Prospekten, (Vorlesungs-)Verzeichnissen, Werkszeitungen etc.) zulässig, wenn dies in der Zweckbestimmung des Arbeitsverhältnisses liegt oder infolge gesetzlicher Publikationspflicht (z. B. Geschäftsführer einer GmbH) erforderlich ist. Ansonsten wird die Erforderlichkeit einer weltweiten Verbreitung der Daten an jedermann selten zu begründen sein. Dann be-

darf die Maßnahme der Einwilligung des Betroffenen. Bei der Abbildung von Mitarbeitern ist im Hinblick auf ihr Recht am eigenen Bild generell eine Einwilligung erforderlich. In jedem Fall sollte eine Interessenabwägung hinsichtlich der gegenseitigen Rechte und Pflichten der Parteien erfolgen.

Ausblick:

Die Bundesregierung hat die Arbeit an einem seit Jahrzehnten geforderten umfassenden Arbeitnehmerdatenschutzgesetz wieder aufgenommen. Mit dem Entwurf über ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollen Lücken im geltenden Recht geschlossen werden. Einen Überblick über die geltenden und geplanten gesetzlichen Bestimmungen finden Sie in dem Aufsatz von Rechtsanwalt Lattreuter auf den folgenden Seiten dieser Ausgabe.

Rechtsanwältin Dr. Maren Augustin,
Fachanwältin für Insolvenzrecht,
Hamburg.

Rechtsanwältin Dr. Augustin ist
Partnerin der überörtlichen Rechts-
anwaltskanzlei Brennecke & Partner
Mail: augustin@brennecke-partner.de

Ann Sohns, wissenschaftliche
Mitarbeiterin, Hamburg



Arbeitnehmerdatenschutz – aktuelle Rechtslage und Ausblick in die Zukunft.

Trotz großer praktischer Bedeutung des Arbeitnehmerdatenschutzes war dieser in Deutschland bis 2009 nicht ausdrücklich geregelt. Vielmehr griff die Rechtsprechung auf die allgemeinen Regelungen des Datenschutzgesetzes (BDSG) zurück. Erst durch Datenschutzaffären des Lebensmittelkonzerns Lidl, der Deutschen Bahn und der Deutschen Telekom rückte der Arbeitnehmerdatenschutz wieder in den Fokus der öffentlichen Wahrnehmung. Alle drei Unternehmen waren 2008/2009 in die Schlagzeilen geraten, weil sie systematisch Mitarbeiter bespitzelten und Details aus deren Privatleben protokollieren ließen. Im Wege dieser Affären verlor sowohl der damalige Bahn-Chef Hartmut Mehdorn als auch der Deutschlandchef von Lidl Frank-Michael Mros ihre Jobs.

Aufgrund dieser Affären ist der allgemeine Datenschutz bei Arbeitnehmern durch den § 32 BDSG gesetzlich verstärkt worden, der in seinem wichtigen Absatz 1 folgendes gesetzlich regelt:

Personenbezogene Daten eines Beschäftigten dürfen 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. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Durch Grundsatzurteile des Bundesverfassungsgerichtes und des zuständigen Bundesarbeitsgerichtes ist es inzwischen unstrittig, dass es arbeitgeberseitig nur in sehr engen Grenzen erlaubt ist, Telefongespräche oder nicht-öffentliche Gespräche

mitzuhören oder den Arbeitnehmer durch Videoüberwachung am Arbeitsplatz zu überwachen.

Üblicherweise werden datenschutzrechtlich relevante Sachverhalte, z. B. Videoüberwachung am Arbeitsplatz bei Verdachtsfällen von Straftaten, Nutzung von Internet und Emails am Arbeitsplatz, Verwendung der Daten von Zeiterfassungssystemen und elektronischen Zutrittskontrollen heute in größeren Unternehmen einvernehmlich zwischen Betriebsrat und Unternehmensführung im Wege von Betriebsvereinbarungen einvernehmlich geregelt. Sollte kein Betriebsrat vorhanden sein, so empfehlen sich entsprechende Regelungen im Arbeitsvertrag.

Welche Veränderungen im Arbeitnehmerdatenschutz sind in der Zukunft zu erwarten?

In der Koalitionsvereinbarung der derzeit regierenden CDU/CSU/FDP-Regierung vom 26.10.2009 heißt es dazu:

„Wir setzen uns für eine Verbesserung des Arbeitnehmerdatenschutzes ein und wollen Mitarbeiterinnen und Mitarbeiter vor Bespitzelungen an ihrem Arbeitsplatz wirksam schützen. Es dürfen nur solche Daten verarbeitet werden, die für das Arbeitsverhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Arbeitsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante

te Gesundheitszustände beziehen, müssen zukünftig ausgeschlossen sein. Es sollen praxisgerechte Regelungen für Bewerber und Arbeitnehmer geschaffen und gleichzeitig Arbeitgebern eine verlässliche Regelung für den Kampf gegen Korruption an die Hand gegeben werden. Hierzu werden wir den Arbeitnehmerdatenschutz in einem eigenen Kapitel im Bundesdatenschutzgesetz ausgestalten.“

Aufgrund dieser Regelung im Koalitionsvertrag hat das zuständige Bundesministerium der Justiz am 31. März 2010 einen entsprechenden Entwurf für eine gesetzliche Verankerung des Arbeitnehmerdatenschutzes im BDSG vorgelegt, welches schließlich am 25.08.2010 vom Bundeskabinett beschlossen wurde und seit dem auf das entsprechende Gesetzgebungsverfahren wartet. Wann mit dem Selbigen zu rechnen ist, steht derzeit noch in den Sternen. Beobachter erwarten jedoch dessen Inkrafttreten nicht vor Mitte / Ende 2012.

Im Einzelnen sollen folgende Arbeitgeberpflichten eingeführt werden:

1. Der Beschäftigte ist auf sein Verlangen über den Inhalt einer bei einem Dritten über ihn eingeholten Auskunft zu unterrichten.
2. Dem Beschäftigten ist das Ergebnis einer ärztlichen Untersuchung oder Prüfung mitzuteilen.
3. Dem Beschäftigten ist das Ergebnis

eines Eignungstests mitzuteilen.

4. Dokumentationspflicht des Arbeitgebers bei einem automatisierten Datenabgleich.

5. Unterrichtungspflicht des Arbeitgebers bei einem automatisierten Datenabgleich.

6. Hinweispflicht des Arbeitgebers auf die Zweckbindung übermittelter Daten gegenüber dem Datenempfänger.

7. Der Arbeitgeber hat die einen Verdacht begründenden Tatsachen zu dokumentieren.

8. Der Arbeitgeber hat die näheren Umstände der Datenerhebung zu dokumentieren.

9. Unterrichtungspflicht des Arbeitgebers über die Datenerhebung, -verarbeitung oder -nutzung.

10. Der Grund der Speicherung und die Löschung sind zu dokumentieren.

11. Der Arbeitgeber hat den Umstand einer Videobeobachtung

durch geeignete Maßnahmen kenntlich zu machen.

12. Benachrichtigungspflicht des Arbeitgebers bei einer offenen Videoüberwachung

13. Der Arbeitgeber hat dem Beschäftigten den Einsatz eines Ortungssystems durch geeignete Maßnahmen erkennbar zu machen.

14. Der Arbeitgeber hat den Beschäftigten beim Einsatz eines Ortungssystems über den Umfang der Aufzeichnungen und deren regelmäßige oder im Einzelfall vorgesehene Auswertung zu informieren.

15. Der Arbeitgeber hat den Beschäftigten und seine Kommunikationspartner im konkreten Einzelfall vorher darüber zu informieren, ob er Inhalte einer ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubten Nutzung von Telefondiensten erhebt, verarbeitet oder nutzt.

16. Der Arbeitgeber hat den Beschäftigten und seine Kommunikationspartner über die Möglichkeit der Erhebung, Verarbeitung und Nutzung

von Inhalten der Nutzung von Telefondiensten zu informieren.

17. Der Arbeitgeber hat den Beschäftigten über die Erhebung, Verarbeitung und Nutzung von Inhaltsdaten nach Satz 2 zu unterrichten.

18. Der Arbeitgeber hat Dritten, an die er Beschäftigtendaten übermittelt hat, die Änderung, Löschung oder Sperrung dieser Daten unverzüglich mitzuteilen, es sei denn, dass die Mitteilung zur Wahrung schutzwürdiger Interessen der Beschäftigten nicht erforderlich ist.

Abschließend sei der Hinweis erlaubt, dass schon heute etliche dieser Arbeitgeberpflichten zu erfüllen sind.

Rechtsanwalt Christoph Lattreuter, Berlin

Rechtsanwalt Lattreuter ist Partner der überörtlichen Rechtsanwaltskanzlei Brennecke & Partner.

Mail: lattreuter@brennecke-partner.de



Kundendaten im Bankgeschäft- weshalb, warum, wofür?

Montagmorgen, 10:30 Uhr, erneut ein Termin bei der Hausbank. Gespräch mit dem Anlageberater, Thema: ein unverhoffter Geldsegen aus einer Erbschaft. Was tun mit dem Geld? Wie kann man sicher, liquide und gewinnbringend anlegen?

Der Berater der Bank erfragt nicht nur eine Vielzahl von Kundendaten, sondern versucht sich auch ein Bild über die Erfahrungen und Kenntnisse des Kunden, seine Vorstellungen, Einstellungen und Wünsche zu verschaffen. Beim Kunden bleibt der Eindruck hängen, jetzt gläsern für die Bank geworden zu sein und er geht eher mit einem unguten Gefühl aus dem für ihn so wichtigen Gespräch hinaus. Muss das so sein? Wenn es um Kundendaten im Bankgeschäft geht, muss man die unterschiedlichen Motive der handelnden Akteure einmal genauer betrachten.

Im Mittelpunkt steht der Kunde. Es liegt in der deutschen Mentalität, so wenig wie möglich über sich preisgeben zu wollen. Auch wenn im Bereich der Jüngeren durch die digitalen Netzwerke häufig der Eindruck entsteht, dass sich die Gesellschaft öffnet, so wird doch in einigen Bereichen des täglichen Lebens weiterhin Verschwiegenheit geübt. Einen vollumfänglichen Überblick haben in der Regel nur Familienmitglieder und beste Freunde, für Teilbereiche eher Spezialisten wie Steuerberater oder der Hausarzt.

Dem Kunden gegenüber steht die Bank. Das Sammeln von Daten hat mehrere Gründe: Viele Informationen sind unerlässlich, um eine zielgerichtete Problemlösung für den Kunden erarbeiten zu können. Und sicherlich ist auch der Wunsch vorhanden, dem Kunden in zukünftigen weiteren Problemstellungen mit anderen Lösungen des Finanzinstituts helfend zur Seite stehen zu können (Cross-Selling). Viele Daten werden häufig nicht aktuell benötigt, aber wer freut sich nicht über Glückwünsche zum Geburtstag, ein kleines Präsent zu besonderen Anlässen oder eine Einladung zu einem Event?

Auch gilt es, die gesetzlichen Bestimmungen einzuhalten. Einerseits soll der Kunde geschützt werden, indem er immer individuellere, auf seine Bedürfnisse zugeschnittene Vorschläge seiner Bank erhält (so muss die Beratung des Kunden und der Weg zu einem empfohlenen Anlageprodukt dokumentiert werden und in einem Protokoll mit einem umfassenden

de, was er (außer den gesetzlich geforderten Daten) von sich preisgeben möchte, jedoch muss er sich bewusst sein, dass weniger nicht unbedingt besser ist. Aufseiten der Bank gilt es besonders verantwortungsvoll mit den Daten umzugehen und diese nicht nur die Vertriebsmaschine anzuwerfen. Aber auch der Staat sollte sich bei all seinen Bemü-



Überblick über die finanziellen Verhältnisse des Kunden zusammengefasst werden). Andererseits müssen auch Daten erhoben werden, die der Staat unter anderem zur Verhinderung von Missbrauch staatlicher Leistungen (Steuer-ID beim Freistellungsauftrag; Meldung der Ausnutzung des Freibetrages) benötigt oder zur Verfolgung von möglichen Straftaten (Geldwäschegesetz). Darüber hinaus gilt es aber auch Anforderungen anderen Drittstaaten gerecht zu werden (Doppelbesteuerungsabkommen z. B. mit den USA).

Schlussendlich entscheidet der Kun-

hungen im Klaren sein, dass die Bürger immer noch frei bestimmende Individuen sind.

Dirk Wittich, Die Max Heinr. Sutor oHG
Mail: dirk.wittich@sutorbank.de

Die Max Heinr. Sutor oHG ist als inhabergeführte Privatbank in Hamburg spezialisiert auf die Anlage in Wertpapieren und wurde 2009 und 2010 für ihre Vermögensverwaltung als „herausragend“ von FocusMoney und n-tv ausgezeichnet.

SCHUFA, Creditreform und Co. – Prüfen Sie ihre Daten!

Die Auskunftsteien wie SCHUFA, Creditreform, Bürgel, Infoscore usw. speichern täglich Daten von uns und unseren Unternehmen, die einen erheblichen Einfluss auf unsere Teilnahme am Wirtschaftsleben haben. Aufgrund der dortigen Einträge kommt es immer wieder zu überraschenden Ablehnungen bei Vertragsschlüssen, die in der einen oder anderen Situation auch schon mal peinlich sein können.

Der Umgang mit personenbezogenen Daten wird durch das Bundesdatenschutzgesetz (BDSG) geregelt. Dieses hat in den letzten Jahren einige bedeutende Änderungen erfahren und seitdem die Stellung des Einzelnen gegenüber den Auskunftsteiunternehmen erheblich gestärkt.

Zweck des BDSG ist es, den Einzelnen vor Beeinträchtigungen seines allgemeinen Persönlichkeitsrechtes durch Dritte zu schützen. Deshalb ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten grundsätzlich verboten. Eine Ausnahme kommt nur dann in Betracht, wenn die Datenerhebung und -verwendung gesetzlich vorgesehen ist oder der Betroffene einwilligt (Verbot mit Erlaubnisvorbehalt). Auch in diesen Ausnahmefällen gilt aber die Maßgabe der Datenvermeidung: Datenverarbeitungssysteme sollen keine oder so wenig personenbezogene Daten wie möglich verwenden und diese weitmöglichst anonymisieren. In den Schutzbereich des BDSG fallen dabei u.a. Daten wie Namen, Telefonnummern, E-Mail-Adressen, IP-Adressen, Personalnummern, die Herkunft, die politische Meinung, religiöse Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit und das Sexualleben.

Die SCHUFA und andere Auskunftsteien speichern neben Namen, Geburtsdaten, gegenwärtigen und früheren Anschriften auch Daten über die Aufnahme und vertragsgemäße Abwicklung von Geschäftsbeziehungen (Positiveinträge) sowie Daten über nichtvertragsgemäßes Verhalten und gerichtliche Vollstreckungsmaßnahmen (Negativeinträge). Die SCHUFA erhält einen Großteil die-

ser Daten von ihren Mitgliedern, insbesondere den Banken und anderen Vertragspartnern, die sich bei der Anbahnung von Vertragsverhältnissen oder im Vertrag selbst durch den Kunden die schriftliche Einwilligung zur Weitergabe und Speicherung der Daten erteilen lassen. Aber auch die anderen Auskunftsteien lassen sich die Zahlungserfahrungen ihrer Mitglieder melden, die Creditreform nennt das bei sich den ZaC-Datenpool. Andere Daten lassen sich aus den öffentlichen Schuldnerverzeichnissen der Amtsgerichte, den Insolvenz bekanntmachungen, dem Handelsregister etc. entnehmen.

Unter Verwendung der gespeicherten Daten erstellen die Auskunftsteien sodann Wahrscheinlichkeitsprognosen für das zukünftige Verhalten der Betroffenen hinsichtlich der Kreditwürdigkeit, Vertragstreue u.a. (sog. „Scoring“). Die Berechnung dieser Wahrscheinlichkeitswerte muss in einem wissenschaftlichen mathematisch-statistischen Verfahren erfolgen sowie nachvollziehbar und allgemein verständlich sein.

Die Auskunftsteien geben die gesammelten Informationen regelmäßig nur an ihre zahlenden Mitglieder heraus. Nicht jedes Mitglied erhält jedoch alle Auskünfte. Die SCHUFA unterscheidet z. B. „A-Vertragspartner“ (z. B. Banken, Kreditkartenunternehmen, Leasinggesellschaften), die bei Bedarf Auskunft über alle gespeicherten Daten erhalten, einschließlich positiver Einträge über bestehende Verträge und negativer Einträge über nichtvertragsgemäßes Verhalten und Zwangsvollstreckungsmaßnahmen. Die „B-Vertragspartner“ (z. B. Versandhandels- oder Telekommunikationsunternehmen,

Versicherungen, Makler) erhalten nur die Negativeinträge. Schließlich gibt es noch die „F-Vertragspartner“ (z. B. Inkassounternehmen), die nur Auskunft über die gespeicherten Adressdaten erhalten. Voraussetzung für die Datenweitergabe von nicht aus öffentlichen Registern stammenden Daten ist die Einwilligung des Betroffenen.

Falls Sie sich also wundern, weshalb Ihr Kreditantrag abgelehnt wurde und woher die Bank von Ihnen nicht bezahlten Handyrechnungen weiß: Im Regelfall hat sich die Bank im Kreditantrag eine Datenabfrage bei der Schufa vorbehalten (sog. „Schufa-Klausel“) und Sie haben mit Ihrer Unterschrift in die Datenübermittlung eingewilligt.

Die SCHUFA und alle anderen Auskunftsteien sind verpflichtet, dem Betroffenen auf Antrag die über ihn gespeicherten Daten mindestens einmal jährlich unentgeltlich offen zu legen (sog. Eigenauskunft). Einige Auskunftsteien haben zu diesem Zweck eigene Internetportale eingerichtet, die Sie über die jeweilige Homepage leicht finden können. Zusätzlich bietet die SCHUFA einen kostenpflichtigen Online-Zugang an, über den man für eine Einmalzahlung von derzeit 18,50 € unbefristet Auskünfte abrufen kann. Um Missbrauch zu verhindern, sind Auskunftsteiunternehmen berechtigt, sich zuvor die Identität des Betroffenen – etwa durch Vorlage des Personalausweises – nachweisen zu lassen. Auskunftsteiunternehmen sind verpflichtet, dem Betroffenen gespeicherte Daten über seine Person, die Herkunft der Daten, die Empfänger und den Zweck der Speicherung offen zu legen. Allerdings können Aus-

künfte über Herkunft und Empfänger verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses das Informationsinteresse des Betroffenen überwiegt. Zusätzlich sind Auskunftseunternehmen in Bezug auf das Scoringverfahren gehalten, den Betroffenen die aktuellen Wahrscheinlichkeitswerte für deren zukünftiges () Verhalten mitzuteilen. Außerdem müssen Auskunftseunternehmen über die erfolgten Übermittlungen der Werte der letzten zwölf Monate, deren Empfänger sowie die der Wertermittlung zugrunde gelegten Daten und die Berechnungsmethode informieren.

Sind die Eintragungen zu Ihrer Person unrichtig, besteht die Pflicht bei den Auskunftseunternehmen, unrichtige Einträge zu berichtigen. Weiter gibt das BDSG den Betroffenen das Recht, die Sperrung von Einträgen zu verlangen. Voraussetzung für die Sperrung ist lediglich, dass der Betroffene die Richtigkeit einer Eintragung bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit der eingetragenen Tatsache feststellen lässt. Achtung: Dies gilt nicht für Daten, die aus allgemein zugänglichen Quellen

entnommen worden sind. In diesen Fällen kann der Betroffene aber eine Gegendarstellung abgeben, die den Daten bei der Übermittlung beigelegt werden muss. Die Auskunftseunternehmen sind bei diesen Vorgängen jedoch nicht besonders kooperativ und die Durchsetzung dieser Rechte gestaltet sich häufig zäh.

Personenbezogene Eintragungen verbleiben nicht auf ewig in den Sammlungen der Auskunftseunternehmen. Die Auskunftseunternehmen müssen gespeicherte Daten löschen, sobald die Speicherung nicht mehr erforderlich ist oder sich herausstellt, dass die Erhebung und Speicherung nach dem BDSG unzulässig war. Die Erforderlichkeit entfällt z. B., wenn Sie Ihren Kredit vertragsgemäß zurückgezahlt haben. Der entsprechende Eintrag über die Begründung, Durchführung und Beendigung des Vertragsverhältnisses muss von den Auskunftseunternehmen auf Ihren Antrag hin spätestens drei Jahre nach Beendigung des Vertrages entfernt werden. Unzulässigkeit liegt z. B. vor bei Informationen über rassische oder ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, strafba-

re Handlungen oder Ordnungswidrigkeiten, den Gesundheitszustand oder das Sexualleben, deren Richtigkeit nicht bewiesen werden kann, oder auch in Fällen, in denen die Einwilligung des Betroffenen fehlt.

Die gesetzlichen Rahmen für die Auskunftseunternehmen und Auskunfts- bzw. Löschungsansprüche für den Betroffenen schützen leider nicht vor Fehlern oder sogar Missbrauch. Wenn dem Betroffenen aus der unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten ein Schaden entstanden ist, steht dem Geschädigten nach dem BDSG gegenüber der verantwortlichen Stelle ein Schadensersatzanspruch zu, soweit diese die nach den Umständen des Falles gebotene Sorgfalt außer Acht gelassen hat.

Rechtsanwalt Andreas Albrecht,
Fachanwalt für Steuerrecht
Turnbull & Irrgang, Hamburg
Mail: aa@turnbullirrgang.de

Ann Sohns, wissenschaftliche
Mitarbeiterin, Hamburg



Der Administrator hat alle Rechte – aber hat er auch das Recht?

Mittlerweile haben viele Unternehmen – nicht zuletzt aufgrund der Artikel in der MuR – den Umgang mit Emails überdacht und geregelt und zumindest die private Nutzung untersagt oder in speziellen Betriebsvereinbarungen geregelt. Für Administratoren stellen sich aber nach wie vor eine Unzahl von Fragen, wenn die Geschäftsleitung von ihnen verlangt, den Zugriff auf Daten von Mitarbeitern zu ermöglichen.

Ein häufiges Beispiel ist der plötzliche Ausfall eines Mitarbeiters, der wichtige Informationen in seinem persönlichen Laufwerk oder seinem Postfach gespeichert hat bzw. bei dem solche Informationen vermutet werden. Möglicherweise liegen dort aber auch dienstliche Mitteilungen an Betriebsärzte, Betriebsrat oder Entwürfe, die anderen bewusst noch nicht präsentiert werden sollen. Wie der jüngste Fall eines gekündigten Administrators zeigt, der unbefugt auf Kalender zugegriffen hatte und Termine an interessierte Kollegen mitgeteilt hatte, benötigen Administratoren dringend Rechtssicherheit – auch wenn sie alle (EDV-)Rechte haben.

Bei der Nutzung von E-Mail zu dienstlichen Zwecken fehlt es an einem Angebot für „Dritte“, sodass das Fernmeldegeheimnis nicht greift. Ist also in einer Betriebsvereinbarung die private Nutzung untersagt, führt dies dazu, dass das TKG wie auch das TMG nicht zur Anwendung kommen. Nach allgemeiner Ansicht kann das Unternehmen den Eingang und Ausgang von E-Mails einschließlich der Zieladressen festhalten.

Ist damit auch der Einblick in das Postfach erlaubt?

Differenziert wird die Einsicht in die E-Mails selbst gesehen:

Einer Ansicht nach dürfen Unternehmen bei Abwesenheit der Mitarbeiter E-Mails lesen, sofern die Mails nicht ausdrücklich als „persönlich“ oder „vertraulich“ gekennzeichnet sind oder anderweitig deren private Natur zu erkennen ist. Ansonsten soll die Lektüre der Mails nur bei Nachweis eines berechtigten Interesses erlaubt sein, wenn etwa ein begründeter Verdacht auf strafbare Handlungen besteht, E-Mails den Betriebsfrieden gefährden (etwa bei Mobbing) oder die Weitergabe von Betriebsgeheimnissen vermieden werden soll.

Da die E-Mail im Geschäftsverkehr immer häufiger den klassischen Geschäftsbrief ersetzt, soll es den Unternehmen gestattet sein, von ein- und ausgehenden E-Mails der Arbeitnehmer im gleichen Umfang Kenntnis zu nehmen, wie von deren dienstlichem postalischen Schriftverkehr.

Was ist z. B. mit Entwürfen oder dienstlichen Datensätzen an Betriebsverfassungsorgane?

Was ist z. B. mit Entwürfen oder dienstlichen Datensätzen an Betriebsverfassungsorgane?

Einer differenzierenden Ansicht nach folgt aus der Nichtanwendbarkeit des TKG /TMG indes nicht, dass damit unbegrenzte Zugriffsmöglichkeiten auf die Daten von Beschäftigten bestehen. Auch nach Verbot privater Nutzung bleibe der Zugriff auf Daten aus dem persönlichen dienstlichen Bereich in jedem Fall unzulässig. Zu diesem persönlichen Bereich gehören z. B. Entwürfe, die nach dem Willen der Beschäftigten noch nicht zur Kenntnisnahme anderer bestimmt sind. Hinzu kommen alle Informationen, die nach dem Willen der Beschäftigten oder aus objektiver Sicht einer besonderen Vertraulichkeit unterliegen, wie beispielsweise E-Mails an Betriebsärzte oder Betriebsverfassungsorgane. Auch ein offener Meinungsaustausch über Kollegen via E-Mail kann dazugehören.

Nach dieser Ansicht haben Unter-

nehmen nur eine Berechtigung, dass ihnen rein dienstliche E-Mails zur Verfügung gestellt werden. Diese »Zurverfügungstellung« muss so gestaltet sein, dass die Beschäftigten hierüber vorab informiert sind.

Handlungsempfehlung

Die Argumente der zweiten Ansicht sind nicht von der Hand zu weisen. Ein Zugriff auf das E-Mail-Postfach könnte in der Tat dienstliche, aber gerade sensible E-Mails offenbaren.

Wenn überhaupt ist der Zugriff auf das E-Mail-Postfach daher so vorzunehmen, dass nur die E-Mails geöffnet und ausgedruckt werden, die klar erkennbaren dienstlichen Charakter haben und sich auf Projekte beziehen. Ist der Betreff nicht eindeutig bzw. ist klar, dass Partner der betrieblichen Kommunikation BR oder Betriebsarzt sind, ist die E-Mail keinesfalls zu öffnen. Bei dem Zugriff sollte ein Mitglied des BR sowie der Datenschutzbeauftragte hinzugezogen werden.

Ferner ist es empfehlenswert, den Zugriff auf einer gesondert erstellten Sicherungskopie vorzunehmen, damit sich der Administrator nicht später einem Vorwurf einer Datenunterdrückung ausgesetzt sieht.

Zugriff auf das persönliche Laufwerk von Mitarbeitern

Die Verarbeitung und Nutzung der auf persönlichen Laufwerken liegenden Dateien mit personenbezogenen Daten ist grundsätzlich zulässig.

Die Verarbeitung und Nutzung personenbezogener Daten ist gestattet,

soweit es zu Wahrung der berechtigten Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen der Nutzung widersprechen. Für den Fall, dass nur dienstliche Dateien gespeichert werden dürfen, sind überwiegende schutzwürdige Interessen der Beschäftigten in der Regel nicht erkennbar. Eine Ausnahme bilden auch hier wieder Entwürfe, die erkennbar (noch) nicht zur Weiterleitung an andere bestimmt sind. Die Entscheidung darüber, ob die Belange des Betroffenen gegenüber den Interessen der verantwortlichen Stelle schutzwürdiger sind, trifft die verantwortliche Stelle, also das Unternehmen.

Hindert ein Passwort den Zugriff?

Die Verwendung eines Passworts, welches die User und nicht das Unternehmen bestimmt haben, hindert nicht an einem Zugriff. Die Möglichkeit der Datensicherung auf einem persönlichen Laufwerk dient nicht etwa dazu, den Beschäftigten die private Nutzung der EDV-Anlage für ihre Zwecke zu ermöglichen. Mit dieser Maßnahme hat das Unternehmen vielmehr dem gesetzlichen Gebot der Anlage zu § 9 BDSG Rechnung getragen. Nach Nr. 3 dieser Anlage muss die verantwortliche Stelle gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die Daten zugreifen können, die sie für die Erledigung ihrer Aufgabe benötigen und nicht von Unbefugten verarbeitet werden können. Dementsprechend dient die Vorgabe der Vergabe eines Passwortes durch die Beschäftigten der Umsetzung einer gesetzlichen Vorgabe.

Darf der Administrator das Passwort überwinden?

Die Zugriffsmöglichkeit durch den Administrator ist schon deshalb erforderlich, weil ansonsten die Erhaltung der Funktionsfähigkeit der Anlage nicht gewährleistet ist. Hinzu kommt, dass Beschäftigte nicht ohne Weiteres darauf vertrauen können, das Unternehmen wolle ihnen einen für sie privat geschützten persönlichen Freiraum zur Verfügung stellen.

Strafrechtliche Betrachtung:

Nach § 202a Abs. 1 StGB wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer unbefugt sich oder einem anderen Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugriff besonders gesichert sind. Wer „berechtigt“ ist, bestimmt der Verfügungsbefugte. Die Verfügungsbefugnis entsteht mit dem sog. „Skripturakt“, also der Erschaffung oder Erstspeicherung von Daten. Danach kann die Befugnis auf andere übertragen werden. Bei der Frage der Befugnis kommt es also nicht auf die Eigentumsverhältnisse an den Speichermedien an. Auch unerheblich ist, ob der Dateninhalt eine Person betrifft; diese kann gleichsam Unbefugter i.S.v. § 202a StGB sein.

Im Ergebnis handelt immer derjenige unberechtigt, dem die Daten nach dem Willen des Verfügungsberechtigten zum Zeitpunkt der Tat handlung nicht zur Verfügung stehen sollen.

Einwilligung nach BDSG reicht nicht aus.

Eine Einwilligung nach BDSG alleine reicht hier nicht aus, da § 202a StGB keine Datenschutzvorschrift i.S.d. BDSG ist.

Die Lösung: Gestaltung der Betriebsvereinbarung

Bei der Gestaltung einer Betriebsvereinbarung sollte eine Regelung getroffen werden, die es dem Administrator Rechtssicherheit in Hinblick auf das BDSG verschafft.

Einrichtung einer Vertrauensperson

Ferner ist es sinnvoll, eine Vertrauensperson einzurichten, die im Falle plötzlicher Abwesenheit von Beschäftigten auf die jeweiligen Mailboxen oder Laufwerke zugreifen kann und die Datensätze auf die o.g. sensiblen innerbetrieblichen Informationen hin sichtet und ggf. nur die rein dienstlich für die Weiterarbeit notwendigen Mails ausdruckt.

Gestaltung einer Nutzungsvereinbarung

Mit den Usern ist eine Nutzungsvereinbarung zu treffen, die nicht nur

die Einwilligung i.S.d. BDSG beinhaltet sondern ausdrücklich auch Befugnisse zum Datenzugriff im strafrechtlichen Sinne erfasst. In einer solchen Nutzungsvereinbarung kann auch geregelt werden, dass keine automatische Weiterleitung aktiviert wird (was oftmals der Fall ist) - eine automatische Weiterleitung würde auch Mails erfassen, von externen Sendern, die von innerbetrieblichen Regelungen keine Kenntnis haben - oder eine Blockade der Mailbox, die möglicherweise zu einer vorwerfbareren Datenunterdrückung führt. Vielmehr ist eine Benachrichtigungsfunktion zu empfehlen, aus der Absender erkennen können, dass die E-Mail (temporär) nicht gelesen wird.

Insgesamt sind diese Dinge aber in einer konkreten Nutzungsvereinbarung zu regeln, damit Administratoren Sicherheit bei dem Zugriff auf Informationen erlangen.

Von Rechtsanwalt Guido Friedrich Weiler, Köln
Rechtsanwalt und Fachanwalt für weiler.de

Rechtsanwalt und
Fachanwalt für
Arbeitsrecht Guido-
Friedrich Weiler ist
Lehrbeauftragter an
der Bundesakademie
für Wehrverwaltung
in Mannheim und
lehrt seit 2005 an der
Rheinischen Fach-
hochschule Köln. u.a.
Arbeitsrecht.
Er schult gleichermaßen
Fachanwälte für
Arbeitsrecht, Unter-
nehmensleitungen wie
Betriebsräte sowie, zu-
sammen mit Kaspersky
Labs und Avira,
Mitarbeiter/innen in
EDV-Abteilungen.

Mail: guido-friedrich.
weiler@kanzlei-

SATO

SAIL

TRANSPARENZ, LEICHTIGKEIT
UND PURE ELEGANZ

Die Bürostuhlfamilie SAIL bietet vielfältige
Funktionalität, Bewegungsfreiheit und un-
geahnten Komfort. Sitzen Sie Probe und
überzeugen Sie sich selbst!

Fröschner Büromarkt GmbH
Greschbachstr. 16 · D-76229 Karlsruhe
Telefon: +49 (0)721 62513 0
Telefax: +49 (0)721 62513 33
E-Mail: info@froescher-buromarkt.de
www.froescher-buromarkt.de

Private E-Mails im Unternehmensnetzwerk – Archivierung verboten?

Wohl in den meisten Unternehmen wird der Austausch privater E-Mails durch die Arbeitnehmer erlaubt oder zumindest geduldet. So arbeitnehmerfreundlich diese Praxis auch ist; nach den Vorschriften zur Speicherung elektronischer Geschäftspost droht sie zum erheblichen Risiko für die Führung des Unternehmens zu werden.

Pflicht zur Archivierung

Nach § 147 der Abgabenordnung (AO) hat das Unternehmen geschäftlichen E-Mail-Verkehr für mindestens sechs Jahre dauerhaft zu archivieren und zu Prüfungszwecken vorzuhalten. Nähere Einzelheiten zur Ordnung und maschinellen Auswertbarkeit der archivierten Daten regeln die „Grundsätze für die Anwendung der Regelungen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU). Danach kann die Finanzverwaltung verlangen, dass ihr die zu archivierenden elektronischen Unterlagen in maschinenlesbarer Form zur Prüfung übergeben werden. Dabei nutzt die Finanzverwaltung eine spezielle Prüfungssoftware (IDEA). Schon heute findet ein Großteil der Außenprüfungen elektronisch statt; dies mit stark steigender Tendenz. Sofern im Unternehmen kein vorgangsbezogenes Dokumentenmanagementsystem (DMS) zum Einsatz kommt, wird zwecks Einhalten der gesetzlichen Vorschriften oftmals der gesamte E-Mail-Verkehr, entweder zentral über den Mailserver oder lokal am einzelnen Arbeitsplatz gespeichert und archiviert. Bei dieser Form der Speicherung wird – und kann – regelmäßig nicht zwischen geschäftlichen und privaten E-Mails unterschieden werden.

Den meisten Unternehmen ist zwar bewusst, dass die von ihnen betriebene unterschiedslose Archivierung datenschutzrechtlich bedenklich sein könnte. Der Blick richtet sich dabei regelmäßig nur auf die – im Ergebnis unproblematischen – Bestimmungen des Bundesdatenschutzgesetzes (BDSG), nicht jedoch auf die wesentlich gefährlicheren des Telekommunikationsgesetzes (TKG).

Archivierung und BDSG

Im Anwendungsbereich des BDSG dürfte die Speicherung privater E-Mails im Rahmen der unterschiedslosen Archivierung bereits nach § 28 BDSG zulässig sein. Die Vorschrift erlaubt die Speicherung privater Daten, wenn dies zur Wahrung berechtigter Interessen des Unternehmens geschieht. Auf jeden Fall zulässig ist die Speicherung privater E-Mails im Rahmen der unterschiedslosen Archivierung, wenn der Arbeitnehmer eingewilligt hat (§§ 4, 4a BDSG). Viele Betriebsvereinbarungen über die private Nutzung der Unternehmens-IT sehen solche Einwilligungen bereits vor.

Archivierung und TKG

Das eigentliche und regelmäßig übersehene Problem für das Unternehmen liegt darin, dass die unterschiedslose Archivierung nicht nur an den Vorschriften des Bundesdatenschutzgesetzes, sondern auch an denen des Telekommunikationsgesetzes zu messen ist.

Denn das Unternehmen, das seinen Arbeitnehmern die Nutzung der Unternehmens-IT für privaten E-Mail-Verkehr gestattet, gilt als Diensteanbieter (§ 3 Nr. 6 TKG) und unterliegt damit denselben Pflichten wie ein „echtes Telekommunikationsunternehmen“, bspw. die TELEKOM oder VODAFONE.

Zu den Pflichten eines Diensteanbieters gehört aber vor allem, das Fernmeldegeheimnis (§ 80 TKG) zu wahren: „Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Tele-

kommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet“ (§ 80 Abs. 1 bis Abs. 2 Satz 1 TKG). Damit untersagt § 80 TKG dem Unternehmen jedwede Speicherung privater E-Mails der Arbeitnehmer.

Allerdings kann auf die Einhaltung des Fernmeldegeheimnisses durch den Betroffenen verzichtet werden. Insoweit wird teilweise die Ansicht vertreten, dass das Fernmeldegeheimnis nicht verletzt wird, wenn eine Vereinbarung zwischen Unternehmen und Arbeitnehmer existiert, die die unterschiedslose Archivierung erlaubt. Mit einer solchen Vereinbarung wäre nicht nur den Vorschriften des BDSG, sondern auch denen des TKG genüge getan.

Diese Auffassung verkennt jedoch, dass ein Verzicht auf die Einhaltung des Fernmeldegeheimnisses nur durch alle Teilnehmer der betroffenen Telekommunikation erklärt werden kann. Es reicht also nicht aus, wenn allein der Arbeitnehmer auf die Einhaltung des Fernmeldegeheimnisses verzichtet, theoretisch müsste auch derjenige verzichten, an den die private E-Mail versandt oder von dem sie abgeschickt wurde.

Dieser – strengen – Ansicht dürfte der Vorzug zu geben sein. Zwar ließe sich vertreten, dass derjenige, der von außen mit einer geschäftlichen E-Mail-Adresse kommuniziert, damit rechnen muss, dass die E-Mails gespeichert werden und deshalb konkludent auf die Einhaltung des Fernmeldegeheimnisses verzichtet. Eine

solche Auslegung würde aber dem Umfang des Fernmeldegeheimnisses nicht gerecht werden. Das Fernmeldegeheimnis schützt nämlich bereits den Umstand, dass überhaupt Telekommunikation stattgefunden hat. Damit gilt das Fernmeldegeheimnis auch, wenn die E-Mail-Kommunikation durch den Arbeitnehmer abgestoßen wird, also der Empfänger gar nicht entscheiden kann, ob er private E-Mails mit einer geschäftlichen E-Mail-Adresse austauschen kann. Auch spricht der Umstand, dass der persönliche Geheimbereich immer stärker Angriffen über die Kommunikationswege des Internets ausgesetzt ist, dafür, das Fernmeldegeheimnis streng auszulegen.

Welche dieser beiden Ansichten die richtige ist, bleibt letztendlich durch die Rechtsprechung oder den Gesetzgeber zu klären. Bislang liegen jedenfalls noch keine einschlägigen obergerichtlichen Urteile vor. Es besteht also erhebliche Rechtsunsicherheit. Dies zumal die Verletzung des Fernmeldegeheimnisses gemäß § 206 des Strafgesetzbuchs (StGB) mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft wird, also für die Führung des Unternehmens ein nicht unerhebliches Risiko besteht, sich strafbar zu machen.

Fazit: Vor diesem Hintergrund sollten Unternehmen, die unterschiedslose Archivierung betreiben, ihren Arbeitnehmern die Nutzung der Unternehmens-IT für private E-Mails bis auf Weiteres untersagen.

Rechtsanwalt Glenn D. Büllsfeld,
Hamburg

Mail: gdb@advo-hamburg.de

Kundendaten – Schutz für den Schatz.

Kundendaten zählen zu den wichtigsten Geschäfts- und Betriebsgeheimnissen eines Unternehmens. Ihr Schutz ist für das Bestehen des Unternehmens unerlässlich. Verlässt ein Mitarbeiter das Unternehmen, werden häufiger als angenommen Kundendaten unerlaubt mitgenommen. Eine fremde Nutzung kann für das Unternehmen erheblichen Schaden verursachen: Oft entsteht ein neuer Konkurrent, der sich nur so finanzieren kann und der das Unternehmen viel Geld oder gar die Existenz kosten kann.

Wann also dürfen Kundendaten nach Beendigung eines Vertrages von einem ehemaligen Mitarbeiter überhaupt genutzt werden? Und wie kann man sich davor wirksam schützen?

I. Datennutzung durch ehemalige Mitarbeiter

Ob ein früherer Mitarbeiter Kundendaten weiter benutzen darf, hängt davon ab, ob der betreffende Mitarbeiter Handelsvertreter, Versicherungsvertreter, Franchisenehmer, Vertragshändler oder Angestellter des Unternehmers war.

1. Handelsvertreter

Ein Handelsvertreter, der selbstständig für ein Unternehmen Geschäfte vermittelt oder sie in dessen Namen abschließt, benötigt zur Ausübung seiner Tätigkeit zwangsläufig die Kundendaten seines Geschäftsherrn. Im Rahmen seiner Tätigkeit erwirbt er auch selbst Kundenkontakte.

Nach Handelsvertretervertragsen ist ein Handelsvertreter regelmäßig verpflichtet, die vom Unternehmer überlassene Kundenliste und die Liste selbst geworbener Kunden an diesen herauszugeben.

Laut HGB darf der Handelsvertreter zudem Geschäftsgeheimnisse nach Beendigung des Vertrages nicht weiterverwerten oder Dritten mitteilen. Geschäftsgeheimnisse sind auch Daten von Kunden, die vom Handelsvertreter selbst für das Unternehmen geworben wurden.

Verstößt der Handelsvertreter gegen seine Verschwiegenheits-

pflcht, entstehen für den ehemaligen Geschäftsherrn Schadensersatz-, Unterlassungs-, Auskunft- und Beseitigungsansprüche.

Allerdings hat auch die Verschwiegenheitspflicht des Handelsvertreters ihre Grenzen: Der ausgeschiedene Handelsvertreter darf Kundendaten verwenden, die in seinem Gedächtnis geblieben sind, die keinen dauerhaften Kontakt zum alten Unternehmer haben und von Kunden, die ohne Zutun des Handelsvertreters entschlossen sind, die Geschäftsbeziehungen zu dem Unternehmer nicht mehr fortzusetzen. Daneben ist eine branchenfremde Verwertung selbsterworbener Kundendaten zulässig. Für Versicherungsvertreter gilt dasselbe.

2. Franchisenehmer

Ein Franchisenehmer führt ein eigenes Unternehmen und schließt seine Geschäfte im eigenen Namen ab. Kundendaten, die der Franchisenehmer über eigene Geschäftskontakte erlangt, stehen in seinem Eigentum. Sie dürfen nach Beendigung des Franchisevertrages vom Franchisenehmer exklusiv weiter genutzt werden – und nicht vom Franchisegeber. Franchiseverträge regeln zuweilen, dass der Franchisenehmer dem Franchisegeber seine Kundendaten zu übermitteln habe. Dies verstößt oft gegen Datenschutzrecht und ist dann nichtig. Verarbeitet der Franchisegeber die übermittelten Daten im Auftrag des Franchisenehmers, darf der Franchisegeber diese Daten nicht zu eigenen Zwecken nutzen und Dritten übermitteln. Der Franchisenehmer bleibt Herr dieser

Kundendaten.

Werden dem Franchisegeber nicht nur die Kundendaten übermittelt, sondern auch die Erfüllung einer Aufgabe übertragen, ist eine Funktionsübertragung gegeben – beispielsweise die Übermittlung von Patientendaten an eine Abrechnungsstelle. Der Franchisenehmer verliert dann seine Herrschaft über die Daten. Hat der Franchisenehmer vor der Datenübermittlung nicht die Einwilligung seiner Kunden eingeholt, ist diese Datenübermittlung datenschutzrechtlich unzulässig. Es drohen Bußgelder bis 250.000,- EUR oder gar Freiheitsstrafe von bis zu zwei Jahren.

Nach Beendigung des Franchisevertrages steht dem Franchisenehmer ein Löschungsanspruch gegenüber dem Franchisegeber in Bezug auf seine Kundendaten zu. Der Zweck der Datenübermittlung fällt mit Beendigung des Vertrages weg; dem Franchisegeber ist die Speicherung dieser Daten damit verwehrt – und folglich auch die weitere Nutzung.

3. Vertragshändler

Ein Vertragshändler führt wie ein Franchisenehmer ein eigenes Unternehmen und schließt seine Geschäfte im eigenen Namen ab. Im Gegensatz zum Franchisenehmer ist der Vertragshändler nicht in das Geschäftssystem des Geschäftsherrn eingebunden. Er enthält kein Know-how durch den Geschäftsherrn, mit Ausnahme des Logos und der Warenzeichen. Der Vertragshändler ist folglich nicht im gleichen Umfang Weisungen ausgesetzt wie der Franchisenehmer.

Aufgrund dieser eigenen Betriebsführung darf der Vertragshändler wie ein Franchisenehmer seine erworbenen Kundendaten exklusiv nach Beendigung des Vertrages weiter nutzen.

4. Angestellte

Ein als Arbeitnehmer angestellter Mitarbeiter darf alle während seiner Tätigkeit bekannt gewordenen Kundendaten nach seinem Ausscheiden aus dem Unternehmen nicht verwenden, wenn ein nachvertragliches

Wettbewerbsverbot vereinbart wurde. Ohne ein solches Wettbewerbsverbot darf der Arbeitnehmer wie ein Handelsvertreter nur die jeweiligen Kundendaten verwenden, die er in seinem Gedächtnis bewahrt hat.

5. Zusammenfassung

Handelsvertreter, Versicherungsvertreter und Angestellte unterliegen auch nach Beendigung ihres Vertragsverhältnisses der Verpflichtung, die bekannt gewordenen und selbst erworbenen Kundendaten geheim zu halten. Verstößen sie gegen diese Pflicht, stehen dem Unternehmer Schadensersatz-, Unterlassungs-, Auskunfts- und Beseitigungsansprüche zu.

Ein Franchisenehmer sowie ein Vertragshändler sind aufgrund ihrer im eigenen Namen führenden Unternehmereigenschaft Eigentümer ihrer selbst erworbenen Kundendaten und dürfen diese nach Beendigung des Vertragsverhältnisses exklusiv nutzen. Sind Franchisenehmer und Vertragshändler aufgrund ihrer Einbindung in das Absatzsystem des Geschäftsherrn - und entgegen ihrer vertraglichen Bezeichnung - als Handelsvertreter zu behandeln, unterliegen sie ebenfalls der Geheimhaltungspflicht.

II. Erkennung der Nutzung und Schutz vor Datendiebstahl

Verlässt ein Mitarbeiter das Unternehmen, ist es schwer zu erkennen, ob Kundendaten unberechtigt entwendet und genutzt wurden. Der Diebstahl von Kundendaten durch Datenkopien ist heute leicht. Die Möglichkeit des Unternehmers hingegen, seine Kunden anzuschreiben, um in Erfahrung zu bringen, ob der ehemalige Mitarbeiter sie angeworben hat, ist mühevoll und würde die Kunden oft erst recht auf einen neuen Konkurrenten hinweisen.

Der Versuch, einen Datendiebstahl durch „Schreibfehler“ in den Adressen nachzuweisen, scheitert regelmäßig. Hierzu bräuchte man zudem die Anschreiben an die betreffenden Kunden – diese bekommt man jedoch kaum. Bei Mailings oder Anrufen ist diese Methode zudem un-

tauglich. Zudem möchte kein Unternehmen seinen guten Kunden Schreibfehler zumuten. Ein Beweis eines Kundendatendiebstahls lässt sich so kaum führen.

Die einzig wirksame Methode zum Schutz der eigenen Kundendaten ist eine regelmäßige Aufnahme einer signifikanten Anzahl von Scheinkundenadressen. Diese Adressen sollten neben dem erfundenen Firmennamen über einen Ansprechpartner, eine existierende Postadresse, eine Telefon- und Faxnummer, eine E-Mail-Adresse und eine (unbenutzte aber registrierte) Domain verfügen. Jede Scheinadresse darf nur einmal verwendet werden. Sie sollte zudem durch echte Bestellungen von außen eingeführt werden - die durch Rückabwicklung oder Stornierung neutralisiert werden mag. Die Existenz dieser „Fake-Kunden“ muss jedoch absolut geheim bleibt. Hier gilt: 100 % Chefsache.

Erhält nun eine Scheinadresse Werbung und Angebote eines konkurrierenden Unternehmens, für das der ehemalige Mitarbeiter nunmehr tätig ist, oder von einem vom ehemaligen Mitarbeiter neugegründeten Unternehmen, ist dies ein fast wasserdichter Beweis für einen Missbrauch. Nur das eröffnet die Möglichkeit einer harten und wirkungsvollen Reaktion im Wege des einstweiligen Rechtsschutzes: Unterlassung, Auskunft, Schadensersatz und strafbewehrte Unterlassungsversprechen. Für einen wirkungsvollen Schutz der Kundendaten braucht es mindestens 30 solcher Adressen, bei größeren Unternehmen bis zu mehreren Hundert Adressen. Wichtig ist, dass auch bei einer nachgewiesenen und offengelegten Verletzung immer noch genug versteckte und nicht aufgedeckte Adressen verbleiben, um vor einer Folgeverletzung desselben oder eines anderen Angreifers schützen zu können. Die Kosten für derartige Adressen müssen etwaige Datendiebe erstatten. Unerlässlich ist nur, dass der Schutz VOR dem ersten Verdacht einer Verletzung installiert wird. Nach dem Angriff ist es zu spät und der neue Konkurrent ist nicht mehr zu verhindern.

Rechtsanwalt Harald Brennecke, Karlsruhe.

Rechtsanwalt Brennecke ist Partner der überörtlichen Rechtsanwaltskanzlei Brennecke & Partner.

Mail: brennecke@brennecke-partner.de

Sozialdatenschutz in der privaten Krankenversicherung – ein Auslaufmodell?

Die Änderungen des Versicherungsvertragsgesetzes führen zu neuen rechtlichen Problemen, vor allem im Bereich des Sozialdatenschutzes: Daten, die im Zusammenhang mit einer medizinischen Behandlung erhoben werden, sind solche höchst sensibler Art. Diese zu schützen ist nicht zuletzt Aufgabe von § 203 StGB, Verletzung von Privatgeheimnissen, sondern auch der ärztlichen Berufspflicht. Die ärztliche Schweigepflicht ist wesentlicher Bestandteil des Arzt-Patientenverhältnisses und Grundlage des notwendigen Vertrauensverhältnisses.

Das Problem: Die Kombination von steigender Nachfrage nach medizinischen Leistungen infolge des demografischen Wandels sowie einem sich rasant entwickelndem medizinischen Fortschritt stellt auch das System der Privaten Krankenversicherungen vor erhebliche Herausforderungen. In diesem Zusammenhang haben diese eine Vielzahl von Instrumenten entwickelt, um einer (unberechtigten) Ausweitung medizinischer Leistungen entgegenzuwirken. Dazu gehören auch immer umfangreichere Schweigepflichtentbindungserklärungen. Diese geben die Patienten häufig bedenkenlos ab. Treffen sie doch in ihrer Eigenschaft als Versicherungsnehmer auch Mitwirkungspflichten.

Neu ist, dass diese jetzt bereits zu Beginn einer Behandlung eingefordert werden, sodass es nicht mehr – wie früher – um die Prüfung geht, ob eine Behandlung korrekt abgerechnet wurde, sondern bereits zu Beginn einer Behandlung möglichst weitgehend, auch medizinischen, Einfluss zu nehmen.

Grundsätzlich gilt das Folgende: Gegenüber privaten Versicherungsgesellschaften darf der Arzt nur Auskunft geben, wenn ihm das Einverständnis seines Patienten oder dessen mutmaßliche Einwilligung vorliegt. Anders formuliert: Solange der Patient keine Schweigepflichtentbindungserklärung abgibt, so lange ist der Arzt nicht berechtigt, Informationen an private Krankenkassen weiterzugeben.

Mit der Neuregelung des Versicherungsvertragsgesetzes (VVG), ursprünglich als verbraucherfreundlich gepriesen, werden die Rechte des privat krankenversicherten Patienten in einem Punkt massiv beschränkt: Dieses betrifft das Zusammenspiel von § 194 VVG i.V.m. § 86 VVG.

Bereits der Wortlaut macht die besondere Brisanz der Vorschriften deutlich: Die Regelung des § 194 VVG bestimmt:

Steht dem Versicherungsnehmer oder einer versicherten Person ein Anspruch auf Rückzahlung ohne rechtlichen Grund gezahlter Entgelte gegen den Erbringer von Leistungen zu, für die der Versicherer aufgrund des Versicherungsvertrags Erstattungsleistungen erbracht hat, ist § 86 Abs. 1 und 2 entsprechend anzuwenden.

§ 86 Übergang von Ersatzansprüchen

1. Steht dem Versicherungsnehmer ein Ersatzanspruch gegen einen Dritten zu, geht dieser Anspruch auf den Versicherer über, soweit der Versicherer den Schaden ersetzt. Der Übergang kann nicht zum Nachteil des Versicherungsnehmers geltend gemacht werden.

2. Der Versicherungsnehmer hat sei-

nen Ersatzanspruch oder ein zur Sicherung dieses Anspruchs dienendes Recht unter Beachtung der geltenden Form- und Fristvorschriften zu wahren und bei dessen Durchsetzung durch den Versicherer soweit erforderlich mitzuwirken. Verletzt der Versicherungsnehmer diese Obliegenheit vorsätzlich, ist der Versicherer zur Leistung insoweit nicht verpflichtet, als er infolgedessen keinen Ersatz von dem Dritten erlangen kann. Im Fall einer grob fahrlässigen Verletzung der Obliegenheit ist der Versicherer berechtigt, seine Leistung in einem der Schwere des Verschuldens des Versicherungsnehmers entsprechenden Verhältnis zu kürzen; die Beweislast für das Nichtvorliegen einer groben Fahrlässigkeit trägt der Versicherungsnehmer.

Bislang musste sich der private Krankenversicherer etwaige Rückforderungsansprüche seines Versicherungsnehmers abtreten lassen, wollte er vermeintlich zu viel gezahlte Beträge vom Arzt zurück verlangen. Bei diesem Vorgehen hatte der Patient stets Kontrolle über die Vergütungsabwicklung. Nach der Neufassung ist eine solche Abtretung zukünftig nicht mehr erforderlich; ein vermeintlicher Rückforderungsanspruch geht kraft Gesetzes auf den Versicherer über, und zwar sobald der Versicherer an den Patienten erstattet. Grundlage der Realisierung dieser Ansprüche sind sodann die aufgrund der Schweigepflichtentbindungserklärung des Patienten erlangten Daten.

Welche sensiblen, medizinischen Daten nunmehr beim Privaten Krankenversicherer landen, kann der Patient nicht beeinflussen. Dass Versicherungsgesellschaften möglichst umfangreiche Daten anfordern, um ihre Interessen durchzusetzen, er-

scheint logisch und nachvollziehbar. Der Verlierer ist indes, der Versicherte, der zum gläsernen Patienten wird.

Die Folgen sind dabei aktuell noch gar nicht absehbar: Als gesichert darf indes gelten, dass die Neuregelungen des Versicherungsvertragsgesetzes für den Patienten keine Vorteile gebracht haben, sondern unverhältnismäßig zugunsten der Versicherer ausgestaltet wurden. Die Versicherungsgesellschaft bekomme eine Generalermächtigung, die ihr Möglichkeiten zur Informationserhebung und Auswertung eröffne, die für den betroffenen Versicherungsnehmer völlig undurchschaubar sind.

Konkret bedeutet dieses, dass die Versicherer Fälle über Jahre sammeln können, um dann gegen einzelne Ärzte gerichtlich vorzugehen. Das bedeutet für den Arzt massive

Rechtsunsicherheit, weil er immer damit rechnen muss, mit Klagen überzogen zu werden.

Diese gesetzliche Regelung hat weitgehende Konsequenzen: Es sind schwerwiegende Folgen für das Arzt-Patientenverhältnis zu befürchten. Daneben kommt es zu einer massiven Entwertung der ärztlichen Schweigepflicht. Die Regelung ist im Übrigen auch unverhältnismäßig, da sie einseitig zugunsten der Versicherer ausgestaltet wurde und den Versicherungsnehmer in seinem grundgesetzlich gewährleisteten allgemeinen Persönlichkeitsrecht in seiner Ausprägung als Recht der informationellen Selbstbestimmung verletzt.

In der Praxis gibt es bereits eine Vielzahl von Fällen, in denen von dieser Regelung Gebrauch gemacht wurde.

Die Folgen sind derzeit noch nicht absehbar, dürften aber vor allem das Verhältnis des Patienten zu seinem Arzt betreffen.

Im Zusammenhang mit § 192 Abs. 3 VVG, der dem Versicherer die Möglichkeit zusätzlicher Dienstleistungen einräumt, u. a. die Abwehr unberechtigter Entgeltansprüche der Erbringer von Leistungen, wird das Arzt-/Patientenverhältnis weiter ausgehöhlt. Jedem Versicherten kann daher nur geraten werden, das Gespräch mit seinem Arzt zu suchen, um eine vertrauensvolle Arzt-Patientenbeziehung durch die neue Regelung nicht zu gefährden.

Rechtsanwältin Dr. Birgit Schröder,
Fachanwältin für Medizinrecht,
Hamburg

Mail: Kanzlei@dr-schroeder.com



Kompetenzmessinstrumente, Datenschutz und Betriebsvereinbarungen.

Kompetenzmanagement ist eine unternehmerische Kernaufgabe, die darin besteht, Mitarbeiterkompetenzen kontinuierlich an neue wettbewerbs- und innovationsbedingte Anforderungen anzupassen.

Ob ein Mitarbeiter situationsgerecht handelt und gegebenenfalls seine Voraussetzungen an neue Aufgaben und Anforderungen „selbst organisiert“ anpasst und sogar weiterentwickelt, hängt vom Umfang seiner beruflichen Handlungskompetenz ab. Diese wird durch persönliche Werte und Ideale beeinflusst.

Die Handlungskompetenz wird in Fach- und Methodenkompetenz, Selbstkompetenz und Sozialkompetenz unterteilt. Fachlich-methodische Kompetenz bewirkt, dass sachliches und methodisches Wissen stets ergebnisorientiert angewandt wird. Selbstkompetenz bedeutet selbstkritisch, belastbar und ethisch zu handeln. Verlässlich, teamfähig und kooperativ sind sozial kompetente Menschen.

Kompetenzen erfassen, bewerten, entwickeln und nutzen sind die Aufgaben des Kompetenzmanagements. Ein systematisches Vorgehen macht Kompetenzen im Unternehmen sichtbar. Die sichtbar gemachten Daten können bewertet werden – für das Unternehmen. Die Personalentscheidung (Auswahl, Einsatz, Beurteilung und (Be-)Förderung) fußt auf gesicherten Erkenntnissen. Bildungsangebote lassen sich anforderungs- und bedarfsgerecht sowie zukunftsorientiert auswählen. Führungskräfteentwicklung kann auf die Kompetenzprofile der Mitarbeiter zurechtgeschnitten werden. Für Entlohnungsmodelle stellt das Kompetenzmanagement gesicherte Daten zur Verfügung.

Es kommt also ganz entscheidend auf ein gutes Datenmaterial an. Doch darf diese Daten der Arbeitgeber ohne Weiteres erheben? Welche Voraussetzungen sind zu schaffen? Wie kann die Mitarbeiterschaft motiviert werden, entsprechende Daten zu liefern?

Qualifikation und Kompetenz sind zwei paar Schuhe. Für die Frage nach der Kompetenz sind weite Bereiche des Mitarbeiters außerhalb des Arbeitsverhältnisses wichtig. Besteht ein Engagement im politischen Bereich? Sind Führungsaufgaben in Sportvereinen wahrgenommen worden? Vieles mehr trägt zum Kompetenzbild des Mitarbeiters bei. Da die Daten nicht unmittelbar im Zusammenhang mit dem Arbeitsverhältnis stehen, ist allen Beteiligten angeraten, mittels Betriebsvereinbarung eine Basis für die Datenerhebung, -speicherung und -auswertung zu schaffen.

Zu regeln sind Art und Weise der Datenerhebung. Die Form der Speicherung. Die Zugriffsrechte der im Betrieb beteiligten Gruppen, auch des Betriebsrats. Einsichtsrechte des Mitarbeiters. Datenbewertung und -verwendung etwa im Bereich Führungskräfteentwicklung / Potenzialanalyse. Zuletzt bedarf es eines Datenschutzkonzepts.

Eine Betriebsvereinbarung sollte folgende Punkte enthalten: Klare unmissverständliche Formulierung des Gegenstands der Betriebsvereinbarung, Angaben zum Geltungsbereich (räumlich und personell), die Geltungsdauer, Begriffsbestimmungen (ist dann unverzichtbar, wenn nicht klar definierte Begriffe verwendet werden), die inhaltlichen Regelungen in positiver Darstellung, Schlussvorschriften.

Rechtsanwalt Martin Kull, Baden Baden.

Rechtsanwalt Kull ist Partner der überörtlichen Rechtsanwaltskanzlei Brennecke & Partner.

Mail: kull@brennecke-partner.de

Die Buchführung wird digital.

Die Gesellschaft befindet sich im Wandel. Das Internet wird immer mehr als blitzschnelle, topaktuelle und ständig verfügbare Informations- und Medienplattform eingesetzt. Auch als 24 Stunden überall zugängiger Marktplatz etabliert sich das Internet immer stärker. Die Verbreitung und der selbstverständliche Umgang mit den neuen Möglichkeiten bringen natürlich nicht nur Komfortvorteile, sondern auch neue Gefahren mit sich. Internetkriminalität und der steigende Bedarf nach Sicherheitssystemen nehmen im gleichen Maße wie die Verbreitung zu.

Auch vor der klassischen Finanzbuchführung macht die Entwicklung keinen Halt. Der Wunsch der Unternehmer nach einem modernen zukunftsorientierten System, das die Möglichkeiten des modernen Internets nutzt, führte zu neuen digitalen Möglichkeiten.

Der antiquierte Pendelordner ist out. In der heutigen schnelllebigen Zeit ist der klassische Buchführungsprozess zu langsam und zu ineffizient. Fehlende Belege und Auswertungen, die sechs Wochen hinter dem aktuellen Geschehen herhinken sind im Unternehmensalltag nicht mehr akzeptabel.

Moderne Unternehmen benötigen eine schlanke Buchführung ohne einen zeitaufwendigen Austausch von Papierbelegen. Kurze Wege zur Steuerkanzlei unter Ausnutzung aller möglichen digitalen Schnittstellen sind Pflicht. Das Unternehmen muss jederzeit Herr über seine Belege sein, um damit allen Kunden- und Lieferantenanfragen aktuell beantworten zu können. Benötigte Auswertungen sind aus einer modernen Buchhaltung tagesaktuell möglich. Dies sichert die notwendige Liquidität im Unternehmen und erspart Doppelarbeit, weil keine eigenen Aufstellungen aus Aktualitätsgründen mehr benötigt werden. Der informierte Unternehmer von heute möchte jederzeit also rund um die Uhr, egal wo er sich gerade befindet, Zugriff auf seine Zahlen und sein Buchführungssystem bekommen. In Zeiten des Internets klingt das selbstverständlich. Online Auswertungssysteme müssen so transparent sein, dass jederzeit von der betriebswirtschaftlichen Auswertung (BWA) über die entsprechenden Buchungskonten bis hin zum digitalen Buchungsbeleg geklickt werden kann. Mühsame Belegsuche gehört der Vergangenheit

an – Komfortbelegsuche im digitalen Belegarchiv über verschlagwortete Digitalbelege lassen verstaubten Ordnern keine Chance.

Soweit möglich werden bereits vorhandene digitale Originaldaten verwendet, sei es, dass die Daten der Ausgangsrechnungen direkt aus der Rechnungsschreibung übernommen werden, oder auch Bankumsätze mit detaillierten Hinweisen direkt von den Banken in die modernen Buchführungssysteme übernommen werden. Alle anderen Belege werden über Scannerlösungen zeitnah im Unternehmen digitalisiert und durch moderne OCR-Erkennung in der Buchführung optimal weiterverarbeitet.

Die immer beliebter werdenden elektronischen Rechnungen müssen mit einer qualifizierten elektronischen Signatur versehen und revisionssicher archiviert werden. Ansonsten droht zumindest der Verlust des Vorsteuerabzugs. Also ausdrucken und zur Buchführung geben reicht wirklich nicht. Die gesetzlichen Auflagen werden direkt über die Buchführung erfüllt. Zahlungsvorschläge direkt aus dem Offenen-Posten-System sind durch die Online-Verbindung der aktuellen Bankstände mit der Buchführung transparent und individuell ausführbar. Arbeitsteilige Möglichkeiten wie die Führung von Online-Kassenbüchern, Rechnungseingangsbüchern oder auch die komplette Inhouse-Buchung über ASP-Lösungen, bei der Unternehmen über fremd gewartete und geschützte Systeme online über VPN-Tunnel Zugriff haben, runden die modernen Möglichkeiten ab.

Bei allen Vorteilen wird natürlich der interne und externe Schutz der Daten und Systeme immer wichtiger. Online-Buchführungssysteme müs-

sen über Rechenzentrumslösungen und hochsichere Verschlüsselung soft- und hardwaremäßig geschützt werden.

Gesetzliche Vorschriften, wie die des Bundesdatenschutzgesetzes sind zu erfüllen. Als Datenschutz bezeichnet man den Schutz personenbezogener Daten. Dabei ist es unerheblich ob es sich hierbei um Daten über Mitarbeiter, Kunden, Lieferanten oder sonstige natürliche Personen handelt. Die aktuellen Ereignisse und Pressemeldungen über Datenschutzvorfälle in Unternehmen zeigen, wie wichtig der Schutz von personenbezogenen Daten sowie von Geschäfts- und Berufsgeheimnissen für ein Unternehmen ist und welcher Schaden bei Verstößen entstehen kann. Viele Anforderungen des Datenschutzes beziehen sich auf die Sicherheit der Informationstechnologie. Nur eine zuverlässig funktionierende und sichere IT-Infrastruktur ermöglicht die reibungslose Abwicklung produktiver und verwaltungstechnischer Geschäftsvorfälle und Prozesse.

Auch aufgrund von gesetzlichen Vorgaben durch das Bundesdatenschutzgesetz (BDSG) ist jede Kanzlei verpflichtet, sich mit Datenschutz und Sicherheit auseinanderzusetzen. Demnach ist unter anderem ein Datenschutzbeauftragter (DSB) zu bestellen, wenn bei automatisierter Datenverarbeitung mehr als neun Personen ständig personenbezogene Daten erheben, verarbeiten oder nutzen.

Die Aufgaben des DSB können einem Beschäftigten (intern) oder einer Person außerhalb der Kanzlei (extern) übertragen werden. Bestellt werden darf jedoch nur, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Der DSB muss daher die technische und rechtliche Seite seiner

Aufgaben kennen und gute Kenntnisse in allen Bereichen haben. Nicht zum DSB bestellt werden dürfen der Inhaber selbst, der Geschäftsführer oder sonstige gesetzlich oder verfassungsmäßig berufene Leiter.

Klaus Buser, Kanzlei Buser
Steuerberatung

Mail:
klaus.buser@kanzlei-
buser.de

www.fibu-flitzer.de

Kostenlos ist nicht umsonst!

Kostenlose und kommerzielle Web-Analyse Systeme im Vergleich

Eine Frage stellt sich bei der Auswahl von neuen Software-Lösungen häufig: Soll man zu einem kostenlosen Tool greifen oder sich für ein kommerzielles System entscheiden? Auch im Bereich Web-Analyse stehen potenzielle Anwender vor genau dieser Fragestellung, denn auf

Web-Analyse: Mit einfachen Veränderungen große Wirkung erzielen. Das Internet ist für viele Unternehmen längst zum unverzichtbaren Vertriebs- und Kommunikationskanal geworden. Web-Portale bestehen nicht nur durch ihre enorme Kosteneffizienz, über das Internet lassen sich auch ganz neue Zielgruppen erreichen. Wirtschaftlichkeit und hoher Nutzen sind ausschlaggebende Kriterien, an denen ein erfolgreiches Internet-Geschäft gemessen wird. Deshalb müssen Online-Maßnahmen heute mehr denn je einer zuverlässigen Erfolgskontrolle und -steuerung unterzogen werden können, um vorhandene Potenziale besser zu nutzen und die Effizienz der Maßnahmen zu steigern. Web-Analyse Lösungen ermöglichen die genaue Analyse des Besucherverhaltens von Webauftreten, Shops oder Portalen und versetzen den Betreiber in die Lage, auf Knopfdruck die wirtschaftlichen Erfolgsfaktoren seiner Website und deren Optimierungspotenziale zu erkennen.

dem Markt existiert eine Fülle von Lösungen aus beiden Lagern. Insbesondere das vermeintlich kostenlose Tool Google Analytics ist heute stark verbreitet. Zudem bieten viele Provider eigene Web-Controlling Tools an, die allerdings auf der ungenauen Logfile-Analyse basieren – diese sollen hier ebenso wenig Thema sein wie Open Source-Lösungen für den Betrieb auf eigenen Servern. Vergleicht man kostenlose mit kommerziellen Web-Analyse-Systemen, wird eines schnell klar: Anwender kostenloser Systeme müssen diese Kostenfreiheit auf anderem Weg oft teuer bezahlen – kostenlos ist nicht umsonst.

Ein Blick in die Geschäftsmodelle der Anbieter gibt ersten Aufschluss über die Unterschiede. Während

Anbieter kommerzieller Lösungen den Betrieb und die Weiterentwicklung ihrer Software über die erhobenen Lizenzkosten finanzieren, erfolgt die Finanzierung bei Anbietern kostenfreier Tools über die Monetarisierung der erhobenen Daten. Sie können ihre Tools nur deshalb lizenzkostenfrei anbieten, weil sie die sensiblen Kundendaten für eigene Zwecke weiterverwenden oder an Dritte veräußern. Die anscheinende Kostenfreiheit erscheint gerade für Kleinstanwender oder für Website-Betreiber, die in Web-Analyse hineinschnuppern möchten, verlockend – zumindest auf den ersten Blick. Ob sich diese vordergründige Kostenersparnis wirklich bezahlt macht, hängt allerdings davon ab, welche Anforderungen ein Website-Betreiber an Aspekte wie Datenschutz, Support, Sicherheit und Funktionalität stellt. Denn genau hier liegen die Risiken kostenfreier Tools. Ein großes Problem ergibt sich unmittelbar aus dem Geschäftsmodell: Die Anwender bezahlen zwar nicht mit Lizenzgebühren, aber mit den Daten ihrer Besucher sowie mit Einblicken in ihr eigenes Geschäftsmodell und in die Effektivität ihres Online-Marketings. Vorsicht ist insbesondere dann geboten, wenn kostenfreie Anbieter gleichzeitig als Werbepartner fungieren und diese Einblicke nutzen können, um ihre eigene Rendite etwa durch die Erhöhung der Klickpreise bei besonders effektiven Kampagnen zu optimieren. Bei seriösen kommerziellen Anbietern dagegen gehören die Daten dem Kunden: Eine Weiterverwendung oder Veräußerung der Daten würde gegen die AGBs verstoßen.

Vor der Entscheidung für ein kostenloses Tool, bei dem der Website-Betreiber seine Daten-Hoheit abgibt, sollte er unbedingt eines bedenken: Wenn er seine Daten an einen Web-Analyse-Anbieter übermittelt, be-

deutet dies nach deutschem Recht eine Datenverarbeitung im Auftrag. Das heißt: Der Website-Betreiber haftet, wenn die Erhebung und die Weiterverarbeitung der Daten durch seinen Dienstleister nicht datenschutzkonform erfolgen. Da viele kostenlose Tools datenschutzrechtlich erwiesenermaßen illegal sind und derzeit nur noch toleriert werden, stellt die Nutzung ein erhebliches Risiko für den Website-Betreiber dar. Hinzu kommt, dass bei kostenlosen Tools in der Regel kein Vertragsverhältnis besteht und es damit weder einen Leistungsanspruch noch eine Gewährleistung etwa im Schadensfall gibt. Kommerzielle Anbieter dagegen garantieren hohe Datenverfügbarkeit und sind zur Leistungserbringung verpflichtet. Für kommerzielle Anbieter spricht auch der kostenfreie, kompetente und schnelle Support. Bei kostenlosen Web-Analyse Tools dagegen ist der Support – wenn es überhaupt einen gibt – häufig kostenpflichtig, die Reaktionsgeschwindigkeit auf Anfragen ist deutlich langsamer und es steht auch kein persönlicher Ansprechpartner zur Verfügung. In der Regel verfügen kommerzielle Web-Analyse Systeme zudem über weiterreichende Funktionalitäten – gerade sie verschaffen dem Anwender dank ihrer tieferen Datenanalyse entscheidende Wettbewerbsvorteile.

Insbesondere für private Anwender oder kleinere Website-Betreiber mögen kostenfreie Web-Analyse Tools aus finanzieller Hinsicht erst einmal verlockend erscheinen. Das Argument der Kosteneinsparung relativiert sich jedoch schnell – ihm stehen die beträchtlichen Risiken wie fehlende Datenschutz-Konformität oder fehlende Gewährleistungen entgegen. Für einen professionellen Anwender können gerade diese Risiken unkalkulierbare Kosten nach sich ziehen, die die Lizenzen für ein kom-

merzielles System bei Weitem übersteigen. In seine Entscheidung sollte ein Website-Betreiber zudem einbeziehen, dass auch einige kommerzielle Web-Analyse Unternehmen kostenlose Demoversionen ihrer Systeme und kostenfreie Versionen mit beschränktem Funktionsumfang anbieten – und zwar mit denselben hohen Standards in Sachen Sicherheit, Support und Datenschutz wie bei der kommerziellen Variante des Systems.

Christian Bennefeld

Geschäftsführer (CEO)
der etracker GmbH

E-Mail: info@etracker.com
www.etracker.com

Technik: Um eine Website mit einer Web-Analyse Lösung auswerten zu können, wird ein kleines Stück HTML-Code auf den Webseiten eingebracht. Sobald ein Besucher eine Webseite öffnet, auf der eine Web-Analyse-Technologie eingesetzt wird, lädt er damit ein kleines unsichtbares Pixel, das zu dieser Seite gehört, jedoch aus dem Rechenzentrum des Web-Analyse-Anbieters geladen wird. Im Rechenzentrum werden Zugriffe auf die gekennzeichnete Seite und einige Daten des Besuchers gespeichert.

Kennzahlen und Erfolgsindikatoren
Oft zählen die Kosten-Umsatz-Relation und die Konversionsraten zu den zentralen KPIs einer Internet-Präsenz. Darüber hinaus sind es aber auch aussagekräftige Analyse-Ergebnisse beispielsweise zur Steigerung der Usability einer Website unerlässlich. Schlüsselindikatoren wie Besucherströme setzen sich aus einer Reihe von unterschiedlichen Kennzahlen zusammen. Zu den erhobenen Basisdaten zählen konkrete, direkt ableitbare Ergebnisse wie beispielsweise Seitenaufrufe, Besucheranzahl, Herkunft, Zeitpunkt des Besuchs oder Verweildauer. Unter Anwendung statistischer Berechnungsformeln werden diese Kennzahlen zu den festgelegten KPIs zusammengeführt. So werden vollständige Informa-

tionsprozesse beobachtet und Website-Betreiber erkennen auf einen Blick, welche Themen am meisten nachgefragt werden, an welchem Glied der Navigation besonders viele Abbrüche zutage treten oder wo Schwierigkeiten etwa beim Ausfüllen von Online-Formularen auftauchen. Letztendlich lassen sich sogar geografische Reichweitenanalysen der Website-Benutzer bis hinunter auf Stadt-Ebene durchführen. Zudem kann man so auch Marketing-Kampagnen wie Keyword-Advertising, Bannerwerbung, Affiliate-Marketing oder die Suchmaschinenoptimierung einer ganzheitlichen Erfolgs- und Effizienzkontrolle unterziehen.

Benefits: Die Vorteile einer intelligenten Web-Analyse Lösung liegen auf der Hand: Mit fundierter Nutzer-Kennntnis können Website-Betreiber die Usability ihres Online-Auftritts deutlich verbessern und Beratung, Antragsabwicklung oder auch die Betreuung von Bestandskunden optimal gestalten. Und noch etwas gehört zu den Benefits einer erfolgreichen Web-Analyses: Liefert ein Online-Portal dank Echtzeit-Analyse Inhalte, die die Website-Besucher interessieren und die leicht zu navigieren sind, hat das erfreuliche Auswirkungen auf die Verweildauer und die Zufriedenheit der Nutzer.



Der Modernisierungsbegriff im Wohnungseigentumsrecht.

Wann bedarf es der Zustimmung aller beeinträchtigten Wohnungseigentümer zu einer baulichen Veränderung und wann liegt eine Modernisierungsmaßnahme nach § 22 Abs. 2 WEG vor.

Die von § 22 Abs. 2 Satz 1 WEG angeordnete entsprechende Heranziehung der mietrechtlichen Regelung des § 559 Abs. 1 BGB gibt Raum für eine großzügigere Handhabung des Modernisierungsbegriffes. Der BGH hatte sich in seiner Entscheidung vom 18.2.2011 (V ZR 82/10) mit der Frage zu beschäftigen, wann eine bauliche Veränderung im Sinne des § 21 Abs. 1 WEG und wann eine Modernisierungsmaßnahme gemäß § 22 Abs. 2 WEG vorliegt. Das hat eine entscheidende Bedeutung für die Frage, welche Anforderungen die Beschlussfassung, insbesondere im Hinblick auf die Abstimmung an die Ordnungsgemäßheit des Beschlusses zu stellen sind.

Der BGH vertritt die Auffassung, dass der Begriff der „Modernisierung“ im Sinne des § 22 Abs. 2 WEG großzügig zu handhaben ist. Im Zweifel müsse man sich immer für die Modernisierung entscheiden. Im Streit stand die Wirksamkeit von Beschlüssen über Baumaßnahmen an Schornsteinen. Die Eigentümer hatten einstimmig beschlossen, die Schornsteine in den Häusern zu verschließen und die zugehörigen Dachleitern abzureißen. Anlass für die Baumaßnahmen war die Umstellung der Heizungsanlage. Einige Jahre später wollten mehrere Eigentümer ihre Schornsteine zum Anschluss eines Kamins wieder in Betrieb nehmen, weshalb die Eigentümerversammlung im Juli 2007 beschloss, den „Schornstein-Beschluss“ aufzuheben. Es wurde ferner beschlossen, dass die Eigentümer die Schornsteine wieder zur Nutzung öffnen können, wobei zu jeder Einzelmaßnahme die Zustimmung der Eigentümerversammlung erforderlich sein soll. Die Kosten sollen die jeweiligen Schornstein-Nutzer tragen. Ein Eigentümer hat die Beschlüsse angefochten mit der Begründung, dass es sich bei der Wiederin-

betriebnahme der Schornsteine um eine bauliche Veränderung handle, der sämtliche Wohnungseigentümer zustimmen müssten.

Der BGH ist der Ansicht, dass die Zustimmung sämtlicher Eigentümer nicht erforderlich war. Die von den Wohnungseigentümern gestattete Wiederherstellung der Schornsteine sei eine bauliche Veränderung, die von den Wohnungseigentümer als Modernisierungsmaßnahme mit der erreichten qualifizierten Mehrheit nach § 22 Abs. 2 Satz 1 WEG beschließen konnten. Nach § 559 Abs. 1 BGB, auf den § 22 Abs. 2 WEG verweist, fallen unter den Begriff der Modernisierung alle Maßnahmen, die den Gebrauchswert nachhaltig erhöhen, die allgemeinen Wohnverhältnisse auf Dauer verbessern oder nachhaltig Einsparungen von Energie oder Wasser bewirken.

Vorliegend ist nach Ansicht des BGH von einer nachhaltigen Gebrauchswertsteigerung auszugehen. § 559 Abs. 1 BGB gibt zu einer großzügigeren Handhabung des Modernisierungsbegriffes Anlass. Zum einen kommen den Wohnungseigentümern auch solche Verbesserungen zugute, von denen im Mietrecht nur der Vermieter, nicht aber auch der Mieter profitiert. Zum anderen sollten die Eigentümer mit der Erweiterung der Beschlusskompetenz nach § 22 Abs. 2 WEG die Befugnis erhalten, durch Anpassung der Wohnungsanlage an die „Erfordernisse der Zeit“ mit qualifizierter Mehrheit einer Verkehrswertminderung entgegenzuwirken - unabhängig von einem Reparaturbedarf. Deshalb genügt es, dass die Maßnahme aus der Sicht eines verständigen Wohnungseigentümers eine sinnvolle Neuerung darstellt, die voraussichtlich geeignet ist, den Gebrauchswert nachhaltig zu erhöhen. Die Möglichkeit, einen Kamin

zu befeuern, führt zu einer nachhaltigen Erhöhung des Gebrauchswerts des Wohnungseigentums. Hierdurch kann eine Möglichkeit geschaffen werden, den Wohnkomfort zu steigern und einen anderen Brennstoff zu nutzen und hierdurch ggf. Kosten zu sparen. Außerdem können die Eigentumswohnungen auf dem Immobilienmarkt attraktiver werden.

Ob die Einrichtung einer zusätzlichen Heizquelle eine Einsparung des Energieverbrauchs bewirkt, ist für die Frage einer nachhaltigen Erhöhung des Gebrauchswerts ebenfalls unerheblich. Diesem Umstand kommt nur Bedeutung für die dritte der - jeweils selbstständigen - Modalitäten des § 559 Abs. 1 BGB zu, unter denen die Eigentümer nach § 22 Abs. 2 Satz 1 WEG eine bauliche Veränderung mit qualifizierter Mehrheit beschließen können. Die beschlossene Maßnahme ändert auch nicht die Eigenart der Wohnungsanlage. Ebenso stellt sie keine Luxussanierung dar und die ablehnenden Eigentümer werden nicht unbillig benachteiligt.

Rechtsanwalt Peter Hesse, Fachanwalt für Miet- und Wohnungseigentumsrecht, Potsdam.

Rechtsanwalt Hesse ist Partner der überörtlichen Rechtsanwaltskanzlei Brennecke & Partner.

Mail: hesse@brennecke-partner.de

„Compliance“ – braucht mein Unternehmen so etwas?

Immer wieder liest man in der Presse von „Compliance“, „Compliance-Abteilungen“ oder „Compliance-Managern“. Was bedeuten diese Begriffe und für welche Unternehmen ist z. B. die Einrichtung einer „Compliance-Abteilung“ sinnvoll oder gar notwendig?

I. Bedeutung

Der Begriff Compliance leitet sich vom englischen „to comply with“ (übereinstimmen mit) ab. Er bezeichnet die Selbstverpflichtung eines Unternehmens bzw. dessen Führungskräfte, sich an alle vom Gesetzgeber, den Anteilseignern oder dem Aufsichtsgremium aufgestellten Regeln zu halten. Damit soll sowohl ein negatives Image vermieden als auch Haftungsfälle bzw. Schadensersatzklagen ausgeschlossen werden. Damit ist Compliance heute eine Aufgabe, die sich durch alle Rechtsgebiete zieht. Somit müssen Juristen, Revision, Controlling, Personalabteilung, Öffentlichkeitsarbeit, Marketing und vor allem die Geschäftsleitung einbezogen werden. Compliance soll Geschäftsleitung und Mitarbeiter vor bewussten und unbewussten Regelverstößen sowie die Kunden vor nicht interessengerechter Behandlung schützen. Es handelt es sich vor allem um Organisationsrecht, das zur Überwachung der Einhaltung der Vorschriften entsprechende Strukturen schafft.

Die rechtlichen Grundlagen von Compliance sind vielfältig: So ordnen z. B. §§130, 30 OWiG an, dass Betriebsinhaber, Vorstände und Geschäftsführer Aufsichtsmaßnahmen ergreifen müssen, die verhindern, dass im Unternehmen bestimmte betriebsbedingte Pflichten – z. B. der Arbeitsschutz – umgangen werden.

Besonders „bekannt“ ist Compliance im Bereich des Wertpapierhandelsrechts, also bei Banken und sonstigen Finanzdienstleistungsunternehmen. Dort ist die Bestellung eines Compliance-Beauftragten gemäß §§ 33 Abs. 1 Satz 2 Nr. 1 WpHG in Verbindung mit § 12 Abs. 4 Satz 1 WpDVerOV sogar gesetzlich vorgeschrieben. Oft ist der Complian-

ce-Beauftragte dort zugleich auch Geldwäschebeauftragter.

In Unternehmen kann auch die Funktion des Datenschutz- oder eines Gleichstellungsbeauftragten in der Complianceabteilung angesiedelt sein.

II. Anforderungen an die Compliance Organisation

Die Compliance Abteilung kann ihre Aufgaben natürlich nur wahrnehmen, wenn sie die entsprechenden Mittel vom Unternehmen zur Verfügung gestellt bekommt, und zwar in Form von Personal- und Sachmitteln.

Eine Compliance Abteilung ist außerdem nur sinnvoll, wenn sie in fachlicher, organisatorischer und disziplinarischer Hinsicht unabhängig tätig werden kann. Sie darf fachlich nur der Unternehmensführung, der die Gesamtverantwortung für die Geschäftsorganisation und damit auch für die Funktionsweise der Compliance Abteilung im Unternehmen zugewiesen ist, weisungsgebunden sein.

Die entsprechenden Mitarbeiter dürfen selbst nicht an den Aufgaben bzw. Leistungen, die sie in Compliance Abteilung zu überwachen haben, beteiligt sein. Ihre Vergütung darf weder mittel- noch unmittelbar vom Ergebnis der Geschäftsbereiche abhängig sein, die von ihnen zu überwachen sind. Nur die Verknüpfung mit dem Gesamtergebnis der Unternehmen ist zulässig.

Nach § 12 Abs. 4 Satz 2 WpDVerOV – dessen Rechtsgedanke auch auf alle anderen Unternehmen übertragbar ist – müssen die mit der Wahrnehmung der Compliance-Aufgaben betrauten Mitarbeiter über die „erforderlichen Fachkenntnisse, Mittel

und Kompetenzen sowie über Zugang zu allen für ihre Tätigkeit relevanten Informationen verfügen“. Einen „Lehrberuf“ für den Compliance-Beauftragten gibt es nicht. Es gibt auch keine normierten Vorgaben etwa hinsichtlich Berufserfahrung oder –ausbildung, sodass das Unternehmen einen gewissen Spielraum hat, welche Mitarbeiter es im Compliance-Bereich einsetzt. Insgesamt macht die Einrichtung einer Compliance Abteilung jedoch nur Sinn, wenn die Compliance-Mitarbeiter aufgrund ihrer Ausbildung und ihrer Erfahrung in der Lage sind, die von ihnen überwachten Tätigkeiten im Unternehmen nachzuvollziehen.

III. Aufgaben

Grundsätzlich hat die Compliance Abteilung die Aufgabe, die sich aus dem Betrieb des Unternehmens und aus einer möglichen Verletzung gesetzlicher Pflichten ergebenden Compliance-Risiken herauszufinden, zu benennen und entsprechend zu bewerten. Auch Art und Häufigkeit von Kundenbeschwerden können dabei hilfreich sein. Darauf aufbauend sollen dann Strategien, Vorgehensweisen und Abläufe festgelegt werden, die die Wahrscheinlichkeit, dass sich ein erkanntes Risiko auch realisiert, vermindern oder besser noch ausschließen sollen.

Die Compliance-Abteilung ist (neben einer eventuell vorhandenen Rechtsabteilung) auch dafür zuständig, dass gesetzliche und richterrechtliche Vorgaben (z. B. beim Arbeitsschutz) umgesetzt werden.

Schließlich sollte man die beratende Funktion einer Compliance-Abteilung nicht unterschätzen. Werden z. B. neue Geschäftsmodelle erarbeitet, sollte die Compliance-Abteilung eingebunden werden, um von Beginn

an eine regelkonforme Ausgestaltung zu fördern.

Zusätzlich sollten sämtliche Mitarbeiter über compliancerelevante Inhalte geschult werden (Präsenzschulung oder IT-gestützt).

IV. „Whistleblowing“

„Whistleblowing“ ist das, was man früher unter „petzen“ verstand: die Weitergabe eines im Unternehmen begangenen Verstoßes an zuständige Stellen innerhalb oder außerhalb des Unternehmens. Das Bundesarbeitsgericht hat bereits mit Urteil vom 03.07.2003 (2 AZR 235/02) festgestellt, dass die Einreichung einer Strafanzeige eines Mitarbeiters gegen einen Vorgesetzten als Wahrnehmung staatsbürgerlicher Rechte grundsätzlich keine Kündigung rechtfertigen kann.

Gesetzlich ist das bisher nicht geregelt. Im Jahr 2008 gab es den Versuch, den bestehenden § 612 a BGB wie folgt zu ändern:

„§ 612a · Anzeigerecht

A. Ist ein Arbeitnehmer aufgrund konkreter Anhaltspunkte der Auffassung, dass im Betrieb oder bei einer betrieblichen Tätigkeit gesetzliche Pflichten verletzt werden, kann er sich an den Arbeitgeber oder eine zur innerbetrieblichen Klärung zuständige Stelle wenden und Abhilfe verlangen. Kommt der Arbeitgeber

dem Verlangen nach Abhilfe nicht oder nicht ausreichend nach, hat der Arbeitnehmer das Recht, sich an eine zuständige außerbetriebliche Stelle zu wenden.

B. Ein vorheriges Verlangen nach Abhilfe ist nicht erforderlich, wenn dies dem Arbeitnehmer nicht zumutbar ist. Unzumutbar ist ein solches Verlangen stets, wenn der Arbeitnehmer aufgrund konkreter Anhaltspunkte der Auffassung ist, dass

1. aus dem Betrieb eine unmittelbare Gefahr für Leben oder Gesundheit von Menschen oder für die Umwelt droht,
2. der Arbeitgeber oder ein anderer Arbeitnehmer eine Straftat begangen hat,
3. eine Straftat geplant ist, durch deren Nichtanzeige er sich selbst der Strafverfolgung aussetzen würde,
4. eine innerbetriebliche Abhilfe nicht oder nicht ausreichend erfolgen wird.

C. Beschwerderechte des Arbeitnehmers nach anderen Rechtsvorschriften und die Rechte der Arbeitnehmervertretungen bleiben unberührt.“

Dieser Entwurf ist nicht Gesetz geworden. Auf dem G 20 Gipfel in

Seoul (November 2010) hat sich die Bundesregierung jedoch verpflichtet, durch ein entsprechendes Gesetz bis Ende 2012 Hinweisgeber zu schützen.

Schon jetzt unterhalten einige Unternehmen ein innerbetriebliches Whistleblowing-System, damit Mitarbeiter innerbetriebliche Straftaten ohne Sorge vor Repressalien von Vorgesetzten und / oder Mitarbeitern melden können. Die Compliance-Abteilung ist dabei Ansprechpartner für die Arbeitnehmer. Allerdings darf nicht verkannt werden, dass immer auch die Möglichkeit der Denunziation gegeben ist.

V. Fazit

Außer für Banken und sonstige Wertpapierdienstleistungsunternehmen ist die Einrichtung einer Compliance-Abteilung gesetzlich nicht vorgeschrieben. Dennoch kann sie – zumal in größeren Unternehmen – durchaus sinnvoll sein, vor allem, wenn sie mehrere Funktionen, z. B. den Datenschutzbeauftragten, auf sich vereint.

Rechtsanwältin Anja Uelhoff, Fachanwältin für Bank- und Kapitalmarktrecht, Hamburg.

Rechtsanwältin Uelhoff ist Partnerin der überörtlichen Rechtsanwaltskanzlei Brennecke & Partner

Mail: Uelhoff@brennecke-partner.de



Führung ist nicht nur Chefsache, Führung ist auch Gehirnsache.

Bei Worten wie "Führung", "Führer" und "Macht" zucken wir Deutschen irgendwie innerlich immer noch ein ganz kleines bisschen zusammen. Die gleichen Worte im Englischen erscheinen uns weniger verdächtig: "Leadership", "leader" und "power" fühlen sich irgendwie besser, sportlicher, an. In der englischen Sprache sind wir leichter bereit, auf die Frage: „What does it take to be a leader?“ ins Ersinnen einer brauchbaren Antwort zu kommen, in der deutschen Sprache fragen wir doch lieber: Was bedeutet Führungskompetenz?

Historisch betrachtet ist interessant, dass diese Frage noch gar nicht so alt ist, noch vor ca. siebzig Jahren war die allgemein vorherrschende Meinung die, dass Führung ein unerklärbares Phänomen, eine Naturbegabung von besonders charismatischen Persönlichkeiten sei.

Aber wonach wird eine Führungskraft letzten Endes tatsächlich beurteilt? Die pragmatische Antwort ist: nach ihren Ergebnissen für das Unternehmen oder das Projekt, das sie führt. Also ist die vielleicht hilfreichere Frage die: Welche Eigenschaften machen eine Führungskraft erfolgreich? Das hängt davon ab, welches Ziel das Unternehmen verfolgt.

Machtpositionen sind Vertrauenspositionen. Führungskräften wird von Menschen Vertrauen entgegengebracht, in der Erwartung das Unternehmen nachhaltig zu führen, die ihnen anvertrauten Unternehmensressourcen richtig zu behandeln und die Unternehmensprodukte oder die Unternehmensdienstleistung optimal zu verkaufen. Und verkauft wird das Produkt an Menschen. Und gemacht wird das Produkt von Menschen für Menschen.

Was also führt eine Führungsperson? Richtig: in erster Linie Menschen.

Heute ist man sich jedenfalls in der wissenschaftlichen - auch der neurowissenschaftlichen - Theorie darüber einig, dass eine erfolgreiche Führungskraft in erster Linie gut mit Menschen umgehen können soll.

Es wird postuliert, dass Führungs-

kräfte selbst Vorbild sind, anspruchsvolle und sinnvolle Ziele im Unternehmensinteresse vorgeben, ihre Mitarbeiter zu entsprechender Leistungsbereitschaft und Loyalität motivieren und - selbst innovativ-flexibel - die Kreativität und die Stärken der Mitarbeiter fördern und entwickeln.

Die Notwendigkeit sich immer schneller wirkenden Veränderungsprozessen anzupassen, beantworten viele Unternehmen mit starren Organisationsstrukturen von Zielvorgaben, Arbeitsanweisungen, Richtlinien und Ablaufplänen, um möglichst von vornherein Fehlerquellen auszuschalten. Diese Rechnung geht aber nicht auf, wie Studien und Sachverständigengutachten zum Thema Mitarbeiterzufriedenheit und Loyalität gezeigt haben: mehr als 60 % der Mitarbeiter der untersuchten Unternehmen sind unzufrieden und unmotiviert, Führungskräfte halten dem Druck nicht mehr stand und Stress, Burn-out und Depression nehmen kontinuierlich zu. Weil der "Faktor Mensch" bei all diesen strategischen Maßnahmen auf der Strecke bleibt. Funktionierende Führung, erfolgreiche Führung, bedeutet in erster Linie: die Anwendung von Fähigkeiten im Umgang mit Menschen.

Und wie man das am besten macht, damit hat sich auch die jüngste Gehirnforschung beschäftigt und Antworten gefunden. Wenn man Mitarbeiter motivieren will, dann ist es nützlich zu wissen, dass unser menschliches Gehirn unter vielen anderen Aspekten über vier wichtige Systeme verfügt: das Belohnungssystem, das Emotionssystem, das Erinnerungssystem und schließlich das

Entscheidungssystem. Diese vier Systeme sind maßgeblich dafür verantwortlich, ob und in welchem Umfang Führung und Motivation von Mitarbeitern gelingt. Und übrigens auch, wie die jüngsten Erkenntnisse im Bereich des Neuromarketings herausgefunden haben, wie man potenzielle Kunden motiviert das Unternehmensangebot zu erwerben. Es sind diese vier Systeme im menschlichen Gehirn, die Menschen dazu bewegen "mitzuspielen" oder nicht.

Daher stellt sich also für Führungskräfte die Frage, wie, mit welchem Verhalten und mit welchen Maßnahmen, man die vier Systeme von Mitarbeitern so aktiviert, dass das gewünschte Ergebnis herauskommt. Unstreitige Voraussetzung ist, dass die Führungsperson selbst Vorbild sein muss, damit sie für den Mitarbeiter glaubwürdig ist und dass die Führungskraft die Einzigartigkeit des Gehirns - seines eigenen und das der Mitarbeiter - anerkennt. Die Vorbildfunktion ist für die menschliche Lernbereitschaft das stärkste Instrument. Lernen am Vorbild hat uns unsere ersten grundsätzlichen Fähigkeiten wie Sprache, soziales Verhalten und Werte schon in frühester Kindheit gelehrt und das bleibt auch bei Erwachsenen so.

Das Belohnungssystem wird sehr vereinfacht auf den Punkt gebracht durch eine erhöhte Ausschüttung des Neurotransmitters Dopamin bewegt. Dopamin ist ein "Glückserwartungshormon", das dafür sorgt, dass sich eine Bemühung als lohnenswert erfahren lässt. Solange das angestrebte Ziel noch verfolgt wird, also

auf dem Weg zum Ziel, wird Dopamin, eine Art körpereigene Wohlfühl- und Belohnungsdroge, ausgeschüttet. Ist das Ziel erreicht, verringert sich die Dopaminausschüttung. Dann wird statt dessen Serotonin, ein Neurotransmitter, der Gefühle von Beruhigung und Zufriedenheit erzeugt, wirksam. Herkömmlicherweise werden in Unternehmen zur Belohnung von Mitarbeitern Geschenke, Incentives oder Zusatzeinkünfte am Jahresende eingesetzt. Diese Maßnahmen aktivieren aber das Belohnungssystem, die Dopaminausschüttung der Mitarbeiter, nicht kontinuierlich, sie erzeugen statt dessen einen Gewöhnungseffekt, eine "Sucht nach mehr". Erfolgen Anerkennung, Wertschätzung und Belohnung dagegen unerwartet und situativ, so tritt der Gewöhnungseffekt im Gehirn nicht ein.

Eine freundliche, echte Anerkennung, ein sympathisches Lächeln, aufrichtig gegebene Aufmerksamkeit aktivieren das Belohnungssystem im Gehirn ebenso wie kleine, angenehme Überraschungen.

Das Emotionssystem im Gehirn ist die Bewertungszentrale für eingehende neuronale Reize. Aus der Sicht der Gehirnforschung sind Emotionen wie Freude, Trauer, Wut oder Angst ganz unromantisch "chemische Prozesse" im limbischen Gehirn. Der "Bewerter" eingehender Reize in diesem Hirnareal ist die "Amygdala", der sogenannte Mandelkern, der entscheidet, ob ein Gefühl als angenehm oder unangenehm erlebt wird. Dies geschieht unbewusst und rasend schnell, viel schneller, als die erst später einsetzende bewusste Verstandesbewertung, die im Neokortex, im linken Stirnbereich des Großhirns, erfolgt. Wir fühlen schon, ob etwas gut für uns ist, längst bevor unser Verstand zum Zuge kommt. Deshalb ist es wenig wirksam von Mitarbeitern ein auf verstandesmäßigen Argumenten beruhendes Verhalten einzufordern, das emotional auf Widerstand stößt.

Eine Weile lang kann das scheinbar gut gehen, auf Dauer aber verweigert der gefühlsmäßig übergangene Mitarbeiter die Kooperation und Loyalität. Diese "innere Kündigung"

ist die konsequente Folge eines Gefühls von Hilflosigkeit gegenüber unsozialem, unfairem oder werteverachtendem Verhalten aufseiten einer "durchsetzungsstarken", mitgeföhlsarmen Führungspersönlichkeit. Die Chemie stimmt dann eben nicht. Rachegefühle und Sabotage von Mitarbeitern sind nicht selten die Konsequenz. Herrscht in einem Unternehmen gar ein Klima von Misstrauen und dauerhaftem Druck vor, so wird im Mitarbeiter-Gehirn vermehrt das Stresshormon Cortisol ausgeschüttet, das Angstgefühle erzeugt. Dauerstress schließlich verursacht den krankhaften Zustand, den wir als Burn-out bezeichnen.

Umgekehrt, wenn die Führungsperson sich ehrlich interessiert, anerkennend und wertschätzend gegenüber dem Mitarbeiter verhält, wird der Motivationsmix aus Dopamin, dem Bindungshormon Oxytocin und körpereigenen Opioiden für hoch motivierte Mitarbeiter im Unternehmen sorgen. Nichts stimuliert Menschen so sehr wie das Bedürfnis von ande-

ren gesehen zu werden, die Erfahrung von positiver Zuwendung und Liebe.

Oder weniger psychologisch ausgedrückt: Unser Gehirn ist ein soziales Organ. Führen FührerInnen unter Berücksichtigung dieser urmenschlichen Grundbedürfnisse der Mitarbeiter, führen sie sozial kompetent, klar und aufrichtig, dann motivieren sie zu leistungstarker Mitarbeit. So wird aus gehirnwissenschaftlicher Sicht Kooperation erzeugt.

Rechtsanwältin Friederike Matheis

Die Autorin ist Juristin, Mediatorin, freie Dozentin für Schlüsselqualifikationen an der rechtswissenschaftlichen Fakultät der Universität Hamburg und Mitinhaberin des Unternehmens Pro-Viel-Seminare GbR.

Mail:
f.matheis@pro-viel-seminare.de

www.pro-viel-seminare.de



Vereinsmitgliedschaft – in steuerrechtlicher Hinsicht

Der arbeitsrechtliche und der steuerrechtliche Arbeitnehmerbegriff sind nicht identisch. Für die Bestimmung der Arbeitnehmerereignis in Lohnsteuerrechtlicher Hinsicht enthält § 1 I LStDV eine eigenständige steuerrechtliche Definition. Danach sind Arbeitnehmer alle natürlichen Personen, die in einem privaten Dienstverhältnis angestellt oder beschäftigt sind und daraus ihren Arbeitslohn beziehen. Nach § 1 II LStDV ist dafür entscheidend, dass der Steuerpflichtige in die Organisation des Arbeitgebers eingegliedert ist oder/und dessen Weisungen unterliegt.

Ein Vereinsmitglied kann als Arbeitnehmer, als Vereinsmitglied oder

aber auch als Selbstständiger für den Verein tätig werden. Übt das Mitglied Tätigkeiten aus, die die Mitgliedschaftsgebundene Erfüllung von Vereinsaufgaben wie z. B. die Teilnahme an Mitgliederversammlungen, Tagungen und Sitzungen darstellt, so begründet dies nicht die Annahme eines Arbeitnehmerstatus gegenüber dem Verein. Die Mitglieder werden allein aufgrund vereinsvertraglicher Verpflichtungen tätig. Übt das Vereinsmitglied allerdings eine weisungsgebundene Tätigkeit aus, die der Verein organisiert und in der Regel vergütet, geht diese über die Erfüllung von mitgliedsgebundenen Vereinsaufgaben hinaus und es ist von einem Dienstverhältnis und einem Arbeitnehmerstatus des Mitgliedes auszugehen.

Grundsätzlich ist das ehrenamtlich tätige Vereinsmitglied nicht als Arbeitnehmer in steuerrechtlicher Sinne zu behandeln. Maßgebendes Kriterium für die Beurteilung ist auch hier, ob eine Eingliederung in die Vereinsorganisation vorliegt. Diese fehlt bei gelegentlichen Tätigkeiten. Auch die Vergütung ist ein Ansatzpunkt für die Qualifizierung: Erhält der ehrenamtlich Tätige vom Verein keine Vergütung, sondern lediglich einen Aufwendungsersatz (d. h. tatsächliche Unkostenerstattung wie z. B. Reise-, Porto- oder Telefonkosten), ist der Arbeitnehmerstatus nicht gegeben. Zahlt der Verein dagegen eine Kostenpauschale, die den tatsächlich entstandenen Aufwand nicht nur unwesentlich überschreitet, ist der ehrenamtlich Tätige als Arbeitnehmer zu behandeln mit der Folge, dass die Einnahmen als sonstige Einnahmen nach § 22 Nr. 3 EStG zu versteuern sind.

Ob das Vorstandsmitglied oder der Geschäftsführer eines Vereins als Arbeitnehmer zu qualifizieren ist, hängt nicht von deren Organstellung ab, sondern richtet sich nach

den allgemeinen Kriterien zur Lohnsteuerrechtlichen Bestimmung des Arbeitnehmerbegriffs. Entscheidende Kriterien sind also die Weisungsgebundenheit durch die Mitgliederversammlung sowie die Integration in die Vereinsorganisation. Trotz weitgehender Unabhängigkeit des Vorstandes und des Geschäftsführers bejaht die Rechtsprechung deren Arbeitnehmerstellung in steuerrechtlicher Hinsicht.

Ob die Vergütungen des einzelnen Arbeitnehmers eines gemeinnützigen Vereins letztendlich der Einkommensteuer unterliegen, hängt davon ab, ob die Steuerbefreiung nach § 3 Nr. 26 EStG greift. Nach dieser Vorschrift sind u.a. Einnahmen aus nebenberuflichen Tätigkeiten als Übungsleiter, Ausbilder, Erzieher, Betreuer oder vergleichbaren nebenberuflichen Tätigkeiten bis zur Höhe von insgesamt 2.100 Euro für Tätigkeiten zur Förderung gemeinnütziger, mildtätiger oder kirchlicher Zwecke grundsätzlich steuerfrei.

Marc Wandersleben, Rechtsanwalt
Hannover

Rechtsanwalt Wandersleben ist Partner der überörtlichen Rechtsanwaltskanzlei Brennecke & Partner.

Ass. jur. Isabell Hartung.



Private Krankenversicherungen – (k)eine gute Wahl?

Auch die Privaten Krankenversicherer bleiben von steigenden Ausgaben nicht verschont – mit erheblichen Folgen für ihre Versicherungsnehmer:

Privat krankenversicherte Patienten entscheiden sich gerade für einen privaten Krankenversicherungsschutz, weil sie sich bessere Leistungen und besseren Service versprechen. Um so größer ist der Ärger, wenn anstelle vollmundiger Werbeversprechen Ärger um die Rechnungserstattung tritt. Sie erleben es immer häufiger, dass die Erstattung von Arztrechnungen nicht problemlos vonstattengeht. Immer häufiger wird die medizinische Indikation einzelner Leistungen infrage gestellt oder gebührenrechtliche „Nebenkriegsschauplätze“ eröffnet.

Patienten müssen trotz umfangreicher Begründung seitens des behandelnden Arztes immer häufiger klagen, um ihre Rechte durchzusetzen. Dabei darf als gesichert gelten, dass die privaten Krankenversicherungen mit einer Vielzahl von Versicherungsnehmern rechnen, die wegen des Aufwandes eines Gerichtsverfahrens ihr berechtigtes Erstattungsverlangen nicht prozessual geltend machen.

Dieses Geld als „ersparte Aufwendungen“ dürfte eine wirtschaftliche nicht zu unterschätzende Größenordnung einnehmen. Dabei sind es nicht immer große Beträge, sondern vielmehr die Summe aus vielen Kleinbeträgen, die sich summieren. Eine Salamtaktik, die aufgeht.

Das Problem

Im Rahmen der privaten Krankenversicherung gibt es keinen vorgegebenen Leistungskatalog – vielmehr stellt sich der Versicherungsnehmer seinen Krankenversicherungsschutz individuell und bedarfsgerecht zusammen. Das führt dazu, dass die

Verträge selbst innerhalb einer Versicherungsgesellschaft stark variieren und damit für den Versicherungsnehmer nicht immer erkennbar ist, welche Leistungen er beanspruchen kann. Anders als bei der gesetzlichen Krankenversicherung, in der das Sachleistungsprinzip gilt, bekommt der privat krankenversicherte Patient von seinem behandelnden Arzt eine Rechnung. Er ist Kostenschuldner des (zahn)ärztlichen Honorars. Der Patient befindet sich damit in einer für ihn ungünstigen Dreiecksbeziehung wieder: Er schließt einen Behandlungsvertrag mit dem Arzt, dem er sein Honorar schuldet und bekommt – jedenfalls im Idealfall – von einer privaten Krankenversicherung den Betrag erstattet. So weit die Theorie.

Wenn alles problemlos läuft, gut – was aber, wenn die Erstattung ganz oder teilweise ausbleibt? Die Versicherung erstattet eine Arztrechnung nicht oder nur unvollständig. Zur Begründung werden formelhafte Textbausteine angegeben, die etwa auf die fehlende medizinische Indikation verweisen, die Abrechenbarkeit einer einzelnen Leistung negieren oder den Gebührensatz für überhöht halten. Überweist der Patient dem Arzt sein Honorar nicht oder nur unvollständig, so sieht er sich ggf. einer Klage seitens des Arztes/Abrechnungsgesellschaft ausgesetzt.

Hat der Patient den vollen Betrag bereits an den Arzt überweisen, wird er sich überlegen müssen, ob und wie er mit der immer schlechter werden den Zahlungsmoral umgeht. Ein Anruf oder ein Schreiben an die Leistungsabteilungen der Versicherer hilft in der Regel nicht weiter. Bestenfalls lässt sich damit eine Kulanzentscheidung erreichen, die zumindest einen Teilbetrag umfasst. Wer allerdings den vollen Erstattungsbetrag erreichen möchte, kommt in der Regel um eine gerichtliche Klärung nicht

umhin. Genau diesen Weg scheuen Versicherte – und das nicht ohne Grund. Streitigkeiten mit dem Versicherer müssen vor den Zivilgerichten ausgetragen werden und bergen immer ein gewisses Prozessrisiko. Und dennoch: Der Kampf lohnt sich (fast) immer. Gerichte entscheiden tendenziell versicherungsnehmerfreundlich, sodass sich die Weiterverfolgung der Ansprüche anbietet. Dazu kommt, dass die Vergleichsbereitschaft der Versicherungsgesellschaften vor Gericht deutlich ausgeprägter ist – nicht zuletzt deshalb, weil sie Urteile vermeiden möchten. Im Internet und den Medien verbreiten sich diese in der Zwischenzeit schnell und unkompliziert und bieten somit anderen Versicherungsnehmern gute Argumentationsmöglichkeiten.

Der Weg vor Gericht

Nach Eingang der Klagschrift und Austausch der Argumente wird das Gericht entweder direkt einen Vergleichsvorschlag unterbreiten oder zunächst einen Beweisbeschluss erlassen und einen Sachverständigen beauftragen. Dieser Sachverständige wird, die seitens des Gerichts formulierten Fragen beantworten und damit das Gericht fachlich unterstützen.

Anders als die „beratenden Ärzte“ der Versicherungen, die quasi einen klaren Arbeitsauftrag haben und beispielsweise den Begriff der medizinischen Notwendigkeit entsprechend restriktiv verfolgen, treffen Sachverständige eine unabhängige Entscheidung.

Häufige Streitpunkte

Immer wieder wird um die Frage gestritten, was medizinisch notwendig ist. Dabei ist zunächst zu berücksichtigen, dass dabei ein objektiver, allein medizinischer Maßstab gilt. Nicht entscheidend ist daher, was der behandelnde Arzt bzw. Versicherungs-

nehmer oder Versicherungsgesellschaft meint. Es muss also nicht jede beliebige Behandlung bezahlt werden, sondern nur für solche, die objektiv geeignet sind, Leiden zu heilen, zu bessern oder zu lindern. Dabei dürfen jedoch Kostengesichtspunkte keine Rolle spielen. Die Versicherung schuldet dem Patienten aus dem Krankenversicherungsvertrag die Erstattung der Kosten für die medizinisch notwendige Heilbehandlung.

Dauerbrenner sind in diesem Zusammenhang die LASIK-Operationen, bei denen die Versicherer in der Regel nicht damit gehört werden, dass die Behandlungsmethode gegenüber Brille und Kontaktlinsen nachrangig sei oder vorrangig günstigere oder gefahrlosere Behandlungen durchzuführen seien.

Im Rahmen zahnprothetischer Arbeiten beschränken sich die Versicherer gerne darauf, pauschal und ohne nähere Darlegung der Sach- und Rechtslage die Angemessenheit der Material- und Laborkosten zu bestreiten. Auch im Rahmen der Versorgung mit Zahnimplantaten hat die Rechtsprechung entschieden, dass sich der Patient nicht auf die kostengünstigste Methode verweisen lassen muss. Bei sog. Analogleistungen, also solchen, die nicht in der Gebührenordnung der Ärzte/Zahnärzte beschrieben sind, gibt es ebenfalls Diskussionen um die medizinische Notwendigkeit.

Fazit:

Für Versicherungsnehmer lohnt es sich, sich der Salamtaktik des Versicherers nicht zu beugen und Erstattungsansprüche offensiv zu verfolgen.

Rechtsanwältin Dr. Birgit Schröder,
Fachanwältin für Medizinrecht,
Hamburg

Mail: Kanzlei@dr-schroeder.com



Aktuelle Zinssätze

Für den Zeitraum 01.01.2011-30.06.2011:

Basiszinssatz (§ 247 Abs. 1 BG) 0,12 %

Zinssatz für Verbrauchergeschäfte

(§ 288 Abs. 1 S. 2 BGB) 5,12 %

Zinssatz für Handelsgeschäfte

(§ 288 Abs. 2 BGB) 8,12 %

Quelle: www.basiszinssatz.info

Absage an Netzsperrern im Kampf gegen Kinderpornografie

Das Bundeskabinett hat am 25.05.2011 einen Regierungsentwurf zur Aufhebung des Zugangser schwerungsgesetzes beschlossen. Die Bundesregierung setzt auf den Grundsatz „Löschen statt Sperren“. Die Bundesregierung will in einem weiteren Schritt eine „Stiftung Datenschutz“ auf den Weg bringen. Die Stiftung soll Strategien zur Sensibilisierung der Bürgerinnen und Bürger beim Umgang mit den eigenen persönlichen Daten entwerfen sowie Gütesiegel für Produkte und Dienstleistungen entwickeln. Damit sollen neue Standards für sichere Internetangebote gesetzt und der Datenschutz in doppelter Hinsicht gefördert werden: Die Gütesiegel könnten für die Unternehmen ein echter Wettbewerbsvorteil sein, und Verbraucher könnten sich bewusst für ein hohes Datenschutzniveau entscheiden.

Die in den letzten Monaten intensivierte Zusammenarbeit zwischen dem Bundeskriminalamt und den Beschwerdestellen der Internetwirtschaft hat zu diesen Ergebnissen geführt.

Der am 25.05.2011 beschlossene Regierungsentwurf enthält im Wesentlichen folgende Regelungen:

Aufhebung des Zugangser schwerungsgesetzes (Artikel 1 des Gesetzes zur Bekämpfung von Kinderpornografie in Kommunikationsnetzen vom 18.02.2010), mit dem Internetzugangsp provider verpflichtet wurden, die Zugänge zu kinderpornografischen Seiten auf Basis einer vom Bundeskriminalamt erstellten sogenannten „black list“ zu sperren, Folgeänderungen im Telekommunikations-

gesetzes, Aufhebung der für das Verfahren der Zugangser schwerung vorgesehene Evaluierungs- und Berichtspflicht.

Quelle: <http://www.juris.de>

Zugang zum Notarberuf

Der EuGH hat entschieden, dass auch ausländischen Juristen in Deutschland der Notarberuf offen stehen muss. Im Gegensatz zu Belgien, Deutschland, Griechenland, Frankreich, Luxemburg und Österreich ist das Gericht der Auffassung, dass mit den Tätigkeiten, die die Notare in den betreffenden Mitgliedstaaten derzeit ausüben, zwar im Allgemeininteresse liegende Ziele verfolgt werden, sie jedoch nicht mit der Ausübung öffentlicher Gewalt im Sinne des EG-Vertrags verbunden sind. Nur dann, wenn „öffentliche Gewalt“ ausgeübt werde, sei es legitim, solche Ämter allein mit Staatsbürgern des jeweiligen Landes zu besetzen.

EuGH, Urteile vom 24.05.2011 zu den Akz. C-47/08, C-50/08, C-51/08, C-53/08, C-54/08, C-61/08 und C-52/08

Keine doppelten GEZ-Gebühren bei gewerblich genutztem internetfähigen PC

Ein Freiberufler muss keine doppelten Rundfunkgebühren zahlen, wenn er einen internetfähigen Computer gewerblich nutzt und auf demselben Grundstück bereits ein Rundfunkgerät zum Empfang bereithält. Dies entschied der Bayerische Verwaltungsgerichtshof in München. Die Revision wurde zugelassen (Urteil vom 27.04.2011, Az.: 7 BV 10.443).

Urheberrecht in der EU soll modernisiert werden.

2009 wurden in den EU-Ländern 118 Millionen gefälschte Artikel beschlagnahmt, von denen 18 % eine Gefahr für die öffentliche Gesundheit darstellten. Mit einer koordinierten Strategie will die EU die Rechte des geistigen Eigentums besser schützen und Nachahmern und Fälschern das Handwerk legen. Die Kommission schlägt vor, die Rechte des geistigen Eigentums in der EU zu modernisieren. Diese Rechte schützen literarische, musikalische und

künstlerische Werke (Urheberrecht), Erfindungen (Patente) sowie Worte, Satzteile, Symbole und Designs (Marken). Folgende Maßnahmen sind geplant:

- Schaffung eines einheitlichen Patentschutzes, sodass Erfinder nur einmal einen Patentantrag stellen müssten, der für die meisten EU-Länder gilt; dadurch werden Kosten und Verwaltungsaufwand reduziert.

- Schaffung eines moderneren Systems für den Markenschutz: einfacher, schneller, wirksamer und kohärenter.

- Vereinfachung des Zugangs zu urheberrechtlich geschützten Werken, vor allem über das Internet und im Hinblick auf das Kulturerbe Europas.

Quelle: http://ec.europa.eu/news/business/110524_de.htm

Mehr Wettbewerb und Transparenz für Telefon- und Internetkunden

Bis zum 25.5.2011 mussten die neuen EU-Telekommunikationsvorschriften, mit denen mehr Wettbewerb in diesem Sektor und bessere Dienstleistungen für Kunden sichergestellt werden sollen, in nationales Recht umgesetzt sein - für EU-Bürger bedeutet dies neue Rechte und Dienstleistungen bei Festnetz, Mobilfunk und Internet. So etwa das Recht für Kunden, den Telekommunikationsbetreiber innerhalb eines Tages ohne Änderung der Telefonnummer wechseln zu können, der Anspruch auf klarere Informationen über die angebotenen Dienstleistungen und einen besseren Online-Datenschutz. Die verstärkten Aufsichtsrechte der EK und neue Regulierungsbefugnisse des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation werden mehr Rechtssicherheit schaffen und damit das Wachstum der Telekommunikationsbetreiber in einem europäischen Telekommunikationsbinnenmarkt fördern.

Quelle: <http://www.europainfo.at/to-pnews2.asp>

Impressum

Ständige Autoren:

- Andreas Albrecht, Fachanwalt für Steuerrecht, Hamburg
- Dr. Maren Augustin, Rechtsanwältin, Fachanwältin für Insolvenzrecht, Hamburg
- Harald Brennecke, Fachanwalt für Insolvenzrecht, Karlsruhe
- Peter Hesse, Rechtsanwalt, Fachanwalt für Miet- und Wohnungseigentumsrecht, Potsdam
- Cornelia Hübner, Fachwältin für Handels- und Gesellschaftsrecht und Bank- und Kapitalmarktrecht, Karlsruhe
- Martin Kull, Rechtsanwalt, Baden Baden
- Christoph Lattreuter, Rechtsanwalt, Berlin
- Anja Uelhoff, Fachanwältin für Bank- und Kapitalmarktrecht, Hamburg
- Valeska Walter, Rechtsanwältin, Kiel
- Marc Wandersleben, Rechtsanwalt, Hannover

Herausgeber:

DMA Deutsche Mittelstandsakademie, vertreten durch die Deutsche Mittelstandsakademie GbR Andreas Albrecht, Harald Brennecke, Cornelia Hübner, Martin Kull. Fechtstr. 4, 76227 Karlsruhe, Tel.: 0721 – 941 54 55, Fax: 0721 – 941 54 54. Mail: info@s-dma.de

Redaktion:

Dr. Maren Augustin (VISDP)
Stahlwiete 3, 22761 Hamburg,
Tel.: 040 – 853 99 666,
Fax: 040 – 853 99 661
Mail: redaktion@mittelstand-und-recht.de
Harald Brennecke / Anja Uelhoff

Verlag:

Verlag Mittelstand und Recht
Inhaber Harald Brennecke
Fechtstr. 4, 76227 Karlsruhe.
Mail: info@vmur.de

Copyright:

Mit Namen gekennzeichnete Beiträge stellen nicht unbedingt die Meinung der Redaktion dar. Für unverlangt eingesandte Manuskripte übernimmt der Verlag keine Haftung. Mit Annahme und Veröffentlichung erwirbt der Verlag alle Rechte an dem Manuskript, einschließlich des Rechts zur weiteren Vervielfältigung und gewerblichen Zwecken. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt.

Grafikdesign, Layout und Satz:

Sven Lorenz artwork & communication
www.artwork.de · Tel. 0721-6259 79 22-2
Turmbergstr. 4 · 76227 Karlsruhe.
Mail:
agentur@artwork.de · www.artwork.de

Druck:

WALTER Medien GmbH
Raiffeisenstraße 49-55
74336 Brackenheim
info@walter.de · www.walter.de

Erscheinungsweise:

Vierteljährlich

Leser- und Abonentenservice:

Leserservice@mittelstand-und-recht.de

Werbung/Anzeigenservice:

Anzeigen@mittelstand-und-recht.de
Bezugspreis: Jahres-Abo 25,- €.

Mit freundlicher Unterstützung

von Brennecke & Partner Rechtsanwälte
www.brennecke-partner.de
Mail: info@brennecke-partner.de

ISSN 1865-598Xw



Der Künstler Klaus Eppele

Klaus Eppele wurde 1959 in Heidelberg geboren und lebt seit 1969 in Karlsruhe. Der Diplom-Informatiker fotografiert seit seinem 16. Lebensjahr. Dabei konzentriert er sich nicht auf ein

Themengebiet, sondern fotografiert, was ihm gefällt oder interessant erscheint. Sein Credo: „Meine Fotografien sollen Spaß machen und Freude bringen und das Besondere und Schöne dieser Welt konservieren.“

Um auf die Schönheit alltäglicher Dinge aufmerksam zu machen, verfremdet Klaus Eppele seine Motive durch ungewöhnliche Perspektiven oder Bewegungsunschärfe oder er isoliert seine Objekte, indem er sie aus ihrer natürlichen Umgebung herausnimmt, sie im Fotostudio ablichtet und danach wieder unversehrt in die Natur zurückgibt.

Anfang 2010 veranstaltete der Fotograf seine Erste von bisher fünf Fotoausstellungen bei der gleich 13 Werke einen Abnehmer fanden. Außerdem nimmt Klaus Eppele gerne und erfolgreich an Fotowettbewerben teil, was ihm in den letzten zwölf

Monaten über 20 Veröffentlichungen in Fotozeitschriften, Kalendern oder Fotoausstellungen einbrachte.

Alle abgebildeten Motive stammen aus der Werkreihe „Buchenwald“.

Weitere Informationen unter
www.foto.welcheinglueck.de.

Go headtricks!



Berater und Ideengeber fürs Kommunikationsmarketing

Kommunikation ist der Antrieb jeder Organisation und der Treibstoff für den Erfolg. Wer es versteht strategisch und im richtigen Ton zu kommunizieren wird den entscheidenden Vorsprung gewinnen.

Die headtricks:

- Interne Kommunikation
- Markenkommunikation
- Online- und Social-Network communication
- Corporate-Kommunikation
- B-to-B communication
- One-to-One communication
- Zielgruppen-Kommunikation
- Veränderungskommunikation
- Kommunikations-Strategien
- Kommunikations-Ideen

headtricks – die trickreiche Art der Kommunikation!

www.headtricks.com