beraten
bilden
forschen

Datenschutz am Arbeitsplatz

Meine Rechte als Arbeitnehmer

Arbeitskammer des Saarlandes

Herausgeber:

Arbeitskammer des Saarlandes
Fritz-Dobisch-Straße 6-8, 66111 Saarbrücken
Fon: (0681) 4005-0, Fax (0681) 4005-411
Mail: info@arbeitskammer.de
Web: arbeitskammer.de

Stand: 7/2012

Redaktion:

Thomas Hau, Jens Göcking

Beratungsstelle für sozialverträgliche
Technologiegestaltung BEST e. V.
c/o Arbeitskammer des Saarlandes
Fritz-Dobisch-Straße 6-8, 66111 Saarbrücken
Fon: (0681) 4005-249, Fax (0681) 4005-259
Mail: best@best-saarland.de
Web: best-saarland.de

Hinweis:

**Datenschutz ist nichts anderes,
als der Respekt vor der Entscheidung des Anderen,
was er mit seinen persönlichen Daten machen
möchte und was nicht.**

T. Hau

Wie kann man dieses Handbuch benutzen?

Dieses Handbuch versucht einen Überblick über den Datenschutz in Deutschland zu geben, zu erklären, welche Rechte Beschäftigte am Arbeitsplatz haben und was bei speziellen Aspekten der Arbeitswelt zu beachten ist. Wenn Sie nicht alles interessiert, können Sie auch gezielt einsteigen.

Interessiert Sie, wie der Datenschutz grundsätzlich funktioniert?

Steigen Sie ein mit dem Kapitel ***Wie funktioniert der Datenschutz und was macht ihn so kompliziert?***

Interessieren Sie sich für den Datenschutz am Arbeitsplatz?

Steigen Sie ein mit dem Kapitel ***Datenschutz am Arbeitsplatz - die Grundlagen.*** Informieren Sie sich im Abschnitt ***Geltungsbereiche***, welches Datenschutzgesetz das für ihren Arbeitsplatz zutreffende ist.

Interessiert Sie nur ein spezielles Thema zum Datenschutz am Arbeitsplatz?

Eine Reihe von speziellen Themen ist in Teil II des Handbuchs beschrieben. Sehen Sie im ***Inhaltsverzeichnis*** nach, ob das von Ihnen gewünschte Thema dort behandelt ist. Eine weitere Möglichkeit bietet das ***Stichwortverzeichnis.*** Informieren Sie sich jedoch zuvor im Abschnitt ***Geltungsbereiche***, welches Datenschutzgesetz das für ihren Arbeitsplatz zutreffende ist.

Inhalt

Abkürzungsverzeichnis

Die verwendeten Abkürzungen werden im Textzusammenhang erklärt.

AGG	Allgemeines Gleichstellungsgesetz
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BEM	Betriebliches Eingliederungsmanagement
BfD	Beauftragte(r) für Datenschutz
BGB	Bürgerliches Gesetzbuch
BetrVG	Betriebsverfassungsgesetz
BildschArbV	Bildschirmarbeitsplatzverordnung
DSG-EKD	Datenschutzgesetz der evangelischen Kirche Deutschlands
GG	Grundgesetz
GewO	Gewerbeordnung
KDO-DVO	Verordnung zur Durchführung der Anordnung über den Kirchlichen Datenschutz
KunstUrhG	Kunsturheberrechtsgesetz

MAVO	Mitarbeitervertretungsordnung
OWiG	Ordnungswidrigkeitsgesetz
RFID	Radio Frequency Identification
SDSG	Saarländisches Datenschutzgesetz
SOX	Sarbanes-Oxley-Act
StGB	Strafgesetzbuch
SPersVG	Saarländisches Personalvertretungsgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
VoIP	Voice over IP
WpHG	Wertpapierhandelsgesetz
ZPO	Zivilprozessordnung

Vorwort

1983 bekräftigte das Bundesverfassungsgericht in der als Volkszählungsurteil bekannt gewordenen Entscheidung, das Recht eines jeden Bürgers, selbst darüber zu entscheiden, wer welche Daten von ihm zu welchem Zweck erheben und verarbeiten darf.

Es ist nicht leicht, dieses Recht wahrzunehmen, wenn man abhängig beschäftigt ist. Das hat die Arbeitskammer des Saarlandes frühzeitig erkannt und bereits 1994 ein Handbuch für ihre Mitglieder herausgegeben, das bis zum Jahr 2004 mit 45.000 Exemplaren eine der auflagenstärksten Veröffentlichungen zum Beschäftigtendatenschutz geworden ist. Seitdem erscheint das Handbuch in digitaler Form, um auf eine veränderte Rechtslage schneller reagieren zu können.

Die Skandale der letzten Jahre, in denen Mitarbeiter in teilweise entwürdigender Art bespitzelt wurden, machen jedoch deutlich, dass es mehr denn je notwendig ist, Orientierung zu liefern, was am Arbeitsplatz zulässig ist und wo die Grenzen des Erlaubten sind.

Aus diesem Grund wurde ein neues Handbuch erstellt, das sich sowohl sprachlich als auch inhaltlich konsequent an den aktuellen Anforderungen der Beschäftigten ausrichtet, und gezielt auf Fragen zu Datenschutz, Technik und Mitbestimmung am Arbeitsplatz eingeht.

Rechte kann nur wahrnehmen, wer sie auch kennt.

Dieses Handbuch will Kenntnisse vermitteln, um die konkrete Situation am Arbeitsplatz zu bewerten und handeln zu können. Seitdem das Volkszählungsurteil ergangen ist, sind fast 30 Jahre vergangen. Doch noch immer klafft eine große Lücke zwischen dem Recht auf informationelle Selbstbestimmung und der Realität, der die Beschäftigten an ihren Arbeitsplätzen ausgesetzt sind.

Dieses Werk will dazu beitragen, diese Lücke zu schließen.

Saarbrücken im Juli 2012

Hans Peter Kurtz
Vorsitzender des Vorstandes

Horst Backes
Hauptgeschäftsführer

Allgemeiner Teil

Datenschutz schützt den Menschen

In diesem Kapitel erfahren Sie:

Worum geht es beim Datenschutz?

Warum ist der Datenschutz so wichtig?

Wie die Risiken persönlicher Benachteiligung gestiegen sind und

warum man etwas tun muss.

Beim Begriff *Datenschutz* denkt man in erster Linie daran, Daten zu schützen, um Missbrauch und unbeabsichtigte Kenntnisnahme zu verhindern. Das klingt nach Aufgaben, die der Staat und Informationsdienstleister zu erledigen haben, nach Spionage, Hackerangriffen und Wirtschaftskriminalität. Doch darum geht es eigentlich nicht.

Worum geht es beim Datenschutz?

Deutschland ist ein freiheitliches Land, und das Grundgesetz sichert jedem Bürger das Recht zu, selbst darüber zu entscheiden, wer welche Daten von einem selbst erhält und zu welchen Zwecken er sie verwenden darf. Dieses unabdingbare Recht auf informationelle Selbstbestimmung, so wird dieses Recht in Fachkreisen genannt, wurde vom Bundesverfassungsgericht 1983 in dem sogenannten Volkszählungsurteil bekräftigt.

Es ist ein hohes Gut, selbst entscheiden zu können, wer was mit den Angaben über die eigene Person machen darf und was nicht. Dieses Privileg gibt es in den wenigsten Staaten der Welt. Vielerorts gilt, wer Daten von Personen erhebt, dem gehören diese Daten auch, und er kann sie zu allen erdenklichen Zwecken verwenden. Nicht so in Deutschland.

Daten, die Personen beschreiben, dürfen nicht beliebig verwendet werden. Die betroffene Person kann über die Verwendung ihrer Daten grundsätzlich frei entscheiden.

Dieses in der Bundesrepublik Deutschland durch die Verfassung garantierte Persönlichkeitsrecht auf informationelle Selbstbestimmung gilt es zu respektieren und zu schützen. Dazu dient der Datenschutz.

Um den Datenschutz zu konkretisieren, also festzulegen, wie das Recht auf informationelle Selbstbestimmung in welcher Situation geschützt wird, wurde eine Reihe von Gesetzen erlassen. Allen voran das Bundesdatenschutzgesetz (BDSG).

Bereits der erste Satz des Bundesdatenschutzgesetzes macht klar, worum es beim Datenschutz wirklich geht:

> ***Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.***
>
> § 1 Nr. 1 Bundesdatenschutzgesetz

Datenschutz ist folglich nichts anderes, als der Respekt vor der Entscheidung des Anderen, was er mit seinen persönlichen Daten machen möchte und was nicht.

Datenschutz sichert persönliche Freiheit

Wer sich zum ersten Mal mit dem Thema Datenschutz beschäftigt, wird spätestens an dieser Stelle stutzig. Es gibt das Recht auf informationelle Selbstbestimmung und sogar mehrere Gesetze, die dieses Recht schützen und trotzdem hat man nicht die Erfahrung machen können, dass man im wirklichen Leben diese Entscheidungen treffen kann.

Die Welt in der wir leben, ist nicht die Welt, in der man Menschen fragt, ob man persönliche Angaben sammeln, verwenden, speichern und veröffentlichen darf. Man kann den Eindruck gewinnen, dass die eigenen Daten überall kursieren und zu allen erdenklichen Zwecken herangezogen werden.

Anschriften lassen sich nicht nur für das Versenden von (unerwünschter) Werbung verwenden. Das Wohngebiet gibt auch Aufschlüsse zur finanziellen Situation der Person und lässt sich wunderbar für das sogenannte Scoring verwenden. Ein Scoring ist eine Sammlung von Finanz- und Sozialdaten einer Person zur „Berechnung“ ihrer Zahlungsfähigkeit und Einschätzung ihrer Zahlungsmoral. Das Unternehmen Creditreform bietet zur Bonitätsprüfung umfassende persönliche Finanzauskünfte von 77 Millionen Bürgern an (Stand 2012), inklusive der durch-

schnittlichen Finanzkraft ihres näheren Wohngebiets.

Doch nicht nur Unternehmen sammeln und verarbeiten diese personenbezogenen Daten. Selbst die kommunalen Melderegisterstellen verkaufen die Anschriften der Einwohner an Adressbuchverlage oder andere Interessenten, um Geld in die Städte- und Gemeindekassen zu bekommen, ohne dass die Einwohner nach ihrem Einverständnis gefragt werden. Den Verkauf der eigenen Daten kann man recht einfach untersagen, aber das ist weitgehend unbekannt. Musterschreiben hierfür gibt es auf der Webseite der Landesbeauftragten für Datenschutz.

Mit persönlichen Daten wird vieles gemacht, und längst nicht alles ist zulässig. Doch nur Wenige können das beurteilen. Die Rechtslage beim Datenschutz ist ausufernd und schwer zu verstehen. Deshalb ist es wenig verwunderlich, dass den wenigsten Menschen in Deutschland ihre Persönlichkeitsrechte bekannt sind.

Aber es ist eine ebenso unumstößliche Erkenntnis, dass nur der seine Rechte einfordern kann, der sie auch kennt.

Das Missbrauchsrisiko ist extrem gestiegen

Dass der Datenschutz bei den Bürgern lange Zeit nicht als Thema angekommen ist, erklärt sich relativ einfach. Früher ist man von der Gefahr eines allmächtigen und alles wissen wollenden Staates ausgegangen. Auch wenn man in der Bevölkerung die Datensammlungen des Staates und der Verwaltung beargwöhnt hat, so wurde das Thema damit abgetan, dass man ohnehin nichts dagegen tun kann und dass der Schaden, der einem daraus entstehen kann, relativ gering ist. Bei der Volkszählung ging es unter anderem darum, ob der Staat wissen muss, ob man seine Küche zusammengestückelt hat, oder ob man stolzer Besitzer einer Einbauküche ist.

Man hat es, aus damaliger Sicht, verschrobenen Personen überlassen, gegen die staatlichen Eingriffe in die Privatsphäre vorzugehen. Diesen, aus heutiger Sicht, klugen Köpfen verdanken wir viel: Nicht nur das Volkszählungsurteil, das durch ihre Hartnäckigkeit zustande kam, sondern auch die Erkenntnis, dass man als einfacher Bürger seine Rechte mit Erfolg ein-

fordern kann - selbst einem mächtigen Staat gegenüber.

Es mutet an wie ein Ausflug in die gute alte Zeit, als man es als unzulässigen und eklatanten Eingriff in die Privatsphäre gewertet hat, dass der Staat in einer Volkszählung wissen wollte, welche Art von Küche man besitzt.

Heute sind wir damit konfrontiert, dass Einzelhandelsketten die Vermögensverhältnisse von Bewerbern überprüfen. Wer verschuldet ist, wird im Auswahlverfahren nicht berücksichtigt, weil er - so wurde argumentiert - ein höheres Risiko für Diebstahlanfälligkeit und damit für den Arbeitgeber darstellt. Faktisch wird ihm die Chance genommen, durch Arbeit seine Schulden abzubauen.

An anderer Stelle wurden Bewerber für Ausbildungsplätze grundsätzlich und ohne begründete Anlässe Drogenscreenings unterworfen, mit dem Argument, dass Drogen unter Jugendlichen weit verbreitet sind und man sich bei der Unterzeichnung eines Ausbildungsvertrags sicher sein will.

In anderen Betrieben ist es üblich, dass Bewerber gebeten werden Bescheinigungen ihrer Krankenkassen über zurückliegende Erkrankungen der letzten fünf Jahre anzufordern und ins Vorstellungsgespräch mitzubringen. Freiwillig natürlich. Das Unternehmen möchte sich vorab darüber klar werden, ob es sich überhaupt lohnt, den Bewerber einzustellen oder auszubilden, da er womöglich eine schlechte Krankheitsprognose hat.

Das alles sind Vorfälle, die sich in den letzten Jahren zugetragen haben. Man muss auch davon ausgehen, dass die Daten aus Sozialen Netzwerken eine immer stärkere Rolle spielen werden.

Die Benachteiligungen, die eine Person heute durch den Missbrauch ihrer Daten erfahren kann, sind zum Teil elementar und können über Lebensläufe entscheiden.

Aktiv werden - Missbrauch verhindern, Gebrauch kontrollieren

Es gilt allerdings, nicht nur den Missbrauch von Daten zu verhindern, sondern auch den verantwortungsvollen Gebrauch zu sichern. Denn ohne die Nutzung von persönlichen Daten ist ein Leben, wie wir es kennen, nicht möglich.

Deshalb ist es außerordentlich wichtig, dass man den Schutz der eigenen Daten nicht dem Staat oder der Wirtschaft überlässt, sondern selbst aktiv wird.

Das Thema Datenschutz wird oft mit der Floskel abgetan, dass man nichts zu verbergen hat. Doch es geht nicht um das Verbergen von Daten. Es geht einfach darum, selbst entscheiden zu können, wie „öffentlich“ man sein möchte. Die Konsequenzen daraus bekommt man am eigenen Leib zu spüren, deshalb sollte man sich diese Entscheidung nicht von anderen nehmen lassen.

Wie funktioniert der Datenschutz?

Inhalt:

Was ist Datenschutz im juristischen Sinn?

Welche Gesetze gibt es?

Was ist das Prinzip des Datenschutzes?

Warum ist der Datenschutz so kompliziert?

Der Begriff *Datenschutz* ist in Deutschland etwas unglücklich gewählt, denn er legt eine falsche Vorstellung nahe, worum es geht. Der Schutz von vertraulichen oder gar geheimen Daten zum Beispiel Herstellungsverfahren, die Kreditwürdigkeit eines Unternehmens, Betriebsgeheimnisse oder militärische Informationen fallen in Deutschland nicht unter den Begriff *Datenschutz*.

Beim *Datenschutz*, im juristischen Sinn, geht es darum, Menschen davor zu schützen, dass sie durch den Missbrauch ihrer Daten benachteiligt werden. Es geht um den Schutz der Privatsphäre und darum, wie es das Grundgesetz garantiert, Herr über seine eigenen Daten zu sein und zu bleiben.

Um welche Daten geht es?

Insofern ist es logisch, dass es sich beim Datenschutz um Regelungen zum Umgang mit Daten handeln muss, die im Bezug zu einzelnen Menschen stehen. Man spricht in diesem Zusammenhang von personenbezogenen und personenbeziehbaren Daten:

> ***„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.“***
>
> Bundesdatenschutzgesetz § 3 Abs.1

Allem voran ist das natürlich der Name der Person. Wichtig ist, dass im Bundesdatenschutzgesetz aber auch die personenbeziehbaren Daten genannt sind. Personenbeziehbare Daten sind Angaben, die es erst indirekt ermöglichen, also mit Hilfe weiterer Daten, Rückschlüsse auf eine bestimmte (natürliche) Person zu ziehen.

Beispiele hierfür sind die Personalausweisnummer, Personalnummer, Kreditkartennummer. In allen Fällen handelt es sich um reine Zahlenkombinationen, die in dieser Form zunächst keine Bedeutung haben. Weiß man allerdings, dass es sich um eine Personalnummer handelt, lässt sich auch herausfinden, wer sich zweifelsfrei hinter dieser Nummer verbirgt.

Welchen Aufwand man für eine solche Ermittlung auf sich nehmen muss, spielt für das Gesetz nur eine Nebenrolle, da sich der Aufwand mit den technischen Möglichkeiten ändert. Früher war es nahezu unmöglich auf der Grundlage einer Telefonnummer herauszufinden, welche Person sich hinter dem Anschluss verbirgt. Man musste ein „Fräulein vom Amt“ kennen oder Zugang zu einem numerischen Telefonbuch der Strafverfolgungsbehörden haben. Heute ist das über eine einfache und inzwischen auch legale Inverssuche in Internet-Telefonbüchern für jeden zu realisieren.

Deshalb gilt als Faustregel:

Wenn es prinzipiell möglich ist - ggf. auch erst im Abgleich und unter Hinzuziehung weiterer Informationen - Rückschlüsse auf eine einzelne Person zu ziehen, handelt es sich um personenbeziehbare Daten. Dann gelten die Datenschutzgesetze, denn die betroffenen Menschen könnten benachteiligt werden.

Beispiele:

Name, Vorname - personenbezogene Daten

Geburtsdatum - personenbeziehbares Datum, gemeinsam mit anderen Angaben lässt sich eine Person identifizieren

Adresse - bei Wohnhaus: personenbeziehbare Angabe; bei Firmenadresse: keine personenbeziehbare Angabe

Betriebsgeheimnisse - üblicherweise keine personenbezogenen oder personenbeziehbare Daten

Benutzername für PC und Internet - personenbezogenes Datum, außer bei einem gemeinsamen Benutzernamen für mehrere Personen

Eindeutige Bezeichnungen - z. B. *„Der Schwerbehindertenbeauftragte“* - perso-

nenbezogene Angabe innerhalb eines Betriebes, es gibt in der Regel nur einen.

Besondere Arten personenbezogener Daten

Im wirklichen Leben unterscheiden wir Daten in vielerlei Hinsicht. Die Datenschutzgesetze beschränken sich im Wesentlichen auf zwei Kategorien. Aus den personenbezogenen Daten wird eine Gruppe hervorgehoben, die sogenannten *besonderen Arten personenbezogener Daten*:

> ***Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.***
>
> Bundesdatenschutzgesetz § 3

Wie man bereits auf den ersten Blick erkennen kann, handelt es sich um sehr persönliche Angaben. Das Risiko, das durch den Missbrauch dieser Daten für den Betroffenen entstehen kann, ist deutlich höher als bei konventionellen personenbezogenen Daten. Deshalb knüpfen die Datenschutzgesetze eine Reihe spezieller Auflagen an die Verwendung dieser Daten.

Wem gehören die Daten?

Üblicherweise wird davon ausgegangen, dass Daten, auch personenbezogene Daten, dem gehören, der sie sammelt und dass er sie für alle erdenklichen Zwecke verwenden kann. In der Bundesrepublik Deutschland ist das nicht so.

Einfach ausgedrückt gehören die Daten über eine Person der Person, die damit beschrieben wird - dem Betroffenen, so der Fachausdruck. Ohne seine Erlaubnis ist die Verwendung seiner Daten grundsätzlich verboten. Dieses Rechtsprinzip gilt in Deutschland, aber längst nicht in allen Staaten rund um den Globus.

Vielen Menschen in mehr oder weniger verantwortlichen Positionen ist das allerdings auch in Deutschland nicht bekannt. Datenschutz gehört üblicherweise nicht zur Schulbildung und darf nicht als bekanntes Wissen vorausgesetzt werden.

Datenschutz und Persönlichkeitsrechte

Der Datenschutz steht in direkter Beziehung zu den allgemeinen Persönlichkeitsrechten, die das Grundgesetz allen Menschen in Deutschland zusichert.

Einige Persönlichkeitsrechte:

- *Schutz der Privatsphäre*
- *Schutz der Intimsphäre*
- *Recht auf informationelle Selbstbestimmung*
- *Recht am eigenen Bild*
- *Recht am gesprochenen und am geschriebenen Wort*

Das „neueste“ Grundrecht wurde 2008 vom Bundesverfassungsgericht als Reaktion auf Beschwerden zur sogenannten Online-Durchsuchung formuliert:

- *Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*

Dieses Recht garantiert uns, dass wir grundsätzlich nicht über Computer ausspioniert werden dürfen.

Die Funktion der Datenschutzgesetze

Das Grundgesetz garantiert unsere informationelle Selbstbestimmung, lässt aber offen, wie dieses Recht im praktischen Leben umgesetzt wird. Diese Aufgaben übernehmen die Datenschutzgesetze. Es gibt gleich mehrere davon.

Welche Datenschutzgesetze gibt es?

Da Deutschland ein föderalistischer Staat ist, der es zudem den Staatskirchen ermöglicht, ihre Angelegenheiten in eigenen Gesetzen zu regeln, gibt es gleich 19 Datenschutzgesetze, die parallel nebeneinander existieren. Jedes Gesetz hat einen abgegrenzten Bereich, in dem es Geltung hat. Daneben gibt es eine Vielzahl von Gesetzen, in denen auch Datenschutzthemen behandelt werden z. B. im Sozialgesetzbuch unter dem Stichwort Sozialgeheimnis. Den Rahmen geben jedoch die eigentlichen Datenschutzgesetze vor.

Jedes der 16 Bundesländer hat ein eigenes Datenschutzgesetz für den sogenannten öffentlichen Bereich. Damit sind jedoch nicht die Öffentlichkeit oder frei betretbare Areale gemeint. „*Öffentlicher Bereich*“ be-

zeichnet im Amtsdeutsch die öffentlichen Einrichtungen (Verwaltung) des jeweiligen Bundeslandes, die unter anderem auch für den öffentlichen Raum zuständig sind. Öffentlicher Raum sind einfach ausgedrückt, Flächen, die im Besitz der Kommunen, des Landes oder des Bundes sind z. B. Marktplätze und Straßen. Das Saarländische Datenschutzgesetz (SDSG) gilt also nicht für alles und jeden im Saarland, sondern betrifft nur öffentliche Einrichtungen des Saarlandes, der Landkreise und Kommunen.

Es gibt weiterhin ein Datenschutzgesetz für Einrichtungen katholischer Träger (KVO), ein Datenschutzgesetz für protestantische Einrichtungen (DSG-EKD) und allen voran das Bundesdatenschutzgesetz (BDSG) für die Einrichtungen des Bundes und der Privatwirtschaft.

Die Norm, der alle genannten Gesetze folgen, wird durch das Bundesdatenschutzgesetz vorgegeben. In weiten Teilen sind die Gesetze sogar wortgleich. Im Wesentlichen sind es die speziellen Fälle der einzelnen Geltungsbereiche, in denen sich die Datenschutzgesetze unterscheiden. Allen ist jedoch das Prinzip des Datenschutzes gemeinsam. Und das Prinzip, wie das informationelle Selbstbestimmungsrecht des Einzelnen geschützt wird, ist eigentlich ganz einfach.

Datenvermeidung und Datensparsamkeit

Die informationelle Selbstbestimmung ist ein hohes Rechtsgut. In dieses Recht einzugreifen ist logischerweise kein Vorgang, den man leichtfertig und nach eigenem Belieben vornehmen kann. Es handelt sich schließlich um die personenbezogenen Daten eines Betroffenen. Aus diesem Grund machen es die Datenschutzgesetze zur Auflage, vor dem Erheben von personenbezogenen Daten einige Prüfungen anzustellen.

1. Prüfung - Legalität des Einsatzzwecks

Es muss geprüft werden, ob das angestrebte Ziel, für das man die personenbezogenen Daten erheben will, rechtmäßig ist. Derjenige, der die Daten erheben will, muss darstellen können, dass die Datenerhebung legal ist. Die Datenerhebung bedarf einer Erlaubnis, doch dazu später mehr. Fehlt dieser Nachweis, muss die

Erhebung personenbezogener Daten unterbleiben.

2. Prüfung - Datenvermeidung

Das Prinzip der Datenvermeidung ist in den Datenschutzgesetzen formuliert (§ 3 BDSG/SDSG/KDO/DSG-EKD). Wer personenbezogene Daten erheben und verarbeiten will, muss vorab überprüfen, ob dies zum Erreichen des angedachten Ziels überhaupt objektiv notwendig ist. Es muss überprüft werden, ob man den Personenbezug nicht weglassen kann, also zu anonymisieren oder durch erfundene Identitäten - Pseudonyme - zu ersetzen, um bereits bei der Datenerhebung eine spätere Rückverfolgbarkeit der Daten auszuschließen. Ist das Weglassen (ersatzweise das Anonymisieren oder Pseudonymisieren) der personenbezogenen Daten möglich, dann muss es erfolgen.

3. Prüfung - Datensparsamkeit

Sofern es die Verwendung personenbezogener Daten in einem legalen Datenverarbeitungsverfahren unvermeidlich ist, muss sichergestellt werden, dass nur die absolut notwendigen Daten erhoben werden. Mehr Daten auf Vorrat zu erheben, oder weil es das Verfahren vereinfacht, ist nicht zulässig. Auch diese Anforderung geben die Datenschutzgesetze in § 3 vor.

Wie zuvor erwähnt, ist es jedoch unumgänglich zu überprüfen, ob überhaupt eine rechtmäßige Erlaubnis für das Erheben und Verarbeiten von personenbezogenen Daten vorliegt. Das lässt sich über die Anforderungen der Datenschutzgesetze herausfinden.

Datenschutz - Ein Nutzungsverbot mit Erlaubnisvorbehalt

Datenschutz geht davon aus, dass die Erhebung und Verarbeitung von personenbezogenen Daten verboten ist:

> ***Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.***
>
> § 4 Abs. 1 Bundesdatenschutzgesetz

Bei den Datenschutzgesetzen handelt es sich in der juristischen Bezeichnung um Verbote mit nachgelagertem Erlaubnisvorbehalt.Anders ausgedrückt:

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist grundsätzlich verboten. Aber Ausnahmen sind möglich:

1. Ausnahme: Der „Inhaber“ der Daten, der sogenannte Betroffene, hat im Rahmen seines Rechts auf informationelle Selbstbestimmung in die Verwendung seiner Daten freiwillig eingewilligt.

2. Ausnahme: Im Datenschutzgesetz steht, dass die personenbezogenen Daten in dort beschriebenen Zusammenhängen auch ohne ausdrückliches Einverständnis verwendet werden dürfen.

3. Ausnahme: Es gibt eine Rechtsvorschrift, die die Verwendung der personenbezogenen Daten in bestimmten Zusammenhängen zu bestimmten Zwecken ohne freiwilliges Einverständnis erlaubt oder sogar anordnet.

Datenschutz: Ein einfaches Prinzip mit vielen komplizierten Ausnahmen

Um es deutlich auszudrücken: Die 3. Ausnahme ist der Grund dafür, dass dieses und viele weitere Handbücher zum Datenschutz verfasst wurden. Die Ausnahmen vom „einfachen“ Prinzip des Datenschutzes sind zahllos, schwer verständlich und stehen oft genug auch noch mit anderen Normen im Widerspruch. Warum diese verworrene Situation vorherrscht, erklärt sich wiederum recht einfach.

Datenschutz ist der Schutz von Persönlichkeitsrechten, aber er kann auch eingeschränkt werden.

Einschränkungen bei der informationellen Selbstbestimmung oder

warum man nicht gefragt wird.

Grundsätzlich ist die Nutzung von personenbezogenen Daten an die Erlaubnis des Dateninhabers gebunden, da er nur so von seinem Recht auf informationelle Selbstbestimmung Gebrauch machen kann. Von diesem Grundsatz kann allerdings abgewichen werden, wenn das Gemeinwohl in den Vordergrund rückt. Diese Ausnahmen müssen jedoch verbindlich in Gesetzen, Verordnungen oder sonstigen Rechtsvorschriften begründet und geregelt werden.

Beispiel: Abwehr von Gefahren

Jeder Einzelne hat das Recht darauf, nicht an seinem Computer ausspioniert zu werden. Besteht hingegen aufgrund eines konkreten Terrorverdachts Gefahr für die Allgemeinheit, kann in dieses individuelle Grundrecht eingegriffen werden. In welchen Fällen und auf welche Art und Weise dies erfolgen darf, regelt das Gesetz zur Online-Durchsuchung. An diese Beschränkungen müssen sich sowohl die Strafverfolgungsbehörden wie auch die Geheimdienste halten.

Beispiel: Arbeitsverhältnis

Sozialversicherungssysteme (Renten-, Pflege-, Krankenversicherung…) dienen dem Wohle aller Versicherten. Um dies sicher zu stellen, wurden Gesetze erlassen z. B. die Datenerfassungs- und -übermittlungsverordnung (DEÜV), die den Arbeitnehmer verpflichten, eine Reihe von zum Teil sehr persönlichen Daten über sich preiszugeben z. B. Kontonummer, Familienstand, Angehörigkeit zu einer der Staatskirchen und vieles mehr.

Im wirklichen Leben wird das Recht des Einzelnen auf informationelle Selbstbestimmung durch eine Vielzahl von Gesetzen, Verordnungen und sonstigen Rechtsvorschriften zugunsten des Gemeinwohls eingeschränkt. Diese Rechtsvorschriften regeln die Verwendung persönlicher Daten in bestimmten Zusammenhängen: Beim Einwohnermeldeamt, beim Zulassen eines Fahrzeuges, beim Entrichten der Hundesteuer oder am Arbeitsplatz.

Es gibt kaum einen Lebensbereich, der nicht in irgendeiner Form die Verwendung von persönlichen Daten per Gesetz oder Verordnung regelt. Diese Rechtsvorschriften ermöglichen es, die personenbezogenen Daten ohne ausdrückliches Einverständnis des Betroffenen zu nutzen oder ordnen es sogar an wie im Fall der DEÜV.

Wer ist verantwortlich?

In jedem Fall aber ist derjenige, der die personenbezogenen Daten erhebt und verarbeitet, dafür verantwortlich und haftbar, dass sie ausschließlich so verwendet werden, wie es die Rechtsnorm vorgibt. Im Amtsdeutsch spricht man hier von einer

sogenannten „verantwortlichen Stelle“. Das ist vorrangig derjenige, der für die Datenerhebung und -verarbeitung verantwortlich ist, z. B. Geschäftsführer, Dienststellenleiter o. ä. , aber auch die Mitarbeiter von Personalabteilungen, die diese Aufgaben umsetzen.

Wozu dürfen personenbezogene Daten verwendet werden?

Um es gleich vorweg zu nehmen: die Verwendung von personenbezogenen Daten ist streng zweckgebunden und nicht beliebig. Auch dieses Prinzip der Zweckbindung verdanken wir dem Volkszählungsurteil von 1983, in dem klargestellt wird, dass es verboten ist „Daten auf Vorrat zu unbestimmten Zwecken“ zu erheben.

Anders ausgedrückt: Daten dürfen nur zu vorher festgelegten und zulässigen Zwecken erhoben und verarbeitet werden. Ein Verarbeiten von bereits erhobenen Daten zu anderen Zwecken als denen, für die sie erhoben wurden, ist unzulässig.

Beispiel: Kontonummer bei Lastschrift

> *Es ist praktisch, wenn man seiner Kommune erlaubt, kommunale Abgaben per Lastschrift vom Konto abbuchen zu lassen. Hierzu muss man der Kommune eine sogenannte Einzugsermächtigung ausstellen: Der Kommune wird die Bankverbindung mitgeteilt und erlaubt z. B. die Müllgebühren abzubuchen. Jetzt - wo die Bankverbindung vorliegt, wäre es doch praktisch für die Kommune darüber auch die Hundesteuer einziehen zu können, dann könnte man sich die Kontrollen ersparen und müsste säumige Bürger nicht anmahnen. Das ist jedoch unzulässig. Auch wenn die Bankverbindung mitgeteilt wurde, so ist die Erlaubnis zur Verwendung ausschließlich an diesen Zweck gebunden, zu dem die Erlaubnis erteilt wurde.*

Im Arbeitsalltag wird die Zweckbindung oft kritisch gesehen, weil sie Verfahren umständlich macht. Wenn man bereits personenbezogene Daten zu einem bestimmten Zweck erhoben hat, und sie nun einfach für einen anderen Zweck verwenden könnte, darf man es nicht. Man muss sie erneut beim Betroffenen erheben: Doppelte Arbeit ohne sichtlichen Nutzen - zumindest aus Sicht des Arbeitgebers.

Der Nutzen für die Betroffenen - die Arbeitnehmer - ist allerdings schon da. Wenn man in einem freiheitlichen Land über seine Daten frei entscheiden kann, dann kann man dies nur tun, wenn man weiß, zu welchen Zwecken die Daten verarbeitet werden sollen. Datenschutz funktioniert nicht ungefragt über die Köpfe der Betroffenen hinweg. Es gilt das Gebot der Transparenz und das Prinzip der Zweckbindung, von dem nur in absoluten Ausnahmefällen abgewichen werden darf.

Hinweis:

Wenn vom Prinzip der Zweckbindung abgewichen wird, ist der gesamte Datenschutz hinfällig.

Datenschutz versucht sicherzustellen, dass personenbezogene Daten nur zu legalen Zwecken verwendet werden. Lässt man die Verwendungszwecke außer Acht, kann man das nicht mehr feststellen.

Wer darf personenbezogene Daten erheben, verarbeiten und einsehen?

Die Frage nach dem Zugriff

Diese Frage steht in enger Beziehung zur Zweckbindung. Selbst ein Datenschutz-Laie weiß, dass es nicht sein kann, dass jeder auf alle erdenklichen Daten zugreifen kann. Aber ob es eine konkrete Regel gibt, weiß kaum jemand zu beantworten.

Es gibt eine Regel, und die ist recht einfach: Personenbezogene Daten erheben, einsehen und verarbeiten darf nur derjenige, der nachweislich mit der Erfüllung des Zwecks beauftragt ist, für den die Daten erhoben wurden.

Beispiel: Arbeitsplatz

> *Ein Mitarbeiter möchte wissen, ob sein Kollege, der die gleiche Arbeit macht, besser verdient und fragt in der Personalabteilung nach. Er erhält dort keinen Einblick in dessen Personalakte, da er nicht für die Personalaktenführung eingestellt ist und auch nicht dafür, die korrekte Eingruppierung anderer zu begutachten. Man verweist ihn an den Betriebsrat. Warum? Der Betriebsrat hat ausdrücklich die gesetzliche Aufgabe darüber zu wachen, dass die zugunsten von Beschäftigten geltenden Gesetze ein-*

gehalten werden. Aus diesem Grund hat der Betriebsrat ein berechtigtes Interesse, Unterlagen einzusehen zum Zweck der Überprüfung der Eingruppierung beider Kollegen. Allerdings erhält auch der Betriebsrat so wenig personenbezogene Daten wie es eben geht, um den Vorgang zu bewerten. Die Datensparsamkeit greift auch hier.

Bei der Frage, ob ein Zugriff auf personenbezogene Daten zulässig ist, darf man sich nicht von dem Obrigkeitsgedanken leiten lassen.

Beispiel: Datenzugriff und Hierarchien

Ein Unternehmen wird geleitet durch Vorstände. Es gibt einen Finanzvorstand, einen technischen Vorstand und einen Personalvorstand. Auch wenn ein technischer Vorstand an der Spitze eines Unternehmens steht, hat er kein generelles Einblicksrecht in die Personalakten aller Mitarbeiter. Ein „einfacher" Personalsachbearbeiter hingegen schon, wenn die Personalaktenpflege nachweislich zu seinen Arbeitsaufgaben gehört. Aber auch er darf die Akten nur zu diesem Zweck und nicht aus persönlichem Interesse einsehen.

Der Datenschutz kennt keine Hierarchien und macht keinen Unterschied zwischen Mitarbeitern und Vorgesetzten, sondern zwischen Betroffenen und verantwortlichen Stellen. Ob jemand berechtigt ist, auf personenbezogene Daten zuzugreifen, macht sich ausschließlich daran fest, ob die Person im Rahmen des Verwendungszwecks der Daten beschäftigt ist.

Was passiert mit den Daten?

Wer etwas sammelt, hat normalerweise die Absicht, seine Sammlung zu pflegen, zu bewahren und auszubauen. Oder er kann auch die Entscheidung treffen, sich von allem oder von Teilen zu trennen.

Die Haltung „Ich speichere die personenbezogenen Daten, man weiß ja nie, ob man sie nochmal braucht" ist unzulässig. Bei personenbezogenen Daten kann man definitiv nicht frei entscheiden, wie lange man die Daten aufhebt und wann man sie

löscht. Das ergibt sich aus dem Prinzip der Zweckbindung.

Personenbezogene Daten wurden für einen ganz bestimmten Zweck erhoben und verarbeitet. Ist der Zweck erfüllt, müssen die Daten gelöscht werden.

Ein längeres Aufbewahren ist nur möglich, wenn der Betroffene nachweislich sein freiwilliges Einverständnis hierzu gegeben hat. Von einem stillschweigenden Einverständnis darf nicht ausgegangen werden, da es hierfür keine Gesetzesgrundlage gibt, und der Betroffene so seiner Entscheidung enthoben wird, ob er das möchte. Das Transparenzgebot und die informationelle Selbstbestimmung verbieten das.

Wie lange Daten gespeichert werden dürfen oder müssen, ergibt sich ausschließlich aus dem Zweck ihrer Erhebung. Danach müssen sie unverzüglich gelöscht werden.

Beispiel: Telefondaten

Telefonieanbieter erheben die Verbindungsdaten, um ihren Kunden korrekte Rechnungen zu erstellen. Die Verwendung der Daten ist an diesen Zweck gebunden, wenn nichts anderes zwischen Kunde und Anbieter vereinbart wurde.

Ein Kunde wollte wissen, wie lange die Telekom AG seine Verbindungsdaten speichert. Ihm wurde mitgeteilt, dass die Speicherung über mehrere Monate betrieben wird.

Er forderte das Unternehmen auf, dies zu unterlassen, da es sich um personenbezogene Daten zum Zweck der Rechnungsstellung handele, und der Zweck der Speicherung nach Begleichen der Rechnung erfüllt sei.

Letztlich wurde der Telekom per Gericht die monatelange Speicherung der Verbindungsdaten untersagt.

Allerdings dürfen die Daten auch noch einige Wochen nach Begleichen der Rechnung gespeichert werden, denn zum Zweck der Datenerhebung - das Stellen einer korrekten Rechnung - gehört auch

die Wahrung einer Reklamations- und Widerspruchsfrist. Für die Dauer dieser Frist sind die Daten zu speichern. Danach allerdings müssen die personenbezogenen Daten vollständig gelöscht werden.

Doch keine Regel ohne Ausnahmen. Wenn die Erhebung und Verarbeitung von personenbezogenen Daten durch ein Gesetz oder eine andere Rechtsvorschrift erfolgt, ist es möglich, dass die Rechtsvorschrift nicht nur einen Verwendungszweck, sondern auch feste Aufbewahrungsfristen vorgibt.

Beispiel: Geschäftsunterlagen

Kaufverträge zwischen Käufer und Verkäufer sind bei Endverbrauchern zweifellos personenbezogene Daten. Ist ein Kauf getätigt und die Gewährleistungsfristen abgelaufen, müsste man die personenbezogenen Daten löschen, das sagen die Datenschutzgesetze.

Allerdings gelten die nur dann, wenn der konkrete Zusammenhang nicht bereits in einem der vielen Spezialgesetze und Verordnungen geregelt ist. Bei Geschäftsunterlagen ist das der Fall.

Damit Finanzämter auch nach Jahren noch Steuersündern auf die Spur kommen können, gibt es die sogenannte Abgabenordnung (AO). In ihr ist festgelegt, dass kaufmännische Unterlagen je nach Art sechs oder zehn Jahre aufbewahrt werden müssen. Eine Speicherung über den ursprünglichen Zweck (z. B. Verkauf) hinaus ist in diesem Fall legal.

Das Recht auf Auskunft

Bei personenbezogenen Daten ist es wichtig zu wissen, was mit ihnen passiert. Der Betroffene hat natürlich ein Recht das zu erfahren, es sind schließlich seine Daten. Und: Dieses Recht auf Auskunft kann ihm nicht genommen werden.

Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie

sich auf die Herkunft dieser Daten beziehen,

2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

§ 34 Bundesdatenschutzgesetz

Jeder, der vermutet, dass ein Unternehmen, eine Behörde oder Einrichtung Daten über ihn erhebt, verarbeitet oder speichert, kann dort - ohne konkreten Anlass - nachfragen. Es gibt nur wenige Fälle z. B. bei Strafverfolgungsbehörden oder Geheimdiensten, wo ein Auskunftsersuchen zu keinem Ergebnis führt.

Wer also personenbezogene Daten erhebt, verarbeitet und speichert und nicht zu den genannten Branchen gehört, muss damit rechnen, dass er Auskunft geben muss über alle oben genannten Aspekte. Diese Auskunft muss zeitnah erfolgen, schriftlich, verständlich und in der Regel kostenlos. Auch das geht aus den Datenschutzgesetzen hervor.

Löschung, Sperrung, Berichtigung von Daten

Oft genug stellt es sich heraus, dass Daten fehlerhaft und unvollständig sind oder über den Verwendungszweck hinaus gehen. Dann hat man die Möglichkeit, eine Berichtigung, Löschung oder Sperrung der Daten zu verlangen. Was in welchen Fällen zum Tragen kommt, ist den entsprechenden Datenschutzgesetzen zu entnehmen.

Wie kann man seine Rechte durchsetzen?

Wenn man vermutet, dass ein Betrieb, eine Einrichtung oder eine Behörde personenbezogene Daten über die eigene Person erhebt, verarbeitet und/oder speichert, genügt ein schriftliches Auskunftsersuchen, die Rechtmäßigkeit des Handelns nachzuweisen und gegebenenfalls Unzutreffendes und Unzulässiges zu löschen oder zu korrigieren. Doch es gibt auch renitente Fälle, in denen nicht auf die Rechte nach Auskunft, Berichtigung, Löschung und Sperrung reagiert wird.

In einer solchen Situation kann man die Aufsichtsbehörden für den Datenschutz einschalten. Durch ihren offiziellen Cha-

rakter können sie helfen, den Sachverhalt zu klären oder Anfragen Nachdruck zu verleihen. Im Gegensatz zu Rechtsanwälten ist die Anfrage bei den Aufsichtsbehörden kostenlos. Welche Aufsichtsbehörde zuständig ist, hängt wiederum davon ab, mit welcher verantwortlichen Stelle man es zu tun hat.

Im Saarland leitet die Landesbeauftragte für Datenschutz die Aufsichtsbehörde für die Einrichtungen des Saarlandes, der Kreise und Kommunen. Darüber hinaus ist sie auch für die saarländische Privatwirtschaft zuständig.

Kirchliche Einrichtungen haben ihre eigenen Aufsichtsgremien. Die Kontaktdaten finden sich im Anhang.

Zusammenfassung:

Das Grundgesetz sichert uns das Recht auf informationelle Selbstbestimmung zu, und die Datenschutzgesetze regeln, wie wir Herr über unsere Daten bleiben. Denn in Deutschland gehören personenbezogene Daten dem Betroffenen und eine Verwendung seiner Daten regeln die Datenschutzgesetze. Je nach Betriebsstätte können unterschiedliche Datenschutzgesetze zum Einsatz kommen.

Allen ist gemeinsam, dass sie den Einzelnen davor schützen wollen, dass er durch die Verwendung seiner Daten Schaden erfährt. Deshalb gilt immer das Prinzip der Datenvermeidung: Wenn es möglich ist, ein Verfahren ohne personenbezogene Daten durchzuführen, dann muss es ohne personenbezogene Daten durchgeführt werden.

Ist es erforderlich, personenbezogene Daten zu verwenden, dann braucht derjenige, der die Daten verwenden will, eine Erlaubnis hierfür. So wollen es die Datenschutzgesetze. Diese Erlaubnis kann in der Regel nur der Betroffene erteilen. Man braucht seine Erlaubnis allerdings nicht, wenn eine Rechtsvorschrift (Gesetz, Verordnung, Tarif, Betriebsvereinbarung) die Nutzung der Daten ermöglicht oder anordnet. In der Praxis gibt es eine Vielzahl dieser Sonderregelungen. Sie gehen der persönlichen Entscheidung des Betroffenen vor. Wer allerdings Daten ohne das Einverständnis des Betroffenen erheben und verarbeiten will, muss diese Rechtsgrundlage nachweisen können.

Und auch dann gilt der Grundsatz der Datensparsamkeit: Es dürfen nur so viele personenbezogene Daten erhoben und verarbeitet werden, wie zwingend erforderlich sind, um den Zweck, der in der Rechtsvorschrift stehen muss, zu erreichen.

Daten dürfen ausdrücklich nur für den Zweck verwendet werden, für den sie erhoben worden sind. Alle Verwendungszwecke müssen vor der Datenerhebung bekannt sein. Eine nachträgliche Änderung des Nutzungszwecks darf nicht erfolgen. Es gilt der Grundsatz der Transparenz: Auch wenn Daten ohne Einverständnis auf einer Rechtsgrundlage erhoben werden, ist es dem Betroffenen möglich festzustellen, ob seine Daten im Rahmen der rechtlichen Vorgaben genutzt

werden oder ob die Verwendung unzulässig ist.

Um dies feststellen zu können, gibt es für alle Betroffenen das Recht auf Auskunft.

Wer personenbezogene Daten erhebt und nutzt, ist verpflichtet, den Betroffenen auf deren Verlangen darüber ausführlich, verbindlich, verständlich und kostenlos Auskunft zu erteilen. Er kann diese Auskunft in der Regel nicht verweigern. Stellt sich dabei heraus, dass mehr Daten erhoben wurden als zulässig ist oder dass Angaben falsch sind, kann der Betroffene verlangen, dass die unzulässig erhobenen Daten gelöscht und die falschen Angaben berichtigt werden.

Personenbezogene Daten dürfen nicht beliebig lange gespeichert werden. Es gibt zwar keine einheitliche Frist, aber eine klare Regel: Personenbezogene Daten dürfen nur so lange gespeichert werden, bis der Zweck, für den sie erhoben wurden, erfüllt ist. Danach müssen sie unverzüglich und restlos gelöscht werden. Die Löschfrist ist in der Regel von der Zweckbindung abhängig. Es kann jedoch Ausnahmen geben. Wenn personenbezoge Daten auf der Grundlage einer Rechtsvorschrift erhoben wurden, ist es möglich, dass in dieser Rechtsvorschrift eine ausdrückliche Aufbewahrungs- oder Löschfrist benannt ist.

In jedem Fall dürfen nur die Personen auf personenbezogene Daten zugreifen, die ausdrücklich mit der Umsetzung des Zwecks der Datenerhebung (z. B. Personalabrechnung) beschäftigt sind. Dieses Zugriffsrecht vererbt sich nicht automatisch auf deren Vorgesetzte.

Für Fragen zum Datenschutz steht im Saarland die Landesbeauftragte für Datenschutz zur Verfügung. Dreht es sich um Fragen zum Datenschutz am Arbeitsplatz, sind bei kirchlichen Einrichtungen die jeweiligen kirchlichen Datenschutzbeauftragten zuständig. Die Adressen finden sich im Anhang.

Datenschutz am Arbeitsplatz

Inhalt:

Der Datenschutz am Arbeitsplatz ist nur eine Facette des Datenschutzes und auch hier gelten die Grundlagen, die im Kapitel „Wie funktioniert der Datenschutz?“ dargestellt wurden. Es geht also um die Erhebung, Verarbeitung, Löschung oder Speicherung von personenbezogenen Daten von Beschäftigten und darum, dass bei diesen Vorgängen ihre Rechte gewahrt bleiben.

Die Diskussion um den betrieblichen Datenschutz beginnt in aller Regel mit der skeptischen Frage eines Beschäftigten, ob der Arbeitgeber seine personenbezogenen Daten verarbeiten darf, auch wenn er nicht damit einverstanden ist.

> ***Darf der Arbeitgeber meine personenbezogenen Daten erheben und verarbeiten - auch wenn ich das nicht will?***

Diese Frage ist für die Betroffenen nicht immer einfach zu beantworten. Auf den folgenden Seiten wird beschrieben, wie man herausfinden kann, was geht und was nicht und was man im Zweifelsfall unternehmen kann, um seine Privatsphäre am Arbeitsplatz zu schützen und gegen Benachteiligung vorzugehen.

Die unterschiedlichen Interessen von Arbeitgeber und Beschäftigten

Man muss sich vor Augen halten, dass Arbeitgeber und Arbeitnehmer die Erhebung und Verarbeitung von Mitarbeiterdaten aus unterschiedlichen Perspektiven betrachten.

Der Arbeitgeber möchte die Daten von Beschäftigten erheben und verarbeiten, um seine berechtigten Interessen wahrnehmen zu können, zum Beispiel den Schutz seines Eigentums vor Diebstahl. Der Beschäftigte hingegen hat Anspruch darauf, dass seine schutzwürdigen Belange wie das Recht auf Privatsphäre, Meinungsfreiheit und informationelle Selbstbestimmung gewahrt werden. Zwischen diesen natürlichen Interessengegensätzen versuchen die Gesetze einen tragfähigen Weg zu finden, so dass beide Seiten zu ihrem Recht kommen.

Welches Datenschutzgesetz gilt an welchem Arbeitsplatz?

Es wurde bereits beschrieben, dass es in der Bundesrepublik Deutschland eine Reihe von Datenschutzgesetzen gibt, die parallel nebeneinander gelten. Bis zum heutigen Tag gibt es allerdings kein einheitliches und verbindliches Beschäftigtendatenschutzgesetz, das an allen Arbeitsplätzen in Deutschland anwendbar ist.

Welches Datenschutzgesetz am jeweiligen Arbeitsplatz gilt, hängt davon ab, welchem Geltungsbereich der Arbeitgeber bzw. das Unternehmen, die Einrichtung oder Behörde zuzuordnen ist. Nur wenn zweifelsfrei geklärt ist, welches Gesetz zur Geltung kommt, lässt sich überhaupt klären, was zulässig ist oder nicht. Die Frage nach dem am Arbeitsplatz geltenden Datenschutzgesetz ist also äußerst wichtig und muss vorrangig geklärt werden.

Geltungsbereiche:

Unternehmen der Privatwirtschaft
→ *Bundesdatenschutzgesetz*

Öffentliche Stellen, Behörden und Einrichtungen des Bundes
→ *Bundesdatenschutzgesetz*

Öffentliche Stellen, Behörden und Einrichtungen des Saarlandes
→ *Saarländisches Datenschutzgesetz*

Öffentliche Stellen, Behörden, Einrichtungen, Verwaltungen der saarländischen Landkreise und Kommunen
→ *Saarländisches Datenschutzgesetz*

Einrichtungen in katholischer Trägerschaft z. B. Pfarrgemeinden, Krankenhäuser, Pflege- und Sozialeinrichtungen
→ *KDO*

Einrichtungen in protestantischer Trägerschaft z. B. Pfarrgemeinden, Kirchenkreise, Krankenhäuser, Pflege- und Sozialeinrichtungen
→ *DSG-EKG*

Wann ist es schwierig zu klären, welches Datenschutzgesetz gilt?

Welches Datenschutzgesetz bei einem Klempner (BDSG), bei einem katholischen Krankenhaus (KDO) oder bei der Bundespolizei (BDSG) gilt, lässt sich auf Anhieb klären. Es gibt jedoch eine Reihe von Fällen, die nicht einfach zuzuordnen sind.

Beispiel: Stadt- und Gemeindewerke.

> *Üblicherweise handelt es sich um kommunale Einrichtungen - im Geltungsbereich des Saarländischen Datenschutzgesetzes. In aller Regel wurden sie privatisiert und in eine GmbH oder in eine andere Rechtsform überführt. Damit wären sie üblicherweise als privatwirtschaftliche Unternehmen im Geltungsbereich des Bundesdatenschutzgesetzes.*
>
> *Es gibt jedoch noch zwei weitere Kriterien zu überprüfen. Gehört die Mehrheit eines Unternehmens einer Kommune, dem Kreis oder Land, dann könnte auch das Saarländische Datenschutzgesetz gelten. Ein weiteres Kriterium ist die Art der Tätigkeit. Werden nur solche Aufgaben erfüllt, die auch ein konventionelles Unternehmen aus der Privatwirtschaft erfüllt z. B. Energieversorgung, dann ist das ein Hinweis darauf, dass das Bundesdatenschutzgesetz gilt. Werden hingegen Tätigkeiten ausgeübt, die typischerweise nur von den Kommunen selbst ausgeübt werden, gilt das Saarländische Datenschutzgesetz. Möglich ist allerdings auch, dass für bestimmte Aspekte das Saarländische Datenschutzgesetz und für andere Aspekte das Bundesdatenschutzgesetz gilt.*

Diese Problematik findet sich auch bei anderen Betrieben, Einrichtungen, Vereinen und Zweckverbänden, die in Kooperation von Privatwirtschaft, Bund, Land, Kreis, Kommune oder kirchlichen Trägern betrieben werden.

Wie findet man in Zweifelsfällen heraus, welches Datenschutzgesetz am eigenen Arbeitsplatz gilt?

Hier sollte man als Beschäftigter keine komplizierte Recherche anstellen, sondern einfach beim Arbeitgeber oder - sofern vorhanden - beim Datenschutzbeauftragten am Arbeitsplatz nachfragen. Der Arbeitgeber müsste es wissen, da er verpflichtet ist die gesetzlichen Regelungen umzusetzen. Kann er diese Frage nicht eindeutig beantworten, oder gibt es Zweifel an der Auskunft, sollte man sich kurzerhand an die Landesbeauftragte für Datenschutz im Saarland wenden (Kontaktdaten im Anhang). Die Mitarbeiter ihrer Dienststelle können die Frage nach dem Geltungsbereich zweifelsfrei beantworten.

Datenschutzgesetze sind (arbeits-)weltfremd

Nachdem man festgestellt hat, welches Datenschutzgesetz das richtige für die eigene Betriebsstätte ist, stellt sich schnell Ernüchterung ein. Auch wenn die Art der Betriebsstätte ausschlaggebend dafür ist, welches Gesetz gilt, so handelt es sich bei den Gesetzen nicht um reine Gesetze zum Datenschutz im Arbeitsverhältnis. Sie sollen vielmehr alle Aspekte des Datenschutzes aufgreifen, die im sogenannten Geltungsbereich des Gesetzes liegen.

Es liegt in der Natur der Sache, dass ein Datenschutzgesetz wie das BDSG, das gleichermaßen den Datenschutz auf einer Ostseefähre, bei der Gebühreneinzugszentrale, in einem Versicherungskonzern und in einer Arztpraxis gelten soll, allgemein gehalten sein muss. Die Verständlichkeit eines Gesetzes wird dadurch jedoch nicht gefördert.

Die abstrakten Regelungen werden als das größte Problem der Datenschutzgesetze angesehen. Wie beim Steuerrecht müssen auch die Datenschutzgesetze von jeder Person im Geltungsbereich eingehalten werden, ob sie die Regelungen versteht oder nicht.

Hinzu kommt der Umstand, dass Gesetze erlassen werden als Reaktion auf eine Situation, die bereits seit längerem exis-

tiert. Gesetze reagieren oft recht träge auf die Veränderungen in der Welt.

Die Datenschutzgesetze sind da keine Ausnahme. Sie stammen alle aus einer Zeit, als Computer ausnahmslos Großrechenanlagen waren und Fax eine Schlüsselinnovation. Natürlich haben die Datenschutzgesetze von Zeit zu Zeit Novellierungen erfahren. Letztlich wurden aber immer nur Details geändert. Die Praktikabilität der Gesetze zu hinterfragen und den Beschäftigtendatenschutz vollständig zu modernisieren, hat bislang noch kein Parlament geschafft.

Datenschutz lebt seit vielen Jahren aus der Rechtsprechung

Aber gerade das wäre notwendig. Denn aufgrund der Trägheit, mit der die Datenschutzgesetze modernisiert werden - es hat von 1977 bis 2009 gedauert, bis der Begriff der „Beschäftigten“ in das Bundesdatenschutzgesetz eingeführt wurde - lebt das Datenschutzrecht aus der Rechtsprechung. Und das ist problematisch für alle Beteiligten.

Gesetze gelten für alles und jeden im jeweiligen Geltungsbereich. Urteile sind hingegen richterliche Entscheidungen, die unter Abwägung aller Gesichtspunkte in einem speziellen Einzelfall entschieden wurden. Das heißt, im Klartext, dass es nicht immer möglich ist, die Entscheidung eines Gerichts auf einen anderen Fall zu übertragen. Hinzu kommt, dass Gerichtsurteile ungleich schwerer zu recherchieren sind als Gesetze. Das ist ein Hindernis speziell für Laien, die nichts anderes als ihre Rechte wahren wollen.

Derzeit müssen wir mit diesem Zustand leben, denn nur in richterlichen Urteilen finden sich, zumindest fallbezogen, eindeutige Regelungen zu einzelnen Aspekten. So gibt es Urteile zur Videoüberwachung, zur Datenverwendung bei der Korruptionsbekämpfung, zur betrieblichen Nutzung des Internets und vieles mehr. Wer sich mit dem Datenschutz im Arbeitsverhältnis beschäftigen will oder muss, kommt nicht umhin, alle erdenklichen Gerichtsurteile zu recherchieren. Aus diesem Grund ist es unumgänglich, bei der Vorstellung des Datenschutzes im Arbeitsverhältnis die Rechtsprechung mit einzubeziehen.

Die betrieblichen Akteure beim Datenschutz

Datenschutz am Arbeitsplatz entsteht nicht aus sich selbst. Es gibt ihn nicht, weil es Gesetze gibt oder Gerichtsurteile, sondern weil Personen die Gesetze aufgreifen und umsetzen. Datenschutz lebt oder scheitert mit den handelnden Personen. Deshalb ist es sinnvoll, sich damit zu beschäftigten, wer in den Betriebsstätten in welcher Funktion mit dem Datenschutz zu tun hat.

EDV-Mitarbeiter, Personalsachbearbeiter, Mitarbeiter in der Lohnbuchhaltung aber auch der Werksarzt mit seiner Schweigepflicht fallen einem hierzu ein. Die Datenschutzgesetze kennen diese Personen allesamt nicht. Selbst wenn man den Kreis erweitert um Personalleiter, Suchtbeauftragte und andere, die im Betrieb mit persönlichen und vertraulichen Informationen konfrontiert werden, wird man in den Datenschutzgesetzen nicht fündig. Einzig die Beauftragten für Datenschutz sind den Gesetzen namentlich bekannt; seit 2009 kennt das BDSG nun auch Interessenvertreter der Beschäftigten. Mit etwas Phantasie kann man hier den Betriebs- oder Personalrat identifizieren.

Die Sicht der Datenschutzgesetze:

Betroffene und verantwortliche Stellen

Die Datenschutzgesetze „denken“ in anderen Kategorien als „normale“ Menschen. Im Wesentlichen wird unterschieden zwischen Betroffenen, also natürlichen Personen, deren Daten erhoben und verarbeitet werden sollen, und denen, die die Daten erheben und verarbeiten. Letztere nennt das BDSG und das SDSG „verantwortliche Stelle“, auch wenn es sich dabei nur um eine einzelne Person handelt, die die Daten verarbeitet. In der KDO und im DSG-EKD wird hierfür der Begriff „speichernde Stelle“ verwendet, auch wenn nicht nur gespeichert, sondern auch verarbeitet wird.

Beschäftigte als Betroffene

Bei allen, deren Daten erhoben und verarbeitet werden, handelt es sich um Betroffene. Das sind prinzipiell alle Betriebsangehörigen, gleich welcher Position. Selbst die personenbezogenen Daten eines Geschäftsführers müssen für die Entgeltberechnung verwendet werden. In diesem Zusammenhang ist auch er ein Betroffener, obwohl er aus anderer Perspektive

auch die verantwortliche Stelle repräsentiert.

Am Arbeitsplatz gelten die allgemeinen Datenschutzregeln, die vorgeben, wie mit den Daten der Betroffenen verfahren werden muss. Deshalb sind diese Regelungen natürlich auch für alle Beschäftigten anzuwenden. Allerdings gibt es bei der Datenverwendung am Arbeitsplatz besondere Regelungen in einigen Gesetzen.

2009 wurde im BDSG mit § 32 eine spezielle Regelung zum Umgang mit Beschäftigtendaten eingeführt. Damit klar ist, für wen diese Regelung zutrifft, wurde der Begriff der Beschäftigten im Sinne des Bundesdatenschutzgesetzes definiert.

Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,

2. zu ihrer Berufsbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,

6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3 Abs. 11 Bundesdatenschutzgesetz

Dass es diese Definition bislang nur im BDSG gibt, bedeutet jedoch keine Schlechterstellung der Beschäftigten, die im Geltungsbereich von SDSG, KDO und DSG-EKD arbeiten. Alle, die in Betriebsstätten arbeiten und deren Daten erhoben und verarbeitet werden, sind Betroffene. Ihre Rechte sind in jedem Fall gewahrt.

Diese Definition von „Beschäftigten“ ist insofern wertvoll, wie der Begriff in anderen Zusammenhängen anders definiert wird. Im BDSG ist der Begriff der Beschäftigten weit gefasst und der Interpretationsspielraum gering. So fallen z. B. auch Auszubildende, Heimarbeiter, Bewerber und Zivildienstleistende darunter und profitieren ausdrücklich von den speziellen Regelungen des § 32 BDSG, ohne dass darüber diskutiert werden muss, ob die Personengruppen darunter fallen oder nicht.

Im Betriebsverfassungsgesetz (BetrVG), der Handlungsgrundlage für Betriebsräte, wird der Begriff „Arbeitnehmer“ in § 5 anders definiert und schließt z. B. Bewerber nicht mit ein.

Neben den Betroffenen und der verantwortlichen Stelle werden in den Datenschutzgesetzen noch die Begriffe „Dritter“ und „Empfänger“ benutzt. Diese Begriffe werden zum besseren Verständnis auf den nachfolgenden Seiten im jeweiligen Zusammenhang vorgestellt.

Der Arbeitgeber als verantwortliche Stelle

Die Lohnbuchhaltung, die Personalabteilung, die Personalleitung und ähnliche Einheiten sind Teile der verantwortlichen (BDSG/SDSG) bzw. speichernden (KDO/DSG-EKD) Stelle. Sie alle sind mit der Erhebung und Verarbeitung von personenbezogenen Daten der Mitarbeiter für den Arbeitgeber beschäftigt. Die Verantwortung für die Einhaltung der gesetzlichen Vorgaben in den einzelnen Abteilungen liegt beim Arbeitgeber. Letztlich ist er die verantwortliche Stelle. Die Personalabteilung, Lohnbuchhaltung usw. handeln nur in seinem Auftrag.

Hinweis: Interessenvertretungen als verantwortliche Stellen

Oft gibt es allerdings noch eine weitere verantwortliche Stelle am Arbeitsplatz. Im Rahmen ihres gesetzlichen Auftrages (das

ist in diesem Zusammenhang die Zweckbindung) können Betriebsräte, Personalräte und Mitarbeitervertretungen die hierzu notwendigen personenbezogenen Daten der Beschäftigten erheben und verarbeiten.

Die Interessenvertretungen sind wie jede andere verantwortliche Stelle an die Einhaltung der Datenschutzgesetze gebunden und sind natürlich auch allen Betroffenen - also allen Beschäftigten - zur Auskunft verpflichtet.

Der Beauftragte für den Datenschutz

Die speziellen Aufgaben und Befugnisse, die Zugangsvoraussetzungen und Rechtsstellung sind in den jeweiligen Datenschutzgesetzen vorgegeben. Sie werden in einem eigenen Kapitel vorgestellt. An dieser Stelle erfolgt nur eine Kurzbeschreibung seiner Aufgaben.

Der Beauftragte für Datenschutz (BfD) hat die Aufgabe, darauf hinzuwirken, dass die Einhaltung des Datenschutzes im Sinne des Gesetzes erfolgt. Er ist für die gesamte Spannbreite des Datenschutzes zuständig, nicht nur für den Beschäftigtendatenschutz. Datenverarbeitungsverfahren auf ihre Rechtmäßigkeit hin zu überprüfen ist nur eine Aufgabe.

Er ist daneben auch ein interner Datenschutz-Berater und Ansprechpartner für alle, die wissen wollen, was mit ihren Daten passiert oder auch die Fachabteilungen, die wissen möchten, ob sie bestimmte personenbezogene Daten erheben und verarbeiten dürfen.

Der Beauftragte für Datenschutz informiert und berät. Daneben führt er allerdings auch Kontrollen aus, ob die Datenschutzgesetze eingehalten werden. Gerade dann, wenn es sich um besonders sensible personenbezogene Daten handelt, oder Daten von Betroffenen in elektronischen Systemen verarbeitet werden, ist er gefordert. Er kontrolliert, ob die verantwortliche Stelle - der Arbeitgeber - mit personenbezogenen Daten so umgeht, wie es die Gesetze erfordern. Damit er diese Aufgaben auch unabhängig und durchaus kritisch erledigen kann, ist er nicht weisungsgebunden und genießt einen besonderen Kündigungsschutz.

Es ist allerdings nicht seine Aufgabe, den Datenschutz umzusetzen. Das ist die Auf-

gabe der verantwortlichen Stelle, also des Arbeitgebers. Der BfD unterstützt ihn nur bei dieser Verpflichtung mit Rat und Kontrollen.

Die unterschiedlichen Arten von Beschäftigtendaten

Selbst ein unbedarfter Laie wird feststellen, dass ein Beschäftigungsverhältnis ohne personenbezogene Daten der Mitarbeiter nicht möglich ist. Ohne eine Reihe von persönlichen Angaben wie Name, Anschrift, Bankverbindung, kann keine Lohnabrechnung und Überweisung erfolgen und auch keine Meldung an die Sozialversicherungen.

Der Arbeitgeber muss also personenbezogene Daten von Beschäftigten verarbeiten. Die Frage ist also nicht, ob er personenbezogene Daten verarbeiten darf, sondern vielmehr, welche Daten von den Beschäftigten er für welchen Zweck verarbeiten kann oder muss.

Zunächst ist es ratsam zu überprüfen, ob es sich tatsächlich um personenbezogene oder personenbeziehbare Daten handelt, die der Arbeitgeber erheben möchte oder bereits erhebt. Zur Erinnerung: Daten (Angaben) sind personenbeziehbar, wenn unter Zuhilfenahme weiterer Informationen Rückschlüsse auf Einzelne gezogen werden können.

Beispiel: Maschinendatenerfassung

> *Eine Maschine protokolliert automatisch reine Produktionsdaten nach Uhrzeit: Anzahl der Teile, Bearbeitungszeit, Stillstandzeiten, Störungen und Störungsgründe. Mit einem Blick auf den Schichtplan, oder Nachfragen, lässt sich auf einfachem Weg herausfinden, wer diese Maschine zu der Uhrzeit bedient hat, als sie die Störung registriert hat.*
>
> *Das kann zweifellos sinnvoll sein, um die näheren Umstände der Störung zu erfragen und Produktionsprozesse zu verbessern. Entscheidend ist jedoch, dass es sich bei den Maschinendaten zweifelsfrei um personenbeziehbare Daten handelt, auch wenn das auf Anhieb nicht zu erkennen ist. Es greift das*

Bundesdatenschutzgesetz mit allen Auflagen.

Wichtig ist, beim Analysieren von Daten daran zu denken, alle Umstände mit einzubeziehen.

Beispiel: Rückverfolgbarkeit durch Kombination von Daten

Im Eingangsbereich steht ein Computer mit Internetzugang. Nachts wird dieser Computer zu illegalen Zwecken genutzt. Das soll aufgeklärt werden.

Es kommen fünf Kollegen in Frage. Drei Kollegen haben in dieser Zeit Maschinen bedient, die nicht verlassen werden können, ohne dass die Maschinen einen Stillstand, oder Arbeitsunterbrechung registriert. Ein Kollege vom Sicherheitsdienst hat zum Zeitpunkt, als der Computer genutzt wurde, einen persönlichen Sicherheitscode an einem entfernten Kontrollpunkt auf seinem Rundgang eingegeben. Auch das lässt sich überprüfen. Der Verdacht konzentriert sich auf den zweiten Kollegen des Sicherheitsdienstes.

Im betrieblichen Alltag ist es oft gar nicht notwendig viele Daten abzugleichen, um einen Einzelnen identifizieren zu können. In der Praxis genügt es oft, dass man bestimmte Umstände auf eine kleine Gruppe möglicher Verursacher zurück verfolgen kann, um dann bei näherer Betrachtung der sozialen Umstände oder einfaches Nachfragen den eigentlichen Verursacher auszumachen.

Keine Anonymität in kleinen Gruppen

In kleinen Gruppen von Beschäftigten, gibt es keine wirkliche Anonymität. Zu dieser Erkenntnis kam das Bundesarbeitsgericht (BAG) bereits vor Jahrzehnten. In einem Urteil wurde festgestellt, dass die Mitbestimmung der Betriebsräte auch dann gegeben ist, wenn Leistungen von Arbeitnehmern mit technischen Einrichtungen festgestellt werden, die sich auf eine kleine Gruppe beziehen. Das BAG ging in seinem Urteil vom 18.02.1986 davon aus, dass der daraus resultierende Leistungsdruck auf den Einzelnen durchdringen wird. Als „klein“ definierte das BAG eine

Gruppe, die aus weniger als fünf Personen besteht.

Hinweis:

Die Feststellung des Bundesarbeitsgerichts behandelt die Frage, ob ein Betriebsrat Mitbestimmungsrechte einfordern kann, wenn ein technisches System eine Leistungs- und Verhaltenskontrolle von kleinen Gruppen ermöglicht.

Da Personalräte und Mitarbeitervertretungen ebenfalls Mitbestimmungsrechte zu technischen Einrichtungen aus den Personalvertretungsgesetzen und der Mitarbeitervertretungsordnung geltend machen können, ist davon auszugehen, dass auch für sie die Feststellung des Bundesarbeitsgerichts angewendet werden kann.

***Aber:* Das Urteil des BAG beantwortet die Frage nur für die Arbeitswelt. Das Urteil ist nicht automatisch auf allgemeines Datenschutzrecht zu übertragen.**

Besonders sensible persönliche Daten

Im Alltag wird gerne zwischen wichtigeren und unwichtigeren, zwischen unbedenklichen und sensiblen Daten unterschieden. Und auch am Arbeitsplatz finden solche Abgrenzungen statt. Urlaubs- und Schichtpläne als personenbezogene Daten am schwarzen Brett auszuhängen ist üblich und oft auch notwendig, ohne dass man das Gefühl haben muss, in seinen Persönlichkeitsrechten benachteiligt zu werden. Bei Personalakten ist es ebenso selbstverständlich, dass sie unter Verschluss gehalten werden und nur für einen sehr engen Personenkreis einsehbar sind. Zwischen beiden Datenarten - Urlaubspläne und Personalakten - wird man noch eine Reihe von Abstufungen einführen können, nach denen man die Schutzwürdigkeit von persönlichen Daten einstuft. Die Datenschutzgesetze als verbindliche Regelungen gehen hier allerdings ein wenig anders vor.

Die Gesetze gehen von dem Grundsatz aus, wenn personenbezogene oder personenbeziehbare Daten erhoben und verarbeitet werden dürfen, muss das grundsätzlich zweckgebunden, sicher und vertraulich erfolgen, weil den Betroffenen ein

Schaden durch Missbrauch entstehen kann. Ein laxer Umgang mit personenbezogenen Daten darf es also unter keinen (legalen) Fällen geben.

Allerdings gehen von bestimmten Angaben von Personen besonders hohe Risiken für die Betroffenen aus. Am Arbeitsplatz kann das Bekanntwerden einer psychischen Erkrankung das Ende der beruflichen Laufbahn bedeuten. Das Bekanntwerden einer homosexuellen Identität stellt nicht nur Fußballer und Bundeswehrsoldaten vor ernsthafte Probleme.

Diesem Umstand tragen alle Datenschutzgesetze Rechnung. Sie sprechen in diesem Zusammenhang von besonderen Arten von personenbezogenen Daten, für die besondere Vorgaben zu beachten sind.

> ***Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.***
>
> § 3 Abs. 9 Bundesdatenschutzgesetz
>
> § 4 Abs. 2 SDSG
> § 2 Abs. 10 KDO
> § 2 Abs. 11 DSG-EKD

Allerdings machen die kirchlichen Datenschutzgesetze folgenden Ausschluss:

> ***Dazu** (= zu den besonderen Arten personenbezogener Daten, A. d. H.) **gehört nicht die Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft.***
>
> § 2 Abs. 10 KDO
> § 2 Abs. 11 DSG-EKD

Vor der Erhebung und Verarbeitung von solch kritischen Daten muss natürlich geprüft werden, ob dies im Beschäftigungsverhältnis überhaupt zwingend erforderlich ist, denn der beste Schutz vor Benachteiligung durch den Missbrauch von personenbezogenen Daten ist die Datenvermeidung. Alle erforderlichen und damit unvermeidlichen Datenverarbeitungsprozesse bergen persönliche Risiken, die man durch Sorgfalt und Verantwortungsbewusstsein zwar minimieren, aber nicht ausschließen kann.

Gelten die Datenschutzgesetze nur für elektronische Daten?

Die Datenschutzgesetze legen zwar fest, was personenbezogene oder personenbeziehbare Daten sind, treffen aber keine Aussage darüber, ob es sich dabei um digitale und somit maschinenlesbare Daten handelt oder um handschriftliche Notizen. Einen entscheidenden Hinweis findet man allerdings an anderer Stelle, bei der Verwendung der Daten (§ 3 Abs. 4 BDSG, § 3 Abs. 2 SDSG, § 2 Abs. 4 KDO, § 2 Abs. 4 DSG-EKD). Dort geht hervor, dass beim Verarbeiten personenbezogener Daten die Art der angewendeten Verfahren keine Rolle spielt.

Noch deutlicher wird das Bundesdatenschutzgesetz in § 32 Abs. 2. Es gibt vor, dass die Regeln zum Erheben, Verarbeiten und Nutzen von Daten für Zwecke des Beschäftigungsverhältnisses auch anzuwenden sind, „wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, *ohne dass sie automatisiert verarbeitet* oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.“

Einfacher ausgedrückt: Es muss sich nicht um digitale personenbezogene Daten handeln. Im Beschäftigungsverhältnis greifen die Datenschutzgesetze auch bei handschriftlichen Daten. Entscheidend ist nur, ob sie personenbezogen oder personenbeziehbar sind.

Erstes Fazit:

Beim Erheben und Verarbeiten von Daten am Arbeitsplatz

- ist es wichtig, herauszufinden, ob sie personenbezogen sind,
- ist es wichtig, festzustellen, ob sich nicht mit Zuhilfenahme anderer Daten ein Personenbezug herstellen lässt,
- greifen die Datenschutzgesetze auch, wenn es nicht möglich ist Rückschlüsse auf Einzelne zu ziehen, sondern auch bei kleinen Gruppen von maximal vier Personen,

- dürfen personenbezogene Daten nur erhoben werden, wenn es unvermeidbar ist, und dann auch nur so wenige Daten wie möglich,
- spielt es keine Rolle, in welcher Form Daten vorliegen,
- müssen besondere Arten von personenbezogenen Daten besonders geschützt werden,

damit die Datenschutzgesetze und damit die strengen Regeln der Datenerfassung und -verarbeitung beachtet werden müssen.

Erheben personenbezogener Daten am Arbeitsplatz

In den vorausgegangenen Abschnitten wurde dargestellt, welches Datenschutzgesetz an welcher Betriebstätte gilt und für welche Daten die Gesetze gelten. Eine entscheidende Frage am Arbeitsplatz lautet jedoch:

Zu welchen Zwecken dürfen Daten von Beschäftigten erhoben und verarbeitet werden?

Diese Frage ist einfach zu beantworten, doch die Antwort ist unbefriedigend.

> ***Daten von Beschäftigten dürfen zu allen erdenklichen Zwecken erhoben und verwendet werden, zu denen der Beschäftigte sein vorheriges Einverständnis gegeben hat.***
>
> und
>
> ***Daten von Beschäftigten dürfen ohne Einverständnis des Beschäftigten nur erhoben und verarbeitet werden, sofern dies eine Rechtsvorschrift anordnet oder ermöglicht oder das zutreffende Datenschutzgesetz es ermöglicht.***

Mit dieser Erkenntnis erhält man in der Praxis zwar keine konkrete Antwort, aber eine gute Hilfestellung, wie man vorgehen kann, um dies zu klären.

Zur Erinnerung: Die Datenschutzgesetze sind Verbote, die die Verwendung personenbezogener Daten grundsätzlich untersagen und nur durch Rechtsvorschrift oder explizite Erlaubnis des Betroffenen Ausnahmen gestatten. Wer personenbezogene Daten erheben und verarbeiten möchte, muss also nachweisen können, dass er über eine solche Erlaubnis verfügt.

Die Arbeitswelt, wie sie sein soll…

Im Arbeitsverhältnis ist es in aller Regel der Arbeitgeber, der als verantwortliche Stelle personenbezogene Daten von Beschäftigten erheben und verarbeiten möchte. Man kann als Beschäftigter nicht alle Rechtsvorschriften kennen, die eine Datenerhebung und -verarbeitung ohne Einverständnis ermöglichen. Aber die verantwortliche Stelle, also der Arbeitgeber oder dessen Beauftragter, der die Daten erheben und verarbeiten will, muss die

Rechtsvorschrift kennen und auch Auskunft geben können.

Die Arbeitswelt, wie sie leider allzu oft ist…

Bereits bei der Einstellung muss man als Beschäftigter eine Vielzahl von Angaben machen. Aber muss man wirklich alles angeben, wenn man von einem Mitarbeiter der Personalabteilung ausgefragt wird? Auch am Arbeitsplatz gilt schließlich das Recht auf informationelle Selbstbestimmung. Üblicherweise wird nach der Kontonummer gefragt, einer doch sehr persönlichen Angabe, ebenso wie der Anzahl der Kinder.

Ein kritischer Beschäftigter könnte den Personalsachbearbeiter bitten, die Rechtsgrundlage seiner Fragen darzustellen. Und ein belesener Personalsachbearbeiter würde, in diesem Fall die Datenerfassungs- und Übermittlungsverordnung (DEÜV) zitieren.

Die DEÜV als Rechtsvorschrift verpflichtet den Arbeitgeber zur Erfassung und Übertragung einer Vielzahl von Angaben an die Sozialversicherungen. Die Kontonummer gehört dazu, die Anzahl der Kinder auch, ebenso wie die Postanschrift. Der Beschäftigte muss also diese Fragen beantworten.

Man muss sich nichts vormachen. Die geschilderte Situation ist weltfremd und unrealistisch. Auch wenn einige Fragen bei der Einstellung Unbehagen hervorrufen, will niemand bereits zu diesem Zeitpunkt am Arbeitsplatz anecken, und zeigt sich kooperativ. Auch bei Fragen, die dem Betroffenen unrechtmäßig vorkommen. Antworten werden wahrheitsgemäß erteilt, Fragen nach der Rechtmäßigkeit unterbleiben. Dem Betroffenen ist es in diesem Stadium nicht möglich, seine Rechte einzufordern - eine Kündigung ohne Begründung ist innerhalb der Probezeit jederzeit möglich. Der Begriff der abhängigen Beschäftigung wird hier sehr deutlich.

Oft genug werden bereits beim Unterzeichnen des Arbeitsvertrages weitere „Einverständniserklärungen“ vorgelegt, in denen sich der künftige Beschäftigte einverstanden erklärt, dass bestimmte personenbezogene Daten über ihn erhoben und verarbeitet werden. Gängig ist, dass man sich einverstanden erklärt, dass man am Arbeitsplatz mit Kameras überwacht wird, dass Ortungssysteme in Fahrzeugen und Protokolldaten aus Computersystemen

auch zu Verhaltenskontrollen genutzt werden können. Aber inzwischen ist es auch weit verbreitet, dass die künftigen Beschäftigten vor Aufnahme des Beschäftigungsverhältnisses ihr freiwilliges Einverständnis geben, dass alle von und über sie verfügbaren Daten dauerhaft gespeichert werden können, um sie später zur Aufklärung und Vermeidung von Korruptionsfällen zu nutzen.

Rechtlich ist es nicht zulässig, das Eingehen eines Beschäftigungsverhältnisses von einem freiwilligen Einverständnis in die Erhebung und Verarbeitung von personenbezogenen Daten abhängig zu machen, die im juristischen Sinne nicht erforderlich ist. Dennoch ist dieses Prinzip nicht unüblich.

Hinweise: Einstellungsverfahren

> *Der Beauftragte für Datenschutz sollte sich das Einstellungsverfahren sehr genau ansehen und auf seine Rechtmäßigkeit überprüfen. Die Erfassungsbogen der Personalabteilung müssen begutachtet werden. Entdeckte unzulässige Fragen und Eingabefelder müssen entfernt werden und der BfD muss dafür sorgen, dass die Situation nicht genutzt wird, dem Beschäftigten „freiwillige“ Angaben zu entlocken - zum Beispiel die private Telefonnummer, auch dann nicht, wenn sie im Telefonbuch steht. Denn dort steht sie zu einem anderen Zweck.*

Erforderlichkeit von Daten überprüfen

Es gibt keine gesetzliche Grundlage, auf der der Arbeitgeber die Herausgabe einer privaten Telefonnummer verlangen kann. Sofern dies für betriebliche Zwecke erforderlich ist, kann man das explizit in einem Arbeitsvertrag regeln. Einfacher ist es, ein mobiles Dienstttelefon bereit zu stellen und Rufbereitschaften zu organisieren. Das kann z. B. der Fall sein, wenn ein Hausmeister auch außerhalb seiner regulären Dienstzeiten für den Notrufdienst in einem Fahrstuhl zuständig ist. Oder damit ein IT-Mitarbeiter kontaktiert werden kann, um in einem Schadenfall (z. B. Wasserschaden) noch größeren Schaden an den EDV-Anlagen zu

vermeiden. Aber in allen Fällen muss die Erforderlichkeit im juristischen Sinn gegeben sein. Die Regel ist es nicht.

Die Frage nach der Religionszugehörigkeit wird bei der Einstellung üblicherweise auch gefragt. Das ist eine sehr persönliche Angabe, die im Datenschutz als „besondere Art" personenbezogener Daten einen besonderen Schutz genießt. Es muss einen zwingenden Grund geben, diese Angabe zu erheben. Den gibt es, der Arbeitgeber muss die Kirchensteuer für den Betroffenen entrichten. Aber, wenn keine Kirchensteuer abgeführt werden muss, ist diese Angabe überflüssig. Die Frage müsste vielmehr lauten, ob der künftige Beschäftigte einer der beiden Staatskirchen angehört. Wer einer anderen oder keiner Religionsgemeinschaft angehört, ganz gleich, ob er Zeuge Jehovas ist, Muslim oder Hindu, spielt im Beschäftigungsverhältnis keine Rolle.

Eine Ausnahme stellen die kirchlichen Arbeitgeber dar. Ihnen ist durch ihre Datenschutzgesetze gestattet, die Frage nach der Zugehörigkeit zu einer Religionsgemeinschaft zu stellen.

Zulässigkeit freiwilliger Einverständniserklärungen überprüfen

Weiterhin muss überprüft werden, ob dem künftigen Beschäftigten „freiwillige" Einverständniserklärungen zu anderen Themen abverlangt werden. Dies ist zum Zeitpunkt der Einstellung, aber auch später nur in Ausnahmefällen zulässig.

Aber es ist sehr wohl zulässig und auch ratsam, bereits zum Zeitpunkt der Einstellung den künftigen Mitarbeiter auf die Einhaltung des Datenschutzes und zur Wahrung der Vertraulichkeit zu informieren.

Auch die Interessenvertretung sollte sich den Einstellungsprozess ansehen und sich dafür stark machen, dass freiwillige Angaben auch nur freiwillig gemacht werden.

Personenbezogene Daten von Beschäftigten müssen beim Beschäftigten erhoben werden, begründete Ausnahmen sind aber möglich.

Beim Einstellungsverfahren werden üblicherweise alle Daten, die man benötigt, in einem gemeinsamen Gespräch zwischen dem künftigen Beschäftigten und einem Mitarbeiter der Personalverwaltung erhoben. In diesem Zusammenhang kann der Betroffene nachfragen, welchem Zweck das dient. Dieses Verfahren geben die Datenschutzgesetze als das übliche Prinzip vor:

> ***Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn***
>
> ***1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder***
>
> ***2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder***
>
> ***b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.***
>
> § 4 Bundesdatenschutzgesetz

Nahezu wortgleiche Entsprechungen dieser Vorgabe finden sich in § 12 Abs. 1 SDSG, § 4 Abs. 2 DSG-EKD, § 9 Abs. 2 KDO. Diese Vorgabe ermöglicht auch eine Datenerhebung aus anderen Quellen, aber als begründete Ausnahme. Die Regel ist ein transparentes Verfahren, in dem den Betroffenen auch die Tatsache bewusst wird, dass man „ihre“ Daten erhebt.

Die verantwortliche Stelle muss darstellen können, dass sie personenbezogene Daten rechtmäßig erheben und verarbeiten darf.

Wer als Beschäftigter oder Interessenvertreter von seinen Rechten Gebrauch macht und die Frage nach der Rechtsvorschrift für die Datenerhebung stellt, erntet

allzu oft ungläubige Blicke oder wird konfrontiert mit der Frage:

> ***Wo steht das?***
>
> ***Das steht im Bundesdatenschutzgesetz, in § 4, im SDSG in § 4, im DSG-EKD in § 4 und in der KDO in § 3.***

Damit ist klargestellt, dass die verantwortliche Stelle verpflichtet ist, die Rechtmäßigkeit darzustellen. Peter Schaar, der Bundesbeauftragte für Datenschutz, drückt dies in seiner Veröffentlichung BDSG-Info1 so aus:

> ***Grundsätzlich ist verboten, was nicht ausdrücklich erlaubt ist!***

Es ist nicht die Aufgabe des Betroffenen/Beschäftigten nachweisen zu müssen, dass das Erheben von personenbezogenen Daten verboten ist. Davon muss man beim Datenschutz grundsätzlich ausgehen. Es ist die Verpflichtung desjenigen, der personenbezogene Daten erheben und verarbeiten will, darzustellen, dass er die Erlaubnis hat.

Qualitätsmanagement und Controlling sind keine Rechtsvorschrift

Bei der Frage nach der Zulässigkeit der Datenerhebung erhält man oft auch Antworten wie zum Beispiel „Wir brauchen die Daten für unser Qualitätsmanagement“ oder „Wir brauchen die Daten für das Controlling“.

Das mag zwar eine sachliche Antwort sein, Qualitätsmanagement und Controlling stellen jedoch keine Rechtsgrundlage dar, aufgrund derer personenbezogene Daten erhoben werden können. Selbst bei etablierten und weit verbreiteten Normen wie z. B. DIN ISO 9000ff handelt es sich lediglich um Industrie-Standards. Ein Verweis auf solche Verfahren genügt nicht, um in Deutschland personenbezogene Daten erheben und verarbeiten zu können.

Will man Beschäftigtendaten für diese Zwecke verwenden, kann man das in der Regel nur auf der Grundlage von Gesetzen, Verordnungen oder Tarifen tun. Oder es wurden Betriebs- oder Dienstvereinbarungen eigens für diesen Zweck abgeschlossen. Betriebs- oder Dienstvereinbarungen haben innerbetrieblich den Status

einer Rechtsvorschrift. Das, was darin steht, gilt unmittelbar und zwingend für alle Beschäftigten. Allerdings können in solchen Vereinbarungen nur Themen geregelt werden, die nicht bereits abschließend in einem Gesetz geregelt sind.

Mit anderen Worten: Wenn Daten von Beschäftigten für Controllingzwecke oder für das Qualitätsmanagement verwendet werden sollen, kann das der Arbeitgeber als verantwortliche Stelle nur in wenigen Fällen eigenmächtig festlegen. Aber in welchen?

Das Direktionsrecht des Arbeitgebers und der Datenschutz

Das Weisungsrecht des Arbeitgebers ist konkret geregelt in der Gewerbeordnung (GewO):

> ***Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind. Dies gilt auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb. Bei der Ausübung des Ermessens hat der Arbeitgeber auch auf Behinderungen des Arbeitnehmers Rücksicht zu nehmen.***
>
> § 106 Gewerbeordnung

Mit Bezug auf das Weisungsrecht kann der Arbeitgeber rechtfertigen, Daten von Beschäftigten zu erheben, um zu kontrollieren, ob die Arbeit zu der Zeit und an dem Ort erledigt wird, die er bestimmt hat. § 106 GewO ermöglicht also eine Anwesenheitskontrolle, soweit nichts Näheres in Arbeitsverträgen, Tarifen oder Betriebsvereinbarungen geregelt ist. Allerdings ist bei der Wahl der Mittel „wie“ die Anwesenheitskontrolle erfolgen soll, die Verhältnismäßigkeit zu wahren. Für den Zweck einer Anwesenheitskontrolle ist das Bedienen einer Zeiterfassung verhältnismäßig. Die Beschäftigten mit Ortungsgeräten auszustatten, Diensthandys zu orten oder ihre Arbeitsplätze flächendeckend mit Kameras zu überwachen, ist zum Zweck der Anwesenheitskontrolle nicht verhältnismäßig. Solche Maßnahmen werden von der Gewerbeordnung ausgeschlos-

sen. Somit ist das Weisungsrecht nach § 106 GewO auch keine Rechtsgrundlage, auf der man die personenbezogenen Daten von Beschäftigten mit Überwachungseinrichtungen erheben kann. Allerdings ist es dem Arbeitgeber jederzeit möglich, die Anwesenheit persönlich ohne Technik zu kontrollieren.

Wenn nicht bereits in Arbeits- oder Tarifverträgen, in Betriebs- oder Dienstvereinbarungen Regelungen festgelegt wurden, kann der Arbeitgeber auch den Inhalt der Arbeit bestimmen. Daraus lässt sich natürlich auch ein Kontrollrecht ableiten. Der Arbeitgeber kann jederzeit persönlich kontrollieren, ob der Beschäftigte die angewiesenen Inhalte der Arbeit tatsächlich umsetzt. Er kann, das hat das Bundesarbeitsgericht in einem Urteil bestätigt (BAG 19.04.2007 AP BGB § 611 Direktionsrecht Nr. 77), die Beschäftigten anweisen, detaillierte und qualifizierte Tätigkeitsberichte zu führen - in Papierform.

Allerdings sind auch hier alle genannten Faktoren zu überprüfen, zum Beispiel ob dies mit abgeschlossenen Betriebs- und Dienstvereinbarungen oder tariflichen Regelungen im Einklang steht. Das Erstellen von Tätigkeitsnachweisen muss einem sachlichen Grund erwachsen und darf nicht willkürlich angeordnet werden. Und auch die Verhältnismäßigkeit muss gewahrt bleiben. Weitergehende Rechte zur Kontrolle der Beschäftigten lassen sich aus dem Direktionsrecht allerdings nicht ableiten und begründen.

Hinweis: Abschluss von Betriebs- und Dienstvereinbarungen zu Kontrollen

> *Betriebsräte, Personalräte und Mitarbeitervertretungen sollten von ihren Mitbestimmungsrechten Gebrauch machen und die Kontrolle von Ort und Zeit der Arbeitserbringung in Betriebs- und Dienstvereinbarungen klar regeln.*
>
> *In Fragen der Ordnung und des Verhaltens in der Betriebsstätte wie auch beim Einsatz von technischen Anlagen zur Kontrolle von Leistung und Verhalten stehen den Interessenvertretern weitreichende Mitbestimmungsrechte zu, um ihre Kollegen vor willkürlicher und unverhältnismäßiger Kontrolle zu schützen.*
>
> *In diesen Vereinbarungen sollten zweckmäßigerweise Art der Tätig-*

keitsnachweise, Verwendungszweck der Daten und sämtliche Kontrollarten verbindlich festgelegt werden.

Datenerhebung auf der Grundlage des Arbeitsvertrages

Im Zusammenhang mit der Datenerhebung auf der Grundlage des Direktionsrechts wurde erwähnt, dass auch der Arbeitsvertrag eine Rechtsgrundlage darstellt, aufgrund dessen personenbezogene Daten von Beschäftigten erhoben und verarbeitet werden können.

Ein Arbeitsvertrag ist, einfach ausgedrückt, ein Vertrag zwischen zwei Parteien. Näheres hierzu regelt das Bürgerliche Gesetzbuch (BGB) und die Gewerbeordnung:

> ***Arbeitgeber und Arbeitnehmer können Abschluss, Inhalt und Form des Arbeitsvertrages frei vereinbaren, soweit nicht zwingende gesetzliche Vorschriften, Bestimmungen eines anwendbaren Tarifvertrages oder einer Betriebsvereinbarung entgegenstehen. Soweit die Vertragsbedingungen wesentlich sind, richtet sich ihr Nachweis nach den Bestimmungen des Nachweisgesetzes.***
>
> § 105 Gewerbeordnung

Für die Überlegungen zum Datenschutz am Arbeitsplatz ist es wichtig festzustellen, was alles rechtmäßig in Arbeitsverträgen formuliert werden kann. Denn alles, wozu sich der Beschäftigte im Arbeitsvertrag verpflichtet, kann anschließend auch kontrolliert werden.

Beim Direktionsrecht des Arbeitgebers sind die Gestaltungsspielräume wesentlich geringer, als vielfach angenommen. Bei der Gestaltung des Arbeitsvertrages gilt ähnliches. Auch wenn § 105 die Überschrift trägt „Freie Gestaltung des Arbeitsvertrages“, gibt es doch enge Beschränkungen. Grundsätzlich können zwischen Arbeitgeber und Arbeitnehmer nur Konditionen festgehalten werden, die nicht bereits in Gesetzen, in Tarifverträgen oder Betriebs- bzw. Dienstvereinbarungen geregelt sind. Gibt es z. B. eine Betriebsvereinbarung zur Gleitzeit, dann gilt die automatisch auch für alle, die neu eingestellt

wurden, ohne Ausnahme. Gibt es einen Tarif, der für bestimmte Tätigkeiten ein bestimmtes Entgelt festlegt, kann der Arbeitgeber als Tarifpartner in einem Arbeitsvertrag nicht nach unten ausweichen.

Vieles ist also im Voraus festgelegt und nicht frei gestaltbar.

Hinweis:

Beschäftigte, die sich nicht sicher sind, ob ihre Arbeitsverträge nicht doch unzulässige Klauseln enthalten, können sich an ihre Betriebs- und Personalräte wenden und sie auffordern das zu überprüfen.

Sozialversicherungspflichtig Beschäftigte saarländische Arbeitnehmerinnen und Arbeitnehmer können sich kostenlos (und auch anonym) an die Rechtsberatung der Arbeitskammer des Saarlandes wenden.

Der Arbeitsvertrag beschreibt die Hauptpflichten von Arbeitnehmer und Arbeitgeber im Gegenseitigkeitsverhältnis.

Hauptpflichten des Beschäftigten:

- Die Leistungsfähigkeit muss ausgeschöpft werden - aber nach mittlerer Art und Güte.
- Die Leistung muss persönlich erbracht werden.
- Die Art der Leistung ist festgelegt (durch Berufsbezeichung und/oder Stellenbeschreibung).
- Die Leistungserbringung kann hinsichtlich Ort und Zeit festgelegt sein. Pflicht zur Pünktlichkeit und Zuverlässigkeit.
- Neben den Hauptpflichten gibt es eine Reihe von Nebenpflichten, die grundsätzlich bestehen, ohne dass sie im Arbeitsvertrag explizit aufgeführt sind.

Nebenpflichten des Beschäftigten:

- Treuepflicht: keine ruf- oder kreditschädigenden Äußerungen
- Verschwiegenheitspflicht: Wahrung von Betriebs-/Dienstgeheimnissen

- Aufklärungspflicht: Verpflichtung zur Mitwirkung
- Loyalitätspflicht: Ehrlichkeit und keine Annahme von Schmiergeldern
- Sorgfaltspflicht: Pfleglicher Umgang mit Betriebsmitteln, Abwehr von Schäden
- Achtung der Persönlichkeitsrechte: kein Mobbing, sexuelle Belästigung etc.
- …

Kontrolle arbeitsvertraglicher Pflichten - Rechtfertigung für Totalüberwachung?

Alle genannten Pflichten hat der Beschäftigte zu erfüllen; sie können mit Bezug auf den Arbeitsvertrag als Rechtsgrundlage kontrolliert werden. Wenn man alles rigoros kontrollieren würde, hätte man eine permanente, umfassende und unausweichliche Überwachung der Beschäftigten am Arbeitsplatz. Ist das legal?

Das ist unzulässig, denn es gibt ja Gesetze und andere Rechtsvorschriften, die dem Arbeitsvertrag vorgeschaltet sind, zum Beispiel die allgemeinen Persönlichkeitsrechte des Beschäftigten. Diese stehen den Kontrollrechten des Arbeitgebers gegenüber.

Diese bereits im Grundgesetz verbürgten Grundrechte, können durch „schwächeres“ Recht wie einen Arbeitsvertrag nicht ausgehebelt werden. Eine Kontrolle der Ehrlichkeit des Beschäftigten auf der Grundlage eines Arbeitsvertrages kann nicht so weit gehen, dass man den Schutz des gesprochenen Wortes missachtet und seine Telefongespräche mithört. Arbeitsvertragliche Pflichten können kontrolliert werden, aber nur in engen Grenzen.

Die Grenzen der Kontrollmöglichkeiten

Das Arbeitsverhältnis basiert auf einer vertrauensvollen Zusammenarbeit und auf einem Verhalten nach Recht und Billigkeit.

Unter Beachtung aller geltenden Gesetze, Tarifverträgen und Betriebsvereinbarungen, kann der Arbeitgeber mit Bezug auf Arbeitsvertrag und Weisungsrecht, also ohne explizites Einverständnis des Mitarbeiters, lediglich die Anwesenheit kontrol-

lieren und Tätigkeitsnachweise in Papierform verlangen. Aber der Beschäftigte ist dem Arbeitgeber immer zur wahrheitsgemäßen Auskunft verpflichtet - was die Erfüllung seiner arbeitsvertraglichen Pflichten betrifft.

Will der Arbeitgeber personenbezogene Daten von Beschäftigten erheben, um Leistungskontrollen vorzunehmen, das Verhalten im Betrieb kontrollieren, Maßnahmen zur Personalplanung oder -beurteilung durchzuführen, kommen die Datenschutzgesetze zur Geltung. Wie bereits erwähnt gelten auch am Arbeitsplatz die Grundsätze der Datenerhebung. In den Geltungsbereichen von BDSG, SDSG und DSG-EKD gibt es weitere Regelungen, die nur für die Erhebung und Verarbeitung von Daten im Beschäftigungsverhältnis zur Anwendung kommen.

> ***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.***
>
> § 32 Bundesdatenschutzgesetz

> ***Daten von Bewerberinnen oder Bewerbern und Beschäftigten dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.***
>
> § 31 SDSG
>
> ***Die kirchlichen Stellen dürfen Daten ihrer Beschäftigten, Bewerber und Bewerberinnen nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung,***

Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

§ 24 DSG-EKD

Das Problem der Erforderlichkeit

In diesen Paragraphen liegt die Ursache aber auch die Lösung von vielen Datenschutzproblemen am Arbeitsplatz begründet.

Vereinfacht sagen diese Regelungen aus, dass der Arbeitgeber personenbezogene Daten von Beschäftigten erheben und verarbeiten kann, wenn es für Einstellungen, für die Durchführung von Beschäftigungsverhältnissen oder deren Beendigung erforderlich ist. Aber was ist erforderlich? Da gehen Arbeitgeber- und Arbeitnehmermeinung üblicherweise weit auseinander. Der Arbeitgeber hält elektronische Leistungsnachweise bei der Durchführung eines Beschäftigungsverhältnisses für erforderlich, der Beschäftigte nicht. Was ist die richtige Bedeutung?

Wer sich nicht intensiv mit dem Thema Datenschutz im Arbeitsverhältnis beschäftigt hat, kann sich die Bedeutung des Begriffs „erforderlich“ in diesem Zusammenhang nicht erschließen. Das geht nicht nur den Beschäftigten so, sondern in vielen Fällen auch der verantwortlichen Stelle am Arbeitsplatz. Arbeitgeber interpretieren die Erforderlichkeit gerne zu ihren Gunsten und argumentieren „aber wir brauchen die Daten doch.“ Doch das trifft nicht die Bedeutung von „Erforderlichkeit“ im juristischen Sinn.

Der Grundsatz, dass die Nutzung personenbezogener Daten verboten ist, besteht auch im Arbeitsverhältnis. § 32 BDSG, § 31 SDSG und § 24 DSG-EKD stellen einen sogenannten Ausnahmetatbestand dar und räumen ein, dass dennoch Beschäftigtendaten - auch gegen den Willen des Betroffenen - erhoben und verarbeitet werden dürfen, wenn die Erforderlichkeit gegeben ist. Das macht sich jedoch an den folgenden Kriterien fest.

Erforderlichkeit ist gegeben, wenn:

1. *der Zweck, wofür die Daten erhoben werden sollen, rechtmäßig ist (ein aus einer Rechtsvorschrift abgeleitetes objektives berechtigtes Interesse des Arbeitgebers),*
2. *es nach objektiver Prüfung keine alternative Maßnahme gibt, um das angestrebte Ziel zu erreichen,*
3. *eine Datenvermeidung nicht zu dem legitimen Ziel führt,*
4. *eine Anonymisierung und Pseudonymisierung nicht zum Ziel führen,*
5. *wenn alternative Maßnahmen prinzipiell zwar möglich, in der Praxis aber unzumutbar sind und*
6. *die Verhältnismäßigkeit zwischen den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Belangen der Beschäftigten gewahrt ist.*

Wenn alle Kriterien überprüft wurden und zutreffen ist eine Erhebung und Verarbeitung von Beschäftigtendaten als erforderlich anzusehen und darf ggf. auch ohne Einverständnis des Betroffenen für die festgelegten Zwecke erfolgen.

Eine Erforderlichkeit ist hingegen nicht gegeben, wenn

1. *der Anlass der Datenerhebung nicht aus einer Rechtsvorschrift ableitbar ist, sondern aus wirtschaftlichen oder organisatorischen Gründen, und*
2. *es alternative Möglichkeiten gibt, das angestrebte Ziel ohne personenbezogene Daten zu erreichen.*

Erforderlich ist nicht mit nützlich, praktisch, hilfreich oder sinnvoll gleichzusetzen. Und die Erforderlichkeit muss das Ergebnis einer objektiven Prüfung und nicht einer subjektiven Einschätzung sein. Erforderlich ist das, was nach Prüfung aller Vorgaben notwendig ist, um einen vom Datenschutz legitimierten Zweck zu verfolgen. Die Grenze ist sehr eng zu ziehen.

In der Praxis lassen die §§ 32 BDSG, 31 SDSG und 24 DSG-EKD kaum mehr zu, als die grundlegenden Verwaltungs- und Organisationsaufgaben, ohne die ein Betrieb oder eine Dienststelle nicht funktionieren kann. Der Arbeitgeber kann Dienst-

und Schichtpläne erstellen, die Personalverwaltung durchführen und Personalakten führen, ohne dass die Beschäftigten gefragt werden oder einverstanden sind. Die Grenze ist allerdings schon bei der Personalakte schnell erreicht. Sogenannte qualifizierte Personalakten, die auch außerberufliche Qualifikationen ausweisen oder eigene Datenbanken zur Qualifizierungsplanung der Beschäftigten, sind durch diese Paragraphen nicht mehr gedeckt, auch keine elektronischen Tätigkeitsnachweise oder personenbezogene Controllingverfahren. Das heißt jedoch nicht, dass solche Verfahren unzulässig sind, sondern nur dass sie nicht ungefragt über die Köpfe der Betroffenen hinweg eingeleitet und durchgeführt werden dürfen.

Hinweis:

Im Geltungsbereich des BDSG wurde die Erhebung und Verarbeitung von Beschäftigtendaten lange Zeit auf der weniger strengen Vorgabe von § 28 „Datenerhebung und -speicherung für interne Geschäftszwecke“ begründet.

Das wurde nach den großen Datenschutzskandalen geändert. Am 01.09.2009 trat im Arbeitsverhältnis § 32 BDSG an diese Stelle, um die Beschäftigten durch eine enge Zweckbindung zu schützen. Dies machte der Innenausschuss des Deutschen Bundestages in der Drucksache 16/13657 deutlich.

§ 28 BDSG gilt im Beschäftigungsverhältnis nur noch als absoluter Ausnahmetatbestand, wenn Beschäftigtendaten für einen über das Beschäftigungsverhältnis hinausgehenden Zweck verwendet werden sollen z. B. für angegliederte Sozialwerke und -einrichtungen.

Keine Vorratsdatenspeicherung von Beschäftigten - Keine Rasterfahndung im Betrieb

In den Jahren 2002 und 2003 hat die Deutsche Bahn die Konten von 180.000 Mitarbeitern überprüft, um mögliche Korruptionsfälle aufzudecken. Die Kontendaten wurden der Deutschen Bahn von den

Beschäftigten mitgeteilt, um Löhne und Gehälter auszahlen zu können, nicht für anlassunabhängige Korruptionsuntersuchungen. Dieser Skandal hat erstmals in der Geschichte der Bundesrepublik dazu geführt, dass ein Vorstandsvorsitzender wegen Datenschutzverstößen seinen Stuhl räumen musste.

§ 32 BDSG geht auch auf den Umstand der Erhebung von Beschäftigtendaten zum Zwecke der Aufdeckung von Straftaten ein. Darin wird klargestellt, dass dies nur dann zulässig ist, „wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat.“ Wichtig ist der Hinweis, dass es sich um tatsächliche Hinweise handeln muss (die nachzuweisen sind). Eine Behauptung, eine Vermutung oder ein vager Verdacht sind kein rechtmäßiger Grund. Manipulierte Buchungen, Inventurbestände, Diebstähle, also Vorfälle, die objektiv darstellbar sind, sind ein rechtmäßiger Grund diesen Vorfällen auch mit Hilfe von Beschäftigtendaten nachzugehen, die für einen anderen Zweck erhoben wurden.

Aber auch hier ist es nicht zulässig, nach einer Straftat alle Beschäftigten unter Generalverdacht zu stellen. Die Persönlichkeitsrechte unbescholtener Bürger gelten auch im Beschäftigungsverhältnis. Die Verhältnismäßigkeit der Untersuchung ist zu wahren.

Die Vorratsdatenspeicherung zur Abwehr terroristischer Gefahren wurde vom Bundesverfassungsgericht für ungültig erklärt, weil sie nicht in Einklang mit geltendem Recht steht. Eine anlass- und verdachtsunabhängige Speicherung von Beschäftigtendaten durch den Arbeitgeber oder von ihm beauftragte Dienstleister ist absolut unzulässig.

Verdecktes Erheben von Beschäftigtendaten ist verboten

Auf der Grundlage von Arbeitsverträgen, dem Weisungsrecht und den Regelungen der Datenschutzgesetze können Beschäftigtendaten für erforderliche Zwecke auch ohne Einverständnis des Beschäftigten erhoben werden. Wenn kein Einverständnis erforderlich ist, heißt das jedoch nicht, dass die Datenerhebung und -erfassung

verdeckt, also ohne Kenntnisnahme des Beschäftigten erfolgen darf.

Es gilt auch hier das Transparenzgebot. Daten sind beim Betroffenen zu erheben. Ist das nicht möglich oder unverhältnismäßig, ist der Betroffene grundsätzlich vor der ersten Datenerhebung zu benachrichtigen. Die Benachrichtigung des Betroffenen wird geregelt in § 33 BDSG, § 12 SDSG, § 15a DSG-EKD, § 13a KDO. Davon kann nur in den dort beschriebenen Ausnahmefällen abgesehen werden. Zum Beispiel dann, wenn die Benachrichtigung einen unverhältnismäßigen Aufwand darstellt. Dieses Argument ist durch die Vielfalt betrieblicher Kommunikationsmittel inzwischen hinfällig. Selbst dort, wo es nicht möglich ist, sämtliche Betroffene per E-Mail zu benachrichtigen, ist es problemlos möglich solche Informationen - ob für einzelne oder alle Beschäftigten - mit der monatlichen Entgeltabrechnung auszuhändigen.

Keine verdeckte Kontrollen an PCs, IT-Systemen und Smartphones

Da die Art der Datenverarbeitung - digital oder Papier - keine Rolle für die Anwendbarkeit der Datenschutzgesetze spielt, versteht es sich von selbst, dass die Benachrichtigungspflicht und das Transparenzgebot auch auf technische Einrichtungen wie Netzwerke, PCs, Smartphones und andere IT-Systeme anzuwenden sind.

Allerdings gibt es eine inzwischen fast vergessene übergeordnete Rechtsnorm, die dies für alle Bildschirmarbeitsplätze in der Bundesrepublik regelt, ganz gleich welches Datenschutzgesetz gilt: Die Bildschirmarbeitsplatzverordnung (BildschArbV).

> ***Ohne Wissen der Benutzer darf keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden.***
>
> BildschArbV Anhang Nr. 22

Hinweis:

> ***Die Bildschirmarbeitsplatzverordnung hat einen bestimmten technischen Geltungsbereich. Für Kassen und Steuerungseinrichtungen von Maschinen gilt sie nicht. Sie gilt auch nicht für mobile Systeme, „sofern sie***

nicht regelmäßig am Arbeitsplatz eingesetzt werden“ (BildschArbV § 1 Nr. 4).

Regelmäßig ist allerdings nicht permanent. Bei Notebooks, Tablets, Blackberrys oder Smartphones, die vom Arbeitgeber für berufliche Zwecke zur Verfügung gestellt werden, muss man von einer regelmäßigen Nutzung ausgehen. Somit greift die Bildschirmarbeitsplatzverordnung und damit auch das Verbot der heimlichen Datenerhebung bzw. Überwachung durch den Arbeitgeber.

Datenerhebung auf der Grundlage von Betriebs- und Dienstvereinbarungen

Betriebsräten, Personalräten und Mitarbeitervertretungen ist es aufgrund ihrer Rechtsstellung möglich, als gewählte Interessenvertretungen der Beschäftigten Verträge mit dem Arbeitgeber zu bestimmten Themen abzuschließen. Personalräte und Mitarbeitervertretungen können Dienstvereinbarungen abschließen, Betriebsräte können Betriebsvereinbarungen abschließen.

Diese Vereinbarungen sind nicht einfach nur Schriftstücke, die etwas dokumentieren, sie sind vielmehr Rechtsnormen, ähnlich wie Gesetze. Allerdings gelten sie nur für die Betriebsstätte. Der Arbeitgeber ist verpflichtet sie umzusetzen und alle Beschäftigten sind verpflichtet sie einzuhalten - unmittelbar und zwingend.

Betriebs- und Dienstvereinbarungen können die Erhebung und Verarbeitung von Beschäftigtendaten zum Thema haben. Das ist weit verbreitet, wenn es um Verfahren zur elektronischen Datenverarbeitung geht.

Im Sinne des Datenschutzrechts gelten Betriebs- und Dienstvereinbarungen als „andere Rechtsvorschrift“. Auch sie können die Grundlage dafür sein, dass personenbezogene Daten von Beschäftigten ohne deren ausdrückliches Einverständnis erhoben und verarbeitet werden können. Und das hat in diesem Zusammenhang sogar Vorteile.

Große Chancen für einen praktikablen Datenschutz

Betriebsräte, Personalräte und Mitarbeitervertreter haben die gesetzliche Aufgabe, die Interessen der Beschäftigten zu

vertreten und soziale Härte am Arbeitsplatz zu verhindern. Um dies auch tatsächlich tun zu können, sind sie mit einer Reihe von Rechten ausgestattet. In der Praxis können sie Regelungen zu technischen Einrichtungen erzwingen, sie können sich kompetent von internen und externen Sachverständigen, z. B. BEST e. V., beraten lassen, sie können kontrollieren, ob getroffene Regelungen zum Datenschutz eingehalten werden und vieles mehr. Vor allem aber können sie aufgrund ihrer Rechtsstellung deutlich bessere Verhandlungsergebnisse erzielen, als einzelne Beschäftigte.

Betriebs- und Dienstvereinbarungen stehen in einem ausgewogenen Verhältnis von Geben und Nehmen zwischen den Betriebsparteien. Nicht nur die Beschäftigten profitieren von klaren, transparenten Regeln und einem verbindlichen Schutz ihrer Persönlichkeitsrechte, auch der Arbeitgeber hat klare Vorteile. Er hat Planungs- und Investitionssicherheit für seine Systeme und zudem ein geregeltes Verfahren, das einheitlich für alle Beschäftigten gilt.

Wie so oft sind allerdings auch Betriebs- und Dienstvereinbarungen Grenzen gesetzt. Vereinbarungen können nicht zu Aspekten abgeschlossen werden, die explizit in Gesetzen, Verordnungen oder Tarifverträgen geregelt (oder ausgeschlossen) sind. Eine Überwachung von Sozialräumen oder sanitären Anlagen kann zum Beispiel nicht geregelt werden.

Weiterhin gilt das Prinzip der Verhältnismäßigkeit und Zumutbarkeit. Eine Maßnahme, die im Einzelfall unzulässig ist, kann nicht legalisiert werden, indem sie durch Abschluss einer Betriebs- oder Dienstvereinbarung auf alle ausgeweitet wird.

Es ist allerdings sehr wohl möglich, das Schutzniveau anzuheben, das die Gesetze für den Beschäftigten vorsehen. Man spricht hier vom Günstigkeitsprinzip.

Dennoch: Großes Risiko mit langer Laufzeit

Betriebsvereinbarungen im Umfeld des Datenschutzes bergen jedoch auch ein erhebliches Risiko. Das BDSG ermöglicht die Datenerhebung und Verarbeitung auf der Rechtsgrundlage einer Betriebsvereinbarung. In dieser Betriebsvereinbarung

kann auch eine Datenerhebung legalisiert werden, die ohne Betriebsvereinbarung unzulässig wäre. Das hat das Bundesarbeitsgericht bestätigt. Ein Problem entsteht vor allem daraus, dass solche Vereinbarungen auch nach Kündigung bis zum Abschluss einer neuen Vereinbarung gelten. Das kann Jahre dauern oder nie erfolgen.

Hinweis:

> ***Interessenvertreter sollten Betriebs- und Dienstvereinbarungen abschließen, um den allgemeinen Datenschutz in den Gesetzen allgemeinverständlich für die Betriebsstätte zu konkretisieren und das Schutzniveau nach Möglichkeit anzuheben. Die Datenerhebung sollte auf die vorhandenen rechtlichen Grundlagen begrenzt bleiben und keine neuen Möglichkeiten geschaffen werden.***

Betriebsräte, Personalräte und Mitarbeitervertretungen erfahren mehr über diese Thematik im Kapitel „Datenschutz und Mitbestimmung“.

Einwilligung des Beschäftigten

Die letzte Möglichkeit, Beschäftigtendaten zu erheben und verarbeiten, basiert auf der Einwilligung der Betroffenen. Dieses Prinzip ist nicht ohne Grund in diesem Rahmen als letzte Möglichkeit benannt. Sie sollte weitestgehend unterbleiben.

Auch wenn es das informationelle Selbstbestimmungsrecht des Beschäftigten gibt, so ist es nur eine theoretische Frage, wie freiwillig eine Einwilligung im Rahmen einer abhängigen Beschäftigung überhaupt sein kann.

In der Praxis ist es heute nicht einmal möglich sogenannte „Freundschaftsanfragen“ von Vorgesetzten in Sozialen Netzwerken abzulehnen, ohne gegen Konventionen des menschlichen Miteinanders zu verstoßen. Bejaht man die Freundschaftsanfrage hingegen, erhält der Vorgesetzte Zutritt in die Privatsphäre, Einblick in die Sozialkontakte und Teilhabe an persönlicher Kommunikation.

In den einzelnen Datenschutzgesetzen ist dargestellt, wie eine Einwilligung zustande kommen muss, um rechtswirksam zu sein.

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.

Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4a Bundesdatenschutzgesetz

Diese Vorgaben finden sich auch nahezu wortgleich in § 4 Abs. 1b, 2 SDSG, § 3 Abs. 2 u. 4 KDO, § 3a DSG-EKD.

Große Risiken für Beschäftigte und Arbeitgeber

Für den Arbeitgeber als verantwortliche Stelle ist es notwendig, objektiv nachweisen zu können, dass eine Einwilligung durch den Beschäftigten erfolgt ist. Wenn das nicht möglich ist, gilt eine Einwilligung als nicht erteilt und die Erhebung und Verarbeitung von Daten des Beschäftigten bleibt unzulässig.

Aber auch für den Arbeitgeber ist das Prinzip der freiwilligen Einwilligung in die Datenverarbeitung sehr ungünstig. Der Aufwand, die geforderte Aufklärung zu leisten und individuelle Einwilligungen zu organisieren und zu dokumentieren steigt natürlich mit der Anzahl der betroffenen Beschäftigten. Hinzu kommt, dass dieses Verfahren dem Arbeitgeber keine Verfahrenssicherheit und Investitionsschutz für seine Datenverarbeitungssysteme bietet, da eine Einwilligung jederzeit und ohne Grund von den Beschäftigten widerrufen werden kann.

Auch der Bundestag, die Arbeitsgerichte und die Aufsichtsbehörden für den Datenschutz stehen der freiwilligen Einwilligung des Beschäftigten sehr kritisch gegenüber. In der geplanten Novelle des Bundesdatenschutzgesetzes soll die Einwilligung im Arbeitsverhältnis nahezu ausgeschlossen werden und die Aufsichtsbehörden der Länder erklären beständig im Arbeitsverhältnis gegebene Einwilligungen der Beschäftigten für unwirksam, da sie bei Datenschutzkontrollen den formalen Kriterien gerade im Hinblick auf die Folgenbelehrung nicht genügen.

Das freiwillige Einverständnis konkretisiert die informationelle Selbstbestimmung. Es ist ein hohes Gut, diese Entscheidungen frei treffen zu können. Das funktioniert auch in vielen Lebensbereichen. Die Arbeitswelt gehört allerdings nur theoretisch dazu.

Nach Möglichkeit sollte zum Vorteil aller Beteiligten im Arbeitsverhältnis auf individuelle Einwilligungen verzichtet und Betriebs- oder Dienstvereinbarungen den Vorrang gegeben werden. Dort, wo das nicht möglich ist, z. B. wenn es keine Interessenvertretung gibt, muss darauf geachtet werden, dass die Anforderungen an die Einwilligung korrekt umgesetzt werden. Das kann zum Beispiel der Fall sein, wenn es sich um die Privatnutzung betrieblicher Telefone handelt. Das Telekommunikationsgesetz (TKG), das dieses Thema regelt, sieht keine Möglichkeit vor, mit Betriebs- oder Dienstvereinbarungen als andere Rechtsvorschriften bestimmte Sachverhalte zu regeln.

Zweites Fazit:

- Die Erhebung von Beschäftigtendaten erfolgt grundsätzlich nach den gleichen Regeln wie in allen anderen Lebensbereichen.
- Personenbezogene Daten von Beschäftigten müssen beim Betroffenen selbst erhoben werden. Nur in Ausnahmefällen dürfen die Daten aus anderen Quellen bezogen werden.
- Die informationelle Selbstbestimmung gilt auch am Arbeitsplatz und kann nur durch Rechtsvorschriften eingeschränkt werden.
- Arbeitsverträge und das Weisungsrecht des Arbeitgebers sind Rechtsgrundlagen, mit denen sich Beschäftigtendaten auch ohne deren Einverständnis erheben und verarbeiten lassen, allerdings nur zur Anwesenheitskontrolle und handschriftlichen Tätigkeitsnachweise.
- Auch auf der Grundlage von § 32 BDSG, §31 SDSG und § 24 DSG-EKD kann der Arbeitgeber Beschäftigtendaten ohne Einverständnis der Beschäftigten erheben und verarbeiten, allerdings nur in den engen Grenzen, in denen es im juristischen Sinn erforderlich ist. Das trifft jedoch nur für die grundlegenden Verwaltungs- und Organisationsaufgaben zu. Das schließt Personalplanung und Personaleinsatzplanung mit ein.
- Auch wenn kein Einverständnis des Beschäftigten notwendig ist, besteht die Pflicht, ihn über die Datenerhebung zu informieren. Das kann nur in geregelten Ausnahmefällen unterbleiben; selbst dann ist dem Beschäftigten Auskunft zu gewähren.
- Eine anlass- und verdachtsunabhängige Speicherung und Nutzung von Beschäftigtendaten zur Aufdeckung von Straftaten ist unzulässig. Die Nutzung von Beschäftigtendaten zur Aufklärung von Straftaten ist nur nach einem objektiv nachweisbaren Vorfall und in begründbaren Einzelfällen möglich.

- Die verdeckte Erhebung ohne Kenntnisnahme des Betroffenen ist unzulässig, speziell wenn dies durch technische Systeme mit Bildschirmen erfolgt.

Nüchtern betrachtet, wird das informationelle Selbstbestimmungsrecht bei allen grundlegenden und notwendigen Verwaltungsaufgaben am Arbeitsplatz eingeschränkt, die rechtlich erforderlich sind.

Überwachung und Kontrolle, elektronische Leistungserfassung, Workflowsysteme, Qualitätsmanagement und Controlling über die Personalabrechnung und Schichtplanung hinaus und die Protokollierung in Computersystemen sind weit verbreitet, organisatorisch sinnvoll, wirtschaftlich oft rentabel. Aber rechtlich sind sie sehr selten erforderlich. In solchen Verfahren personenbezogene Daten von Beschäftigten zu erfassen und zu verarbeiten ist nur über das persönliche Einverständnis oder Betriebs- und Dienstvereinbarungen möglich.

Alle anderen Arten der Erhebung und Verarbeitung personenbezogener Daten im Arbeitsverhältnis bedürfen einer Betriebs- bzw. Dienstvereinbarung oder, falls das nicht möglich ist, der schriftlichen Einwilligung des Beschäftigten. Und das ist praktisch nur in wenigen Fällen möglich, da die Freiwilligkeit glaubhaft dargestellt werden muss. Ein einseitiges Entgegenkommen des Arbeitnehmers belegt dies nicht.

Verarbeiten personenbezogener Daten im Beschäftigtenverhältnis

Bisher wurde dargestellt, welche Daten von Beschäftigten erhoben werden können und welche Rahmenbedingungen gelten. Jetzt geht es darum, wie die eigentliche Datenverarbeitung stattfinden muss, zu welchen Zwecken Daten verarbeitet werden dürfen oder nicht, wie die Daten vor unbefugtem Zugriff geschützt werden und was anschließend mit ihnen passiert.

Ein ganz wesentliches Element beim Beschäftigtendatenschutz ist die Zweckbindung. Es wurde gezeigt, welche Daten auch ohne Einverständnis durch den Arbeitgeber erhoben werden dürfen. Das sind z. T. sehr persönliche Angaben über den Sozialstatus bis hin zu Lohnpfändungen. Deshalb ist es wichtig, zu erfahren, wofür diese Angaben verwendet werden dürfen oder im Umkehrschluss wofür nicht.

Zweckbindung gilt auch am Arbeitsplatz

Der Datenschutz basiert auf dem Gedanken, dass personenbezogene Daten nur zweckgebunden verwendet werden dürfen. Im Volkszählungsurteil von 1983 wurde festgestellt, dass es verboten ist „Daten auf Vorrat zu unbestimmten Zwecken“ zu erheben. Das gilt natürlich auch am Arbeitsplatz.

Ist es also zulässig, eine Liste aller Beschäftigten mit Lohnpfändung zu machen, da von ihnen aufgrund der materiellen Engpässe ein höheres Betrugs-, Diebstahl- und Korruptionsrisiko ausgeht? Es ist schließlich ein berechtigtes Interesse des Arbeitgebers sein Eigentum zu schützen.

Kaum ein Arbeitgeber kommt auf solche Ideen. Sie wären auch unzulässig. Das liegt in diesem Fall nicht darin begründet, dass zwischen den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Belangen des Arbeitnehmers eine Rechtsgüterabwägung stattfinden muss, sondern an der unausweichlichen Zweckbindung.

Der Arbeitgeber hat die Angabe über die Lohnpfändung erhalten, da er gesetzlich verpflichtet ist, dieser Pfändung Folge zu leisten. Er muss einen bestimmten Teil des Entgelts auf ein anderes Konto über-

weisen. Die Information dient ausschließlich diesem in § 840 Zivilprozessordnung (ZPO) beschriebenen Zweck und darf folglich für nichts anderes verwendet werden.

Der Zweck der Datenverwendung muss bereits beim Erheben bekannt sein

Die Zweckbindung gilt für die Verwendung aller personenbeziehbaren Daten von Beschäftigten. Bereits vor dem Erheben der Daten muss der Zweck verbindlich beschrieben sein. Das ist allein schon deshalb notwendig, um festzustellen, ob es überhaupt rechtmäßig ist, die Daten zu verwenden. Fortan ist die Verwendung der personenbezogenen Daten an diesen Verwendungszweck gebunden. Ein nachträgliches Umwidmen des Verwendungszwecks ist nicht zulässig, auch wenn das oft praktisch wäre.

Eine andere Nutzung, als zu dem festgelegten Zweck, ist unzulässig

Der naheliegende Gedanke derjenigen, die Daten verarbeiten, ist, sich keine doppelte Arbeit zu machen. Beschäftigtendaten, die man einmal zum Beispiel für die Personalverwaltung erhoben hat, kann man ja auch für andere Zwecke verwenden. Alles andere wäre doch unpraktisch.

Das ist richtig. Dennoch ist eine Nutzung zu anderen Zwecken im Regelfall unzulässig, und es gibt einen guten Grund dafür. Würde man eine freie Verwendung der Daten zulassen, könnte der Betroffene natürlich nicht mehr nachvollziehen und auch nicht entscheiden, was mit seinen Daten passiert. Diese Einschränkung der informationellen Selbstbestimmung ist deshalb nur in Ausnahmefällen zulässig. Zum Beispiel dann, wenn dies - im Wortlaut der Gesetze - einen „unverhältnismäßigen“ Aufwand darstellen würde. Was in diesem Zusammenhang auch oft vergessen wird, ist die Vorgabe der Datenschutzgesetze, dass personenbezogene Daten beim Betroffenen zu erheben sind.

Ausnahmen sind möglich - im Rahmen nachweisbarer Erforderlichkeit

Allerdings wurde bereits dargestellt, dass die Daten von Beschäftigten auf der Rechtsgrundlage von Arbeitsvertrag, Weisungsrecht und § 32 BDSG, 31 SDSG und 24 DSG-EKD zu erforderlichen Zwecken auch ohne Einverständnis erhoben wer-

den können. In diesen Fällen liegt eine rechtmäßige Zweckbindung vor, die sich anhand der Kriterien zur „Erforderlichkeit“ auch überprüfen und nachweisen lässt. Eine Datenverwendung ist zu allen erforderlichen Zwecken zulässig, ohne dass die Daten erneut erhoben werden müssen.

Hinweis:

> ***Die Aussage, bestimmte Daten seien erforderlich, ist eine Behauptung.***
>
> ***Der objektive Nachweis der Erforderlichkeit ist eine rechtmäßige Begründung.***

Wie dürfen die Daten von Beschäftigten verarbeitet werden?

Bei personenbezogenen Daten von Beschäftigten handelt es sich um Daten, die mit einer besonderen Sorgfalt verarbeitet werden müssen. Es kann also nicht sein, dass die Daten unbefugt genutzt werden. Aber was ist eine unbefugte Nutzung und wer ist überhaupt befugt, mit den Daten zu arbeiten?

Wer darf mit meinen Daten arbeiten?

Je kleiner die Betriebsstätte ist, desto einfacher ist die Frage zu beantworten. In einem Handwerksbetrieb mit einer Geschäftsführerin, einem Verwaltungsangestellten und sieben Monteuren muss man nicht viel spekulieren. Die Geschäftsführerin ist letztlich die verantwortliche Stelle, der Verwaltungsangestellte ist ihr Beauftragter, der die Personalangelegenheiten regelt. Zur Wahrnehmung dieser Aufgaben ist es sowohl im juristischen als auch im praktischen Sinn erforderlich, dass er mit den Daten der Monteure arbeitet.

Anders sieht es schon aus, wenn es sich um einen Betrieb mit der gleichen Verwaltungsstruktur handelt, aber fünfzig Mitarbeiter in vier Abteilungen arbeiten. Dürfen die Abteilungsleiter jetzt auch die Beschäftigtendaten einsehen oder nicht? Und falls ja, haben sie Zugriff auf alle Daten? Konkrete Regelungen, wer Beschäftigtendaten erheben und nutzen darf, sucht man in den Datenschutzgesetzen vergebens.

Die Meinungen darüber, wer auf solche Daten zugreifen darf, orientiert sich üblicherweise an den Hierarchien in der Betriebsstätte: Als Beschäftigter darf man

bestenfalls die eigenen Daten einsehen, der Chef darf alle Daten von allen einsehen. Doch so funktioniert der Datenschutz nicht.

Die Berechtigung, Daten von Beschäftigten zu erheben und zu nutzen, ergibt sich beim Datenschutz ausschließlich aus der Zweckbindung der Daten. Kriterien der Betriebsorganisation und Hierarchien spielen keine Rolle; Ein Zugriffsrecht ergibt sich nicht aus der Tatsache, dass jemand Vorgesetzter ist.

Es muss individuell geklärt werden, ob es im juristischen Sinn erforderlich ist, dass er für die Erfüllung eines rechtmäßigen Zwecks Zugriff auf personenbezogene Daten von Beschäftigten haben muss.

Beispiel:

Darf ein Abteilungsleiter die Personalakte eines ihm zugeordneten Mitarbeiters einsehen?

Personalakten sind Sammlungen von Angaben zu einzelnen Beschäftigten, die als Nachweise gesetzlich erforderlich sind. Personalakten können darüber hinaus auch freiwillige Angaben des Beschäftigten enthalten. Alle Dokumente und Nachweise sind zweifellos personenbezogen und wurden für einen jeweils eigenen Zweck erhoben. Krankmeldungen dienen zum Beispiel zur Umsetzung des Entgeltfortzahlungsgesetzes und des betrieblichen Eingliederungsmanagements. Qualifizierungsnachweise sind hingegen erforderlich bei der Ausübung vieler Tätigkeiten vom Bedienen einer Kettensäge bis zur Personenbeförderung in Bussen.

Da es sich um personenbezogene Daten des Beschäftigten handelt, ist es für niemanden zulässig, die Personalakte aus reinem Interesse einzusehen. Es muss einen rechtmäßigen Grund geben, der eine Einsicht erforderlich macht. Der Abteilungsleiter muss einen solchen Grund angeben. Die Person, die im Auftrag des Arbeitgebers mit der Personalaktenführung beauftragt ist, muss prüfen, ob dieser Grund rechtmäßig ist und ob dieser Aspekt überhaupt im Verantwortungsbereich des Abteilungsleiters ist.

Nicht legitim wäre in diesem Fall, Informationen über Lohnpfändung, Religionszugehörigkeit oder ähnliches einsehen zu wollen. Es wäre hingegen nachvollziehbar, wenn er sich versichert, dass ein Mitarbeiter eine notwendige arbeitsmedizinische Untersuchung - z. B. Höhentauglichkeit - erfolgreich durchgeführt hat und eingesetzt werden kann. Ihm steht hierzu nur das Ergebnis der ärztlichen Untersuchung zu (tauglich oder nicht), nicht jedoch die Diagnose.

Allerdings darf dem Abteilungsleiter auch für den letztgenannten legitimen Grund keinesfalls die Einsicht in die vollständige Personalakte gewährt werden. Er darf nur die Angaben erhalten, die zwingend für seine Aufgaben erforderlich sind.

Zugriffsrechte auf Beschäftigtendaten

Der Zugriff auf personenbezogene Daten von Beschäftigten ist zweckgebunden. Mit dieser Information stößt man aber gelegentlich an Grenzen, zum Beispiel dann, wenn diese Daten mit IT-Systemen erhoben, gespeichert und verarbeitet werden.

Ein Zugriff für Sachbearbeiter lässt sich anhand der Zweckbindung der Daten und der Tätigkeitsbeschreibungen der Personen relativ gut nachvollziehen: Wer mit der Lohnabrechnung beauftragt ist, hat einen rechtmäßigen Grund, auf diese Beschäftigtendaten zuzugreifen. Aber wie ist das mit dem Systemadministrator?

Der Systemadministrator hat die Aufgabe, das System zu warten und zu verwalten und benötigt für diese Aufgaben auch uneingeschränkte Zugriffsrechte auf das System. Es ist ihm dadurch auch möglich, sich alle erdenklichen persönlichen Daten in dem System anzusehen, vom Pförtner bis zur Vorstandsvorsitzenden. Er darf es jedoch nicht, da er nicht mit dem Erheben und Verarbeiten von personenbezogenen Daten beauftragt ist, sondern mit der Systemwartung. Technisch lässt sich dieses Dilemma nicht auflösen.

Natürlich kann die Situation entstehen, dass auch ein Systemadministrator bei der Durchführung seiner Aufgaben, zum Beispiel bei der Datenrettung, Einblick in personenbezogene Daten erhält. In solchen Fällen muss die Vertraulichkeit gewahrt werden. Er sollte solche Aufgaben nur im Beisein eines Verantwortlichen im Sinne

der Datenschutzgesetze, ggf. auch des Beauftragten für Datenschutz, ausführen. Wichtig ist in jedem Fall, den Systemadministrator mit dem Datenschutzrecht vertraut zu machen.

Systemadministration ist eine Vertrauensstellung mit hohem Missbrauchspotenzial in wirtschaftlicher wie persönlicher Hinsicht. Wer sich Zugriff auf Daten verschafft, die nicht für ihn bestimmt sind, riskiert nicht nur eine Kündigung. Es handelt sich um eine Straftat im Sinne des Strafgesetzbuchs (StGB) § 202a, die mit einer Freiheitsstrafe bis zu drei Jahren geahndet werden kann.

Prüfschema:

Zugriff auf personenbezogene Daten

Ein Zugriff auf personenbezogene Daten darf nur dann erfolgen, wenn alle Kriterien erfüllt sind.

1. **Welche Daten sollen eingesehen oder bearbeitet werden?**
2. **Was ist der rechtmäßige Zweck, für den die Daten erhoben worden sind?**
3. **Entspricht die Anfrage dem rechtmäßigen Zweck der Erhebung?**
4. **Gehört es nachweislich zu den Aufgaben der Person, die Datenzugriff haben möchte, diese Daten einzusehen oder zu bearbeiten? (Auskunft geben ggf. Organigramme und Stellenbeschreibungen)**
5. **Personenbezogene Daten müssen in der Regel beim Betroffenen erhoben werden. Ist ein Zugriff auf erhobene Daten überhaupt erforderlich, oder können die Angaben auch direkt beim Beschäftigten erfolgen?**

In diesem Zusammenhang verwenden die Datenschutzgesetze den Begriff „Dritter“.

> ***Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.***
>
> § 3 Abs. 8 BDSG
> § 3 Abs. 5 SDSG
> § 2 Abs. 9 DSG-EKD
> § 2 Abs. 9 KDO

Die Zugriffsprüfung ergibt, ob es sich bei der anfragenden Person um einen befugten oder unbefugten Dritten im Sinne der Datenschutzgesetze handelt.

Schutz vor unbefugtem Zugriff ist Pflicht

Die Datenschutzgesetze machen es zur Auflage, dass für alle Verfahren, bei denen personenbezogene Daten erhoben und verarbeitet werden, alles unternommen wird, um Missbrauch oder Schäden durch fahrlässigen Umgang zu verhindern. So verlangt das Bundesdatenschutzgesetz, dass sogenannte technische und organisatorische Maßnahmen ergriffen werden.

> ***Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.***
>
> § 9 BDSG

Entsprechende Anforderungen finden sich auch in § 11 Abs. 1 SDSG, § 9 DSG-EKD und § 6 KDO.

Konkrete Vorgaben zum Schutz von Beschäftigtendaten in IT-Systemen

Diese allgemeinen Vorgaben werden konkreter gefasst, wenn personenbezogene Daten mit IT-Systemen verarbeitet werden:

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. *Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),*
2. *zu verhindern, dass Datenverarbeitungssysteme von Unbefugten ge-*

nutzt werden können (Zugangskontrolle),

3. *zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),*

4. *zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),*

5. *zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),*

6. *zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),*

7. *zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),*

8. *zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

Anlage zu § 9 Satz 1 BDSG

Entsprechende Vorgaben finden sich auch in § 11 Abs. 2 u. 3 SDSG, in Anlage zu § 9 DSG-EKD und III. Anlage zu § 6 Verordnung zur Durchführung der KDO.

Vorabkontrolle bei Datenverarbeitung mit großen Risiken

Darüber hinaus gibt es im Geltungsbereich von BDSG in § 4d Abs. 5 und SDSG in § 11 besonders strenge Auflagen, wenn von der elektronischen Datenverarbeitung besondere Risiken für die Betroffenen ausgehen. Das ist der Fall, wenn es sich um die Verarbeitung von besonderen personenbezogenen Daten handelt, oder die Daten zur Beurteilung, zur Leistungs- oder Verhaltenskontrolle eingesetzt werden können. Dann ist vor dem Einsatz des Systems eine sogenannte Vorabkontrolle erforderlich.

Umgangssprachlich würde man davon sprechen, dass es ein Zulassungsverfahren für das EDV-System ist. Wenn es den Datenschutztest besteht, ist es zugelassen für die Verarbeitung von personenbezogenen Daten.

Diese Vorabkontrolle ist insofern sinnvoll, wie IT-Systeme und Software in der Regel von Menschen erstellt werden, die sich zwar auf Datensicherheit, nicht aber auf den Datenschutz verstehen. Viele solcher Systeme sind ohnehin auf einen internationalen Markt ausgerichtet und müssen auf die Datenschutzanforderungen des jeweiligen Landes und des Einsatzzwecks erst angepasst werden. Ob das tatsächlich erfolgt ist, muss vor dem erstmaligen Betrieb rechtsverbindlich festgestellt werden. Das ist die Aufgabe des Beauftragten für Datenschutz.

Hinweis:

> ***Über den Verlauf und das Ergebnis der Vorabkontrolle kann sich jeder Auskunft verschaffen, der als Beschäftigter von dem EDV-System betroffen ist.***
>
> ***Es ist ratsam nicht nur nach dem Ergebnis der Vorabkontrolle, sondern auch nach dem Zustandekommen des Ergebnisses (Prüfbericht) zu fragen. Das Ergebnis muss schließlich rechtmäßig und sachlich begründet sein.***

Was geschieht im Anschluss mit den Daten?

Es wurde bisher dargestellt, wie Daten erhoben werden müssen, von wem sie verarbeitet werden dürfen und wie sie geschützt werden müssen. Aber was pas-

siert, wenn die Verarbeitung abgeschlossen ist?

Selbst erfahrene Personalsachbearbeiter haben gelegentlich Schwierigkeiten, diese Frage rechtsverbindlich zu beantworten. Denn wie so oft beim Datenschutz ist das Grundprinzip recht einfach, aber nicht konkret.

Wenn Daten von Beschäftigten erhoben und verarbeitet werden, dann sind das „ihre“ Daten, die zu einem bestimmten Zweck verwendet werden. Ist der Zweck erfüllt, besteht keine Notwendigkeit mehr für den Arbeitgeber diese Daten vorzuhalten. Sie gehen zurück an „ihre“ Besitzer, sprich: Die personenbezogenen Daten müssen gelöscht werden. In der juristisch korrekten Formulierung klingt das so:

> ***Personenbezogene Daten sind zu löschen (…), sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (…).***
>
> § 35 Abs. 2 Nr. 3 BDSG

Entsprechende Regelungen finden sich auch in § 21 Abs. 3 b SDSG, § 16 Abs. 2 Nr. 2 DSG-EKD und § 14 Abs. 2 Nr. 2 KDO.

Ausnahme: Aufbewahrungsfristen aus anderen Rechtsvorschriften

Diese Regelung steht in den Datenschutzgesetzen. Diese Gesetze kommen aber erst nachrangig zum Tragen, wenn keine andere Rechtsvorschrift etwas festlegt, das von diesem Grundsatz abweicht. Wie zu vermuten, gibt es allerdings eine Reihe von Ausnahmen, die für bestimmte Zwecke Aufbewahrungsfristen formulieren. Arbeitszeitnachweise dienen dem Zweck der Lohnabrechnung. Entsprechend der Datenschutzregelungen müssten sie nach der Lohnzahlung, spätestens jedoch nach einer Reklamations- oder Widerspruchsfrist gelöscht werden, weil der Zweck erfüllt ist. Bei den Arbeitszeitnachweisen gelten jedoch die Regelungen des Arbeitszeitgesetzes (ArbZG) vorrangig. Nach § 16 ArbZG müssen die Daten zwei Jahre aufbewahrt werden. Danach sind sie allerdings zu löschen. Bei Lohn- und Abrechnungsdaten gilt nach § 28 Sozialgesetzbuch IV, dass die Daten aufbewahrt werden müssen bis zum Ablauf des auf

die letzte Prüfung folgenden Kalenderjahres. Das kann bis zu drei Jahren sein.

Hinweis:

Wichtig ist, daran zu denken, dass die Löschung der Daten rückstandslos und unwiederbringlich erfolgt:

- ***Daten in den IT-Systemen auf Servern,***
- ***lokale Speicherungen auf PCs,***
- ***Sicherungskopien auf Datenträger,***
- ***Ausdrucke,***
- ***einfach alles.***

Rechte der Beschäftigten: Auskunft, Berichtigung, Löschung, Sperrung

Ein Arbeitsverhältnis ist natürlich ein Vertrauensverhältnis. Aber auch wenn Vertrauen gut ist, ist Kontrolle nicht schlecht. Das trifft auch für den Datenschutz zu. Die Erhebung und Verarbeitung von Beschäftigtendaten basiert auf Rechtmäßigkeit und die basiert auf objektiven Kriterien. Was liegt also näher, als sich davon zu überzeugen, dass die eigenen Daten im Betrieb so verwendet werden, wie das sein soll. Aber wie geht man am geschicktesten vor?

Grundsätzlich müssen die verantwortlichen Stellen im Betrieb den Beschäftigten Auskunft gewähren. Aus der Erhebung und Nutzung von personenbezogenen Daten entsteht unweigerlich eine Auskunftsverpflichtung:

> ***Der Betroffene kann Auskunft verlangen über***
>
> 1. ***die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,***
> 2. ***Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und***
> 3. ***den Zweck der Speicherung.***

und weiter:

> ***Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.***
>
> ***Die Auskunft ist unentgeltlich.***
>
> § 34 BDSG

Die einzige Verpflichtung, die für die Beschäftigten besteht, ist folgende: *Er (der Betroffene, A.d.R.) soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen (§ 34 Abs. 1 BDSG)*.

Der Auskunftswunsch muss nicht zwangsläufig schriftlich erfolgen. Allerdings gilt

dies nur im Geltungsbereich des Bundesdatenschutzgesetzes.

Einschränkungen des Auskunftsrechts in *SDSG, DSG-EKD und KDO*

Im Geltungsbereich des Bundesdatenschutzgesetzes gibt es kaum Möglichkeiten die Auskunft zu verweigern. An Arbeitsplätzen, die in den Geltungsbereichen des SDSG, DSG-EKD und der KDO liegen, gibt es allerdings Einschränkungen der Auskunftsrechte (§ 20 SDSG, § 15 DSG-EKD und § 13 KDO).

Sofern der Betroffene die Art der Daten, die er einsehen möchte, nicht näher beschreiben kann und die Suche und Bereitstellung einen unverhältnismäßigen Aufwand darstellen würde, kann ein Auskunftsersuchen abgelehnt werden: Eine Anfrage an die Landesregierung - „Nennen Sie mir alle personenbezogenen Daten, die in der saarländischen Verwaltung von mir vorliegen.“ - kann nicht sachgerecht bearbeitet werden. Ein zielgerichteter Antrag hingegen schon: „Welche Daten von mir liegen dem Einwohnermeldeamt vor und was wird damit gemacht?“

Am Arbeitsplatz ist ein solcher zielgerichteter Antrag auf Auskunft kaum mehr mündlich zu formulieren und stellt Beschäftigte, für die das Formulieren von Anträgen nicht zu den täglichen Aufgaben gehört, vor eine große Herausforderung.

Nüchtern betrachtet offenbaren sich hier Gestaltungsspielräume der Arbeitgeber in Dienststellen und Einrichtungen, die zu Ungunsten der Beschäftigten genutzt werden können. Als Beschäftigter müsste man darstellen, dass die Begründung eines unverhältnismäßigen Aufwandes falsch ist.

Hinweis:

Betriebsräte, Personalräte und Mitarbeitervertretungen haben die Möglichkeit, ihre Kollegen darin zu unterstützen Auskunft zu erhalten.

Die Interessenvertretungen haben auch weitergehende Möglichkeiten, zu überprüfen, ob eine Ablehnung hingenommen werden muss, oder nicht.

Praktische Hindernisse

Dem Beschäftigten darf keine Benachteiligung daraus erwachsen, dass er von seinen Auskunftsrechten Gebrauch macht. Das ist allerdings nicht immer auszuschließen. Oft genug wird der Wunsch am Arbeitsplatz, Auskunft über seine Daten zu erhalten, als Misstrauensbekundung gewertet. Dieses Risiko besteht grundsätzlich, und es ist in der Praxis auch weit verbreitet. Vieles kann man allerdings in die richtigen Bahnen lenken, indem man den Wunsch auf Einsicht persönlich vorbringt und sich die Art der Datenerhebung und Nutzung auch persönlich zeigen lässt. Man sollte nicht davon absehen, die eigenen Daten einzusehen, aus Angst, einem Personalverantwortlichen oder Sachbearbeiter auf die Füße zu treten.

Keine Begründung notwendig

Der Auskunftswunsch muss auch nicht begründet sein. Jeder Beschäftigte kann sich, auch ohne konkreten Anlass, von der korrekten Verarbeitung selbst überzeugen und eine zeitnahe Auskunft verlangen. Er muss sich nicht auf einen späteren unbestimmten Zeitpunkt vertrösten lassen und er muss keine Verzögerungen hinnehmen, eine im Verhältnis angemessene Bearbeitungszeit hingegen schon.

Auskünfte müssen ohne Verzögerung erteilt werden

Konkrete Werte lassen sich hier nicht angeben, deshalb ein paar Beispiele:

Wenn sich die gewünschte Auskunft zum Beispiel aus einem Personalwirtschaftsprogramm per Knopfdruck erteilen lässt, erscheint es angemessen, nicht länger als einen Tag auf die Auskunft warten zu müssen.

Die Einsicht in die Personalakte sollte direkt möglich sein. Der Standort der Daten sollte bekannt sein und die Akte vollständig, es gibt auch keinen Grund, warum ein Personalsachbearbeiter die Akte vorher durchsehen und Bestandteile entfernen sollte. Das Einsichtsrecht des Mitarbeiters bezieht sich auf die vollständige Personalakte, wie sie vorliegt. Lediglich das Beschaffen von Teil- und Nebenakten, die an anderen Stellen gelagert und ggf. angefordert werden müssen, begründet eine Verzögerung.

Auch eine umfassende und schriftliche Auskunft über sämtliche personenbezogenen Daten eines Beschäftigten an der Betriebsstätte kann, ganz praktisch, nicht sofort erteilt werden.

Überprüfen der eigenen Daten

Anhand der erteilten Auskunft kann man seine Daten überprüfen und feststellen, ob alle Angaben korrekt sind. Natürlich kann es vorkommen, dass man feststellen muss, dass Angaben falsch sind, unzulässig oder einfach nicht mehr aktuell. Was tun? Die Datenschutzgesetze regeln (in § 35 BDSG, § 21 SDSG, § 16 DSG-EKD, § 14 KDO) die Verfahren zur Berichtigung, Löschung oder Sperrung von Daten.

Berichtigung, Löschung und Sperrung

Allen Datenschutzgesetzen ist gemeinsam, dass Daten, die offensichtlich falsch sind, berichtigt werden müssen.

Gemeinsam ist auch, dass Daten, die unzulässig sind oder nicht mehr erforderlich sind, gelöscht werden müssen. (Zur Erinnerung, es muss dargestellt werden, dass es erforderlich ist und nicht, dass es nicht erforderlich ist!)

Ersatzweise können Daten auch für den Zugriff oder eine Nutzung gesperrt werden, wenn ein Löschen aus technischen Gründen nicht möglich ist, oder die Daten zwar nicht mehr verarbeitet werden müssen, eine Löschung aber aufgrund von Aufbewahrungsfristen nicht erfolgen kann.

Gemeinsam ist allen Datenschutzgesetzen auch ein Widerspruchsrecht. Der Betroffene kann der Verarbeitung seiner Daten grundsätzlich widersprechen, außer sie erfolgt auf Grundlage einer anderen Rechtsvorschrift oder die Interessen der verantwortlichen Stellen am Arbeitsplatz überwiegen. Diese Widerspruchsmöglichkeit leitet sich direkt von den Rechtsprinzipien der Datenerhebung ab. Die Widerspruchsmöglichkeit drückt im Zusammenhang mit der Auskunft aus, dass einer Datenverwendung eine Absage erteilt werden kann, wenn nicht festgestellt werden kann, dass die Daten rechtmäßig erhoben wurden.

Daneben gibt es noch Regelungen zur Übermittlung von gesperrten Daten und darüber, dass die Stellen, an die Daten übertragen werden, auch von Korrekturen erfahren.

Was tun, wenn die Richtigkeit bestritten wird?

Eine wesentliche Regelung findet sich hingegen nur in den weltlichen Datenschutzgesetzen. In § 35 Abs. 4 BDSG und in § 21 Abs.2a SDSG wird geregelt, wie man verfährt, wenn der Beschäftigte seine Daten kontrolliert und die Richtigkeit von Angaben bestritten wird, es sich aber nicht klären lässt, was letztlich stimmt. Es steht quasi Aussage gegen Aussage. Für diesen Fall verlangen BDSG und SDSG, dass die Daten gesperrt werden.

Die Kontrolle des Datenschutzes am Arbeitsplatz

Das Auskunftsrecht der Beschäftigten ist eine Möglichkeit, die Einhaltung des Datenschutzes zu kontrollieren. Das muss aber jeder Beschäftigte für sich selbst in Angriff nehmen. Natürlich kann man sich als Beschäftigter durch den Betriebs- oder Personalrat unterstützen lassen, aber die personenbezogenen Daten eines Kollegen können nicht ohne dessen ausdrückliches Einverständnis kontrolliert werden. Das Auskunftsrecht ist eine individuelle Kontrollmöglichkeit.

Hinweis:

> ***Das SDSG ermöglicht jedermann, also auch allen Beschäftigten, nach § 9 Abs. 2 weitere Kontrollen im Hinblick auf die Verfahrensbeschreibungen und die Vorabkontrollen.***

Will man allgemein den Beschäftigtendatenschutz am Arbeitsplatz überprüfen, können das die Beauftragten für Datenschutz tun, aber auch die Betriebsräte, Personalräte und Mitarbeitervertretungen. Sofern es solche Institutionen am Arbeitsplatz gibt.

Die Aufsichtsbehörden für den Datenschutz

Als übergeordnete Instanz gibt es sowohl für die Arbeitsstätten im Geltungsbereich von BDSG und SDSG als auch für die kirchlichen Einrichtungen eigene Aufsichtsbehörden für den Datenschutz. Die Kontaktdaten finden sich im Anhang. Die Aufsichtsbehörden haben die Möglichkeit, den Datenschutz vor Ort zu kontrollieren und Auskunft zu verlangen. Sie haben

auch die Möglichkeit, bei Verstößen Sanktionen gegen den Arbeitgeber zu verhängen.

Aus Sicht der Beschäftigten sind die Aufsichtsbehörden jedoch aus anderen Gründen sehr interessant. Man kann sich als Beschäftigter - auch anonym - an die Aufsichtsbehörde wenden, wenn man Zweifel hegt, ob die vor Ort erteilten Auskünfte korrekt sind, wenn man die Umsetzung des Datenschutzes bemängelt aber auf taube Ohren stößt, oder wenn man eine kompetente Einschätzung zu einem Aspekt des Datenschutzes braucht. Dies ist ohnehin eine gute Möglichkeit zur Klärung von Sach- und Rechtsfragen rund um den Datenschutz. Es hilft zum Teil gravierende Fehler zu vermeiden.

Überblick über die Datenverarbeitung - die Pflicht Verfahrensverzeichnisse zu führen

Die Frage ist aber, wie eine Überprüfung des Datenschutzes am Arbeitsplatz ganz praktisch erfolgen kann. Personenbezogene Daten werden schließlich an allen erdenklichen Stellen erhoben, mit allen erdenklichen Systemen bearbeitet, gespeichert und übertragen. Wer kann da den Überblick haben?

Wer als verantwortliche Stelle am Arbeitsplatz personenbezogene Daten erhebt und mit EDV-Systemen verarbeitet, muss diese Prozesse in Verfahrensverzeichnissen oder Verarbeitungsübersichten dokumentieren und unter Umständen auch bei der jeweiligen Aufsichtsbehörde anmelden.

Verfahrensverzeichnisse beschreiben den vollständigen Prozess von der Datenerhebung über die Verarbeitung bis hin zur Löschung. Sie geben unter anderem Auskunft darüber,

- welche Daten werden erhoben (detaillierte Auflistung aller Datenfelder, keine Pauschalangabe wie z. B. Personaldaten,
- wer sind die Betroffenen,
- auf welcher Rechtsgrundlage werden Daten erhoben und welche Zweckbindung haben die Daten,
- mit welchem EDV-System werden die Daten erhoben und verarbeitet,

- wer ist für die Datenverarbeitung verantwortlich, wer ist zugriffsberechtigt,
- wo werden die Daten gespeichert,
- wann werden die Daten gelöscht,
- werden Daten (an Dritte, in Drittstaaten) übermittelt,
- welche Maßnahmen wurden zum Datenschutz unternommen,
- …

Die Mindestanforderungen an Verfahrensverzeichnisse ergeben sich aus der Meldepflicht. Konkrete Angaben finden sich in den jeweiligen Datenschutzgesetzen in § 4e BDSG, § 9 Abs. 1 SDSG, § 14 Abs. 2 DSG-EKD und VII. zu § 17 Abs. 3 Satz 3 KDO Verordnung zur Durchführung der KDO.

Inzwischen werden Beschäftigtendaten in der Regel mit Computersystemen verarbeitet. Die Papierform ist die Ausnahme und wird in Zukunft durch elektronische Nachweissysteme und die elektronische Personalakte immer weiter an Bedeutung verlieren. Wo welche Daten hinterlegt, verarbeitet und gespeichert wird, ist oft nicht einmal für die Bediener ersichtlich.

Nur über Verfahrensverzeichnisse lassen sich also Fragen zur elektronischen Verarbeitung von Beschäftigtendaten klären und den Betroffenen Auskunft erteilen. Sie verschaffen den nötigen Überblick und die geforderte Transparenz. Ihre Bedeutsamkeit steigt, und kein Unternehmen, keine Dienststelle oder Einrichtung sollte sich leichtfertig darüber hinweg setzen und keine Verfahrensverzeichnisse anlegen. Auskunftsersuche können nicht nur von Beschäftigten, sondern von allen Betroffenen also auch von Kunden, Patienten, Mandanten usw. erfolgen.

Hinweis:

In vielen Betrieben ist es unbekannt, dass Verfahrensverzeichnisse auch dann erstellt werden müssen, wenn kein Beauftragter für Datenschutz bestellt ist, weil der Betrieb zu klein ist.

In § 4g Abs. 2a BDSG wird dem Arbeitgeber auferlegt, in diesen Fällen den Datenschutz „in anderer Weise sicherzustellen“. Der Arbeitgeber muss dann eine

andere Person beauftragen, Verfahrensverzeichnisse zu führen. Die Verfahrensverzeichnisse müssen in jedem Fall geführt werden.

Meldepflicht und schriftliche Freigabe für saarländische Behörden und Kommunalverwaltungen

Im Saarländischen Datenschutzgesetz sind die Regelungen zum Umgang mit personenbezogenen Daten sehr stringent geregelt. Bevor elektronische Verfahren, in denen personenbezogene Daten verarbeitet werden, zum Einsatz kommen dürfen, muss die Landesbeauftragte für Datenschutz in dieser Angelegenheit gehört werden. Das kann natürlich nur erfolgen, wenn sie von der Datenverarbeitung erfährt.

Jede Dienststelle oder kommunale Einrichtung, die unter den Geltungsbereich des Saarländischen Datenschutzgesetzes fällt, muss diese Verfahren nach den Vorgaben einer Verfahrensbeschreibung melden. Erst nachdem die Begutachtung durch die Landesbeauftragte für Datenschutz erfolgt ist, darf ein solches Verfahren betrieben werden. Das schließt eine Vorabkontrolle des Systems mit ein.

Hinweis:

Das SDSG macht keine Unterschiede zwischen einzelnen automatisierten Verfahren und fordert generell die Einhaltung der geschilderten Prüfverfahren. Rechtlich ist es egal, ob es sich um eine Excel-Tabelle mit personenbezogenen Daten zur Urlaubsplanung handelt, um den Betrieb von Überwachungskameras oder um die komplexen IT-Systeme der Finanzbehörden.

Einfach ausgedrückt: In allen Fällen, in denen Beschäftigtendaten mit Computer verarbeitet werden, muss die Beauftragte für Datenschutz im Vorfeld informiert werden!

Diese Vorgabe aus § 7 Abs. 2 SDSG sollte von allen Verantwortlichen als Appell verstanden werden, das Verarbeiten von personenbezogenen Daten auf ein Mindestmaß zu beschränken und im Vorfeld die Zulässigkeit

zu klären. Das erspart den Verantwortlichen unangenehme Zurechtweisungen, es erspart den Beschäftigten unzulässige und unnötige Kontrollen und es erspart der Aufsichtsbehörde diese Versäumnisse ahnden zu müssen.

Drittes Fazit:

- Die Datenschutzgesetze machen eine Reihe von Vorgaben, die eingehalten werden müssen, wenn Beschäftigtendaten verarbeitet werden.
- Auch bei der Verarbeitung und Nutzung unterliegen die personenbezogenen Daten von Beschäftigten der Zweckbindung. Sie für andere Zwecke zu verwenden, als zu denen, für die sie erhoben wurden, ist verboten.
- Der Zugriff auf Beschäftigtendaten orientiert sich nicht an Hierarchien, sondern an der Zweckbindung der Daten. Zugriff erhält ausschließlich der, der nachweislich mit der Erfüllung des Zwecks beschäftigt ist, für den die Daten erhoben wurden. Ob er ein Vorgesetzter ist oder nicht, ist ohne Belang.
- Neben dem Zugriffsrecht verpflichten die Datenschutzgesetze dazu, weitere Maßnahmen zum Schutz der Daten vorzunehmen. So müssen Beschäftigtendaten u. a. auch technisch vor Manipulationen, einer unzulässigen Weitergabe und Verlust geschützt werden.
- Wenn Beschäftigtendaten mit Computer verarbeitet werden, muss ein Verfahrensverzeichnis angelegt werden, das verbindlich über den gesamten Datenverarbeitungsprozess Auskunft gibt, einschließlich Datenfelder, Verantwortlichkeiten, Speicherorte, Löschfristen usw. Verfahrensverzeichnisse müssen auch dann erstellt werden, wenn es keinen Beauftragten für Datenschutz gibt. Die Verfahrensverzeichnisse sind erforderlich für die Wahrung der Auskunftsrechte.
- Werden besondere Arten von personenbezogenen Daten (Gesundheit/Krankheit, Religion, Parteizugehörigkeit, Gewerkschaftszugehörigkeit..) mit Computer verarbeitet, muss eine Vorabkontrolle stattfinden, die verbindlich feststellt, ob das System zulässig ist.
- Für alle öffentlichen Einrichtungen und Kommunen des Saarlandes

gilt: Bei allen Verfahren, in denen personenbezogene Daten mit Computer verarbeitet werden, muss die Landesbeauftragte für Datenschutz vor dem erstmaligen Einsatz gehört werden.

- Personenbezogene Daten von Beschäftigten müssen nach Erfüllung des Zwecks vollständig gelöscht (notfalls gesperrt) werden. Nur wenn es eine Aufbewahrungsfrist aus einer anderen Rechtsvorschrift gibt oder dem Beschäftigten ein Nachteil aus der Löschung entstehen kann, dürfen die Daten gespeichert werden.

- Alle Beschäftigten haben ein unabdingbares Recht auf Auskunft, welche Daten über sie am Arbeitsplatz erfasst, verarbeitet, gespeichert und weitergegeben werden. Diese Auskunft muss die verantwortliche Stelle, also der Arbeitgeber erteilen.

- Stellt man bei Durchsicht seiner Daten fest, dass Angaben nicht vollständig, nicht korrekt oder unzulässig sind, gibt es das Recht auf Berichtigung und Löschung. Können Daten aus unterschiedlichen Gründen nicht gelöscht werden, müssen sie für eine weitere Verwendung gesperrt werden.

- Übergeordnete Kontrollen der gesamten Betriebsstätte können die Aufsichtsbehörden für den Datenschutz vornehmen. Sie sind vor allem ein wichtiger Ansprechpartner, um verbindliche Auskunft zu erhalten, ob bestimmte Sachverhalte mit dem Datenschutz in Einklang stehen oder schlichtweg illegal sind. Die Aufsichtsbehörden können auch anonym angefragt werden.

Ausblick

Man muss sich keiner Illusion hingeben. Der Datenschutz am Arbeitsplatz ist nach wie vor ein heikles Thema.

Gläserne Belegschaften

Seit Einführung der PCs am Arbeitsplatz ist es ein Leichtes, unterschiedlichste Daten zu sammeln, zusammen zu stellen und bedarfsgerecht zu sortieren. Komplizierte Verfahren und mächtige IT-Systeme sind oft gar nicht notwendig. Vieles lässt sich mit einfachen Office-Anwendungen wie Excel oder Access realisieren, deren Nutzung inzwischen zum Alltagswissen gehört. Dies darf nicht leichtfertig erfolgen, sondern nur nach eingehenden Prüfungen. Deshalb ist es an dieser Stelle wichtig, noch einmal auf die gesetzliche Verpflichtung zur Datenvermeidung und Datensparsamkeit hinzuweisen.

Datenschutz, eine Frage der Betriebskultur

Vieles, was im Umfeld des Datenschutzes geschieht und unterbleibt liegt an mangelhaftem Wissen, nicht an krimineller Energie. Dem kann man mit Qualifizierungsangeboten entgegenwirken. Untersuchungen zeigen aber auch, dass es dort, wo es Interessenvertretungen gibt und wo das Betriebsklima gut ist, kaum Verstöße gegen den Datenschutz gibt. Und auch das kann man begünstigen: Viele Schattenseiten entstehen gar nicht erst, wenn der Respekt vor den Mitarbeitern von oben vorgelebt und Abweichungen nicht geduldet werden.

Als Mitarbeiter sind die Einflussmöglichkeiten auf den betrieblichen Datenschutz begrenzt. Es gilt die Privatsphäre und Arbeitsbereiche der Kollegen und Vorgesetzten zu respektieren und sich auch den Respekt zu verschaffen, der einem zusteht.

Beim Datenschutz geht es nicht darum, dass man etwas zu verbergen hat.

Datenschutz sichert das Grundrecht, eigene Entscheidungen treffen zu können.

Warum sollte man auf dieses Recht verzichten und anderen erlauben, über sich zu bestimmen?

Interessenvertretungen und der Beschäftigtendatenschutz

Inhalt:

Nicht an jedem Arbeitsplatz gibt es Betriebsräte, Personalräte oder Mitarbeitervertretungen. Aber wo es sie gibt, dort kommt ihnen eine besondere Rolle beim betrieblichen Datenschutz zu. Das ist allerdings aus ihrer Rechtsstellung nicht direkt erkennbar.

Natürlich kann man sich als Beschäftigter immer selbst um die eigenen Angelegenheiten am Arbeitsplatz kümmern. Doch manchmal ist das heikel, mit Risiken verbunden oder auch von vornherein aussichtslos.

Interessenvertretungen wurden gewählt, um - das sagt schon der Name - die Interessen der Beschäftigten zu vertreten. Um diesen Aufgaben gerecht werden zu können, sind sie per Gesetz mit einem besonderen (Kündigungs-)Schutz und weitergehenden Mitwirkungs- und Mitbestimmungsrechten ausgestattet, damit sie sich für gute Arbeitsbedingungen stark machen können.

Wenn man Fragen hat, oder sich beschweren will

In aller Regel ist die Interessenvertretung die erste Anlaufstelle, wenn man als Beschäftigter den Eindruck hat, dass man benachteiligt wird oder wenn man Fragen zur persönlichen Arbeitssituation hat.

> ***Der Betriebsrat hat Beschwerden von Arbeitnehmern entgegenzunehmen und, falls er sie für berechtigt erachtet, beim Arbeitgeber auf Abhilfe hinzuwirken.***
>
> § 85 Abs. 1 BetrVG
>
> Entsprechende Regelungen für Personalräte und Mitarbeitervertretungen finden sich in § 68 Abs. 1 Nr. 3 BPersVG, § 71 c SPersVG, § 35 Abs. 2 u. 3c, MVG, § 30 Abs. 3 Nr. 2 MAVO

Die Gesetze lassen bewusst offen, um welches Thema sich die Beschwerden drehen. Die Interessenvertreter sind Ansprechpartner für (fast) alles, was einen als Beschäftigter am Arbeitsplatz bewegt. Auch, wenn es darum geht, die Privatsphäre zu schützen oder unzulässige Überwachung zu beenden.

Betriebsräte, Personalräte und Mitarbeitervertretungen sind gewählte Gremien, die dadurch eine besondere Vertrauensstellung genießen. Zu ihren allgemeinen Aufgaben gehört:

> ***(…) darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden***
>
> § 80 Abs. 1 Nr. 1 BetrVG
>
> Entsprechende Regelungen für Personalräte und Mitarbeitervertretungen finden sich in § 68 Abs. 1 Nr. 2 BPersVG, § 71b SPersVG, § 35 Abs. 3 b MVG, § 30 Abs. 1 MAVO.

Die unterschiedlichen Datenschutzgesetze zum Schutz der informationellen Selbstbestimmung, aber auch die Gesetze zum Schutz des gesprochenen und geschriebenen Wortes, zum Recht am eigenen Bild und zum Recht auf freie Entfaltung der Persönlichkeit gehören zweifellos dazu. Dadurch sind die Interessenvertreter per Gesetz zur Kontrolle des Datenschutzes verpflichtet.

Hinweis:

> *Betriebsräte, Personalräte und Mitarbeitervertretungen haben zwar die Aufgabe, sich um die Einhaltung des Datenschutzes zu kümmern, allerdings nur soweit es sich um die Belange der Beschäftigten handelt. Ihre Aufgabe ist es, über die Einhaltung des Beschäftigtendatenschutzes zu wachen und über Betriebs-/Dienstvereinbarungen gestaltend mitzuwirken. Weitere Aspekte wie z. B. der Kunden- oder Patientendatenschutz sind kein Thema für Interessenvertreter, ebenso wenig die Durchsetzung der Datenschutzgesetze. Dazu ist der Arbeitgeber verpflichtet.*

Durchblick, Kompetenz und Unterstützung für Interessenvertreter

Damit die Interessenvertreter ihren gesetzlichen Aufgaben nachkommen können, müssen sie über eine Grundausstattung verfügen, die ihnen ein vertrauliches Arbeiten möglich macht. Es muss gewährleistet sein, dass Gespräche geführt und Dokumente angelegt werden können, die vor einer unbefugten Kenntnisnahme von Dritten geschützt sind. Ein Besprechungsraum (zumindest eine zeitweilige Nutzung) als auch verschließbare Schränke sind ein absolutes Minimum. In aller Regel gehört auch eine angemessene Ausstattung an PCs, Telefon, Internet- und E-Mail dazu, die ebenfalls so eingerichtet ist, dass die Vertraulichkeit gewahrt bleibt. Diese Betriebsmittel muss der Arbeitgeber stellen. Das liegt allerdings auch in seinem Interesse, denn er ist verpflichtet, Interessenvertreter über Vieles zu unterrichten, was als Betriebsgeheimnis unter die Geheimhaltungspflicht fällt. Nur durch eine vernünftige Ausstattung sind diese Informationen auch bei den Interessenvertretern vor unbefugtem Zugriff geschützt.

Wenn man als Beschäftigter bei der Interessenvertretung wegen Fragen zum Datenschutz vorstellig wird, erwartet man jedoch mehr, als einen Besprechungsraum und einen abschließbaren Schrank. Man erwartet Kompetenz und Durchblick.

Durchblick kann allerdings nur der haben, der weiß, was in der Betriebsstätte geschieht. Interessenvertretung und Arbeitgeber sind deshalb verpflichtet, sich regelmäßig auszutauschen. Damit es zu

einem tatsächlichen Austausch kommen kann, ist der Arbeitgeber verpflichtet, die Interessenvertreter unaufgefordert über alles zu informieren, was in deren Aufgabengebiet fällt. Zum Beispiel wie es um die Durchsetzung des Beschäftigtendatenschutzes bestellt ist und ob technische Einrichtungen wie IT-Systeme, Kameraanlagen usw. geplant sind.

> ***Zur Durchführung seiner Aufgaben (…) ist der Betriebsrat rechtzeitig und umfassend vom Arbeitgeber zu unterrichten;***
>
> § 80 Abs. 1 Nr. 2 BetrVG
>
> Entsprechende Regelungen finden sich in § 68 Abs. 2 BPersVG, § 69 Abs. 3 SPersVG, § 34 Abs. 1 u. 3 MVG, § 30 Abs. 1 u. 2 MAVO
>
> **HINWEIS: In BetrVG, BPersVG, SPersVG und MVG muss der Arbeitgeber unaufgefordert und frühzeitig informieren. In katholischen Einrichtungen, in denen die MAVO gilt, muss die Mitarbeitervertretung selbst aktiv werden und relevante Unterlagen einfordern.**

Die Informationsrechte der Interessenvertreter sind sehr weitreichend. Das Landesarbeitsgericht München hat in seiner Entscheidung vom 23.06.2010 festgestellt, dass der Arbeitgeber sogar verpflichtet ist, dem Betriebsrat die Namen der Mitarbeiter mitzuteilen, die aufgrund ihrer Erkrankung vom betrieblichen Eingliederungsmanagement (BEM) betroffen sind.

Entsprechend seiner gesetzlichen Aufgaben, können die Interessenvertreter nicht nur stellvertretend für einzelne Kollegen Aufklärung darüber verlangen, ob deren Rechte bei der Datenverarbeitung gewahrt bleiben. Sie können auch anlassunabhängig „darüber wachen“ dass die Mitarbeiter „nach Recht und Billigkeit“ behandelt werden und der Beschäftigtendatenschutz eingehalten wird. Sie können eine Kontrolle des Datenschutzes und auch eine Kontrolle des Beschäftigtendatenschutzes vornehmen.

So absurd das klingt, so einfach ist der Hintergrund. In der Praxis ist es leider nicht immer so, dass den betrieblichen und behördlichen Datenschutzbeauftragten vom Arbeitgeber die Möglichkeiten (zeitliche Freistellung, Qualifizierung, Ausstattung) eingeräumt werden, damit sie ihren Aufgaben gerecht werden können. Das können Interessenvertreter kontrollieren. Allerdings stehen auch sie nicht über dem Gesetz.

Datenschutzschulungen und Sachverständige für die Interessenvertreter

Bei Betriebsräten, Personalräten und Mitarbeitervertretern handelt es sich um Personen, die dieses Amt ehrenamtlich ausfüllen. In den wenigsten Fällen bringen sie ein umfassendes Wissen zum Beschäftigtendatenschutz mit. Damit sie auch in diesem wichtigen aber schwierigen Thema handlungsfähig sind, haben sie die Möglichkeit, Schulungen zu besuchen und interne wie externe Sachverständige zur Unterstützung anzufordern. Das ist oft auch notwendig, wenn der Beschäftigtendatenschutz im Zusammenhang mit der Einführung von IT-Systemen, Überwachungseinrichtungen, Personalaktenführung oder der Datenübertragung im Konzern einher geht und sich technische, organisatorische und rechtliche Fragen auftun.

> ***Der Betriebsrat kann bei der Durchführung seiner Aufgaben nach näherer Vereinbarung mit dem Arbeitgeber Sachverständige hinzuziehen, soweit dies zur ordnungsgemäßen Erfüllung seiner Aufgaben erforderlich ist.***
>
> § 80 Abs. 3 BetrVG
>
> Entsprechende Regelungen finden sich auch unter § 69 Abs. 3 SPersVG, § 35 Abs. 3b MGV. In den Geltungsbereichen von BPersVG, MVG und MAVO ist die Hinzuziehung eines Sachverständigen über die Wahrnehmung der gesetzlichen Aufgaben zu begründen. Allerdings muss sie erforderlich sein. D. h. der Sachverständige muss für eine Aufgabe erforderlich sein, die nicht durch Selbststudium oder Schulung durch die Gremienmitglieder gelöst werden kann.

In diesem Zusammenhang ist es wichtig Objektivität walten zu lassen und vorurteilsfrei zu handeln. Man sollte interne Sachverständige nicht ablehnen, nur weil sie vom Arbeitgeber benannt wurden. Oft können sie über die technischen, organisatorischen und auch rechtlichen Hintergründe geplanter Vorhaben umfassender Auskunft geben, als externe Sachverständige, weil sie die betriebliche Infrastruktur und die Verfahren kennen.

Doch es geht nicht nur um Auskünfte, sondern auch um Beurteilungen der Rechtmäßigkeit, Erforderlichkeit und Verhältnismäßigkeit von Verfahren, in denen Beschäftigtendaten erhoben und verarbeitet werden. Hierzu ist eine kritische Distanz notwendig, die Externe grundsätzlich

mitbringen. Es geht aber auch darum, Interessenvertreter darin zu unterstützen, durch den Abschluss von Betriebs- und Dienstvereinbarungen den Beschäftigtendatenschutz auszugestalten und so die Mitarbeiter zu schützen. Auch in diesem Punkt stoßen interne (technische) Sachverständige in der Regel an ihre Grenzen. Diese Kompetenz bringen nur externe Sachverständige mit, die sich auf das Thema „Datenschutz und Mitbestimmung“ spezialisiert haben.

Mitwirkung und Mitbestimmung beim Beschäftigtendatenschutz

Betriebs- und Dienstvereinbarungen

In den Grundlagen zum Datenschutz am Arbeitsplatz wurde bereits ausgeführt, dass die Erhebung und Verarbeitung von Beschäftigtendaten nur auf der Grundlage von Rechtsvorschriften und in der Ausnahme auch durch eine Einwilligung des Beschäftigten erfolgen darf. Betriebs- und Dienstvereinbarungen sind solche Rechtsvorschriften.

Vielen ist die Bedeutung von Betriebs- und Dienstvereinbarungen nicht wirklich klar. Es handelt sich nicht nur um ein lapidares Papier, das von Interessenvertretung und Arbeitgeber um des lieben Friedens willen unterzeichnet wird. Betriebs- und Dienstvereinbarungen gelten unmittelbar und zwingend für alle Beschäftigten. Sie müssen vom Arbeitgeber durchgesetzt und von den Betriebsangehörigen eingehalten werden. Sie entscheiden gegebenenfalls über Kündigungen, Abmahnungen, Schadenersatz oder Arbeitsbedingungen. Entsprechend ernsthaft sollte man mit diesem Thema umgehen.

Betriebs- und Dienstvereinbarungen werden üblicherweise nicht generell zum betrieblichen Datenschutz abgeschlossen, sondern dann, wenn Beschäftigte kontrolliert werden sollen oder wenn Verfahren, IT-Systeme oder andere technische Einrichtungen in Betrieb genommen werden sollen, mit denen Mitarbeiter überwacht werden könnten. Ausschlaggebend ist nicht, ob der Arbeitgeber eine Kontrolle der Beschäftigten mit einer Systemeinführung beabsichtigt. Entscheidend ist, ob es (technisch) möglich ist. Ist das der Fall, können Betriebsräte, Personalräte und Mitarbeitervertretungen den Abschluss von Betriebs- und Dienstvereinbarungen fordern und notfalls gerichtlich erzwingen, um einen Schutz der Kollegen zu garantieren.

Chancen und Risiken bei Betriebs- und Dienstvereinbarungen

Der Abschluss von Betriebs- und Dienstvereinbarungen ist für die Interessenvertreter wie auch für die Beschäftigten eine große Chance, selbst gestaltend an den Arbeitsbedingungen mitzuwirken.

Betriebs- und Dienstvereinbarungen können abgeschlossen werden, um zum Beispiel eine Erhebung von Beschäftigtendaten zu ermöglichen, die rechtlich zwar nicht erforderlich, innerbetrieblich zu organisatorischen Zwecken aber sinnvoll ist und ein effektiveres Arbeiten ermöglicht. Durch solche Regelungen kann man unter Umständen mehrfache stupide Datenerfassung vermeiden und Kollegen von solchen Tätigkeiten entlasten. Prinzipiell eine gute Sache. Oder es werden Regelungen getroffen, die allen Beteiligten vor Augen führen, dass Kameras zum Objektschutz und nicht zur Überwachung der Mitarbeiter eingesetzt werden. Positiv ist auch, wenn man sich in Verhandlungen darauf verständigt, möglichst wenige Kameras einzusetzen.

Betriebs- und Dienstvereinbarungen sind nicht nur das stärkste, sondern oft auch das einzige wirkungsvolle Instrument, das Betriebsräte, Personalräte und Mitarbeitervertretungen haben, um ihre Kollegen zu schützen und Arbeitsbedingungen positiv zu gestalten.

Betriebs- und Dienstvereinbarungen stellen allerdings gleichzeitig ein großes Risiko dar. Ist eine Vereinbarung erst mal abgeschlossen, muss sie eingehalten werden. Das gilt auch für ungünstige Regelungen. Betriebsvereinbarungen rund um das Thema Mitarbeiterüberwachung in Form von Leistungs- und Verhaltenskontrolle können nicht einfach gekündigt werden. Sie wirken im Fall der Kündigung nach, bis eine neue Vereinbarung geschlossen wurde. Da dies auch vom Arbeitgeber abhängt, kann das dauern. Außerdem ist der Arbeitgeber auch dann nicht gezwungen eine günstigere Regelung anzubieten.

Bemerkt die Interessenvertretung nach Abschluss einer Vereinbarung, dass sie eine ungünstige Regelung abgeschlossen hat, dann haben sie und alle Beschäftigten ein Problem, das von ihrer Seite kaum mehr gelöst werden kann.

Das Bundesarbeitsgericht (BAG) hat festgestellt (Entscheidung vom 27.05.1986, Az 1 ABR 48/84), dass es durchaus möglich und zulässig ist, über Betriebsvereinbarungen das Datenschutzniveau unter das gesetzliche Maß abzusenken. Das klingt unglaublich, ist aber, genau genommen, nicht überraschend.

Die Datenschutzgesetze verbieten die Erhebung und Nutzung von Beschäftigtendaten. Nur durch Erlaubnis oder eine Rechtsvorschrift kann das Verbot aufgehoben werden. Eine Betriebs- oder Dienstvereinbarung als andere Rechtsvorschrift kann das Verbot und damit den Schutz der Beschäftigten rechtswirksam aufheben.

Das BAG begründet sein Urteil damit, dass es bei einer Betriebsvereinbarung nicht nur um den Datenschutz geht. Es muss geprüft werden, ob die Betriebsvereinbarung in ihrer Gesamtheit nicht eine Partei begünstigt. In der Begründung wurde darauf verwiesen, dass der Betriebsrat geprüft hat, dass er und die Beschäftigten nicht benachteiligt werden. Kommt er zu dem - im Nachhinein falschen - Schluss, die Betriebsvereinbarung sei ausgewogen und unterzeichnet, ist sie rechtswirksam und gilt auch über eine Kündigung hinaus weiter.

Aber auch an anderer Stelle sind unbeabsichtigte Langzeitfolgen möglich. Solche Fälle entstehen, wenn im beidseitigen Einvernehmen zwischen Interessenvertretung und Arbeitgeber Regelungen getroffen wurden, die man rechtlich gar nicht hätte treffen dürfen? Zum Beispiel: Überwachungskameras in Waschräumen zur Aufklärung von Vandalismus, oder eine flächendeckende und ständige Überwachung von Arbeitsplätzen.

Interessenvertreter sind in der Regel keine Juristen, sondern Mitarbeiter im Ehrenamt und auch längst nicht jeder Arbeitgeber ist in juristischen Dingen geschult. In der Praxis verständigt man sich in Verhandlungen zu Betriebs- und Dienstvereinbarungen auf einen Konsens, den man für ausgewogen und tragfähig hält. Eine anschließende Prüfung durch ein Gericht oder eine Aufsichtsbehörde gibt es nicht.

Auch wenn Mitarbeitern solche Vereinbarungen nicht zulässig erscheinen, müssen sie sie zunächst einhalten. Es steht allerdings jedem zu, der davon betroffen ist, Rechtsmittel dagegen einzulegen. Oft ge-

nügt es, eine unabhängige juristische Prüfung zu verlangen. Stellt sich heraus, dass in der Betriebs- oder Dienstvereinbarung Dinge geregelt wurden, die bereits abschließend (und unveränderlich) in Gesetzen oder Tarifverträgen stehen, dann sind diese Aspekte gegenstandslos. Ob die gesamte Vereinbarung dadurch unwirksam wird, hängt davon ab, ob man diesen Fall in einer sogenannten salvatorischen Klausel geregelt hat. Eine salvatorische Klausel legt fest, dass eine Vereinbarung in allen übrigen Teilen weiter gilt, wenn ein Teil weg fällt.

In Fragen der Ordnung und des Verhaltens im Betrieb, bei der Gestaltung von Arbeitsplätzen, bei der Einführung von technischen Einrichtungen, die zur Kontrolle der Mitarbeiter führen können, sind die Interessenvertreter gefordert. In all diesen Fällen ist es möglich, den Datenschutz über die Zweckbindung und Datenverarbeitung in Vereinbarungen zu konkretisieren, Verantwortlichkeiten und Löschfristen festzulegen und dafür zu sorgen, dass gesetzliche Vorschriften eingehalten und Auskunftsrechte gewährt werden. Die Risiken, die beim Abschluss von Betriebs- und Dienstvereinbarungen lauern, kann man ausschließen, indem man sich qualifiziert und Sachverständige - zum Beispiel BEST - als Berater der Interessenvertretung hinzuzieht.

Zusammenarbeit mit dem Beauftragten für Datenschutz

Ein wichtiger Akteur beim Beschäftigtendatenschutz ist der Beauftragte für Datenschutz. Ähnlich wie die Interessenvertretung ist er weisungsunabhängig in der Ausübung seines Amtes und ebenfalls mit einem besonderen Kündigungsschutz ausgestattet. Und auch er ist zuständig für die Einhaltung des Beschäftigtendatenschutzes.

Bei so vielen Überschneidungen ist die Frage naheliegend, ob es sinnvoll ist, dass sich gleich zwei Institutionen des Themas annehmen - und am Ende die Arbeit zweimal machen. Oder gar nicht, weil jeder auf die Sorgfalt des anderen vertraut.

Da sich weder die Interessenvertretungen noch die Beauftragten für Datenschutz über einen Mangel an Arbeit beklagen können, ist es sinnvoll, kooperativ miteinander zu arbeiten. Das muss man allerdings auf beiden Seiten wollen. Die Inter-

essenvertretung ist nicht zur Zusammenarbeit mit dem Beauftragten für Datenschutz verpflichtet; ihr Ansprechpartner ist der Arbeitgeber. Der Beauftragte für Datenschutz hingegen ist nicht zur Zusammenarbeit mit der Interessenvertretung verpflichtet. Auch er ist per Gesetz im Auftrag des Arbeitgebers tätig.

Aus der Kooperation zwischen Interessenvertretung und Beauftragtem für Datenschutz kann aber eine Zusammenarbeit entstehen, von der beide profitieren. Die Interessenvertretung braucht verlässliche und kompetente Informationen zu allem, was den Beschäftigtendatenschutz betrifft. Das kann ein Beauftragter für Datenschutz (z. B. als interner Sachverständiger) leisten. Dieser hat zwar die Kompetenz zum Datenschutz, allerdings keine Durchsetzungsfähigkeit.

Der Beauftragte für Datenschutz ist in der Regel nicht weisungsbefugt und kann nur von Mängeln berichten. Er kann sie aber nicht selbstständig abschalten. Das muss der Arbeitgeber tun. Betriebsräte, Personalräte und Mitarbeitervertretungen können allerdings auch seinen Rat und seine Empfehlungen in Betriebs- und Dienstvereinbarungen einfließen lassen. Dadurch werden sie rechtsverbindlich und auch dem Beauftragten für Datenschutz ist geholfen.

Bei der Zusammenarbeit ist es allerdings wichtig, sich vor Augen zu halten, wer aus welcher Perspektive handelt. Das gilt es zu respektieren. Beauftragte für Datenschutz raten zum Beispiel dazu, die private Nutzung von Internet und E-Mail am Arbeitsplatz zu verbieten. Das ist aus ihrer Warte auch schlüssig: Wenn es keine privaten Daten gibt, kann auch kein Missbrauch daraus erfolgen. Für Betriebsräte, Personalräte und Mitarbeitervertretungen stehen neben dem Datenschutz allerdings auch die generellen Arbeitsbedingungen zur Debatte. Aus ihrer Perspektive ist es nicht mehr angebracht, ein rigoroses Verbot auszusprechen, das nicht mehr zeitgemäß ist, weil sich nicht einmal mehr die Vorgesetzten daran halten. Hier muss man eine ausgewogene Lösung finden, die nicht weltfremd ist.

Doch nicht immer ist das Verhältnis zwischen Betriebsrat und Beauftragtem für Datenschutz spannungsfrei. Der Beauftragte für Datenschutz ist schließlich direkt dem Arbeitgeber unterstellt und arbeitet ihm zu. Hinzu kommt, dass der Beauftrag-

te für Datenschutz nicht wie die Interessenvertreter von den Beschäftigten gewählt ist. Der Beauftragte für Datenschutz ist vom Arbeitgeber bestellt. Die Kombination, dass eine solch wichtige Position mit weitreichenden Kontrollmöglichkeiten direkt vom Arbeitgeber bestellt wird und ihm direkt unterstellt ist, trägt nicht zwangsläufig zur vertrauensvollen Zusammenarbeit bei. Diese kann nur durch den wechselseitigen Respekt entstehen.

Aber auch wenn der Beauftragte für Datenschutz in erster Linie vom Arbeitgeber bestellt wird, heißt das nicht, dass die Interessenvertreter keinen Einfluss darauf haben, wer dieses Amt inne hat. Wenn ein Beschäftigter die Aufgaben eines Beauftragten für Datenschutz wahrnehmen wird, bedeutet das ganz konkret eine Änderung seiner Tätigkeiten. Datenschutzbeauftragter kann man nicht sein, ohne dass ein nachweisliches Maß an Arbeitszeit darauf verwendet werden muss. Diese Tätigkeitsänderung entspricht folglich einer Versetzung. Eine Versetzung ist eine personelle Maßnahme, die sich nur mit Zustimmung der Interessenvertreter durchsetzen lässt.

Weiterhin haben die Interessenvertreter im Rahmen ihrer allgemeinen Aufgaben die Pflicht zu kontrollieren, ob der Beauftragte für Datenschutz auch die gesetzlichen Voraussetzungen im Hinblick auf Sachkunde und Zuverlässigkeit erfüllt. Der Beauftragte für Datenschutz darf auch nicht in einem Interessenkonflikt stehen, indem er zum Beispiel das als Datenschutzbeauftragter kontrollieren muss, was er als Personalleiter betreibt. Personalleiter, IT-Leiter, Geschäftsführer und Interessenvertreter sind für dieses Amt nicht geeignet; ebenso wenig Mitarbeiter, die mit der Korruptionsbekämpfung beschäftigt sind, da dies zur maximalen Datensammlung und nicht zur Datensparsamkeit verleitet. Sollten diese Voraussetzungen nicht zutreffen, können Interessenvertreter die Abbestellung des Beauftragten für Datenschutz verlangen und notfalls auch durch die Aufsichtsbehörde oder gerichtlich erwirken.

Interessenvertreter als eigene verantwortliche Stelle

Betriebsräte, Personalräte und Mitarbeitervertretungen haben nicht nur die Aufgabe, zu kontrollieren, ob der Arbeitgeber

den Beschäftigtendatenschutz ernst nimmt. Die Interessenvertretung ist eine eigene verantwortliche Stelle mit allen damit verbundenen Verpflichtungen. Es ergibt sich aus ihren gesetzlichen Aufgaben, dass die Interessenvertretung Beschäftigtendaten erhebt und verarbeitet. Sie erhält Namen von Beschäftigten zum Betrieblichen Eingliederungsmanagement (BEM), sie erhält Einblick in die Bruttoentgelte und so weiter.

Für die Verarbeitung für Beschäftigtendaten gelten die gleichen Vorgaben wie für den Arbeitgeber. Die Rechtmäßigkeit der Datenerhebung muss gesichert sein, die Art der Verarbeitung und die Zugriffsberechtigungen müssen dokumentiert sein und auch die Löschungen müssen fristgerecht erfolgen, um nur einige Aspekte zu nennen. Jeder, auch ein Abteilungsleiter, Geschäftsführer oder Vorstand kann bei den Interessenvertretern Auskunft darüber verlangen, welche Daten zu welchem Zweck von ihm erhoben und verarbeitet wurden. Eine Auskunft muss wie beim Arbeitgeber zeitnah und vollständig erfolgen. Das sollte man bedenken, bevor man jemandem vorwirft, die Persönlichkeitsrechte anderer nicht zu respektieren.

Datenschutzkontrolle der Interessenvertretung

Betriebsräte, Personalräte und Mitarbeitervertretungen sind selbst dafür verantwortlich, dass der Datenschutz auch bei der Ausübung ihrer Tätigkeiten umgesetzt wird. Und auch sie müssen damit rechnen, kontrolliert zu werden. Da sie eine besondere Vertrauensstellung genießen, ist es ausgeschlossen, dass sie vom betrieblichen oder behördlichen Datenschutzbeauftragten kontrolliert werden, da der vom Arbeitgeber bestellt wurde und ihm zum Bericht verpflichtet ist. Allerdings kann die Aufsichtsbehörde eine Prüfung vornehmen.

Hinweis:

Immer wieder fragen Arbeitgeber bei Aufsichtsbehörden an und bitten darum, die Interessenvertretung zu überprüfen, weil sie dort Verstöße gegen den Datenschutz vermuten.

Die Aufsichtsbehörden weisen in diesem Zusammenhang darauf hin, dass sie aufgedeckte Verstöße der Interessenvertretung mit Bußgeldern ahnden müssen. Da die Inte-

ressenvertretung per Gesetz über keine Mittel verfügt und vom Arbeitgeber für die Ausübung ihrer Tätigkeiten ausgestattet wird, ist es auch der Arbeitgeber selbst, der mögliche Bußgelder für die Verstöße der Interessenvertretung zahlt. Die meisten Anfragen werden nach dieser Aufklärung zurückgezogen.

Fazit:

Betriebsräte, Personalräte und Mitarbeitervertretungen haben eine wichtige Rolle beim betrieblichen Datenschutz. Sie haben auch eine große Verantwortung und viele Aufgaben:

- Sie wachen über die Einhaltung des Beschäftigtendatenschutzes;
- sie nehmen sich den Fragen ihrer Kollegen an und sorgen für rechtsverbindliche Aufklärung ggf. unter Mithilfe von Sachverständigen und der Aufsichtsbehörde für den Datenschutz;
- sie begleiten aktiv die Erforderlichkeits- und Verhältnismäßigkeitsprüfungen und sorgen so dafür, dass bereits zu Beginn den Rechten der Beschäftigten Rechnung getragen wird;
- durch Betriebs- und Dienstvereinbarungen konkretisieren sie den Datenschutz, heben das Schutzniveau und sorgen für transparente und rechtsverbindliche Verfahren, die auch praxistauglich sind;
- und sie müssen vorbildlich mit den Daten ihrer Kollegen umgehen, den Datenschutz einhalten und Vertraulichkeit wahren.

Unterstützung für Betriebsräte, Personalräte und Mitarbeitervertretungen im Saarland

Die Arbeitskammer des Saarlandes und der DGB Saar waren sich schon frühzeitig der verantwortungsvollen Aufgaben der Interessenvertretungen beim Datenschutz bewusst. Bereits 1989 wurde die „Beratungsstelle für sozialverträgliche Technologiegestaltung“, kurz BEST, gegründet, um Betriebsräten, Personalräten und Mit-

arbeitervertretungen eine kompetente Unterstützung anbieten zu können.

Heute reicht die Themenpalette von der Arbeitszeitgestaltung bis zur Zutrittskontrolle. Der Beschäftigtendatenschutz spielt allerdings nach wie vor eine zentrale Rolle. Unter anderem wurden über tausend Betriebs- und Dienstvereinbarungen auf den Weg gebracht, Dutzende von Seminaren zu Datenschutzthemen abgehalten und Wissenswertes zu diesem Thema veröffentlicht. Auch dieses Handbuch wurde von BEST im Auftrag der Arbeitskammer des Saarlandes erstellt. Weitere Informationen zu BEST und vielen Sachthemen finden sich unter best-saarland.de

BEST e. V.
c/o Arbeitskammer des Saarlandes
Fritz-Dobisch-Straße 6-8
66111 Saarbrücken
Telefon: (0681) 4005-249
E-Mail: best@best-saarland.de

Alles im Blick - der/die Beauftragte für Datenschutz

Inhalt:

Einer der wichtigsten Akteure beim betrieblichen Datenschutz ist der sogenannte *Beauftragte für den Datenschutz*. Oft ist jedoch nicht ganz klar, was es damit auf sich hat. Das liegt nicht zuletzt daran, dass es ihn nicht an jedem Arbeitsplatz gibt. Jedes Unternehmen und jede Dienststelle kann einen Datenschutzbeauftragten bestellen.

Ob es einen Datenschutzbeauftragten geben *muss*, oder nicht, regeln die Datenschutzgesetze. Darin ist auch beschrieben, wer diese Position einnehmen kann und welche Aufgaben damit verbunden sind. Das ist allerdings in den einzelnen Geltungsbereichen unterschiedlich geregelt.

Wann muss ein Beauftragter für Datenschutz bestellt werden?

Privatwirtschaft und Bundeseinrichtungen:

Ein Datenschutzbeauftragter muss nach § 4f BDSG benannt werden, wenn mindestens einer der folgenden Punkte zutrifft:

- Es werden besondere Arten von personenbezogenen Daten nicht nur für interne Zwecke verarbeitet

- Es werden personenbezogene Daten geschäftsmäßig verarbeitet (z. B. Adresshandel, Lettershop, Meinungsforschung etc.)
- Mindestens zehn Personen erheben und verarbeiten regelmäßig personenbezogene Daten mittels Computer. Darunter fallen auch alle, die regelmäßig Personenlisten oder Ähnliches mit dem Computer erstellen, auch Schichtplaner, Lohnbuchhalter, Pförtner mit Besucherlisten o. ä.
- Es werden personenbezogene Daten von mehr als zwanzig Personen nicht automatisiert, also von Hand verarbeitet

Öffentliche Einrichtungen des Saarlandes, der Kreise und Kommunen

Grundsätzlich ist die Landesbeauftragte für Datenschutz zuständig, allerdings *kann* nach § 8 SDSG ein geeigneter behördlicher Datenschutzbeauftragter bestellt werden. Dadurch werden viele Aufgaben deutlich vereinfacht und (automatisierte) Verfahren handhabbarer. Es besteht jedoch keine Verpflichtung, einen Beauftragten für Datenschutz zu bestellen. Aber auch dann, wenn ein behördlicher Datenschutzbeauftragter benannt ist, muss die Landesbeauftragte für Datenschutz vor dem erstmaligen Einsatz von automatisierten Verfahren, bei denen personenbezogene Daten verarbeitet werden, informiert und gehört werden. Es führt also kein Weg daran vorbei, dass die Landesbeauftragte für Datenschutz IT-Systeme begutachten muss, bevor sie in Betrieb genommen werden dürfen. Dasselbe gilt auch, wenn die (bereits begutachteten) Verfahren und Systeme maßgeblich verändert werden.

Evangelische Kirche und deren Einrichtungen

Die Evangelische Kirche in Deutschland und die Gliedkirchen sind nach § 18 DSG-EKD verpflichtet, Datenschutzbeauftragte zu bestellen. Diese haben eine Funktion, die vergleichbar ist mit denen der Landesbeauftragten für Datenschutz.

Bei kirchlichen Werken und Einrichtungen, die rechtlich selbständig sind, und bei sonstigen kirchlichen Einrichtungen sollen nach § 22 DSG-EKD örtliche Datenschutzbeauftragte bestellt werden, wenn mehr als sechs Personen mit der Erhe-

bung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind. Eine Verpflichtung besteht jedoch nicht.

Falls keine örtlichen Datenschutzbeauftragte bestellt sind, sind die betreffenden Datenschutzbeauftragten der Landes- oder Gliedkirchen zuständig.

Katholische Kirche und deren Einrichtungen

Bei der katholischen Kirche bestellt jeder Bischof einen Diözesandatenschutzbeauftragten, der zuständig ist für das jeweilige Bistum. Katholische Einrichtungen können nach § 18a KDO einen örtlichen Datenschutzbeauftragten bestellen. Eine Verpflichtung besteht jedoch nur für klinische Einrichtungen. Nach § 8 Abs. 2 der Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern müssen Krankenhausträger einen oder mehrere Betriebsbeauftragte für ihre Häuser bestellen. Dabei kann auch ein Beauftragter für mehrere Häuser bestellt werden.

Wer kann Beauftragter für Datenschutz werden?

Der Wortlaut ist in allen Datenschutzgesetzen nahezu identisch: Datenschutzbeauftragter kann werden, wer über die notwendige Fachkunde und die notwendige Zuverlässigkeit verfügt. Anders ausgedrückt, muss sich der oder die Beauftragte für Datenschutz nachweislich mit den entsprechenden Rechtsvorschriften auskennen und auch ein (zumindest grundlegendes) Wissen über das Funktionieren von IT-Systemen mitbringen. Beides ist wichtig. Daneben ist es notwendig, dass man sich auf die Person im Hinblick auf Sorgfalt, Rechtsverbindlichkeit, Objektivität und Engagement verlassen kann. Allerdings darf auch dann kein Interessenkonflikt vorliegen. Wer also in verantwortlicher Stellung personenbezogene Daten verarbeitet oder verarbeiten lässt, zum Beispiel Personalleiter, IT- oder EDV-Leiter, Geschäftsführer sind als Beauftragte für Datenschutz unzulässig. Sie müssten ihre eigene Arbeit beurteilen, das wäre ein Interessenkonflikt.

Interessenvertreter als Datenschutzbeauftragte?

Auch wenn die Rechtsprechung es nicht durchgehend ablehnt, sollten auch keine Betriebsräte, Personalräte und Mitarbeitervertreter dieses Amt bekleiden. Sie sind letztlich demselben Interessenkonflikt

ausgesetzt, wenn sie in der Funktion als Datenschutzbeauftragter etwas Vertrauliches kontrollieren müssten, was sie als Interessenvertreter interessiert, ihnen in dieser Rolle allerdings nicht (oder noch nicht) bekannt ist. Eine solche Doppelrolle hätte zur Folge, dass der Datenschutzbeauftragte unweigerlich dem Vorwurf ausgesetzt wird, seine Aufgabe aus der Perspektive des Interessenvertreters zu betreiben.

Compliancebeauftragter und Datenschutzbeauftragter?

Eine durchaus tragfähige Kombination ist die Personalunion von Innenrevision (interner Buchprüfung) und Beauftragtem für Datenschutz. In den letzten Jahren ist zu beobachten, dass auch die Funktionen des Antikorruptions- (Compliance-) Beauftragter und des Datenschutzbeauftragten von einer Person wahrgenommen werden. Das geht in der Praxis jedoch nicht, da die Ziele beider Ämter entgegengesetzt sind: Der Datenschutzbeauftragte sorgt dafür, dass so wenig personenbezogene Daten wie irgend möglich verwendet werden und achtet darauf, dass die Daten nur sehr eingeschränkt genutzt werden dürfen. Der Compliance-Beauftragte braucht die maximale Menge an personenbezogenen Daten, um sie in bestimmten Suchstrategien neu zusammenzusetzen und so Hinweise auf Unregelmäßigkeiten zu entdecken und aufzuklären. Diese beiden Ämter können nicht durch eine Person wahrgenommen werden. Wer will letztlich überprüfen, ob vertrauliche Protokolldaten, die nur für den Datenschutzbeauftragten zur Datenschutzkontrolle zugänglich sind, nicht regelmäßig und systematisch für Compliance-Zwecke verwendet werden. Dies wäre nicht mehr überprüfbar.

Wie wird man Datenschutzbeauftragter?

Der Datenschutzbeauftragte wird von der verantwortlichen Stelle bestellt. Im Arbeitsverhältnis ist das üblicherweise die Geschäftsführung oder Dienststellenleitung. Das heißt eine geeignete Person aus dem Unternehmen oder auch ein externer Datenschutzbeauftragter wird gefragt, ob sie oder er das Amt übernehmen möchte. Willigt er oder sie ein, ist die Bestellung erfolgt. Das muss in schriftlicher Form

festgehalten und an der Betriebsstätte bekannt gemacht werden. Er oder sie ist schließlich Ansprechpartner für alle Beschäftigten wie auch für Kunden, Patienten etc. Datenschutzbeauftragter ist nicht zwangsläufig ein Hauptberuf. Viele Datenschutzbeauftragten kümmern sich quasi in Teilzeit um dieses Amt. Allerdings sollte diese Freistellung von anderen Aufgaben auch in einem angemessenen Maß stehen, die es erlauben auch als Ansprechpartner verfügbar zu sein.

Was macht ein Beauftragter für Datenschutz?

Der Datenschutzbeauftragte „macht" den Datenschutz nicht und er setzt ihn auch nicht durch. Das sind Aufgaben des Arbeitgebers.

Der Beauftragte für Datenschutz

- berät das Unternehmen,
- er informiert und schult Mitarbeiter, Verantwortliche und Führungskräfte,
- er kontrolliert, ob die Datenschutzgesetze eingehalten werden,
- er nimmt Fragen und Beschwerden zum Datenschutz entgegen, geht diesen Fragen nach und fordert die Beseitigung eventuell festgestellter Mängel,
- er verwaltet das Verfahrensverzeichnis/Verarbeitungsübersicht, oft genug erstellt er diese Übersichten auch,
- er bearbeitet Auskünfte von Beschäftigten und außenstehenden Personen, die von ihren Auskunftsrechten Gebrauch machen,
- er führt die Vorabkontrollen von automatisierten Verfahren durch.

Die besonderen Rechte (und Pflichten)

In der Ausübung seiner Aufgaben ist der Datenschutzbeauftragte weisungsfrei. Das heißt, dass niemand ihm vorschreiben kann, wie er seine Aufgaben zu erledigen hat. Allerdings ist er aufgrund seiner Bestellung auch nicht weisungsbefugt. Er kann also auch nichts anweisen. Das erklärt sich dadurch, dass prinzipiell der Arbeitgeber dafür verantwortlich ist, dass Gesetze in der Betriebsstätte umgesetzt werden. Der Datenschutzbeauftragte be-

rät, informiert und kontrolliert. Aber der Arbeitgeber muss anweisen, dass festgestellte Mängel beseitigt werden - er ist schließlich die verantwortliche Stelle. Insofern ist es logisch, dass nicht der Datenschutzbeauftragte, sondern der Arbeitgeber für Datenschutzpannen haftet. Ein Haftungsrisiko für den Datenschutzbeauftragten besteht nur dann, wenn er seinen Aufgaben nicht nachkommt. Das ist ein zwingender Grund, dass er abbestellt wird.

Damit der Datenschutzbeauftragte seine Aufgaben auch objektiv wahrnehmen kann, ist er mit einem besonderen Kündigungsschutz ausgestattet, der ihn in den Fällen schützt, wenn er „unbequeme“ Forderungen an den Arbeitgeber stellt und Mängel aufdeckt. In Ausübung seiner Aufgaben ist er letztlich nicht ordentlich kündbar. Das hat die Rechtsprechung bereits mehrfach festgestellt. Weiterhin wurde der Datenschutzbeauftragte im BDSG mit einem sogenannten „Zeugnisverweigerungsrecht“ ausgestattet. Der Datenschutzbeauftragte kann nicht gezwungen werden, Informanten preiszugeben, zum Beispiel, welcher Mitarbeiter ihn über welche Mängel informiert hat.

Kooperation zwischen Datenschutzbeauftragtem und Interessenvertretung ist sinnvoll

Sowohl der Datenschutzbeauftragte als auch die Interessenvertretung haben ein breites Aufgabenspektrum. Der Beschäftigtendatenschutz ist jedoch eine eindeutige Schnittmenge. Deshalb ist es in diesem Bereich sinnvoll zusammen zu arbeiten und sich zu unterstützen. Aus der Kooperation ergibt sich nicht einfach eine Arbeitsersparnis, sondern eine ganz neue Effizienz. Datenschutzbeauftragte sind „durchsetzungsschwach“, verfügen aber über eine hohe Kompetenz in ihrem Fachgebiet. Betriebsräte, Personalräte und Mitarbeitervertretungen können üblicherweise diese Kompetenz nicht in ihren eigenen Reihen finden, allerdings sind sie durch den Abschluss von Betriebs- und Dienstvereinbarungen außerordentlich durchsetzungsstark. Modern ausgedrückt ergibt sich für beide Parteien daraus eine Win-win-Situation.

Darf der Datenschutzbeauftragte die Interessenvertretung kontrollieren?

Die Interessenvertretung ist eine eigene verantwortliche Stelle im Sinne der Daten-

schutzgesetze. Der korrekte Umgang mit den persönlichen Daten der Kollegen ist nicht nur eine gesetzliche Verpflichtung, sondern in diesem Fall auch eine Ehrensache, von der das Image der Interessenvertretung abhängt.

Die Frage ist eher, ob der Beauftragte für Datenschutz die Einhaltung der gesetzlichen Vorschriften auch bei der Interessenvertretung überprüfen darf. Er darf es nicht. Die Rechtsprechung begründet dies damit, dass die Interessenvertretung keine Mitbestimmung bei der Bestellung des Datenschutzbeauftragten hat und er - aus dieser Warte - als Organ des Arbeitgebers anzusehen ist. Interessenvertretungen können nur von der Aufsichtsbehörde kontrolliert werden.

Man darf jedoch das eigentliche Ziel, den Schutz der Persönlichkeitsrechte der Beschäftigten, nicht aus den Augen verlieren. Der Beauftragte für Datenschutz kann Betriebsräte, Personalräte und Mitarbeitervertreter beraten und unterstützen, wie sie den Datenschutz bei der Wahrnehmung ihrer Aufgaben umsetzen können.

Datenschutzbeauftragte sind keine Einzelkämpfer

Generell braucht ein Datenschutzbeauftragter Rückhalt im Betrieb oder der Dienststelle. Dazu müssen alle etwas beitragen. Die Leitungsebene muss nicht nur durch Worte deutlich machen, dass der Datenschutz ein hohes Gut ist. Dazu gehört, dass der Datenschutzbeauftragte in einem angemessenen Maß von anderen Aufgaben freigestellt wird, dass ihm die entsprechende Ausstattung zugestanden wird und er durch den Besuch von Schulungen seine Kompetenz auf und ausbauen kann. Der Datenschutzbeauftragte muss darstellen, dass er vertrauenswürdig, loyal und um Objektivität bemüht ist. Und die Mitarbeiter wie auch die Interessenvertretung müssen mit ihm zusammenarbeiten wollen.

Der Arbeitskreis Datenschutz

Datenschutz ist ein komplexes Thema, das man beständig verfolgen muss, um am Ball zu bleiben. Vor dieser Herausforderung stehen alle Datenschutzbeauftragte, vor allem jedoch die, die diese Aufgabe nur in Teilzeit ausüben können.

Für saarländische Beauftragte für Datenschutz bietet sich die Möglichkeit zu einem Erfahrungsaustausch unter Gleichgesinnten im Arbeitskreis Datenschutz. Der Arbeitskreis wird von BEST e. V. einer Tochter der Arbeitskammer des Saarlandes und des DGB Saar organisiert und bietet eine Plattform zum Wissens- und Erfahrungsaustausch unter Experten aus dem betrieblichen und behördlichen Datenschutz.

Was bietet der Arbeitskreis?

- *Kompetenz* - Wissensaustausch unter Experten fördert Kompetenz und erleichtert Einsteigern die Aufnahme ihrer Arbeit.
- *Aktualität* - Aktuelle Informationen zu Recht, Technik und Verfahren werden angesprochen.
- *Best Practice* - Experten berichten über ihre Arbeit.

Was macht der Arbeitskreis?

Der Arbeitskreis legt die Themen, die bearbeitet werden, selbst fest. Behandelt werden:

- Änderungen in der aktuellen Rechtslage,
- allgemeine Datenschutzaspekte in der betrieblichen Praxis und
- Datensicherheit bei IT und elektronischer Kommunikation.

Die Teilnahme am Arbeitskreis ist kostenlos; er trifft sich etwa fünfmal pro Jahr. Interessierte sind jederzeit willkommen. Aktuelle Termine und weitere Informationen gibt es unter best-saarland.de

Spezielle Themen

Leistungs- und Verhaltenskontrollen

Inhalt:

Worum geht es?

Das Arbeitsverhältnis ist ein Verhältnis auf Gegenseitigkeit. Der Mitarbeiter bringt seine Leistung ein, der Arbeitgeber zahlt ein Entgelt dafür. Welche Leistung für welches Geld erbracht werden soll, wird im Arbeitsvertrag, gegebenenfalls unter Berücksichtigung geltender Tarifverträge festgeschrieben. Jeder der Vertragspartner hat das Recht, die Einhaltung des Vertrages zu überprüfen. Als Beschäftigter ist man daran interessiert, ob die Entgeltabrechnung stimmt; als Arbeitgeber möchte man wissen, ob die erbrachte Leistung stimmt und oft auch, ob sich der Beschäftigte auch angemessen am Arbeitsplatz verhält.

Die Frage ist nur, wie weit dürfen diese Kontrollen gehen?

Kontrolle der Arbeitsleistung

Arbeitsleistung ist in diesem Zusammenhang nicht als physikalische Größe zu sehen, sondern als geleistetes Arbeiten in Erfüllung der arbeitsvertraglichen Pflichten. Daraus lassen sich für Arbeitgeber zwei Fragen ableiten 1. ob gearbeitet wurde, 2. wieviel und in welcher Qualität gearbeitet wurde.

Das erste ist relativ einfach herauszufinden, dazu ist selten mehr notwendig, als eine Anwesenheitskontrolle. Das zweite ist hingegen recht problematisch. Warum? Der Arbeitgeber hat das Recht exakt das zu kontrollieren, was im Arbeitsvertrag als Leistung vereinbart worden ist. Oft genug steht im Arbeitsvertrag allerdings nur die

Stellenbezeichnung. Oft, aber nicht immer, gibt es Stellenbeschreibungen, die ausweisen, welche Tätigkeiten von Beschäftigten zu erbringen sind. Wieviel und in welcher Qualität ist in aller Regel jedoch nicht festgehalten. Wenn man also die Leistung des Beschäftigten feststellen will, hat man neben dem Problem, eine geeignete Messmethode zu finden auch das Problem der Bewertung: Wieviel Leistung ist gut, wieviel ist schlecht?

Lediglich im Spezialfall Leistungslohn (z. B. Akkord) sind solche Bewertungsmaßstäbe festgelegt. Doch dazu später mehr.

Um die Grundfrage zu beantworten, welche Kontrollen zulässig sind, muss man den rechtlichen Rahmen abstecken.

Die üblichen Arbeitsverträge beziehen sich auf einen sogenannten Zeitlohn. Als Beschäftigter hat man die Pflicht, dem Arbeitgeber innerhalb eines vereinbarten zeitlichen Rahmens (tägliche Arbeitszeit, Wochenarbeitszeit) die eigene Leistung anzubieten. Der Arbeitgeber hat die Möglichkeit, die Leistung für die vereinbarten Tätigkeiten abzurufen. Wenn nichts Weiteres vereinbart ist, gilt § 243 des Bürgerlichen Gesetzbuchs (BGB). Danach hat der Beschäftigte eine Leistung mittlerer Art und Güte zu erbringen.

Normal ist eine Leistung mittlerer Art und Güte

Das hat seinen Hintergrund darin, dass gewährleistet sein muss, dass man als Beschäftigter seine Leistung dauerhaft erbringen muss - bis zum Renteneintrittsalter - ohne gesundheitliche Schäden davonzutragen. Deshalb gilt ein solcher gesetzlicher Durchschnittswert. Einen konkreten Wert sucht man im Gesetz jedoch vergebens. Das kann auch ein Gesetz nicht konkret leisten. „Mittlere Art und Güte“ macht sich in einem Produktionsbetrieb an anderen Faktoren fest als in einer Verwaltung, obwohl jeder seine Leistung erbringt. Trotzdem legt § 243 BGB nahe, dass man einen Durchschnittswert über alle Beschäftigten ermittelt. Z. B. die Anzahl produzierter Teile oder bearbeiteter Vorgänge. Doch bei vielen üblichen Arbeitsplätzen ist ein Zählen und Messen gar nicht möglich: EDV-Mitarbeiter, Abteilungsleiterin, Pförtner etc.

Leistungsbeurteilungen müssen individuell erfolgen

Es gibt jedoch noch eine andere Vorgabe der Arbeitsgerichte: Der Beschäftigte muss seine Arbeitsleistung voll ausschöpfen. Er muss tun, was er tun soll und so gut er kann (im Einklang mit den Grundsätzen eines dauerhaften gesunden Arbeitens). Das ist bei jedem Mitarbeiter ein wenig anders. Also selbst dort, wo man Leistung messen kann, muss die Bewertung „gute oder schlechte Leistung“ individuell und nicht automatisiert mit einem IT-System erfolgen.

Da es sich um individuelle Leistungsbetrachtungen handelt, greifen die Datenschutzgesetze. Diese verlangen, dass die Datenerhebung rechtmäßig, erforderlich und verhältnismäßig ist. Außerdem gilt die Zweckbindung. Das heißt, Stückzahlen, die erhoben wurden, um eine Produktionsmenge festzustellen, dürfen nicht zum Zweck einer individuellen Leistungsbeurteilung eines Maschinenbedieners benutzt werden. Es sei denn, das ist bereits vor der Datenerhebung mit dem Arbeitnehmer (vorrangig aber mit den Tarifparteien und örtlichen Interessenvertretern) vereinbart worden z. B. als Leistungslohn.

Leistungskontrolle im Zeitlohn

Es gibt keine klar verständliche und verbindliche Regel, welche Leistungskontrollen ein Arbeitgeber vornehmen darf. Aber es gibt Rahmenbedingungen. Anhand der nachfolgenden Kriterien kann geprüft werden, ob eine Leistungskontrolle zulässig ist, oder nicht:

- Zulässigkeit: Der Arbeitgeber hat natürlich das Recht zu kontrollieren, ob und welche Leistung der Mitarbeiter erbracht hat. Es muss sich allerdings um Tätigkeiten handeln, die direkt im Arbeitsvertrag vereinbart sind oder sich ableiten lassen. Je weniger konkret ein Arbeitsvertrag ist, desto geringer sind die Möglichkeiten einer Leistungskontrolle. Verschiedene Leistungskontrollen sind in jedem Fall unzulässig. Der Arbeitgeber muss Krankmeldungen registrieren und auch Krankentage addieren, da er verpflichtet ist, ein betriebliches

Eingliederungsmanagement für Langzeiterkrankte anzubieten. Das Addieren und Analysieren von Krankmeldungen zur Leistungskontrolle ist allerdings unzulässig.

- Zweckbindung: Soll die Arbeitsleistung eines Mitarbeiters anhand vereinbarter Tätigkeiten kontrolliert werden, müssen die Daten (wann, wieviel, welche Ergebnisse) erhoben werden. Fallen solche Daten ohnehin an (z. B. durch Maschinendaten), dürfen diese Daten nur für eine Leistungskontrolle verwendet werden, wenn Mitarbeiter und Interessenvertretung diesem Zweck zustimmen. Daten im Nachhinein zu anderen Zwecken zu verwenden, als zu denen, für die die Daten ursprünglich erhoben wurden, ist verboten.

- Erforderlichkeit: Wenn Leistungskontrollen vorgenommen werden sollen, muss überprüft werden, ob die Kontrollmethode objektiv erforderlich ist, oder einfach nur praktisch. Es sind nur Kontrollen zulässig, die im juristischen Sinn erforderlich sind. Und es muss die schonendste Kontrollmethode gewählt werden, nicht die praktischste. Persönlichkeitsrechte wiegen schwerer als praktischer Komfort.

- Individualität: Die Leistungsbeurteilung muss auf den individuellen (nicht durchschnittlichen!) Mitarbeiter bezogen sein, um feststellen zu können, ob er den arbeitsvertraglichen Pflichten nachkommt und *seine* Möglichkeiten ausschöpft. Leistungsvergleiche zwischen Mitarbeitern im Zeitlohn sind nur sehr eingeschränkt möglich.

Leistungskontrolle im Leistungslohn

Leistungslohn oder leistungsbezogene Teile des Lohns müssen arbeitsvertraglich geregelt sein und sie müssen im Einklang mit eventuell geltenden Tarifverträgen stehen. Weiterhin bestehen auch Mitbestimmungsrechte der Interessenvertretungen. Sofern also Betriebs- oder Dienstvereinbarungen abgeschlossen wurden, müssen auch diese Vorgaben erfüllt sein.

Unter Einhaltung der genannten Vorgaben wird beim Leistungslohn vorab eine Leistung in Art und Menge festgelegt, es wird

festgelegt, wie die Leistung kontrolliert wird und es wird vereinbart, welches (zusätzliche) Entgelt bei welcher Leistung bezahlt wird. Aber auch in einem solchen Leistungssystem sind bestimmte Aspekte zu beachten:

- Die Leistungskontrolle muss unter Beachtung arbeitswissenschaftlicher Grundlagenlagen erfolgen. Werden Stückzahlen oder Qualitätsmerkmale zur Leistungsmessung herangezogen (typisch für Leistungslohn Akkord), muss das nach anerkannten Messmethoden erfolgen z. B. REFA oder MTM. Bei nicht direkt messbaren Leistungen, können Näherungsverfahren (z. B. Balanced Scorecard) eingesetzt werden, um zu faktisch überprüfbaren Leistungsbeurteilungen zu kommen.
- Die Verhältnismäßigkeit muss auch bei Leistungskontrollen im Leistungslohn gewährleistet sein: Die „Gewinnerwartungen“ durch den Leistungslohn müssen in einem angemessenen Verhältnis zum entstehenden Leistungs- und Kontrolldruck stehen.

Zusammenfassung Leistungskontrollen

Leistungskontrollen sind am Arbeitsplatz möglich, müssen sich allerdings auf die vereinbarten Leistungen aus dem Arbeits- und Tarifvertrag beziehen. Wenn es dort keine konkreten Angaben gibt, können auch kaum konkrete Kontrollen stattfinden.

Heimliche Leistungskontrollen sind heimliche Datenerfassungen. Diese sind in jedem Fall unzulässig, weil auch offensichtlich kontrolliert werden kann, um zu den gleichen Ergebnissen zu kommen. Leistungskontrollen müssen transparent und rechtlich zulässig sein. Weiterhin muss die Verhältnismäßigkeit gewahrt bleiben.

Der Arbeitgeber kann Beschäftigte dazu verpflichten, handschriftliche Arbeitsberichte zu erstellen. Allerdings hat die Interessenvertretung dann das Recht, den Abschluss einer Betriebs- oder Dienstvereinbarung zu fordern.

Verhaltenskontrollen

Ähnlich wie bei den Leistungskontrollen verhält es sich auch mit den Verhaltenskontrollen. Der Arbeitgeber hat das Recht,

das Verhalten der Beschäftigten zu kontrollieren, sofern es in direktem Bezug zu arbeitsvertraglichen Pflichten steht und verhältnismäßig ist. Verhaltensregeln wie Loyalität, Pünktlichkeit, Ehrlichkeit usw. ergeben sich üblicherweise aus den sogenannten Nebenpflichten, die man als Beschäftigter einzuhalten hat. Sie müssen nicht ausdrücklich im Arbeitsvertrag erwähnt sein und werden es auch üblicherweise nicht, da sie allgemeine Formen der Zusammenarbeit darstellen, die vorausgesetzt werden können.

Der Arbeitgeber kann die Einhaltung eines Rauchverbots kontrollieren, er kann die Sauberkeit des Arbeitsplatzes kontrollieren. Er kann auch die Ehrlichkeit der Beschäftigten kontrollieren, doch wie weit darf er dabei gehen?

Auch bei den Verhaltenskontrollen am Arbeitsplatz gibt es keine verbindliche Liste an zulässigen und unzulässigen Kontrollen. In den meisten Fällen muss die Rechtmäßigkeit vor den Kontrollen überprüft werden um festzustellen, was das höhere Rechtsgut ist - die schutzwürdigen Belange und Persönlichkeitsrechte der Beschäftigten oder das berechtigte Interesse des Arbeitgebers.

Wie bei der Leistungskontrolle muss überprüft werden, ob die Verhaltenskontrolle ein rechtlich zulässiges Ziel hat. Sofern das der Fall ist, müssen Geeignetheit, Erforderlichkeit und die rechtliche Zumutbarkeit überprüft werden. Erst wenn alle Prüfungen mit positivem Ergebnis verlaufen, gilt eine Kontrolle als zulässig.

Diese Prüfung muss vom Arbeitgeber (unaufgefordert) vorgenommen werden, und er muss darstellen, dass es in Abwägung der Umstände rechtlich zulässig ist. Kann er nicht darstellen, dass eine Kontrolle rechtlich zulässig ist, dann ist sie durch die Datenschutzgesetze verboten.

Beispiel: *Taschenkontrollen*

- ***Legalität des Ziels:*** *Der Schutz von Eigentum ist ein legitimes Ziel des Arbeitgebers. Aber in die Persönlichkeitsrechte des Mitarbeiters wird eingegriffen, die Tasche gehört zur Privatsphäre. Da es zwei widersprüchliche Rechtsnormen gibt, muss abgewogen werden.*
- ***Geeignetheit:*** *Taschenkontrollen machen natürlich nur Sinn, wenn*

es nur einen oder wenige Zugänge gibt, die man auch kontrollieren kann. Wird nur an einer Vordertür kontrolliert, nicht aber an einer Hintertür, sind Taschenkontrollen ungeeignet.

- ***Erforderlichkeit:*** *Angesichts der Eingriffe muss es natürlich eine Notwendigkeit geben. Wenn noch nie ein Diebstahl begangen wurde, ist eine Kontrolle aus rein vorsorglichen Gründen nicht rechtmäßig erforderlich. Bei objektiv nachweisbaren Diebstählen in der Vergangenheit sieht das anders aus.*

- ***Verhältnismäßigkeit:*** *Die Kontrollen erfolgen ohne einen zielgerichteten Verdacht. Deshalb ist es unzumutbar, dass jeder Mitarbeiter jedes Mal kontrolliert wird. Aber es ist zumutbar, dass stichprobenartig geprüft wird. Es muss allerdings sichergestellt sein, dass nicht immer dieselben Beschäftigten(-gruppen) kontrolliert werden.*

Was können Interessenvertretungen tun?

Betriebsräte, Personalräte und Mitarbeitervertretungen haben die Aufgabe, die Einhaltung geltenden Rechts zum Schutz der Beschäftigten zu kontrollieren. Hierzu gehört, Auskunft zu verlangen, ob Leistungs- oder Verhaltenskontrollen zulässig sind.

Interessenvertretungen haben in Fragen der Ordnung und des Verhaltens der Mitarbeiter im Betrieb ein Mitbestimmungsrecht. Sie sollten eine Betriebs- oder Dienstvereinbarung abschließen, um bei Verhaltenskontrollen den Schutz der Mitarbeiter sicherzustellen.

Wenn technische Einrichtungen in Betrieb genommen werden sollen, die eine Leistungs- und Verhaltenskontrolle der Beschäftigten ermöglichen (z. B. über Stückzahlen), haben die Interessenvertreter ein starkes Mitbestimmungsrecht.

Handlungsmöglichkeiten als Beschäftigter

Die Zulässigkeit und Zumutbarkeit von Leistungs- und Verhaltenskontrollen ist ein schwieriges Thema. Da es keine konkre-

ten Aussagen gibt, gehen die Meinungen, ob Kontrollen zulässig oder unzumutbar sind, zwischen Arbeitgeber und Beschäftigten weit auseinander.

Als Beschäftigter hat man durch die Datenschutzgesetze das Recht, beim Arbeitgeber eine rechtliche Begründung für persönliche Kontrollen zu verlangen. Wie weit man in der Praxis von diesem Auskunftsrecht Gebrauch machen kann, ohne mit Repressalien rechnen zu müssen, muss jeder selbst abschätzen. Sofern vorhanden, sollte man die Interessenvertretung kontaktieren. Die kann Auskunft verlangen, ohne Benachteiligungen befürchten zu müssen.

Gibt es keinen Betriebsrat, Personalrat oder Mitarbeitervertretung, kann diese Frage auch an den internen Beauftragten für Datenschutz gerichtet werden. Gibt es keinen oder bestehen Zweifel an seiner Aussage, kann man sich auch (anonym) an die Aufsichtsbehörde für den Datenschutz wenden.

Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden.

Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktdaten im Anhang.

Bewerbungsverfahren

Inhalt:

Worum geht es?

Nicht erst im bestehenden Arbeitsverhältnis wirft der Umgang mit personenbezogenen Daten aus Arbeitnehmersicht vielerlei Fragen auf. Auch bereits während der Anbahnung eines Beschäftigungsverhältnisses, also innerhalb eines Bewerbungsverfahrens, sind die Rechtmäßigkeit von Datenauswertungen sowie der Schutz der Persönlichkeitsrechte von Bewerbern oft klärungsbedürftig. Es ergeben sich also auch hier viele Fragen des Datenschutzes. Und zwar zum einen, weil es um teilweise sehr persönliche Dinge geht, die etwa im Rahmen eines Vorstellungsgespräches besprochen werden. Arbeitgeber wollen sichergehen, ob der Bewerber auch wirklich alle Anforderungen der Stelle erfüllen kann, die Bewerber erwarten, dass mit den persönlichen Angaben sensibel umgegangen wird. Die im Bewerbungsverfahren thematisierten Informationen sind schließlich meist in besonderem Maße vertraulich: berufliche Qualifizierung, die schulische, betriebliche oder universitäre Ausbildung, die bisherige berufliche Laufbahn oder auch zahlreiche persönliche Sachverhalte (Familienstand, Charaktermerkmale o.ä.).

Zum anderen ist der Datenschutz auch deshalb von großer Bedeutung, weil in den meisten Unternehmen mittlerweile die Bewerberauswahl mit Unterstützung durch Informations- und Kommunikationstechnik erfolgt. Bewerbungen erfolgen nicht mehr nur auf dem Postweg in schriftlicher Papierform, sondern zunehmend als Online-Bewerbungen (via E-Mail oder über spezielle Bewerbungsverfahren im Internet). Dabei werden personenbezogene Daten

elektronisch erhoben und fließen entsprechend in Dateien beim potenziellen Arbeitgeber zusammen.

Wenn personenbezogene Daten elektronisch gespeichert bzw. verarbeitet werden oder wenn dies in „nichtautomatisierten“ Dateien (z. B. Karteikartensystemen, Personalakten oder systematisierten Listen) erfolgt, gelten die Datenschutzgesetze. Sowohl die Erhebung als auch die Verarbeitung und Nutzung von personenbezogenen Daten ist danach nur eingeschränkt erlaubt. Es gelten im Einzelnen (nach unterschiedlichen Geltungsbereichen)

- das Bundesdatenschutzgesetz (BDSG) für nicht-öffentliche Stellen (privatwirtschaftliche Unternehmen) und Bundesbehörden,

- das Saarländische Datenschutzgesetz (SDSG) für Landesbehörden im Saarland sowie

- spezielle Datenschutzvorschriften für kirchliche Einrichtungen (das Datenschutzgesetz der evangelischen Kirche [DSG-EKD] und die kirchliche Datenschutzordnung der katholischen Kirche [KDO]).

Datenerhebung, -verarbeitung und -nutzung im Bewerbungsverfahren

Die Datenschutzgesetze beschränken den Umgang mit personenbezogenen Daten. Insbesondere gilt: Jede Datenerhebung, -verarbeitung und -nutzung personenbezogener Daten unterliegt dem sogenannten „Verbot mit Erlaubnisvorbehalt“. Demnach ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eigentlich grundsätzlich verboten, jedoch im Ausnahmefall zulässig, wenn entweder

1. (je nach Geltungsbereich) das BDSG, das SDSG, das DSG-EKD oder KDO selbst dieses erlaubt oder
2. eine andere Rechtvorschrift dieses erlaubt oder anordnet oder
3. der Betroffene selbst freiwillig und ausdrücklich eingewilligt hat.

Dies gilt sowohl im Beschäftigungsverhältnis als auch im Bewerbungsverfahren. Wenn ein (potenzieller) Arbeitgeber also Daten seiner Beschäftigten oder von Bewerbern sammeln und elektronisch verarbeiten (und auch auswerten) will, so hat er zunächst einmal das Verbot mit Erlaubnisvorbehalt zu beachten.

Zu den drei Rechtsgrundlagen im Einzelnen:

Das BDSG, das SDSG bzw. das DSG-EKD oder die KDO erlauben Datenerhebungen bzw. -verarbeitungen oder -nutzungen nur im Rahmen der Zweckbestimmung des Arbeitsvertrages (vgl. § 32 Abs. 1 BDSG; § 31 Abs. 1, SDSG; §§ 4 Abs. 1, 5 Abs. 1 DSG-EKD; §§ 9 Abs. 1, 10 Abs.1 KDO). Das heißt, dass eine entsprechende Datenerhebung oder -verarbeitung nur rechtens ist, sofern sie für die Durchführung des Arbeitsverhältnisses zwingend notwendig ist. Auch wenn noch kein Arbeitsvertrag zwischen Arbeitgeber und Bewerber geschlossen wurde (also während des Bewerbungsverfahrens) ist dies so. Das bestehende Verhältnis zwischen beiden wird rein rechtlich gesehen als „vertragsähnliches Vertrauensverhältnis“ bewertet. Die Maßgabe der zwingenden Notwendigkeit der Datenerhebung für die Durchführung des Arbeitsverhältnisses gilt also auch hier. Sprich: Es dürfen nur personenbezogene Daten abgefragt bzw. festgehalten und ausgewertet werden, die für die Durchführung des Arbeitsverhältnisses zwingend von Bedeutung sind. Dies ist maßgeblich, sofern nicht eine andere Rechtsgrundlage besteht.

Eine andere Rechtsgrundlage kann auch eine andere Rechtsvorschrift im Sinne der Datenschutzgesetze sein, zum Beispiel eine Betriebs- oder Dienstvereinbarung. Auch auf deren Grundlage kann eine Datenerhebung oder -verarbeitung also rechtens sein. Jedoch muss die Verhältnismäßigkeit der Datenverarbeitung auch hier gewahrt bleiben. Das heißt, es dürfen keine unverhältnismäßigen Eingriffe in das Persönlichkeitsrecht des Betroffenen unternommen werden.

Problematisch sowohl im Arbeitsverhältnis als auch innerhalb eines Bewerbungsverfahrens ist erfahrungsgemäß die dritte mögliche Rechtsgrundlage, die persönliche Einwilligung. Viele Arbeitgeber verlangen diese von den (im Bewerbungsfall potenziellen) Beschäftigten
um die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten rechtskonform zu gestalten.

Dies ist im Arbeitsverhältnis oder eben auch innerhalb eines Bewerbungsverfahrens jedoch nicht ohne Weiteres möglich. Grundlegend für die rechtmäßige Daten-

erhebung auf der Grundlage einer persönlichen Einwilligung ist nämlich deren Freiwilligkeit. Aufgrund des sowohl im Beschäftigungsverhältnis als auch im Bewerbungsverfahren bestehenden Abhängigkeitsverhältnisses zum (potenziellen) Arbeitgeber ist es nämlich mehr als fraglich, ob eine solche Freiwilligkeit überhaupt bestehen kann. Die Rechtsprechung ist sich hierüber keinesfalls einig – eine Mehrzahl von Juristen geht davon aus, dass eine Freiwilligkeit nur dann bestehen kann, wenn im Rahmen der Entscheidung (pro/contra Einwilligung zur Datenverarbeitung) aus Sicht des Betroffenen eindeutig keine negativen Konsequenzen zu erwarten sind.

Auf jeden Fall gilt: Geht man davon aus, dass es auch im Beschäftigungsverhältnis (bzw. im Bewerbungsverfahren) freiwillige Einverständnisse geben kann, so sind bestimmte Anforderungen an eine freiwillige Einverständniserklärung (zur Erhebung und Verarbeitung personenbezogener Daten) zu stellen.

Eine Einwilligung ist gemäß der Datenschutzgesetze nur wirksam, wenn sie – wie beschrieben – freiwillig erfolgt und

- der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung und Nutzung hingewiesen wurde,
- der Betroffene auf die Folgen der Verweigerung einer Einwilligung hingewiesen wurde,
- die Einwilligung schriftlich erfolgt (sofern nicht wegen besonderer Umstände eine andere Form angemessen erscheint),
- sofern sie gemeinsam mit anderen Erklärungen erfolgt, sie besonders hervorgehoben wurde und
- sofern sie besondere Formen personenbezogener Daten (ethnische Herkunft, Gewerkschaftszugehörigkeit, Sexualleben) betrifft, diese Daten konkret genannt werden.

Darüber hinaus ist eine Einwilligung dann unwirksam, wenn sie sich über ein gesetzliches Verbot hinwegsetzt. So ist eine Datenerhebung verboten, wenn sie die Grenzen des Fragerechts z. B. bei Bewerbungsgesprächen überschreitet. Die Frage nach der Schwangerschaft oder dem Kinderwunsch einer Bewerberin ist beispielsweise unzulässig und das auch, weil es eine diskriminierende Frage ist, die dem Allgemeinen Gleichstellungsgesetz (AGG)

widerspricht. Auch ein freiwilliges Einverständnis der Bewerberin kann diese Unzulässigkeit nicht unwirksam machen.

Ebenso darf der (zukünftige) Arbeitgeber nicht verlangen, dass der Bewerber seinen Arzt „freiwillig“ von der Schweigepflicht entbindet, um entsprechende Auskünfte über dessen Gesundheitszustand zu geben.

Besondere personenbezogene Daten

Insbesondere wenn Daten „besonderer Art“ erhoben, verarbeitet oder genutzt werden sollen, wird durch die Datenschutzgesetzgebung ein besonderes Maß an Schutz eingeräumt (vgl. § 3 Abs. 9 BDSG; § 4 Abs. 2 SDSG; § 2 Abs. 11 DSG-EKD; § 2 Abs. 10 KDO).

Zu diesen Daten gehören Angaben über:

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit,
- Sexualleben.

Sowohl im Bewerbungsverfahren als auch im Arbeitsverhältnis sind der Erhebung, Verarbeitung und Nutzung besonderer personenbezogener Daten sehr enge Grenzen gesetzt. Demnach ist dies nur erlaubt, wenn (vgl. § 13 Abs. 2 BDSG; § 4 Abs. 2 SDSG; § 5 Abs. 5 DSG-EKD; § 9 Abs. 5 KDO):

- dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, und
- wenn der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, selbst seine Einwilligung zu geben (was etwa im Rahmen von Unfallbehandlungen zutreffen könnte)
- wenn es sich um Daten handelt, die der Betroffene selbst bereits offenkundig bekannt gemacht hat (z. B. wenn sie bereits auf einer persönlichen Website stehen);
- wenn die Datennutzung erforderlich ist, um rechtliche Ansprüche (z. B. im Rahmen eines Arbeitsvertrags) geltend zu machen, sie auszuüben oder zu verteidigen – das gilt allerdings nur dann, wenn es keinen Grund gibt anzunehmen, dass das Interesse des

Betroffenen an einer Nichtverwendung seiner Daten schwerer wiegt als die mit ihrer Nutzung verbundenen Interessen,

- wenn die Datennutzung zur Durchführung wissenschaftlicher Forschung erforderlich und auch alternativlos ist.

Im Zusammenhang mit der Datenverarbeitung im Rahmen eines Beschäftigungsverhältnisses kann lediglich die Datennutzung zur Erfüllung rechtlicher Ansprüche zum Tragen kommen. Ein solcher Anspruch kann sich dann aus einem Gesetz, einer Gerichtsentscheidung oder einem (Arbeits-) Vertrag herleiten.

Recherchen des Arbeitgebers im Internet und in sozialen Netzwerken

Heute ist es fast schon gängige Praxis, dass Personalverantwortliche innerhalb von Personalauswahlverfahren Informationen über Bewerber aus dem Internet (z. B. über Suchmaschinen) und den sozialen Netzwerken (z. B. Facebook, Wer-kennt-Wen, XING) sichten und für ihre Entscheidungen heranziehen.

Dies ist auf der Grundlage der Datenschutzgesetzgebung ohne Einverständnis des Betroffenen nicht erlaubt. Bei einer Recherche ohne Kenntnis des Betroffenen ist nämlich zu beachten: Nach den Datenschutzgesetzen ist eine Datenerhebung, -nutzung oder -verarbeitung grundsätzlich nur erlaubt, wenn sie unmittelbar beim Betroffenen und mit dessen Wissen erfolgt (Grundsatz der Direkterhebung gemäß § 4 Abs. 2 BDSG; § 12 Abs. 1 SDSG; § 4 Abs. 2 DSG-EKD; § 9 Abs. 2 KDO).

Abweichungen hiervon sind lediglich gestattet, wenn die Persönlichkeitsrechte und schutzwürdigen Interessen des Betroffenen nicht tangiert werden. Dies ist angesichts eines (in Aussicht stehenden) Beschäftigungsverhältnisses sicher nicht der Fall. Insbesondere auch angesichts der Tatsache, dass Informationen aus dem Internet (die vielleicht auch z. B. von Dritten erstellt wurden) kein verlässliches und schon gar kein vollumfängliches Bild über einen Beschäftigten oder einen Bewerber liefern.

Einzige legale Ausnahme stellen Bewerber-Recherchen in Netzwerken dar, die vordergründig der Arbeitsvermittlung dienen (z. B. XING, monster.de, stepstone.de). Dort wurden die Daten von dem Betroffenen selbst zu dem Zweck einge-

stellt, Arbeit- und Auftraggebern Informationen über die eigene Person an die Hand zu geben.

Außerdem gilt: Im Beschäftigungsverhältnis (im Bewerbungsverfahren gilt dies auch) ist eine Datenerhebung oder -verarbeitung und -nutzung nur erlaubt, wenn sie maßgeblich ist für die Durchführung des Beschäftigungsverhältnisses bzw. für die Erfüllung der Aufgaben der Dienststelle ist (vgl. § 32 Abs. 1 BDSG; § 31 Abs. 1 SDSG; §§ 4 Abs. 1, 5 Abs. 1 DSG-EKD; §§ 9 Abs. 1, 10 Abs. 1 KDO). Dies ist bei einer Internet-Recherche in der Regel nicht der Fall. Eine Ausnahme besteht nur, wenn der Bewerber innerhalb seiner Bewerbung selbst auf bestimmte Internetseiten verwiesen hat.

Problematisch bleibt die Frage, inwiefern sich Recherchen über Bewerber im Internet wirklich verhindern lassen. Im Regelfall wird kein Personalverantwortlicher seine Ablehnung einer Bewerbung mit Ergebnissen aus einer Online-Recherche begründen. Daher ist es insbesondere von Bedeutung, dass Betroffene sich bereits vor der Bewerbung darüber bewusst sind, was über sie im Internet zu recherchieren ist und wie freizügig sie gegebenenfalls mit persönlichen Informationen im Internet umgehen.

Arbeitgeberfragerecht

Neben den Datenschutzgesetzen (BDSG, SDSG, DSG-EKD oder KDO) ist insbesondere das Arbeitgeberfragerecht von zentraler Bedeutung bei der Datenerhebung im Rahmen von Bewerbungen und Einstellungen. Dieses Fragerecht leitet sich aus Gesetzen (Datenschutzgesetze, Bürgerliches Gesetzbuch [BGB], Allgemeines Gleichstellungsgesetz [AGG] u.a.), aber auch aus richterlichen Entscheidungen und Grundsatzurteilen ab. Insbesondere das Grundrecht auf den individuellen Schutz der Persönlichkeitsrechte spielt dabei eine wichtige Rolle. Demnach sind dem Recht des Arbeitgebers, Fragen an den Bewerber bzw. dem Beschäftigten zu stellen, enge Grenzen gesetzt. Diese sollen insbesondere einen Schutz innerhalb der besonderen Zwangssituation bieten, in der sich vor allem der Bewerber um einen Arbeitsplatz befindet. Denn: Das Angewiesensein auf einen Arbeitsplatz lässt dem Bewerber eigentlich keine Wahlfreiheit. Verweigert er die Beantwortung einer Frage, so läuft er Gefahr, schon aus diesem Grund nicht eingestellt zu werden.

Es gilt also zu verhindern, dass die Zwangssituation einen Befragten veranlasst, auf Fragen einzugehen, die dem Respekt gegenüber seiner Person, also insbesondere seinem Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung entgegenstehen.

Deshalb gesteht das Bundesarbeitsgericht (BAG) dem Arbeitgeber nur dann ein Fragerecht zu, wenn er ein „berechtigtes, billigenswertes und schutzwürdiges Interesse" an der Beantwortung dieser Frage hat. Dies heißt konkret, dass sich die Fragen auf Informationen beschränken müssen, die einen unmittelbaren Bezug zum (zukünftigen) Arbeitsverhältnis haben. Dabei ist jedes Überschreiten der Grenzen des Fragerechts rechtswidrig – nicht einmal eine eventuelle Zustimmung des Betriebsrats könnte daran etwas ändern. In dieser Situation billigt das BAG den Befragten das Recht ein zu lügen.
Auch eine Verpflichtung, bestimmte Informationen von sich aus (also ohne eine entsprechende Frage des Arbeitgebers) mitzuteilen, kann es nur ausnahmsweise geben. Zum Beispiel dann, wenn ein Bewerber oder Arbeitnehmer eine angebotene Arbeit gar nicht erledigen könnte, oder wenn er erkennen muss, dass bei ihm etwas vorliegt (z.B. eine spezielle Allergie), was für den vorgesehenen Arbeitsplatz von ausschlaggebender Bedeutung ist.

Zusammenfassend lässt sich sagen, dass in Bewerbungsgesprächen nur Fragen gestellt werden dürfen, die mit dem Arbeitsplatz und der zu leistenden Arbeit in Zusammenhang stehen. Es kommt also auf den Einzelfall an:

- Die Frage nach geplanter Eheschließung oder Kinderwunsch ist unzulässig. Der Europäische Gerichtshof (EuGH) sieht hierin eine Diskriminierung nach dem Geschlecht (EuGH vom 08.11.1990 – Rs. 177/88)
- Unzulässig ist die Frage nach einer bestehenden Schwangerschaft.
- Die Frage nach der Schwerbehinderteneigenschaft ist erlaubt, aufgrund der Rechtsfolgen für den Arbeitgeber aus dem Sozialgesetzbuch (SGB) IX, die dem Arbeitgeber umfangreiche Pflichten auferlegen.
- Die Frage nach einer Behinderung ohne Anerkennung oder Gleichstellung gemäß SGB IX ist nur erlaubt,

sofern aufgrund der Behinderung eine Erbringung der arbeitsvertraglich geschuldeten Leistung nicht möglich ist (Bundesarbeitsgericht (BAG) vom 05.10.1995 – 2 AZR 923/94).

- Die Frage nach Erkrankungen ist ebenfalls zulässig, wenn die Tätigkeit beeinträchtigt oder unmöglich wird. Dies betrifft nicht nur Fragen, die die konkrete Tätigkeit beeinflussen, sondern auch Fragen nach schweren oder chronischen Erkrankungen in den letzten zwei Jahren, sofern sie die arbeitsvertraglich zugesicherte Leistung gefährden.
- Die Frage nach einer Mitgliedschaft in einer politischen Partei oder einer Gewerkschaft ist unzulässig, es sei denn man bewirbt sich um eine Anstellung bei einer Partei oder Gewerkschaft.
- Auch die Mitgliedschaft in einer Religionsgemeinschaft darf nur abgefragt werden, wenn es um eine Anstellung bei einer solchen geht.
- Die Frage nach Vermögensverhältnissen (Schulden, Lohnpfändungen) sind nur bei leitenden Angestellten und Angestellten, die in einem besonderen Vertrauensverhältnis zum Arbeitgeber stehen, erlaubt.
- Die Frage nach Vorstrafen ist nur erlaubt, wenn sie in einem engen Bezug zur Tätigkeit stehen (z. B. bei Betrug, Diebstahl oder Unterschlagung im Zusammenhang mit der Tätigkeit als Kassierer, Buchhalter, Geldtransportfahrer o.ä.).

Handlungsmöglichkeiten als Bewerber

Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden. Kontaktdaten im Anhang.

Gesundheitsdaten im Betrieb

Inhalt:

Eines der kritischsten Themen ist der korrekte Umgang mit Angaben über Gesundheit und Krankheit von Beschäftigten. Der Schaden, der den Betroffenen daraus erwachsen kann, ist außerordentlich groß. Das Bekanntwerden einer psychischen oder Suchterkrankung stellt oft die Weichen dafür, wie sich der berufliche Werdegang gestalten wird - im positiven wie im negativen Sinn. Es kann Ausgrenzung und ein Karrierestopp zur Folge haben. Andererseits sind Angaben zu Krankheit und Gesundheit im Arbeitsleben nicht nur zu Abrechnungszwecken notwendig. Sie sind auch sinnvoll, um gesunde Arbeitsbedingungen zu gestalten und um ein betriebliches Eingliederungsmanagement von Langzeiterkrankten vornehmen zu können. Damit stellt sich die Frage:

Welche Informationen zu Gesundheit und Krankheit von Beschäftigten darf der Arbeitgeber sammeln und verwerten?

und

Welchen Einfluss hat man als Beschäftigter, Kontrolle über diese Verfahren zu behalten?

Wo fallen Gesundheitsdaten am Arbeitsplatz an?

Man muss sich zunächst darüber klar werden, wo überall am Arbeitsplatz Gesundheits- bzw. Krankheitsdaten anfallen (können):

Personalbereich/Personalakte

- Krank- und Unfallmeldungen
- (Fach-)Arztangabe auf der AU-Bescheinigung
- Informationsabfragen im Rahmen von Krankengeldbezug (z. B. Psychosozialer Dienst der Krankenkassen)
- Ärztliche Atteste
- Krankheitszeiten
- Durchgeführte und angebotene BEM-Verfahren
- Berufskrankheitsverfahren
- Schwerbehindertenstatus, Erwerbsminderungsstatus
- Betriebliche Gesundheitsberichterstattung
- AU-Daten-Analysen der Krankenkassen
- Mitarbeiterbefragungen (psychische Belastungen)
- (Nicht-)Teilnehmer von Präventionskursen

Medizinische Untersuchungen

- Einstellungsuntersuchungen
- arbeitsmedizinische Eignungsuntersuchungen
- Drogenscreenings
- Arbeitsmedizinische Vorsorgeuntersuchungen
- Betriebsärztliche Versorgung

Sozialer Arbeitsschutz

- Meldepflicht bei Mutterschutz
- Gefährdungsbeurteilungen

Betriebliches Gesundheitsmanagement

- Arbeitsschutz, Erste Hilfe, Verbandbuch
- Betriebliche Gesundheitsförderung
- Krankenrückkehrgespräche
- Betriebliches Eingliederungsmanagement

…

Diese Liste gibt nur eine Auswahl der Daten wieder, die im beruflichen Umfeld über den Gesundheits-/Krankheitszustand von Beschäftigten direkt oder indirekt Auskunft geben.

Hinweis:

In § 32 Bundesdatenschutzgesetz wird dargestellt, dass es im Hinblick auf den Datenschutz keine Rolle spielt, ob Gesundheits-/Krankheitsdaten von Beschäftigten in elektronischer Form vorliegen oder als Papier. Ausschlaggebend ist nur, dass es sich um Angaben handelt, die sich direkt oder auch über Zuhilfenahme anderer Daten auf einen einzelnen Menschen beziehen.

§ 32 BDSG ist sinngemäß auch auf den Geltungsbereich von SDSG, KDO und DSG-EKD anzuwenden, da es sich um einen relativ neuen Paragraphen handelt und es keine Schlechterstellung durch die übrigen Datenschutzgesetze geben darf.

Hohes Missbrauchsrisiko bei Vorsatz und Nachlässigkeit

Gesundheitsdaten bergen ein hohes Missbrauchs- und Schadensrisiko, denn sie lassen sich auch zu unlauteren Zwecken verwenden:

- Bei welchem Mitarbeiter sind „Montags- oder Freitagserkrankungen“ häufig?
- Wer ist häufig krank, bringt dadurch weniger Leistung und verursacht Kosten durch Ausfall und Entgeltfortzahlung?
- Welche Mitarbeiter leiden unter einem Belastungssyndrom und kommen für verantwortungsvolle Aufgaben oder als Führungskraft nicht mehr in Frage?
- Bei welchen Mitarbeitern lohnt es nicht, eine betriebliche Weiterbildung zu finanzieren, weil sie schwer erkrankt sind und es sich „nicht mehr rechnet“?

Solche Auswüchse darf es nicht geben, doch es ist nicht immer einfach, das zu verhindern. Unter dem Deckmantel der Fürsorgepflicht des Arbeitgebers wurden Führungskräfte eines bekannten deutschen Discounters angehalten „Krankenrückkehrgespräche“ zu führen. In einem vorgeblich vertraulichen Gespräch wurden den Mitarbeitern persönliche Informationen über ihre Erkrankungen entlockt, die

einem Arbeitgeber von Rechts wegen nicht zustehen. Diese Angaben wurden systematisch dokumentiert und ausgewertet für „Personalplanungen“. Welcher Mitarbeiter hat den Mut, einen Vorgesetzten vor den Kopf zu stoßen, der einen nach einer Erkrankung mit den freundlichen Worten begrüßt: „Schön dass es Ihnen wieder besser geht. Können wir etwas für Sie tun? Was hatten Sie denn überhaupt?“

Aber auch ohne kriminelle Energie kann durch bloße Nachlässigkeit bereits ein irreparabler Schaden für Mitarbeiter entstehen. Krankmeldungen (Krankenscheine) für den Arbeitgeber werden ohne Diagnose erstellt, um Missbrauch vorzubeugen. Allerdings sind immer die Anschrift und die Unterschrift des Arztes angegeben. Das Schadenspotenzial ist bereits dadurch gegeben, wenn die Krankmeldung von einem Arzt für Onkologie oder Psychiatrie ausgestellt worden ist.

Hinweis:

> *Krankmeldungen, Atteste, Ergebnisse arbeitsmedizinischer Untersuchungen o. ä. müssen **immer** vor der Einsicht unbefugter Dritter geschützt werden und gehören bei der Übermittlung in verschlossene Umschläge.*

Das Dilemma mit den Gesundheitsdaten am Arbeitsplatz

Das Thema Gesundheits-/Krankheitsdaten ist in sich bereits widersprüchlich. Einerseits gilt es, die Rechte der Beschäftigten auf Privat- und Intimsphäre zu wahren - eine einmalige Erkrankung darf nicht zum dauerhaften Karrierehindernis werden.

Andererseits muss man auch zugestehen, dass ein Arbeitgeber seine Fürsorgepflicht den Beschäftigten gegenüber nur in angemessener Form wahrnehmen kann, wenn er über konkrete Informationen zu den Gefährdungen der einzelnen Arbeitsplätze verfügt. Angesichts des hohen Anteils von psychischen Erkrankungen ist es wichtig auch den Aspekt der psychischen Belastungen zu betrachten, um wirksame Gegenmaßnahmen treffen zu können. Herauskommen können allerdings auch sehr brisante Informationen über Mitarbeiter, die diesen Gefährdungen ausgesetzt sind.

Der Umgang mit Angaben zu Gesundheit und Krankheit ist eine verantwortungsvolle Aufgabe, die stellenweise unumgänglich ist - ohne Krankmeldung kann auch keine Entgeltfortzahlung erfolgen werden. Insofern ist es nicht weiter verwunderlich, dass der Umgang mit Angaben zu Gesundheit und Krankheit vom Gesetzgeber stark reglementiert ist.

Rechtlicher Hintergrund

1. Erhebung und Verarbeitung von Gesundheits- und Krankheitsdaten aufgrund von Rechtsvorschriften

Eine Vielzahl von Verfahren, für die Angaben über Gesundheit und Krankheit erhoben werden müssen, ist durch den Gesetzgeber vorgegeben. Am bekanntesten ist das Verfahren der Krankmeldung, das in § 5 Entgeltfortzahlungsgesetz (EntgFG) geregelt ist. Bekannt ist auch das sogenannte Betriebliche Eingliederungsmanagement (BEM) von Langzeiterkrankten nach § 84 Abs. 2 SGB IX oder das Mutterschutzgesetz (MuSchG). Darin wird in § 5 MuSchG festgelegt, welche Informationen der Arbeitgeber von der Mitarbeiterin erhalten muss und wofür er sie - ganz konkret - verwenden darf.

Es ist leider nicht möglich, alle Gesetze und Verordnungen aufzulisten, die als Rechtsgrundlage dienen, um Gesundheits- oder Krankheitsdaten von Beschäftigten zu erheben oder zu verarbeiten. Allein die vorgeschriebenen arbeitsmedizinischen Untersuchungen für Beschäftigte aufzulisten, würde den Rahmen sprengen. Das ist allerdings (aus Beschäftigtensicht) kein großes Problem. Denn der Arbeitgeber, der die Gesundheits- oder Krankheitsdaten erheben und verarbeiten will, kann das nur tun, wenn er dazu eine rechtskräftige Erlaubnis hat. Mehr dazu in den Handlungshinweisen.

2. Erhebung und Verarbeitung von Gesundheits- und Krankheitsdaten aufgrund von Datenschutzgesetzen

Sofern es keine konkreten Gesetze, Verordnungen oder andere Rechtsvorschriften gibt, die den Umgang mit Gesundheits- bzw. Krankheitsdaten anordnen oder ermöglichen, gelten die Datenschutzgesetze (quasi als rechtliches Auffangbecken).

Bei Angaben zu Gesundheit und Krankheit von Beschäftigten handelt es sich um sogenannte personenbezogene Angaben. In den Datenschutzgesetzen wird die Verarbeitung von personenbezogenen Daten (§ 4 BDSG, § 4, SDSG, § 4 DSG-EKD, § 3 KDO geregelt.

Grundsätzlich ist die Erhebung und Verwendung von personenbezogenen Angaben von Mitarbeitern nur zulässig, solange sie für das Eingehen, Durchführen oder Beendigen eines Arbeitsverhältnisses rechtlich erforderlich sind (§ 32 BDSG, § 31 SDSG, § 24 DSG-EKD). Und: Die Verwendung der Daten ist an diesen Zweck gebunden.

Hinweis:

Für die Mitarbeiter der öffentlichen Einrichtungen des Saarlandes, der Landkreise und Kommunen stellt das Saarländische Datenschutzgesetz (SDSG) in § 4 Abs. 2 klar, dass besondere Arten personenbezogener Daten (z. B. Gesundheit oder Krankheit) nur aufgrund einer besonderen Rechtsvorschrift zulässig ist. Das muss die Dienststellenleitung nachweisen können.

Besondere Arten von personenbezogenen Daten

Für die Erhebung und Verarbeitung von Beschäftigtendaten zu Krankheit und Gesundheit kommt noch eine Besonderheit hinzu. Bei dieser Art von Angaben handelt es sich um sogenannte „besondere Arten von personenbezogenen Daten“ (§ 3 Abs. 9 BDSG, § 2 Abs. 11 DSG-EKD, § 2 Abs. 2 KDO).

Mit dem Begriff „besondere Arten personenbezogener Daten“ schaffen die Datenschutzgesetze eine Gruppe von besonders sensiblen Angaben, für deren Verwendung ganz besondere Einschränkungen und Auflagen gelten. Werden diese Daten elektronisch verarbeitet, muss z. B. eine Vorabkontrolle durch den Datenschutzbeauftragten stattfinden.

Problemfall: Freiwilliges Einverständnis in der Regel unzulässig

Leider ist dieses Phänomen in der Praxis häufig anzutreffen: Beschäftigte werden

angefragt, ob sie damit einverstanden sind freiwillig Fragen zu ihrer Gesundheit zu beantworten oder Gesundheitsdaten, die zu gesetzlich vorgeschriebenen Zwecken erhoben werden, auch zu anderen betriebsinternen Zwecken verwenden zu dürfen.

Natürlich ist ein solches Ansinnen unmoralisch - kaum ein Arbeitnehmer kann sich einer solchen Aufforderung praktisch entziehen - aber ist sie deshalb auch unzulässig? Davon ist auszugehen. Die Aufsichtsbehörden für den Datenschutz veranlassen regelmäßig, dass solche Verfahren eingestellt werden. Sie begründen es damit, dass nicht glaubhaft nachgewiesen werden kann, dass ein solches Einverständnis zur Preisgabe intimer Angaben ohne Gegenleistung freiwillig zustande gekommen ist.

Hinweis:

> ***Krankenkassenbescheinigungen im Bewerbungsverfahren***
>
> *Eine Einrichtung hatte es sich zur Praxis gemacht, Bewerber aufzufordern, Bescheinigungen ihrer Krankenkassen vorzulegen, die die Krankheitstage der vergangenen 3 Jahre verbindlich ausweisen.*
>
> *Es wurde festgestellt, dass keine Rechtsgrundlage für die Erhebung solcher Daten vorlag. Die zuständige Aufsichtsbehörde für den Datenschutz (der hamburgische Beauftragte für Datenschutz und Informationsfreiheit Prof. Johannes Caspar) hat diese Praxis folgerichtig untersagt.*
>
> Quelle: 22. Tätigkeitsbericht 2008/2009 HmbBfDI

Freiwillige Einwilligungen von Beschäftigten in die Erhebung und Verarbeitung von Gesundheits- /Krankheitsdaten sind in der Regel unzulässig. Auch aus organisatorischen Gründen ist dieses Prinzip ungeeignet, da solche Einverständniserklärungen jederzeit und ohne Begründung widerrufen werden können. Verfahren, die darauf aufbauen, sind nicht belastbar.

Problemlösung: Gefährdungsbeurteilungen

Es gibt eine Reihe gesetzlicher und tariflicher Möglichkeiten, die eine Erhebung und Verarbeitung von Gesundheits- und

Krankheitsdaten im Betrieb regeln. Die Vermeidung von krankheitsbedingten Ausfällen ist schließlich ein Ziel, das sowohl Arbeitgeber, Interessenvertreter, Gewerkschaften, Sozialversicherungen und auch die Mitarbeiter teilen. Die Methoden, dieses Ziel zu erreichen, müssen jedoch - aus Datenschutzsicht - zulässig, angemessen und verhältnismäßig sein.

Wichtiges Instrument zur Gestaltung „gesunder“ Arbeitsplätze sind Gefährdungsbeurteilungen, die auch psychische Belastungen zum Gegenstand haben können. Diese Verfahren bewegen sich auf einer rechtlichen Grundlage (§ 5 Arbeitsschutzgesetz infolge der Umsetzung europäischer Rahmenrichtlinien zum Arbeitsschutz (1992), § 3 Betriebssicherheitsverordnung, § 6 Gefahrstoffverordnung), unterliegen der Mitbestimmung durch die Interessenvertreter und die hierbei anfallenden Daten haben eine klare Zweckbindung.

Praxisfälle:

Krankmeldung, Kranken- und Abwesenheitslisten

Ungeachtet der rechtlichen Grundlagen ist die Personaleinsatzplanung ein wichtiges Thema. Hierzu ist es natürlich wichtig zu wissen, welcher Mitarbeiter nicht eingesetzt werden kann, weil er erkrankt ist, an einer Reha-Maßnahme teilnimmt oder in Kur ist. Das bereits erwähnte Entgeltfortzahlungsgesetz verpflichtet Mitarbeiter dazu, krankheitsbedingte Ausfälle unverzüglich zu melden.

Auch bei einer telefonischen Krankmeldung ist man als Mitarbeiter nicht verpflichtet, Auskunft über die Erkrankung zu geben, sondern lediglich über die voraussichtliche Dauer der Erkrankung. Dauert die Arbeitsunfähigkeit länger als drei Kalendertage, hat der Arbeitnehmer eine ärztliche Bescheinigung über das Bestehen der Arbeitsunfähigkeit sowie deren voraussichtliche Dauer spätestens an dem darauffolgenden Arbeitstag vorzulegen. Der Arbeitgeber ist berechtigt, die Vorlage der ärztlichen Bescheinigung früher zu verlangen (EntgFG). Der Zweck der Krankmeldung ist eindeutig. Er dient sowohl der Personalabrechnung als auch der Personaleinsatzplanung. Allerdings gibt es einen gravierenden Unterschied. Für die Personaleinsatzplanung ist es völlig unerheblich, aus welchem Grund der Mitarbeiter nicht verfügbar ist - ob ein Mitarbeiter aus Krankheit fehlt oder wegen

eines Trauerfalls, ist letztlich egal. Entscheidend ist lediglich die voraussichtliche Dauer der Abwesenheit. Insofern ist es absolut unnötig und unzulässig, dass die Personaleinsatzplanung den Grund der Abwesenheit erfährt.

Gruppenkalender, Schichtpläne oder Dienstpläne (außerhalb der Personalabrechnung) dürfen keine Angaben über krankheitsbedingte Ausfälle von Mitarbeitern enthalten. Es ist für Mitarbeiter der Personaleinsatzplanung, Teamleiter und Linienvorgesetzte auch nicht zulässig, Krankenlisten von Mitarbeitern zu führen, da hierzu keine Rechtsgrundlage besteht.

Anders sieht das aus im Bereich der Personalverwaltung (Personalabrechnung und Personalaktenführung). Dort müssen die Krankmeldungen für Abrechnungs- und Dokumentationszwecke verarbeitet werden. Es muss weiterhin die Anzahl der Krankentage pro Mitarbeiter über die Dauer der letzten zwölf Monate summiert werden, um den gesetzlichen Anforderungen aus § 84 Abs. 2 SGB IX zum betrieblichen Eingliederungsmanagement nachkommen zu können. Da es sich bei alldem um besonders sensible Daten handelt, müssen alle notwendigen technischen und organisatorischen Maßnahmen ergriffen werden, dass diese Informationen nur für den engsten Kreis der Mitarbeiter aus der Personalverwaltung zugänglich sind.

Betriebsärztliche und amtsärztliche Untersuchungen

Für eine Reihe von Tätigkeiten oder den Umgang mit bestimmten Stoffen schreiben Gesetze und Verordnungen Eignungsuntersuchungen vor z. B.

- Eignung für Fahr-, Steuer- und Überwachungstätigkeiten
- Untersuchungen nach dem Jugendarbeitsschutzgesetz
- Eignung für Nacht- und Schichtarbeit
- Einstellungs- und Tauglichkeitsuntersuchungen für besondere Tätigkeiten (Höhentauglichkeit, Tragen von Atemschutz etc.)

Es gibt eine Vielzahl von arbeitsmedizinischen Untersuchungen. Aus Sicht des Datenschutzes ist allerdings weniger der Untersuchungsgegenstand zu betrachten

als vielmehr die Fragen, welche Untersuchungen verpflichtend sind und wer die anfallenden Daten zu welchen Zwecken verwenden darf.

Die angesprochene Vielzahl von arbeitsmedizinischen Untersuchungen unterscheidet sich in Angebots- und Pflichtuntersuchungen. Der Mitarbeiter kann Angebotsuntersuchungen ablehnen, Pflichtuntersuchungen hingegen nicht, da sie durch eine Rechtsnorm veranlasst werden. Bei Pflichtuntersuchungen kann er sich jedoch für einen anderen Arzt entscheiden als für den, den der Arbeitgeber vorschlägt.

Bei der arbeitsmedizinischen Untersuchungen ist der Arzt an die Schweigepflicht gebunden. Auch wenn es sich um einen Werksarzt handelt, der vom gleichen Arbeitgeber bezahlt wird, darf er keine gesundheitlichen Auskünfte über den untersuchten Mitarbeiter an den Arbeitgeber weitergeben.

Allerdings ist er verpflichtet, das Ergebnis einer Pflichtuntersuchung weiterzuleiten. Darin sind Name des Arztes, Name des Untersuchten, der Zeitpunkt der Untersuchung, die Art der Untersuchung und das abschließende Ergebnis enthalten.

Das kann z. B. in der Form erfolgen, dass berichtet wird, dass der zu einem bestimmten Datum untersuchte Mitarbeiter entsprechend der Pflichtuntersuchung G25 für Fahr- Steuer und Überwachungstätigkeiten geeignet ist. Mehr jedoch nicht.

Diese Angaben erhält der Arbeitgeber zum Führen einer Vorsorgekartei und um nachzuweisen, dass er seinen gesetzlichen Verpflichtungen nachkommt. Damit ist der Verwendungszweck allerdings festgelegt. Eine Verwendung für andere (personelle) Zwecke ist unzulässig und strafbar.

Es ist nicht zulässig, Mitarbeiter zu Angebotsuntersuchungen zu drängen und die dabei entstehenden Angaben für „betriebliche“ Zwecke zu verwenden. Das Wahrnehmen von Angebotsuntersuchungen und die Entscheidung des Mitarbeiters, ob er den Arbeitgeber über das Ergebnis informieren möchte, bleibt ihm überlassen - außer, der Arzt erkennt Anhaltspunkte für unzureichende Schutzmaßnahmen (z. B. hohe Konzentration von gefährlichen Stoffen), dann muss er dies dem Arbeitgeber mitteilen und entsprechende Schutzmaßnahmen vorschlagen.

Betriebliches Eingliederungsmanagement

Das betriebliche Eingliederungsmanagement (kurz BEM) wurde in seiner gesetzlichen Form (§ 84 Abs. 2 SGB IX) geschaffen, um Mitarbeitern mit schweren Erkrankungen den Wiedereinstieg und die Weiterbeschäftigung zu ermöglichen. Das BEM hat die, sich in einer rechtlichen Grauzone bewegenden, Krankenrückkehrgespräche weitgehend ersetzt.

Vereinfacht dargestellt, soll Mitarbeitern, die über einen Zeitraum von zwölf Monaten sechs Wochen oder länger erkrankt waren, ein Gespräch angeboten werden, um die Krankheitsursachen zu erfahren und Maßnahmen zu ergreifen, die den Wiedereinstieg erleichtern und helfen künftige Erkrankungen zu vermeiden.

Tatsächlich ist dieses Verfahren aber umfangreicher. Die Arbeitsgerichte haben festgestellt, dass es nicht damit getan ist, einem betroffenen Mitarbeiter ein Gesprächsangebot zu unterbreiten. Es gibt Mindeststandards an ein solches Verfahren.

Doch ungeachtet des eigentlichen Zwecks ist das BEM datenschutzrechtlich äußerst brisant: Nimmt man als erkrankter Mitarbeiter die Chancen des betrieblichen Eingliederungsmanagements wahr, offenbart man den beteiligten Personen am Verfahren intimste Informationen (z. B. eine psychische Erkrankung, Krebs etc.). Auch wenn sie zum Schweigen verpflichtet sind, es handelt sich um Kollegen und Verantwortliche, mit denen man am Arbeitsplatz tagtäglich umgeht. Akten und Daten lassen sich löschen - für das Gedächtnis der Verantwortlichen trifft das nicht zu.

Deshalb: Es müssen alle datenschutzrechtlichen Maßnahmen ergriffen werden, damit ein erkrankter Mitarbeiter Vertrauen fassen und seine Chance auf Eingliederung wahrnehmen kann.

Die Beteiligten am BEM-Verfahren müssen sorgfältig ausgewählt und zur Verschwiegenheit verpflichtet werden.

Nicht nur der Ablauf des BEM-Verfahrens muss - in der Regel als Betriebs- oder Dienstvereinbarung - festgelegt werden, es muss auch eine datenschutzrechtliche Verfahrensbeschreibung geben:

- Welche Informationen werden erhoben?

- Wer erhebt die Informationen, wer darf sie lesen und bearbeiten?
- Wo werden die BEM-Unterlagen aufbewahrt?
- Wie wird sichergestellt, dass die Unterlagen vor unbefugter Kenntnisnahme, Manipulation, Diebstahl und Weitergabe gesichert sind? Und wie wird gewährleistet, dass die Angaben nur zu den gesetzlich zulässigen Zwecken verwendet werden.
- Wann, wie und von wem werden welche BEM-Unterlagen vernichtet?

Der Arbeitgeber als verantwortliche Stelle im Sinne der Datenschutzgesetze hat dafür zu sorgen, dass diese Vorgaben eingehalten werden.

Dennoch hat man als Mitarbeiter das ausdrückliche Recht das BEM abzulehnen oder abzubrechen. Im Rahmen des Rechts auf informationelle Selbstbestimmung ist man als Mitarbeiter Herr des Verfahrens und kann auch die Löschung der bis zu diesem Zeitpunkt gemachten Angaben verlangen. Allerdings muss dokumentiert werden, dass das Gespräch zum BEM angeboten und vom Mitarbeiter abgelehnt oder abgebrochen wurde (ohne Angabe von Gründen). Da der Arbeitgeber hierzu gesetzlich verpflichtet ist, muss er dokumentieren, dass er das BEM-Gespräch ordnungsgemäß angeboten hat.

Praktische Hinweise:

Es muss kritisch überprüft werden, ob es elektronische Dokumente im BEM-Verfahren geben soll. Nicht nur die Zugriffsberechtigung muss sichergestellt werden, sondern auch der Schutz vor Vervielfältigung. Vertrauliche Informationen landen auch auf Back-Up-Sicherungen.

BEM-Akten müssen für die Verfahrensverantwortlichen zugänglich sein, nicht aber für unbeteiligte Mitarbeiter. BEM-Akten sollten deshalb getrennt von den Personalakten geführt werden. In die Personalakte des Mitarbeiters gehört jedoch der Vermerk, dass ein BEM-Verfahren angeboten wurde und ob es angenommen oder abgelehnt wurde.

Will man die BEM-Akte aus organisatorischen Gründen doch gemeinsam mit der Personalakte führen, kann man die BEM-Akten in versiegelten Umschlägen der Personalakte beilegen, denn Mitarbeiter, die mit der Personalaktenführung beauftragt sind, haben üblicherweise kein Zugriffsrecht auf BEM-Akten. Allerdings muss in einem festgelegten Verfahren sichergestellt werden, dass BEM-Verantwortliche auf die BEM-Akte eines Mitarbeiters zugreifen können, obwohl sie kein Einsichtsrecht in die Personalakte haben.

Handlungshinweise für Mitarbeiter

Die Datenschutzgesetze dienen dazu, Menschen vor Schaden zu bewahren, der ihnen durch den Missbrauch ihrer Daten geschehen kann.

Bei der Erhebungen und -verarbeitung von Beschäftigtendaten über Gesundheit und Krankheit kommen die Datenschutzgesetze zur Geltung (§§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD, § 3 KDO). Der Arbeitgeber muss darstellen, auf welcher Rechtsgrundlage er die Erlaubnis hat, die Daten von Mitarbeitern zu verwenden. Kann er das nicht, ist die Erhebung und Nutzung der Daten unzulässig.

Der Arbeitgeber darf keine Daten verdeckt erheben und verarbeiten.

Der Arbeitgeber muss vollständige Auskunft gewähren, wenn man als Beschäftigter wissen möchte, welche Daten zur eigenen Person erhoben und verarbeitet werden(§ 34 Abs. 1,3,5 BDSG, § 20 Abs. 1,2 SDSG, § 15 Abs. 1,2,4 DSG-EKD, § 13 Abs. 1, 6 KDO). Er kann diese Auskunft nicht verweigern.

Verweigert der Arbeitgeber die Auskunft oder bestehen Zweifel an der Vollständigkeit und Richtigkeit, kann man sich an den internen Datenschutzbeauftragten wenden und auch die Interessenvertretung auffordern, der Sache nachzugehen.

Die Interessenvertretung kann sich darum kümmern, wenn sich der Arbeitgeber weigert geltendes Recht umzusetzen, Auskünfte zu geben, Daten zu löschen oder das Führen und Aushängen von Krankenlisten zu unterbinden.

Sofern es keinen Betriebsrat, Personalrat oder keine Mitarbeitervertretung gibt und

auch kein Datenschutzbeauftragter bestellt ist, kann man sich auch an die Aufsichtsbehörde für den Datenschutz wenden - Kontaktadresse im Anhang. Die Aufsichtsbehörde behandelt solche Anfragen natürlich vertraulich.

Was können Interessenvertreter tun?

Betriebsräte, Personalräte und Mitarbeitervertreter haben die Aufgabe, die Einhaltung der zugunsten von Beschäftigten geltenden Gesetze, Tarife und Betriebsvereinbarungen zu kontrollieren. Interessenvertreter haben das Recht zu kontrollieren, ob alle geltenden Schutzrechte für die Kollegen auch im Umfeld der betrieblichen Gesundheitsfürsorge und des Datenschutzes eingehalten werden.

Eine Vielzahl von Maßnahmen im Zusammenhang mit der Arbeitssicherheit und der betrieblichen Gesundheitsfürsorge sind ganz oder in Teilen mitbestimmungspflichtig. Sie können nur mit Zustimmung des Gremiums oder nach Abschluss von Betriebs- oder Dienstvereinbarungen durchgeführt werden. Das trifft ganz besonders für das Thema Gefährdungsbeurteilungen zu. Aber auch beim BEM sind die Interessenvertreter gefordert. Sie müssen vom Arbeitgeber informiert werden, für welchen Mitarbeiter ein BEM angeboten wird. Darüber hinaus können Interessenvertreter ihre Mitbestimmungsrechte bei der Ausgestaltung des BEM geltend machen.

Weiterführende Unterstützung

Die Arbeitskammer des Saarlandes unterstützt Mitarbeiter, Interessenvertreter und Unternehmen in Fragen des Arbeitsschutzes, der betrieblichen Gesundheitsfürsorge (BEM, Gesundheitszirkel, Gefährdungsbeurteilungen etc.) und in Fragen der Integration schwerbehinderter Arbeitnehmer.

Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden. Kontaktdaten im Anhang.

Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung im Hinblick auf den Schutz von Beschäftigtendaten durch BEST e. V. einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktdaten im Anhang

Compliance - Nutzung von Mitarbeiterdaten zur Korruptionsbekämpfung

Inhalt:

Worum geht es?

Der Begriff „Compliance“ wird in Deutschland im Zusammenhang der Korruptionsbekämpfung verwendet. Auch wenn Compliance im Umfeld der Finanzmärkte als Begriff bekannt geworden ist, hat er inzwischen alle Branchen erreicht. Prominentester Vorfall in Deutschland war der Datenschutzskandal bei der Deutschen Bahn, als die Kontendaten von über 173.000 Mitarbeitern ohne deren Wissen durchforstet wurden, um festzustellen, ob es Korruptionsfälle gegeben hat. Auch wenn der damalige Vorstandsvorsitzende zurücktreten musste, sind die Hintergründe auch Jahre später noch nicht vollends aufgeklärt.

Das, was die Deutsche Bahn unter dem Vorwand der Korruptionsbekämpfung vorgenommen hat, war letztlich nichts anderes, als verdeckt Untersuchungen an Beschäftigtendaten vorzunehmen.

Damit stellt sich die Frage:

Dürfen Arbeitgeber die Daten von Beschäftigten unter dem Vorwand der Korruptionsbekämpfung durchforsten?

und

Dürfen Daten von Mitarbeitern eigens zum Zweck der Korruptionsbekämpfung erhoben und gespeichert werden?

Rechtlicher Hintergrund

Die Verhinderung und Aufklärung von Korruptionsfällen ist ein nachvollziehbares Ansinnen eines jeden Arbeitgebers. Die Frage ist jedoch, wie bei vielen Fragen des Datenschutzes, wie weit diese berechtigten Interessen des Arbeitgebers gehen dürfen und wie die Persönlichkeitsrechte eines Mitarbeiters gewahrt werden z. B. das Recht auf informationelle Selbstbestimmung.

Ein grundlegendes Problem besteht bereits zu Anfang. Der Begriff „Compliance“ ist (bislang) in der deutschen Rechtsprechung nicht definiert. Ähnliches gilt für den Begriff „Korruptionsbekämpfung“. Das, was umgangssprachlich damit gemeint ist, verbirgt sich unter anderen juristischen Begrifflichkeiten wie z. B. Vorteilnahme, unlauterer Wettbewerb, Geldwäsche, Betrug und Insiderhandel, um nur einige zu nennen. Dieser Umstand lässt erahnen, dass eine genauere Betrachtung des jeweiligen Falls notwendig ist.

Compliance bezeichnet in seiner konkreten Übersetzung „das Handeln im Einklang mit geltenden Regeln“. Allerdings muss näher betrachtet werden, um welche Art von Regeln es sich handelt. Im Wesentlichen können folgende Regeln unterschieden werden:

- Deutsche Datenschutzgesetze
- Andere, in Deutschland geltende Rechtsvorschriften
- Ausländische Gesetze
- Branchenspezifische Regeln und Normen
- Unternehmensinterne Richtlinien

Diese Unterscheidung ist wichtig, um feststellen zu können, ob eine Maßnahme zulässig ist oder nicht.

Datenschnüffelei im Grundsatz verboten

Die Verarbeitung von Beschäftigtendaten wird in den Datenschutzgesetzen (§ 4 BDSG, § 4, SDSG, § 4 DSG-EKD, § 3 KDO geregelt. Ohne Rechtsgrundlage oder ausdrückliche Erlaubnis des Mitarbei-

ters dürfen keine personenbezogenen Daten von Beschäftigten erhoben werden.

Grundsätzlich ist die Erhebung und Verwendung von personenbezogenen Angaben von Mitarbeitern nur zulässig, solange sie für das Eingehen, Durchführen oder Beendigen eines Arbeitsverhältnisses rechtlich erforderlich sind (§ 32 BDSG, § 31 SDSG, § 24 DSG-EKD). Und: Die Verwendung der Daten ist an diese Zwecke gebunden.

Beispiel:

> *Als Mitarbeiter ist man gesetzlich verpflichtet, dem Arbeitgeber die Kontonummer mitzuteilen. In der DEÜV, so heißt diese Rechtsvorschrift, ist der Verwendungszweck vorgegeben: Übermittlung an Sozialversicherer und Verwaltung. Der Verwendungszweck „Kontenabgleich zwecks Korruptionsbekämpfung" ist nicht abgedeckt.*

Grundsätzlich lassen es die Datenschutzgesetze nicht zu, die Daten von Beschäftigten, die zu anderen Zwecken erhoben worden sind, zu anlassunabhängigen Korruptionsuntersuchungen heranzuziehen. Das ist unangebracht, unverhältnismäßig und muss unterbleiben. Es gibt jedoch Ausnahmen.

Korruptionsbekämpfung auf der Grundlage einer anderen deutschen Rechtsvorschrift

Es gibt eine Reihe von Gesetzen, die den Datenschutzgesetzen vorgehen. Kann der Arbeitgeber ein solches Gesetz geltend machen, kann (oder muss) er Beschäftigtendaten zur Korruptionsbekämpfung verwenden.

Das ist zum Beispiel im Wertpapierhandel der Fall. Dort gilt u. a. das Wertpapierhandelsgesetz (WpHG). In § 31 Abs. 1 WpHG wird dargestellt, was zu welchen Zwecken dokumentiert werden muss. Aber auch hier sind *sämtliche* gesetzlichen Vorgaben zu beachten. Das WpHG erlaubt es nicht, Datensammlungen von allen Mitarbeitern eines Finanzinstituts anzulegen, sondern nur von denjenigen, die im Wertpapierhandel tätig sind. Mit anderen Worten: Grundsätzlich sind diese Datensammlungen entsprechend der Datenschutzgesetze verboten, für bestimmte Personengruppen wird über das WpHG eine Erlaubnis erteilt, Daten zu sammeln und für die im Gesetz benannten Zwecke zu verwenden.

Ähnliches gilt für das Ordnungswidrigkeitsgesetz (OWiG). In § 130 OWiG werden Betrieben und Unternehmen Aufsichtspflichten auferlegt. Allerdings muss diese Aufsicht für die Betroffenen zumutbar sein und sie muss in einem angemessenen Verhältnis zu der Wahrscheinlichkeit eines Verstoßes stehen. Wer also größeren Missbrauchspotenzialen gegenüber steht, kann stärker kontrolliert werden, als Mitarbeiter, die diesen Potenzialen nicht ausgesetzt sind. Vorrangig betroffen sind Beschäftigte mit Entscheidungsbefugnis und Budgethoheit. Aber auch dann müssen die Aufsichtsmaßnahmen transparent sein. Verdeckte Datensammlungen und eine Zweckentfremdung bestehender Daten zur Wahrnehmung der Aufsichtspflichten sind auch in Hinblick auf das OWiG unzulässig.

Neben dem Ordnungswidrigkeitsgesetz und dem Wertpapierhandelsgesetz gibt es noch eine Reihe weiterer Gesetze, die ein (transparentes) Erheben und Verarbeiten von Beschäftigtendaten zu Compliance-Zwecken zulassen.

Wichtig in diesem Zusammenhang sind natürlich die Gesetze, die sich unmittelbar mit der Aufklärung von Betrug und anderen Straftaten beschäftigen. Auf der Grundlage solcher Gesetze können Strafverfolgungs- und ggf. auch Aufsichtsbehörden (z. B. BaFin, Staatsanwaltschaft) Daten von Beschäftigten analysieren.

Hinweis:

> *Ein Arbeitgeber kann sich nicht auf Gesetze zur Strafverfolgung berufen und Beschäftigtendaten sammeln und auswerten.*

Mitarbeiterüberwachung auf der Grundlage ausländischer Gesetze

Als bekanntestes Gesetz im Umfeld der Korruptionsvermeidung gilt der US-amerikanische Sarbanes-Oxley-Act (kurz SOX). Das Gesetz hat das Ziel, Anleger in die Lage zu versetzen, die Richtigkeit von Unternehmensangaben überprüfen zu können. Alle hierzu relevanten Informationen und Vorgänge des Unternehmens müssen dokumentiert und zugänglich gemacht werden. SOX ist verpflichtend für Unternehmen (und Tochterunternehmen), die an US-amerikanischen Börsen notiert sind. Diese Transparenzpflicht wird in den besagten Unternehmen durch die Schaffung und Einhaltung interner Regeln umgesetzt.

Allerdings hat das Bundesarbeitsgericht am 22.07.2008 (Az: 1 ABR 40/07) festgestellt, dass ausländische Gesetze weder für Arbeitgeber noch für Betriebs- und Personalräte eine Bindungskraft haben.

Hinweis:

> *EU-Verordnungen sind auch in Deutschland einzuhalten. Sie sind gleichwertig zu deutschen Gesetzen.*

Eine Sammlung und Auswertung von Beschäftigtendaten allein auf der Grundlage ausländischer Gesetze ist unzulässig. Mit dem Verweis auf SOX können in Deutschland keine Maßnahmen zur Korruptionsbekämpfung legitimiert werden. So verlangt der SOX beispielsweise von Rechtsanwälten Handlungen, die nach deutschem Recht eine Verletzung der Verschwiegenheitspflicht darstellen.

Sofern ausländische Rechtsvorschriften zur Korruptionsbekämpfung allerdings mit deutschen Rechtsnormen in Einklang stehen, sind sie in Deutschland zulässig. Es gilt das Territorialrecht. Es spielt keine Rolle, ob ein in Deutschland ansässiges Unternehmen mehrheitlich in US-amerikanischem Besitz ist: Es gilt deutsches Recht. Das ist oft nicht bekannt.

Mitarbeiterüberwachung auf der Grundlage von branchenspezifischen oder unternehmensspezifischen Ethik-Richtlinien

Bei der Erhebung und Verwendung von personenbezogenen Daten können die am Arbeitsplatz geltenden Datenschutzgesetze nicht ausgeblendet werden. Daten von Mitarbeitern dürfen nur auf der Grundlage einer Rechtsvorschrift oder mit deren ausdrücklicher Erlaubnis erhoben und verarbeitet werden. Um es klar zu sagen: Richtlinien, ethische Normen und branchentypisches Verhalten sind keine Rechtsvorschriften.

Ein Unternehmen, selbst ein Konzern kann sich keine Richtlinien verordnen, die nicht durch deutsches Recht abgedeckt sind und Mitarbeiter einer unzulässigen Kontrolle unterwerfen oder zu einem unwürdigen und unzumutbaren Verhalten zwingen.

Ethik-Richtlinien sind jedoch in vielen Unternehmen üblich - und auch nach deutschem Recht zulässig. Denn es kommt - wie so oft - ganz konkret darauf an, was geregelt ist. Ethik-Richtlinien sind einfach ausgedrückt Verhaltensrichtlinien. Sie geben vor, wie sich die Mitarbeiter eines Unternehmens oder einer Einrichtung bei der Erledigung ihrer täglichen Aufgaben zu verhalten haben. Innerhalb der am Arbeitsplatz geltenden Rechtsvorschriften gibt es viele Möglichkeiten, zulässige Verhaltensregeln zu gestalten. So eröffnet das Weisungsrecht des Arbeitgebers (§ 106 GewO) eine Reihe von Gestaltungsmöglichkeiten. Doch dieses einseitige Weisungsrecht hat seine Grenzen.

Gemeinsam mit Interessenvertretern können auch Betriebs- und Dienstvereinbarungen abgeschlossen werden, die die Ordnung und das Verhalten der Mitarbeiter im Betrieb betreffen. Dann handelt es sich allerdings nicht mehr um unternehmensinterne Richtlinien. Abgeschlossene Betriebs- und Dienstvereinbarungen stellen eine Rechtsnorm dar.

Im Hinblick auf das Sammeln von Daten von Mitarbeitern für Compliance-Zwecke, können jedoch keine Richtlinien aufgestellt werden, die den Grundsätzen der Datenschutzgesetze (Datenvermeidung, Erforderlichkeit, Zulässigkeit etc.) widersprechen. Also darf in Unternehmensrichtlinien auch keine Sammlung von Beschäftigtendaten angeordnet werden, die nicht mit den Datenschutzgesetzen in Einklang ist.

Formal besteht die Möglichkeit, Mitarbeiter im Voraus um ihre freiwillige (schriftliche) Einwilligung zu einer solchen Datensammlung zu bitten. Diese Einwilligung kann jedoch jederzeit ohne Begründung widerrufen werden. Ein solides, einheitliches und unternehmensweites Verfahren lässt sich auf diesem Wege nicht gestalten. Hinzu kommt, dass die Aufsichtsbehörden für den Datenschutz dieses Verfahren in der Regel für unzulässig erklären, da eine tatsächliche Freiwilligkeit der Mitarbeiter nicht glaubhaft dargestellt werden kann und eine Erforderlichkeit im juristischen Sinne ohnehin nicht gegeben ist.

Es wird dazu geraten, anstelle von Richtlinien gemeinsam mit den Interessenvertretern Vereinbarungen abzuschließen, die als Rechtsnorm den Interessen von Arbeitgeber und Arbeitnehmer gerecht werden können.

Datenschutz und Compliance - zwei wichtige Themen - ein Interessenkonflikt

Auch wenn es sich zweifellos bei der Korruptionsprävention und -bekämpfung um ein legitimes Ziel handelt, so ist es überaus kritisch, wenn diese Aufgaben mit denen des betrieblichen Datenschutzes zusammengelegt werden.

Die Korruptionsprävention und -bekämpfung kann nur effektiv auf der Grundlage weitreichender Überwachung und möglichst großer Datenmengen funktionieren. Der Datenschutz hat die primäre Aufgabe, die Datenvermeidung durchzusetzen und dort, wo eine Verarbeitung von Beschäftigtendaten unumgänglich ist, für Datensparsamkeit und Zweckbindung zu sorgen.

Aus diesen Gründen ist es wichtig, dass Compliance und Datenschutz kritisch und objektiv austariert werden. Das kann nicht erfolgen, wenn beide Aufgaben einer Person (oder Abteilung) übertragen werden. Durch eine solche Personalunion entsteht ein unauflösbarer Interessenkonflikt. Das muss vermieden werden.

Fazit

Compliance ist ein Handeln im Einklang mit allen Rechtsvorschriften, auch mit denen zum Schutz der Persönlichkeitsrechte der Beschäftigten.

Handlungshinweise für Mitarbeiter

Bei der Erhebung und Verarbeitung von Beschäftigtendaten zu Compliance-Zwecken kommen die Datenschutzgesetze zur Geltung (§§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD, § 3 KDO). Der Arbeitgeber muss darstellen, auf welcher Rechtsgrundlage er die Erlaubnis hat, die Daten von Mitarbeitern zu verwenden. Kann er das nicht, ist die Erhebung und Nutzung der Daten unzulässig.

Der Arbeitgeber darf keine Daten verdeckt erheben und verarbeiten.

Der Arbeitgeber muss vollständige Auskunft gewähren, wenn man als Beschäftigter wissen möchte, welche Daten zur eigenen Person erhoben und verarbeitet werden (§ 34 Abs. 1,3,5 BDSG, § 20 Abs. 1,2 SDSG, § 15 Abs. 1,2,4 DSG-EKD,

§ 13 Abs. 1, 6 KDO). Er kann diese Auskunft nicht verweigern.

Verweigert der Arbeitgeber die Auskunft oder bestehen Zweifel an der Vollständigkeit und Richtigkeit, kann man sich an den internen Datenschutzbeauftragten wenden und auch die Interessenvertretung auffordern, der Sache nachzugehen.

Sofern es keinen Betriebsrat, Personalrat oder Mitarbeitervertretung gibt und auch kein Datenschutzbeauftragter bestellt ist, kann man sich auch an die Aufsichtsbehörde für den Datenschutz wenden - Kontaktadresse im Anhang. Die Aufsichtsbehörde behandelt solche Anfragen natürlich vertraulich.

Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden. Kontaktdaten im Anhang.

Was können Interessenvertreter tun?

Betriebsräte, Personalräte und Mitarbeitervertreter haben ganz ähnliche Aufgaben wie Compliance-Beauftragte: Sie haben die allgemeine Aufgabe, die Einhaltung der zugunsten von Beschäftigten geltenden Gesetze, Tarife und Betriebsvereinbarungen zu kontrollieren. Interessenvertreter haben das Recht zu kontrollieren, ob alle geltenden Schutzrechte für die Kollegen auch im Umfeld von Compliance und Korruptionsbekämpfung eingehalten werden.

Eine Vielzahl von Maßnahmen im Zusammenhang mit Ethikrichtlinien, Verhaltensnormen, Datensammlungen und Dokumentationen zur Korruptionsbekämpfung sind ganz oder in Teilen mitbestimmungspflichtig. Sie können nur mit Zustimmung des Gremiums oder nach Abschluss von Betriebs- oder Dienstvereinbarungen angewandt werden.

Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar.

PC- und Internetnutzung

Inhalt:

Worum geht es?

An vielen Arbeitsplätzen ist es heute üblich, dass den Beschäftigten ein Computer mit Internetzugang zur Verfügung gestellt wird. Ob als zentrales Arbeitsmittel oder als Medium zur allgemeinen Information oder Kommunikation (z. B. via E-Mail) – Computer finden sich heute in fast jeder Werkshalle und jedem Büro. Bei deren Nutzung ergeben sich für die Beschäftigten auch viele Fragen hinsichtlich des Datenschutzes. Und zwar insbesondere dann, wenn der jeweilige Rechner einer bestimmten Person zuzuordnen ist. Dies ist etwa der Fall, wenn es für den Computer einen festgelegten Nutzerzugang gibt (zum Beispiel mit Benutzername und Passwort). Dann sind die im System anfallenden Nutzungsdaten zweifelsohne auch personenbezogene Daten. Personenbezogene Daten sind Einzelangaben über eine bestimmte oder bestimmbare natürliche Person (z. B. Beschäftigter). Ihre Verwendung (Erhebung, Verarbeitung, Nutzung) unterliegt den Bestimmungen der jeweils geltenden Datenschutzgesetze. Es gelten im Einzelnen:

- Das Bundesdatenschutzgesetz (BDSG) für nicht-öffentliche Stellen (privatwirtschaftliche Unternehmen) und Bundesbehörden,
- das Saarländische Datenschutzgesetz (SDSG) für Landesbehörden im Saarland sowie
- spezielle Datenschutzvorschriften für kirchliche Einrichtungen (das DSG-

EKD für die Evangelische Kirche und die KDO für die Katholische Kirche).

PC- und Internetnutzung und personenbezogene Daten

Daten, die einen Personenbezug aufweisen, entstehen bei der Computernutzung in großer Zahl. So ist es bei den gängigen PC-Systemen möglich und üblich, dass An- und Abmeldezeiten, benutzte Programme und erstellte oder bearbeitete Dateien (z. B. Textdokumente) elektronisch erfasst bzw. (zwischen-)gespeichert werden. Der Verlauf einer PC-Sitzung lässt sich anhand dieser Daten (dem sogenannten „Cache“) meist ohne großen Aufwand durch eine Auswertung der erstellten Verläufe und Protokolle nachvollziehen.

Dies kann aus Anwendersicht durchaus nützlich erscheinen. Die Erhebung und Verarbeitung dieser Daten erfolgt meist zu Zwecken der Systemsicherheit und ist häufig auch für die eigene Arbeit hilfreich. So kann eine standardmäßige Zwischenspeicherung von Dokumenten im Falle der gewünschten Wiederherstellung eines verlorengegangenen (zum Beispiel irrtümlich gelöschten) Dokumentes sehr nützlich sein.

Im datenschutzrechtlichen Sinne kritisch wird es jedoch, wenn die erhobenen personenbezogenen Daten auch für Auswertungen über den jeweiligen Nutzer herangezogen werden. Etwa dann, wenn ein Vorgesetzter anhand der An- und Abmeldezeiten am PC die Arbeitsleistung eines Mitarbeiters kontrollieren oder bewerten will. Solche Leistungs- und Verhaltenskontrollen anhand von personenbezogenen Daten sind grundsätzlich nicht erlaubt.

Gemäß der Datenschutzgesetze (BDSG, SDSG, DSG-EKD, KDO) gilt die Erhebung und Verarbeitung von personenbezogenen Daten als besonderer Eingriff in die Persönlichkeitsrechte des Betroffenen. Um dessen informationelle Selbstbestimmung zu wahren, gleichzeitig aber auch unbedingt notwendige Datenverarbeitungen zu ermöglichen, gilt für die Erhebung und Verarbeitung personenbezogener Daten das sogenannte *Verbot mit Erlaubnisvorbehalt*. Dieser allgemeine Richtsatz des Datenschutzes besagt, dass die Erhebung und Verarbeitung personenbezogener Daten (also auch Auswertungen) grundsätzlich verboten und nur in Ausnahmefäl-

len erlaubt ist. Und zwar im Beschäftigungsverhältnis entweder

- wenn der Betroffene (hier: der Mitarbeiter) ein freiwilliges Einverständnis dazu gibt (gemäß § 4a BDSG, § 4 Abs. 1 SDSG,§§ 3 und 3a DSG-EKD oder § 3 KDO),
- wenn es ein Gesetz oder eine sonstige Rechtsvorschrift gibt, die die Datenerhebung und -verarbeitung vorsieht
- oder wenn der Vorgang für die Durchführung des Beschäftigungsverhältnisses unbedingt notwendig ist und keine andere (mildere) Möglichkeit besteht, als die Erhebung und Verarbeitung personenbezogener Daten.

Im Beispiel der geplanten Kontrolle eines Mitarbeiters anhand seiner PC-Nutzungsdaten trifft dies in der Regel nicht zu. Eine Kontrolle anhand der im System elektronisch protokollierten Daten wäre also datenschutzrechtlich auch nicht erlaubt. Lediglich zum Zwecke der Sicherstellung der Funktionsfähigkeit der Systeme und zur Sicherung der Daten wäre die Erhebung und Verarbeitung der personenbezogenen Daten gestattet. Nach Erfüllung dieses Zweckes sind die Daten jedoch unmittelbar wieder zu löschen.

Auch und vor allem bei der Nutzung des Internets können zahlreiche weitere, über die erwähnten Daten hinausgehende, personenbezogene Daten anfallen. So werden besuchte Internetseiten oder auch die Zeitpunkte der Zugriffe auf die einzelnen Websites protokolliert. Dies erfolgt meist bereits lokal, also auf dem PC des Nutzers selbst. Oft geschieht dies auch auf oder über einen oder mehrere Zentralrechner. Eine Auswertung dieser Daten (sofern sie personenbezogen sind) darf, wenn überhaupt, nur in sehr engen Grenzen stattfinden. Hierzu gehört die Maßgabe, dass für die Auswertung auf jeden Fall eine Rechtsgrundlage vorliegen muss. Darunter fällt entweder eine persönliche Einwilligung des Betroffenen, ein Gesetz oder – im Falle eines Beschäftigungsverhältnisses – die Notwendigkeit der Datenverarbeitung für die Durchführung des Beschäftigungsverhältnisses. Dabei ist das Schutzniveau der geltenden Datenschutzgesetze (BDSG, SDSG, DSG-EKD, KDO) unbedingt einzuhalten.

Private Internetnutzung am Arbeitsplatz

Zu Konflikten kann es im Beschäftigungsverhältnis kommen, wenn neben der dienstlichen Nutzung des bereitgestellten Internetzugangs auch eine Nutzung in privaten Zusammenhängen erfolgt. Um eine solche Nutzung rechtlich zu beurteilen, ist neben der datenschutzrechtlichen zunächst einmal eine arbeitsrechtliche Einordnung von Bedeutung. Es gilt dabei zunächst festzuhalten: Arbeitnehmer haben grundsätzlich keinen Anspruch auf eine private Nutzung des Internets am Arbeitsplatz.

Wer über diesen Grundsatz einfach hinwegsieht, riskiert als Arbeitnehmer eine Abmahnung oder im ungünstigsten Fall eine Kündigung. Denn: Wer aufgrund der Nutzung des Internets in privaten Zusammenhängen seine arbeitsvertraglich geschuldete Arbeitsleistung (sogenannte „Hauptpflicht“ aus dem Arbeitsverhältnis gemäß § 611 BGB) nicht in vollem Maße erbringt, handelt arbeitsvertragswidrig. Für die Beurteilung eines Vergehens ist also zunächst einmal von Bedeutung, inwiefern durch das „Privatsurfen“ die Erbringung der arbeitsvertraglich geschuldeten Arbeitsleistung beeinträchtigt wird. Hier sind die Grenzen zwischen Erlaubtem und Verbotenem nicht immer klar zu ziehen. Doch eines sollte auf jeden Fall bedacht werden: Ausschweifendes oder exzessives Surfen im Internet während der Arbeitszeit zu privaten Zwecken kann auch ohne vorhergehende Abmahnung eine außerordentliche Kündigung aus einem wichtigen Grund (§ 262 BGB) nach sich ziehen. Es gilt: Je größer der Umfang, in der der Beschäftigte seine Arbeitsleistung schuldig bleibt, desto gravierender die Pflichtverletzung und umso größer die Gefahr, eine außerordentlichen Kündigung zu erhalten.

Nicht nur die Quantität der Pflichtverletzung kann für entsprechende Sanktionen von Bedeutung sein, auch deren Qualität. Besucht ein Mitarbeiter am Arbeitsplatz beispielsweise pornografische oder extremistische Internetseiten (dies müssen nicht unbedingt strafrechtlich relevante Seiten sein), so kann dies eine außerordentliche Kündigung rechtfertigen – unabhängig von der Dauer des Besuches. Hierbei ist entscheidend, ob der Beschäftigte mit dem Abruf der Internetseiten gegen seine aus dem Arbeitsvertrag resultierenden „Nebenpflichten“ verstößt. Zu den Nebenpflichten zählt etwa die Maßgabe,

dass der Beschäftigte keine Rufschädigung gegenüber dem Arbeitgeber verursachen darf. Dies kann – insbesondere wenn der Verstoß an die Öffentlichkeit dringt – durch den Besuch der genannten einschlägigen Internetangebote durchaus der Fall sein.

Sowohl in Fällen, in denen der Beschäftigte seine arbeitsvertraglich geschuldeten Hauptpflichten als auch in Fällen, in denen er seine Nebenpflichten verletzt, ist es insgesamt nicht von Bedeutung, ob der Arbeitgeber eine Internetnutzung im privaten Rahmen duldet oder erlaubt. Ausschlaggebend ist vorrangig das Ausmaß des Verstoßes gegen die arbeitsvertraglichen Pflichten.

Einige Arbeitgeber gestatten (meist in geringfügigem Umfang) eine private Nutzung des dienstlichen Internetzugangs – andere beschränken die Nutzung eher restriktiv auf rein dienstliche Zusammenhänge. Eine erlaubte Nutzung ist in den Grenzen z. B. einer Betriebs- oder Dienstvereinbarung natürlich für den Beschäftigten ohne Folgen. Wenn bei der Nutzung jedoch gegen die dort festgelegten Regeln verstoßen wird, drohen die bereits beschriebenen Konsequenzen. Dabei stellt sich in allen Fällen die Frage, inwiefern der Arbeitgeber die Nutzung des Internets überwachen darf. Klar ist: Egal ob die Privatnutzung erlaubt wird oder nicht, personenbezogene (Nutzungs-)Daten fallen in der Regel an und werden im datenschutzrechtlichen Sinn meist auch verarbeitet. Dies ist zur Gewährleistung der Datensicherheit und zur Sicherstellung der Funktionsfähigkeit der Systeme auch sinnvoll und im datenschutzrechtlichen Sinne erlaubt. Allerdings nur vorübergehend bis der Zweck erfüllt ist.

Eine darüber hinausgehende Auswertung und Kontrolle des individuellen Surfverhaltens ist anhand der erhobenen Daten nur innerhalb von noch engeren Grenzen erlaubt. Und zwar sowohl, wenn eine Privatnutzung gestattet, als auch wenn diese ausdrücklich verboten ist.

Kontrollen, die nicht-personenbezogen sind (z. B. zur Netzauslastung usw.) sind zulässig. Eine personenbezogene dauerhafte Totalüberwachung oder auch verdeckte, heimliche Kontrollen sind dagegen auf keinen Fall statthaft. Weitere Bedingungen für die Rechtmäßigkeit personenbezogener Auswertungen richten sich da-

nach, ob die Privatnutzung erlaubt bzw. geduldet oder verboten ist.

Rechtslage bei Verbot der privaten Internetnutzung am Arbeitsplatz

Ist die Nutzung des dienstlichen Internetzugangs durch den Arbeitgeber untersagt worden, so richtet sich die Verarbeitung der personenbezogenen Daten, also auch etwaige Kontrollen, vorrangig nach den Datenschutzgesetzen (BDSG, SDSG, DSG-EKD oder KDO). Das Recht des Beschäftigten auf informationelle Selbstbestimmung ist dabei in jedem Fall mit dem Interesse des Arbeitgebers an einer geplanten Datenverarbeitung (zum Beispiel zum Zweck der Kontrolle des Surfverhaltens) abzuwägen. Auf jeden Fall gilt: Eine Totalüberwachung von Beschäftigten ist unverhältnismäßig und somit unzulässig.

Der Arbeitgeber darf jedoch eine stichprobenhafte und zeitnahe Auswertung von protokollierten (personenbezogenen) Daten vornehmen. Dabei ist das Verfahren der Protokollierung und der Auswertung möglichst transparent zu gestalten. Das heißt, dem Nutzer muss grundsätzlich bekannt sein, in welchem Umfang die Internetnutzung überwacht wird. Und: Es gilt der datenschutzrechtliche Grundsatz der Zweckbindung: Daten, die zu Zwecken der Datensicherheit oder der Gewährleistung des ordnungsgemäßen Betriebes der Infrastruktur verarbeitet werden, sind auch nur zu diesem Zweck auszuwerten. Eine Verwendung der Daten zur weitergehenden Verhaltens- und Leistungskontrolle der Beschäftigten ist unzulässig.

Rechtslage bei Erlaubnis oder Duldung der privaten Internetnutzung am Arbeitsplatz

Im Falle einer (auch begrenzten) Nutzungsduldung oder -erlaubnis im privaten Zusammenhang hat der Arbeitgeber neben den datenschutzrechtlichen Bestimmungen vor allem das Fernmeldegeheimnis zu beachten. Er gilt in diesem Zusammenhang rein rechtlich betrachtet als Anbieter von Telemediendiensten bzw. Telekommunikationsdiensten. Das heißt insbesondere: Es gelten die Bestimmungen des Telemediengesetzes (TMG) und im Falle der Nachrichtenübertragung (z. B. per E-Mail) das Telekommunikationsgesetz (TKG). Auf der Grundlage der dort festgelegten Bestimmungen dürfen Daten mit Personenbezug nur für die Erbringung

des Internetdienstes und dessen Abrechnung verarbeitet werden.

„ (1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.“

§ 15 Telemediengesetz (TMG)

Ausnahmen ergeben sich, wenn der Beschäftigte einer weitergehenden Datenverarbeitung, also auch möglichen Kontrollen seines Nutzungsverhaltens, freiwillig zustimmt.

Grundsätzlich hat der Arbeitgeber ein berechtigtes Interesse daran, auch bei einer privaten Nutzung des Internets sichergehen zu können, dass Missbrauch oder strafbare Handlungen unterbleiben. Deshalb ist es durchaus gerechtfertigt, eine in begrenztem Rahmen erfolgende Überwachung der Nutzung des Internets (z. B. stichprobenhafte, zunächst noch anonyme, später gegebenenfalls auch personenbezogene Auswertungen) vorzunehmen. Um dies zu ermöglichen und allen rechtlichen Anforderungen hierfür gerecht zu werden, müssen allerdings zunächst wichtige Voraussetzungen erfüllt werden. Hierzu gehört in der Regel eine Einverständniserklärung des Beschäftigten. Oft knüpfen Arbeitgeber aus diesem Grund die Erlaubnis einer Nutzung des Internetzugangs im privaten Rahmen an eine solche Einverständniserklärung. Diese ist übrigens jederzeit durch den Beschäftigten wiederrufbar, jedoch auch meist mit der Konsequenz, dass eine Privatnutzung dann für diese Person untersagt ist.

Neben einem erklärten Einverständnis durch den Betroffenen kann der Arbeitgeber die Erlaubnis zur Privatnutzung noch an weitere Bedingungen knüpfen. Hierzu gehört etwa eine Begrenzung des Zeitrahmens der Nutzung im privaten Zusammenhang, zum Beispiel auf Pausenzeiten.

E-Mail am Arbeitsplatz

Die Nutzung von E-Mail-Diensten am Arbeitsplatz kann in vielerlei Hinsicht weitere Fragen aufwerfen. Neben den näheren Umständen über den jeweiligen Informationsaustausch (Zeitpunkte, Beteiligte an E-Mail-Schriftwechseln) spielen dabei vor allem die Inhalte, also die E-Mails selbst, eine zentrale Rolle. In den meisten Fällen ist bei E-Mails Personenbezug gegeben. Schon allein deshalb, weil E-Mail-Adressen in der Regel einen Namen beinhalten (Maria.Mustermann@Muster.de) und nicht nur rein funktionsbezogen sind (Beraterin1@Muster.de). Auch hier gelten daher die Vorschriften des BDSG bzw. der anderen jeweils geltenden Datenschutzgesetze.

Eine Auswertung oder Kontrolle der E-Mail-Nutzung ist dem Arbeitgeber aus Gründen des Schutzes der Persönlichkeitsrechte der Beschäftigten und auch zur Sicherstellung des Post- und Fernmeldegeheimnisses nur in sehr engen Grenzen gestattet. Unabhängig davon, ob eine Privatnutzung erlaubt oder nicht erlaubt ist, sind auf der Auswertung von personenbezogenen Daten basierende Kontrollen gemäß Telekommunikationsgesetz (TKG) grundsätzlich nur zu Zwecken der Aufrechterhaltung der technischen Funktionsfähigkeit der Systeme oder zu Abrechnungszwecken erlaubt. Inhalte (also auch die elektronische Nachricht selbst) und nähere Umstände des Telekommunikationsvorganges dürfen darüber hinaus deshalb auch nicht ohne ausdrückliche Erlaubnis der Beteiligten (auch des Absenders, nicht nur des Empfängers) ausgewertet werden. Ein Mitlesen der zuzustellenden E-Mail ist also verboten.

> ***„(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.“***
>
> *§ 88 Telekommunikationsgesetz (TKG)*

Ist der Übertragungsvorgang einer E-Mail abgeschlossen, so gelten die Bestimmungen der Datenschutzgesetze (BDSG, SDSG, DSG-EKD, KDO). Das heißt, auch nach Abschluss des Übertragungsvorgan-

ges, wenn die E-Mail im Postfach des Empfängers liegt, ist es nicht ohne weiteres erlaubt, diese ohne Kenntnis von Absender und Empfänger zu kontrollieren. Es ist grundsätzlich verboten, sie unbefugt in Einsicht zu nehmen. Dies ist am Arbeitsplatz ausnahmsweise nur dann erlaubt, wenn es sich – unter der Voraussetzung eines Verbots der Privatnutzung – um eine E-Mail mit eindeutig und ausschließlich dienstlichem Inhalt handeln würde. Doch auch dann gilt: Personenbezogene Kontrollen dürfen nur erfolgen, wenn sie nicht zu stark in die Persönlichkeitsrechte des Betroffenen eingreifen und die Verhältnismäßigkeit gewahrt bleibt. Und: Ein Kontrollverfahren muss transparent sein. Heimliche Auswertungen sind also ebenfalls verboten.

Betriebs- oder Dienstvereinbarungen

Um Klarheit (und Rechtssicherheit) rund um die Nutzung von PC, Internet und E-Mail am Arbeitsplatz zu erlangen, ist es in vielen Unternehmen und Verwaltungen mittlerweile üblich, den Umgang damit im Rahmen von Betriebs- oder Dienstvereinbarungen zu regeln. Mit solchen Vereinbarungen können auch verbindliche Vorgaben zum Ausmaß und zur Umsetzung von Auswertungen und Kontrollen formuliert werden. Auch eine betriebliche Regelung der privaten Nutzung des dienstlichen Internetzugangs steht in der Regel im Zentrum der Vereinbarung. Im Rahmen der Vereinbarung kann außerdem festgelegt werden, was im Falle einer missbräuchlichen Nutzung an Aufklärungsmaßnahmen durch den Arbeitgeber erfolgen darf. Zusätzlich werden oft auch weitere organisatorische Richtlinien festgelegt, wie etwa Vertretungsregeln zur E-Mail-Einsicht (etwa im Falle längerer, ungeplanter Abwesenheiten von Mitarbeitern).

Betriebs- oder Dienstvereinbarungen muss der Arbeitgeber gegenüber allen Arbeitnehmern anwenden. Niemand kann ohne Weiteres davon ausgenommen werden. Sie gelten im datenschutzrechtlichen Sinne als „sonstige Rechtsvorschriften“, die eine Datenverarbeitung – neben der persönlichen Einwilligung, der Erlaubnis durch das jeweilige Gesetz selbst oder durch eine andere übergeordnete Rechtsnorm – erlauben. Sie dürfen das Schutzniveau der Datenschutzgesetze nicht unterlaufen, also keine unverhältnismäßigen Eingriffe in das Persönlichkeitsrecht des Nutzers möglich machen.

Datenübertragung im Konzern und international

Inhalt:

In vielen Fällen ist es inzwischen üblich, dass Daten von Beschäftigten aus dem Unternehmen übertragen werden und an anderer Stelle (weiter-)verarbeitet werden. Natürlich müssen Daten an die Sozialversicherer übertragen werden, das ist gesetzlich geregelt. Aber selbst in Kleinbetrieben wird die Personalabrechnung oft an einen Steuerberater oder einen anderen externen Dienstleister übertragen. Was ist hierbei zu beachten? Eine andere Frage stellt sich, wenn personenbezogene Daten innerhalb eines Konzernverbunds übertragen werden sollen, besonders dann, wenn die Datenübertragung an Standorte außerhalb Deutschlands erfolgen soll.

Im Folgenden geht es um die Frage:

- ***Was ist zu beachten, wenn Daten von Beschäftigten an andere Stellen übertragen werden sollen?***
- ***Welche Rechte habe ich als Beschäftigter?***

Die Frage der Datenübertragung und -weitergabe stellt sich auch in anderer Form:

- ***Darf der Arbeitgeber mündlich oder telefonisch Auskünfte über Mitarbeiter an Außenstehende weitergeben?***

Rechtlicher Hintergrund:

In allen Datenschutzgesetzen ist festgehalten, dass personenbezogene Daten nur zu dem Zweck verwendet werden dürfen, für den sie erhoben wurden. Nicht direkt erkennbar ist jedoch, ob das im Betrieb, in der Dienststelle oder in der Einrichtung erfolgen muss, oder ob dies auch außerhalb möglich ist.

Alle Datenschutzgesetze sehen die Möglichkeit vor, dass Daten von Beschäftigten an andere Stellen übertragen werden können. Das geht jedoch nur unter ganz bestimmten Voraussetzungen, zu genau beschriebenen und rechtlich zulässigen Zwecken. Das muss für die betroffenen Mitarbeiter überprüfbar sein.

Damit das gelingen kann, muss man allerdings wissen, welche rechtlichen Hintergründe es gibt, was zu beachten ist und wer verantwortlich ist.

Datenübertragung innerhalb des Unternehmens

Zunächst muss man festhalten, dass die sogenannte *verantwortliche Stelle*, der Arbeitgeber, oft genug mehrere interne Abteilungen (z. B. Personalabrechnung, Personalentwicklung) beauftragt, Daten von Beschäftigten zu verarbeiten. Dass Daten von Beschäftigten zwischen diesen Abteilungen übertragen werden, ist normal und auch zulässig, wenn die erforderlichen Maßnahmen zum Datenschutz getroffen wurden (z. B. Schutz vor unberechtigtem Zugriff und Manipulation etc.). Genau genommen handelt es sich nicht um eine Datenübertragung im Sinne der Datenschutzgesetze, denn die Daten bleiben ja innerhalb der verantwortlichen Stelle (beim Arbeitgeber), wenn auch in unterschiedlichen Räumen.

Es kann durchaus sein, dass mehrere Arbeitsstätten zu einer rechtlichen Einheit gehören (z. B. mehrere Niederlassungen,

Werke oder Filialen eines rechtlich selbstständigen Unternehmens oder Außenstellen einer Dienststelle oder Einrichtung). Auch dann handelt es sich nicht um Datenübertragungen im Sinne der Datenschutzgesetze, weil die Daten zwar die einzelnen Betriebsstätten, nicht aber das Unternehmen und damit die verantwortliche Stelle verlassen.

Diese Art der Datenübertragung ist unter Beachtung der allgemeinen Regeln zum Datenschutz zulässig: Der Zweck der Erhebung und Verarbeitung muss erforderlich und legal sein, weiterhin müssen die notwendigen Maßnahmen zum Schutz der Daten vor Manipulation und Missbrauch getroffen sein. Auch in diesem Fall kann man als Mitarbeiter verbindliche Auskunft über die Datenverarbeitung verlangen.

Datenübertragung zu externen Stellen

Wird jetzt z. B. die Lohnbuchhaltung ausgelagert zu einem externen Dienstleister oder einem anderen rechtlich selbständigen Unternehmen, dann ist zunächst Folgendes zu beachten: Sofern die Daten an eine externe Stelle übermittelt werden, die praktisch nur als verlängerter Arm zu sehen ist, handelt es sich um eine sogenannte Auftragsdatenverarbeitung. Werden hingegen von dem externen Dienstleister nicht nur Daten in der beauftragten Form verarbeitet, sondern auch Entscheidungen getroffen (z. B. wenn ein externer Dienstleister im Auftrag Stellen ausschreibt und auch eine Bewerber(vor)auswahl vornimmt), dann handelt es sich um eine sogenannte Funktionsübertragung.

Diese Unterscheidung ist nicht immer leicht zu treffen, doch sie ist wichtig. Durch diese Unterscheidung wird festgelegt, wer verantwortlich und zur Auskunft verpflichtet ist.

Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt dann vor, wenn ein externer Auftragnehmer Daten von Beschäftigten erhält, um sie in einer vorgegebenen Art zu verarbeiten, ohne jedoch eigenmächtig Entscheidungen treffen zu können. Die Entgeltberechnung durch einen Steuerberater oder die Durchführung von Mitarbeiterbefragungen durch ein Sozialforschungsinstitut sind gängige Beispiele. Der Auftraggeber, in unserem Fall der Arbeitgeber, bleibt in vollem Umfang verantwortlich dafür, dass

kein Missbrauch mit den Daten erfolgt. Er ist auch den betroffenen Mitarbeitern gegenüber zu Auskunft verpflichtet. Der externe Dienstleister darf nicht einmal Auskünfte erteilen. Der Arbeitgeber ist verpflichtet, dafür zu sorgen, dass der Dienstleister alle datenschutzrechtlichen Vorgaben einhält. Was alles bei der Übermittlung bei einer Auftragsdatenverarbeitung zu beachten ist, gibt § 11 BDSG vor.

> *(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.*
>
> *(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:*
>
> *1. der Gegenstand und die Dauer des Auftrags,*
>
> *2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder*
>
> *Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,*
>
> *3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,*
>
> *4. die Berichtigung, Löschung und Sperrung von Daten,*
>
> *5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,*
>
> *6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,*
>
> *7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,*
>
> *8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm be-*

schäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 11 BDSG

Funktionsübertragung

Funktionsübertragung ist in gewisser Weise die „große“ Variante der Auftragsdatenverarbeitung. Bei der Funktionsübertragung überträgt der Arbeitgeber größere Funktionen wie zum Beispiel den Betrieb einer Personalverwaltung oder eines Rechenzentrums an ein anderes Unternehmen, das in der Wahrnehmung dieser Aufgaben auch berechtigt ist, eigenmächtig Entscheidungen zu treffen. Das ist typisch für das Outsourcing oder Offshoring von Unternehmensteilen oder in Konzernverbünden.

Bei der Funktionsübertragung geht die Verantwortlichkeit für die Einhaltung des Datenschutzes auf den über, der die Funktion erfüllt.

Aus Sicht des Mitarbeiters heißt das, dass die Verantwortlichkeit des Arbeitgebers

nach der Übertragung aufhört. Für die anschließende (externe) Datenverarbeitung ist das Unternehmen verantwortlich, das die Daten empfängt. Das heißt, dass dieses Unternehmen dem betroffenen Mitarbeiter zur Auskunft verpflichtet ist und dass der Mitarbeiter seine Rechte auf Berichtigung falscher Daten sowie die Löschung und Sperrung von Daten erwirken kann, die nicht oder nicht mehr erforderlich sind oder ohne Rechtsgrundlage erhoben wurden. Weiterhin ist das Unternehmen, das die Datenverarbeitung übernimmt, dazu verpflichtet, den betroffenen Mitarbeiter unaufgefordert über Art und Umfang der Datenverarbeitung zu benachrichtigen.

Benachrichtigung der betroffenen Mitarbeiter

Für die Privatwirtschaft und Bundeseinrichtungen ist in § 33 BDSG geregelt, wann ein Mitarbeiter benachrichtigt werden muss. Wenn die Daten aufgrund gesetzlicher Vorschriften übertragen werden müssen oder man davon ausgehen kann, dass der Mitarbeiter weiß, dass seine Daten übertragen werden (müssen) z. B. an die Rentenversicherung, oder wenn die Benachrichtigung einen unverhältnismäßigen Aufwand bedeuten würde, dann ist es nicht notwendig. Angesichts der aktuellen Kommunikationsmedien verliert das Argument des unverhältnismäßigen Aufwands jedoch immer mehr an Bedeutung.

Ähnlich ist auch die Benachrichtigung für die Mitarbeiter katholischer Einrichtungen in § 13a KDO geregelt. Die Vorgaben zur Datenübermittlung an kirchliche und nichtkirchliche Stellen sind beschrieben in den §§ 11 und 12 KDO.

Für Mitarbeiter protestantischer Einrichtungen regelt das DSG-EKD in § 15a, wann ein Mitarbeiter über die Datenübermittlung unterrichtet werden muss. In den §§ 12 und 13 DSG-EKD werden die Vorgaben für die Übermittlung von Mitarbeiterdaten beschrieben.

Bei öffentlichen Einrichtungen des Saarlandes, saarländischer Kommunen und der Landkreise kommt das Saarländische Datenschutzgesetz zum Tragen. Es regelt in § 12 die Benachrichtigung an den betroffenen Mitarbeiter. In §§ 14, 16, 17 SDSG werden die Bedingungen für die Datenübermittlung festgehalten.

Datenübertragung im Konzern

Innerhalb von Konzernen oder anderen Verbünden von Unternehmen, Einrichtungen oder Dienststellen finden sich oft einzelne Einheiten, die als zentrale Dienstleister für die verbundenen Unternehmen auftreten. Ein zentraler EDV-Betrieb oder eine zentrale Personalverwaltung sind die gängigsten Formen.

Hinweis:

> *Es gibt kein Konzernprivileg, das es generell erlaubt, Daten von Mitarbeitern zwischen Unternehmen eines Konzerns (oder Verbundes) zu übermitteln.*
>
> *Ob Daten von Mitarbeitern zwischen einzelnen Betrieben übertragen werden dürfen, hängt vom Einzelfall ab*.

Die Datenschutzgesetze gehen vom Prinzip der verantwortlichen Stelle aus. Das ist eine eigenständige rechtliche Einheit (z. B. eine GmbH). Sollen Mitarbeiterdaten von einer verantwortlichen Stelle an eine andere verantwortliche Stelle übermittelt werden, muss geprüft werden, ob dies im Einklang mit den Datenschutzgesetzen erfolgt. Es spielt keine Rolle, ob die beiden verantwortlichen Stellen den gleichen Besitzern gehören, wie das in einem Konzern üblich ist. Insofern ist keine generelle Antwort möglich, ob eine Übermittlung von Mitarbeiterdaten innerhalb des Konzerns zulässig ist. Eine individuelle Prüfung ist unerlässlich. Im Zweifelsfall, falls also kein Erlaubnistatbestand dargestellt werden kann, ist die Übermittlung unzulässig. Diese Prüfung ist mit besonderer Sorgfalt vorzunehmen, wenn personenbezogene Daten von Mitarbeitern ins Ausland übertragen werden sollen.

Übermittlung von Mitarbeiterdaten ins Ausland

Oft genug besteht der Wunsch oder sogar die Aufforderung innerhalb eines Konzerns Mitarbeiterdaten an eine Zentrale außerhalb der Bundesrepublik Deutschland zu schicken. Praktisch hat man schon große Probleme, die Korrektheit der Datenverarbeitung bei einer Übermittlung an externe Stellen innerhalb Deutschlands zu überprüfen. Man muss sich nichts vormachen, bei einer Übertragung ins Ausland sind die praktischen Möglichkeiten einzugreifen und überprüfen zu können sehr gering. Dennoch gibt es einen rechtlichen Rah-

men, der die Datenübermittlung ins Ausland regelt.

Grundsätzlich gilt ausgehend von deutschem Recht das Territorial-Prinzip: Wenn personenbezogene Daten in Deutschland nach deutschem Datenschutzrecht erhoben wurden, gilt dieses (deutsche) Datenschutzniveau auch für alle nachfolgenden Prozesse der Datenverarbeitung, egal in welchem Staat sie stattfinden. Das ist manchen Konzernspitzen ein Dorn im Auge, die gerne das niedrigere Datenschutzniveau ihres Landes (z. B. USA) anwenden würden. Doch das ist nicht zulässig.

Die verantwortliche Stelle - also z. B. ein deutsches Tochterunternehmen - muss bei Anfragen prüfen, ob eine Übertragung von Mitarbeiterdaten rechtlich zulässig ist. Wenn dem so ist, muss auch sichergestellt werden, dass die Stelle, die die Daten im Ausland erhält, die Daten auch dort nach deutschem Recht behandelt. Wenn das nicht glaubwürdig dargestellt und objektiv überprüft werden kann, dürfen die Daten nicht ins Ausland übermittelt werden. Ob diese rechtliche Anforderung deutscher Tochterunternehmen angesichts der finanziellen Abhängigkeit von ausländischen Konzernzentralen durchgesetzt werden kann, muss an anderer Stelle diskutiert werden.

Datenübertragung innerhalb der Europäischen Union

Seit 2003 hat sich dieses Problem jedoch ein wenig entschärft. Bis zu diesem Jahr musste die EU-Datenschutzrichtlinie in nationales Recht umgesetzt werden. Dadurch wurde ein (rechtlich) einheitliches Datenschutzniveau innerhalb der EU geschaffen und auch darüber hinaus. Für die Schweiz, Guersney, Isle of Man, Argentinien und Kanada hat die EU-Kommission festgestellt, dass sie ebenfalls über ein angemessenes Schutzniveau verfügen.

Sofern eine Datenübermittlung nach deutschem Datenschutzrecht zulässig ist, kann sie auch an verantwortliche Stellen innerhalb der EU oder in Staaten mit nachweislich angemessenem Schutzniveau erfolgen.

Datenübertragung in Staaten außerhalb der EU (ohne angemessenes Schutzniveau)

Sollen personenbezogene Daten in Staaten erfolgen, die kein der EU entsprechendes Datenschutzniveau umsetzen, ist das

sehr kritisch zu sehen und bedarf einer ebenfalls kritischen Prüfung. Da kein Gesetz die Einhaltung des Datenschutzniveaus garantiert, muss die verantwortliche Stelle im Ausland (z. B. der Konzernsitz) glaubhaft nachweisen, dass sie das hohe deutsche Datenschutzniveau einhält. Erst wenn überprüft ist, ob eine Datenübertragung generell zulässig ist und die Einhaltung von deutschem Datenschutzrecht zugesichert wurde, dürfen Daten von Mitarbeitern in Staaten ohne angemessenes Schutzniveau übertragen werden.

Doch dieses Prinzip ist im praktischen Leben kritisch zu sehen. US-amerikanische Unternehmen können durch einen formalen Akt dem sogenannten „Safe Harbour Abkommen“ beitreten. Die Mitglieder des Abkommens verpflichten sich freiwillig zur Einhaltung eines angemessenen Schutzniveaus. Ungeachtet dessen, ob diese Prinzipien tatsächlich umgesetzt werden, gelten diese durch den Beitritt als akzeptiert und ein angemessenes Datenschutzniveau als garantiert.

Hinweis:

> *Öffentliche Einrichtungen der USA z. B. das Verteidigungsministerium als Auftraggeber oder die FDA (Food and Drug Administration) als Kontrollinstanz für Pharmaunternehmen, die den US-Markt beliefern, haben sich nicht zur Einhaltung der Safe Harbour Prinzipien verpflichtet. Sie sind nicht verpflichtet, deutsches Datenschutzrecht einzuhalten*.

Sofern kein angemessenes Datenschutzniveau im Ausland garantiert wird, muss eine Übertragung von personenbezogenen Daten von Mitarbeitern aus Deutschland unterbleiben. Die Verantwortung dafür liegt bei der verantwortlichen Stelle in Deutschland, die die Daten übermitteln soll.

Telefonische und mündliche Auskünfte über Beschäftigte an Dritte

Eine mündliche wie auch telefonische Auskunft über Beschäftigte ist nichts anderes als eine Datenübermittlung. Auf welche Art - schriftlich, elektronisch, mündlich - eine Datenübermittlung erfolgt, ist rechtlich ohne Belang. Insofern gelten auch bei der mündlichen Übermittlung von Mitarbeiterinformationen sämtliche Rahmenbedingungen der Datenerhebung und Übermitt-

lung: Es muss immer geprüft werden, ob Informationen über Mitarbeiter erhoben und verarbeitet werden. Es muss weiterhin geprüft werden, ob es datenschutzrechtlich zulässig ist, die Daten zu übermitteln. Erst wenn beides zulässig ist, und der betroffene Mitarbeiter entsprechend der gesetzlichen Vorgaben benachrichtigt ist, dürfen mündliche Auskünfte erteilt werden.

Handlungsmöglichkeiten als Mitarbeiter

- Wenn Daten übermittelt werden sollen, muss es hierfür eine Rechtsgrundlage geben. Der Arbeitgeber muss (nach §§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD, § 3 KDO) begründen, dass er die Daten übermitteln darf. Er kann die Begründung nicht verweigern.

- Als Beschäftigter hat man das Recht auf Auskunft über alle Daten aus dem System, die die eigene Person betreffen.

- Als Beschäftigter kann man Einblick in das Verfahrensverzeichnis verlangen, um zu erfahren ob und wenn ja wo, welche Daten von wem verarbeitet und wohin sie ggf. übermittelt werden. Liegt kein Verfahrensverzeichnis vor, darf das System nicht betrieben werden. Die Auflagen der Datenschutzgesetze sind nicht erfüllt (gilt nicht bei kirchlichen Einrichtungen)! Das Verfahrensverzeichnis wird vom Arbeitgeber oder vom Beauftragten für Datenschutz gepflegt und kann dort eingesehen werden. Dort steht auch die Rechtsgrundlage für eine eventuelle Speicherung.

- Gibt es Zweifel an der Umsetzung des Datenschutzes, sollte man Beweise für diese Zweifel sammeln und die Interessenvertretung einschalten. Existiert keine Interessenvertretung oder führt das nicht zum Erfolg, dann kann man sich an die Rechtsberatung der Arbeitskammer wenden oder direkt an die Landesbeauftragte für Datenschutz.

- Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden.

Handlungsmöglichkeiten für die Interessenvertretung

- Betriebsräte, Personalräte und Mitarbeitervertretungen haben auch das Recht, die Einhaltung des Datenschutzes zu überprüfen. Dazu gehört auch zu überprüfen, ob bei einer Datenübermittlung deutsches Datenschutzrecht zum Schutz der Beschäftigten eingehalten wird. Die verantwortliche Stelle - der Arbeitgeber - ist zur Auskunft verpflichtet, ob und wenn ja auf welche Art Daten übermittelt werden. Ohne das konkrete Einverständnis eines Mitarbeiters hat die Interessenvertretung jedoch keinen Anspruch auf die Einsicht in die personenbezogenen Daten eines Mitarbeiters. Da Interessenvertreter auch Mitarbeiter sind, haben sie natürlich auch ein konkretes Auskunftsrecht, was die Übermittlung „ihrer“ Daten betrifft.

- Prinzipiell besteht die Möglichkeit, die Datenübertragung in Form einer Betriebsvereinbarung zu regeln. Dies hat allerdings rechtliche wie auch praktische Grenzen. So bezweifeln die deutschen Aufsichtsbehörden für den Datenschutz die Wirksamkeit von Betriebsvereinbarungen im Ausland. Rein rechtlich kann über eine Betriebsvereinbarung zwar das Datenschutzniveau angehoben und ausgestaltet werden. Eine Betriebs- oder Dienstvereinbarung kann jedoch das informationelle Selbstbestimmungsrecht des Mitarbeiters nicht beschränken.

  Sofern es datenschutzrechtlich nicht erforderlich oder angemessen ist, die Daten eines Mitarbeiters ins Ausland zu übermitteln, kann ihm sein Recht auf informationelle Selbstbestimmung nicht durch eine Betriebs- oder Dienstvereinbarung genommen werden.

- Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktdaten im Anhang.

Überwachungskameras, Videoüberwachung

Inhalt:

Worum geht es?

Überwachungskameras sind in vielen Betrieben und Einrichtungen bereits installiert. Was viele nicht wissen: Nur in überprüften Ausnahmefällen ist die Kameraüberwachung zulässig - denn grundsätzlich ist der Einsatz von Überwachungskameras verboten. Der Arbeitgeber kann nicht frei darüber entscheiden, ob solche Kameras installiert und betrieben werden, auch wenn das den Anschein hat.

Die wenigsten Kunden oder Besucher werden einen Betrieb oder eine Einrichtung nicht betreten, nur weil sie mit Kameras überwacht wird. Sie sind auch nur für die kurze Dauer ihrer Anwesenheit in der Betriebsstätte dieser Überwachung ausgesetzt. Als Beschäftigter sieht das anders aus. Hier ist man schnell einer vollständigen Überwachung ausgesetzt - von Beginn bis zum Ende der täglichen Arbeit.

Diese Überwachung, wie sie häufig in Kaufhäusern, aber auch in Produktionshallen anzutreffen ist, registriert jede Bewegung und zeigt, wer sich mit wem unterhält, wer wem aus dem Weg geht, wo sich eine Person befindet, was sie macht und mit welchem Elan. Deshalb sind Kameraüberwachungen ein schwerwiegender Eingriff in die Persönlichkeitsrechte und setzen die Beschäftigten unter einen permanenten Überwachungsdruck.

Durch die Häufigkeit, mit der wir mit solchen Kameras konfrontiert sind, entsteht der Eindruck, dies sei legal. Tatsächlich ist es allerdings ganz einfach so: Wo es keinen Kläger gibt, gibt es bekanntlich auch keinen Richter. Wer als Beschäftigter seinen Arbeitgeber darauf anspricht, ob die Rechtmäßigkeit der Kameraüberwachung

überprüft wurde, riskiert Unannehmlichkeiten und den Vorwurf, ob er etwas zu verbergen hat.

Was kann man tun, wenn Kameras am Arbeitsplatz installiert werden sollen oder bereits installiert worden sind?

Technischer Hintergrund

Oft wird der Begriff Videoüberwachung verwendet. Videoüberwachung ist die ursprüngliche Kameraüberwachung mit analogen Signalen, die auf Magnetband (Videobänder) gespeichert werden. Die Aufzeichnungsdauer hängt von der Bandlänge ab. Die Speicherdauer ergibt sich einfach daraus, wie lange ein beschriebenes Band aufgehoben wird, oder wann sich ein Endlosband selbstständig überschreibt. Die Datenübertragung erfolgt über ein eigenes Kabelnetz oder per Funk.

Inzwischen handelt es sich in den meisten Fällen um sogenannte IP-Kameras. Das sind digitale Kameras, die ihre Daten in das Computernetzwerk des Unternehmens einspeisen. Die Kameras können dann live von unterschiedlichen Computern, oft über den Internet-Browser, betrachtet und auf Festplatten beliebig lange gespeichert werden. Die Datenübertragung kann über Datenleitung erfolgen, über eigene Funksysteme oder über ein Drahtlosnetzwerk (W-LAN).

Die Überwachung mit Digitalkameras ist inzwischen sehr günstig. Es müssen kaum noch Kabel verlegt werden, jeder PC kann als Monitor verwendet werden und Kameras sind bereits für weniger als 100 Euro verfügbar. Viele Kameras haben die Möglichkeit auch im Dunkeln mit Infrarottechnik aufzuzeichnen. Mit nahezu allen Kameras ist es möglich, die überwachten Bereiche abzuhören. Kameras können die Größe eines Schuhkartons haben, es werden aber auch bereits für wenig Geld Modelle angeboten, die in einen Kugelschreiber passen oder in Rauchmeldern installiert sind.

Risiken für Beschäftigte

Die Folgen, denen man durch die Kameraüberwachung am Arbeitsplatz ausgesetzt ist, sind ein massiver Überwachungsdruck und eine Kontrolle des Sozialverhaltens am Arbeitsplatz und der Leistungserbringung weit über das Maß hin-

aus, das in Arbeitsvertrag und Tarif zulässig ist. Kündigungen und Abmahnungen können die Folge sein. Weit häufiger sind es jedoch Stress, psychische Belastungen und damit verbunden auch Krankheit.

Rechtliche Situation:

- Explizit regeln die Datenschutzgesetze (§ 6b BDSG, § 34 SDSG, § 7a DSG-EKD, § 5a) nur die Kameraüberwachung im öffentlichen Raum und in öffentlich zugänglichen Räumen. Darin wird ein Mindestschutz definiert. 1.) Die überwachten Areale müssen erkennbar ausgeschildert sein. 2.) Die Verhältnismäßigkeit muss gewahrt bleiben: Die schutzwürdigen Belange der Überwachten dürfen nicht stärker wiegen als das berechtigte Interesse des Überwachers. Arbeitsplätze liegen üblicherweise nicht in öffentlich zugänglichen Räumen. Es kann kein öffentliches Interesse geltend gemacht werden, deshalb ist das Schutzniveau für die Beschäftigten dort deutlich höher anzusiedeln.
- Heimliches Filmen am Arbeitsplatz ist verboten. Für Strafverfolgungsbehörden ist dies jedoch im Rahmen von Ermittlungsverfahren bei dringendem Tatverdacht mit richterlichem Beschluss möglich.
- Eine Überwachung von Sozialräumen, Umkleideräumen und sanitären Anlagen ist immer unzulässig.
- Eine permanente Überwachung des Arbeitsbereichs eines Beschäftigten, ohne dass er sich aus dem Einsichtsfeld der Kamera bewegen kann, ist unzumutbar und unzulässig.
- Bei der sichtbaren Kameraüberwachung von Beschäftigten gelten die Vorgaben der Datenschutzgesetze (§§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD und § 3 KDO). Das heißt, Kameraüberwachung gilt grundsätzlich als verboten, eine Erlaubnis muss herbeigeführt werden.
- Bevor öffentliche Einrichtungen des Saarlandes, der Landkreise und Kommunen Kameras installie-

ren, muss die Landesbeauftragte für Datenschutz informiert und angehört werden.

- Eine sichtbare, begrenzte Kameraüberwachung zu festgelegten Zwecken, kann unter Einhaltung gesetzlicher Vorgaben zulässig sein. Hierzu bedarf es einer Verhältnismäßigkeitsprüfung und falls eine Interessenvertretung existiert, einer Betriebs- oder Dienstvereinbarung.

Die Verhältnismäßigkeitsprüfung

Bevor eine Kameraanlage installiert werden darf, muss überprüft werden, ob dies überhaupt zulässig ist. Die Datenschutzgesetze verlangen eine rechtsverbindliche Prüfung, ob die schutzwürdigen Belange des Beschäftigten nicht schwerer wiegen als die berechtigten Interessen des Arbeitgebers. Die Kameraüberwachung stellt aufgrund ihrer schweren Eingriffe in das Persönlichkeitsrecht der Betroffenen das letzte Mittel dar, das zum Erreichen eines legalen Zieles eingesetzt werden darf. Im Vorfeld müssen alle Alternativen geprüft werden, die einen weniger schweren Eingriff in die Persönlichkeitssphäre darstellen. Das Bundesarbeitsgericht hat in einer Entscheidung (BAG, 26. August 2008 – 1 ABR 16/07) die Form einer solchen Prüfung vorgegeben. Diese ist auch auf die kirchlichen Datenschutzgesetze zu übertragen. Darin werden folgende Prüfungen verlangt:

1. Prüfung der Geeignetheit

Kann die Kameraanlage das angestrebte (legale!) Ziel überhaupt erreichen? Eine Kamera ist zur Verhinderung von unbefugtem Eindringen ungeeignet, zur Aufklärung ja. Eine Kameraanlage, die lediglich aufzeichnet, ist auch nicht zum Verhindern von Ladendiebstählen geeignet, eine Live-Kamera hingegen schon. Wenn ein Ladendieb erkannt wird, kann der Dieb von dem Sicherheitsdienst am Ausgang abgefangen werden. Also Live-Kamera und Sicherheitsdienst sind zum Diebstahlschutz geeignet.

2. Prüfung der Zulässigkeit

Es muss natürlich immer überprüft werden, ob das angestrebte Ziel überhaupt zulässig ist. Die Wahrung des Hausrechts, die Überwachung gefährlicher Bereiche sind z. B. zulässige Ziele. Eine Leistungs- oder Verhaltenskontrolle der Beschäftigten

über ein Kamerasystem ist hingegen kein legitimes Ziel im Sinne der Datenschutzgesetze. In Sozialräumen, sanitären Anlagen oder Umkleiden dürfen keine Kameras installiert werden, auch nicht zur Aufklärung von Diebstählen und Vandalismus.

3. Prüfung der Zumutbarkeit

Auch wenn eine Kameraanlage geeignet ist, ein legales Ziel zu erreichen, heißt das noch lange nicht, dass dies eine Maßnahme ist, die in einem angemessenen Verhältnis zu der Beeinträchtigung der Persönlichkeitsrechte steht. Zur Aufklärung von Diebstählen an Bleistiften sind Kameras an der Decke der Büros unverhältnismäßig. Zum Zweck der Aufklärung von Banküberfällen sind Kameras im Schalterbereich von Banken für die Beschäftigten zumutbar. Unzumutbar - darauf hat das Bundesarbeitsgericht hingewiesen - ist eine permanente Kameraüberwachung. Das muss ein Beschäftigter nicht hinnehmen.

Diese Prüfungen sind unaufgefordert vom Arbeitgeber vor Installation der Anlage vorzunehmen. Die Ergebnisse müssen rechtsverbindlich dargestellt und von allen Betroffenen - Beschäftigten wie auch Besuchern, Kunden, Patienten etc. einsehbar sein. Erst wenn alle Prüfungen mit einem positiven Ergebnis abgeschlossen wurden, ist der Kameraeinsatz für den geprüften Zweck im Sinne der Datenschutzgesetze zulässig. Eine andere Verwendung der Daten ist jedoch unzulässig.

Aber auch dann, wenn die Verhältnismäßigkeitsprüfung positiv abgeschlossen wurde, gelten die Mitbestimmungsrechte der Interessenvertretungen. Das heißt, die Betriebsräte, Personalräte oder Mitarbeitervertretungen müssen dem Einsatz förmlich zustimmen. Wesentlich besser ist jedoch, den Abschluss einer Betriebs- oder Dienstvereinbarung fordern, in der die betrieblichen Rahmenbedingungen - also wie die Überwachung rechtskonform erfolgen kann - für alle verständlich und verbindlich geregelt wird.

Handlungsmöglichkeiten für Beschäftigte

- Wer an einem Arbeitsplatz tätig ist, hat das Recht, Auskunft darüber zu verlangen, was die Kameras aufzeichnen, was mit den Daten passiert, wann sie gelöscht werden und natürlich, ob die Rechtmäßig-

keit des Kameraeinsatzes überhaupt geprüft wurde. Wer diese rechtmäßigen Fragen stellt, riskiert in der Praxis als Querulant aufzufallen. Mit diesen Fragen sollte man nach Möglichkeit an den Betriebsrat, Personalrat oder die Mitarbeitervertretung herantreten. Die Interessenvertreter können diese Fragen stellen und klären, ohne Repressalien befürchten zu müssen.

- Sofern keine Interessenvertretung existiert, kann man sich auch direkt an den Beauftragten für Datenschutz wenden und die entsprechenden Informationen und Prüfungsergebnisse verlangen.

- Werden die Fragen nach der Rechtmäßigkeit der Kameraanlage nicht oder nicht glaubhaft beantwortet, kann man sich auch an die zuständige Aufsichtsbehörde für den Datenschutz wenden (Kontaktdaten im Anhang), die diese Angelegenheit dann klären kann. Wer Repressalien befürchtet, kann die Aufsichtsbehörde auch anonym einschalten oder die Vertraulichkeit der Anfrage betonen.

- Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden.

Was können Interessenvertreter tun?

- Beim Einsatz von Kamerasystemen sind die Rechte der Interessenvertreter zu beachten. Für den Betrieb einer solchen Anlage ist entweder die formale Zustimmung der Betriebsräte, Personalräte, Mitarbeitervertretungen notwendig oder der Abschluss einer Betriebs- oder Dienstvereinbarung.

  Gerade durch Betriebs- und Dienstvereinbarungen werden die Rechte der Beschäftigten geschützt und der Datenschutz für die jeweilige Betriebsstätte konkretisiert. Es wird verbindlich festgelegt, wo Kameras aufgestellt werden, wer verantwortlich ist, zu welchen Zwecken die Daten verwendet

werden, dass die verbindlichen Prüfungen erfolgt sind usw. Allerdings sind Betriebs- und Dienstvereinbarungen nur in den genannten Grenzen möglich. Heimliche oder flächendeckende Überwachungen, gleich aus welchem Grund, können nicht vereinbart werden, die Überwachung von Sozialräumen, sanitären Einrichtungen und ähnlich intimen Bereichen auch nicht.

- Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar.

Telefonnutzung

Inhalt:

Worum geht es?

Telefonieren gehört heute für die Beschäftigten in fast allen Betrieben und Verwaltungen zum beruflichen Alltag. Ob als Teil der Arbeitsaufgabe, etwa in einem Call-Center, oder im Rahmen der üblichen Kommunikation mit Kollegen, Vorgesetzten, Kunden oder Lieferanten – ohne Telefon läuft so gut wie nichts. Dabei werden die technischen Möglichkeiten beim Telefonieren immer vielfältiger. Längst gibt es Video-Telefonie (z. B. für Konferenzschaltungen), mobiles Telefonieren (über Handys oder Smartphones) und vor allem auch das Telefonieren über das Internet (Voice-Over-IP). Moderne Telefonanlagen sind dabei heute bei Weitem nicht mehr nur für das Führen fernmündlicher Gespräche ausgelegt. Sie bieten oft gleichzeitig zahlreiche zusätzliche Anwendungsmöglichkeiten, wie Sprachaufzeichnung, Um- und Aufschaltung von Gesprächen oder auch Möglichkeiten des Fernabhörens von Nachrichten.

Egal ob privat oder dienstlich – in der Regel geht man davon aus, dass Telefongespräche in einem vertraulichen Rahmen geführt werden können. Kein Unbeteiligter soll ohne Weiteres von den Inhalten eines Gespräches Kenntnis erhalten. Und das nicht ohne Grund. Schließlich werden am Telefon häufig Dinge besprochen, die nicht für Dritte bestimmt und deshalb auch besonders schützenswert sind. Aus diesem Grund gibt es das Fernmeldegeheimnis (oft auch als Telekommunikationsgeheimnis bezeichnet). Es ist in Artikel 10 des Grundgesetzes der Bundesrepublik Deutschland verankert und wird jedem Bürger garantiert. Neben dem gesprochenen Wort, also dem Inhalt, sind auf der Grundlage des Fernmeldegeheimnisses

auch die weiteren Umstände eines Telefongespräches grundrechtlich geschützt. Hierzu zählen Informationen über den Zeitpunkt und die Dauer eines Telefongespräches oder auch Angaben darüber, mit wem telefoniert wurde.

Da es sich in der Regel bei den im Rahmen eines Telefongespräches anfallenden Informationen auch um personenbezogene Daten handelt, sind Fragen des Telefonierens außerdem Fragen des Datenschutzes. Insbesondere im Beschäftigungsverhältnis.

Abhören, Aufzeichnen und Mithören von Telefongesprächen

Gerade hinsichtlich der Inhalte von Telefongesprächen kommt es oft zu Unklarheiten. Auch und besonders am Arbeitsplatz. Es ergeben sich viele Fragen: Dürfen Gespräche vom Chef mitgehört werden? Dürfen Gespräche mitgeschnitten werden? Was ist bei Telefonkonferenzen mit mehreren Beteiligten zu berücksichtigen? Um hier die richtigen Antworten zu finden, ist es notwendig, genau zu differenzieren – und zwar zwischen Abhören, Aufzeichnen und Mithören.

Was das Abhören oder Aufzeichnen von Telefongesprächen angeht: Hier ist die Rechtslage in den meisten Fällen relativ eindeutig. Vor allem gilt: Telefongespräche sind durch das Fernmeldegeheimnis geschützt. In § 80 des Telekommunikationsgesetzes (TKG) wird dies konkretisiert:

> ***„(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.“***
>
> § 88 Telekommunikationsgesetz (TKG)

Mit dem Fernmeldegeheimnis wird bestimmt, dass das heimliche Aufzeichnen (oder Verändern bzw. Manipulieren) eines Gespräches und auch das Abhören mittels einer technischen Einrichtung (Abhörgerät) grundsätzlich verboten sind. Eine Ausnahme vom Verbot der Aufzeichnung besteht nur dann, wenn alle Gesprächsteilnehmer sich ausdrücklich einverstanden damit erklären oder wenn ein Gesetz dies vorsieht. Für das Abhören von Ge-

sprächen bestehen Ausnahmen nur im Rahmen von Gesetzen, die dies ausdrücklich vorsehen. Gesetzlich begründete Ausnahmen liegen hier beispielsweise vor im Falle von Strafverfolgungsmaßnahmen durch die Polizei (nur nach richterlichem Beschluss hierzu).

Jeder dieser Eingriffe in einen Telekommunikationsvorgang kann, sofern er unbefugt unternommen wurde, auch im Beschäftigungsverhältnis als Straftat gemäß § 201 StGB geahndet werden. Es gilt:

> ***(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt***
>
> ***1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder***
>
> ***2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.***
>
> ***(2) Ebenso wird bestraft, wer unbefugt***
>
> ***1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder***
>
> ***2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.***
>
> § 201 Strafgesetzbuch (StGB)

Beim Mithören von Telefongesprächen im Arbeitszusammenhang ist die rechtliche Lage etwas differenzierter. Übliche Mithörmöglichkeiten, wie sie Telefonanlagen bieten (Mithören über Lautsprecher), fallen nach einem Urteil des Bundesgerichtshofes von 1993 (Aktenzeichen: 2 StR 400/93) nämlich nicht unter das verbotene Abhören mit Abhörgeräten im Sinne von § 201 StGB (2) Nr. 1. Das Mithören über eine derartige Funktion ist daher nicht so strikt eingeschränkt wie das Abhören.

Dennoch sind auch beim Mithören die Persönlichkeitsrechte der Betroffenen zu beachten. Erlaubt ist ein solches Mithören entsprechend nur, wenn

- alle Beteiligten darüber in Kenntnis gesetzt sind und dem Vorgang zustimmen,
- wenn es ein Gesetz oder eine sonstige Rechtsvorschrift gesondert erlaubt,

- wenn der Mithörende hierfür ein im Sinne der Datenschutzgesetze berechtigtes Interesse nachweisen kann.

Das Mithören darf darüber hinaus nur einen begrenzten Zeitraum umfassen und muss auch dem Betroffenen bekannt sein. Heimliche oder vollumfängliche Mithöraktivitäten oder auch ein Mithören „einfach so“, ohne Grund, bleiben verboten. Man sollte daher immer darauf achten, etwa während einer Telefonkonferenz, sicherzustellen, dass alle Beteiligten über Einzelheiten des Telekommunikationsvorganges in Kenntnis gesetzt werden. Jeder Teilnehmer muss Bescheid darüber wissen, wer am Gespräch beteiligt ist und wer mithören kann.

Dies gilt grundsätzlich auch beim Mithören von Gesprächen durch Vorgesetzte z. B. zu Schulungszwecken, etwa in Call-Centern. Hier ist es durchaus üblich, dass Gespräche mitgehört oder auch mitgeschnitten werden, um diese später auszuwerten und einer internen Kritik zu unterziehen. Auch hier gilt das Fernmeldegeheimnis. Eine Aufzeichnung darf also nur bei vorliegender Zustimmung der Gesprächsteilnehmer (auch des Beschäftigten) erfolgen und ist andernfalls rechtswidrig.

Telefonieren und Datenschutz

Telefongespräche umfassen längst nicht mehr nur die simple Übermittlung des gesprochenen Wortes. Heute passiert sehr viel mehr. So verarbeiten moderne Telefonanlagen zahlreiche Daten, die über das eigentliche Gespräch hinaus gehen. Man kennt es vom Einzelverbindungsnachweis des privaten Telefondienste-Anbieters: Zeitpunkt, Dauer und angewählte Nummern werden protokolliert, um dem Anschlussinhaber eine Übersicht der erfolgten Gespräche über einen gewissen Zeitraum hinweg (z. B. monatsweise) zu geben. Die anfallenden Daten geben damit über vielerlei Dinge Auskunft.

Kann man den Telefonanschluss oder einzelne Gespräche einer bestimmten Person zuordnen, so sind die Daten, die hierüber Informationen liefern, personenbezogene Daten. Es gilt deshalb zu beachten: Die Erhebung und Verarbeitung der personenbezogenen Daten unterliegt den gesetzlichen Datenschutzbestimmungen. Grundsätzlich gilt: Jeder Bürger hat ein durch das Grundgesetz in den Artikeln

1 und 2 (Allgemeine Persönlichkeitsrechte) verbürgtes und in den Datenschutzgesetzen konkretisiertes Recht auf seine informationelle Selbstbestimmung. Informationelle Selbstbestimmung bedeutet, dass es für jeden Bürger möglich sein muss, so weit wie möglich selbst darüber zu entscheiden, ob Daten, die Auskunft über ihn oder sein Verhalten geben können, erhoben und verarbeitet werden oder nicht.

Nur wenn es im weit überwiegenden Interesse der Allgemeinheit liegt oder wenn es kein nachvollziehbares Schutzinteresse gibt, darf dies auch gegen den Willen des Betroffenen geschehen. Dies ist beispielsweise dann der Fall, wenn ein Gesetz vorsieht, dass bestimmte personenbezogene Daten erhoben oder verarbeitet werden. Im Arbeitsverhältnis liegt dies beispielsweise vor, wenn Angaben für die Sozialversicherung (z. B. Beschäftigungszeiten) an die Sozialversicherungsträger (Krankenkassen, Rentenversicherung) übermittelt werden. Da es Gesetze gibt, die eine entsprechende Versicherungspflicht vorsehen, ist in diesem Fall auch die Übermittlung personenbezogener Daten rechtmäßig.

Eine weitere Ausnahme liegt – neben der persönlichen Einwilligung des Betroffenen – dann vor, wenn eine sonstige Rechtsvorschrift dies verlangt. Auch eine Betriebs- oder Dienstvereinbarung kann eine solche sonstige Rechtsvorschrift darstellen. In ihr kann eine Datenerhebung oder -verarbeitung zwischen betrieblicher Arbeitnehmervertretung und dem Arbeitgeber vereinbart sein. Sie muss dabei dem grundsätzlichen Schutzniveau des jeweils geltenden Datenschutzgesetzes entsprechen. Es gelten:

- Das Bundesdatenschutzgesetz (BDSG) für nicht-öffentliche Stellen (privatwirtschaftliche Unternehmen) und Bundesbehörden,
- das Saarländische Datenschutzgesetz (SDSG) für Landesbehörden im Saarland sowie
- aufgrund der kirchlichen Sonderstellung spezielle Datenschutzvorschriften für kirchliche Einrichtungen (das DSG-EKD für die Evangelische Kirche und die KDO für die Katholische Kirche).

Wird vereinbart, dass die Nutzung der dienstlichen Telefonanlage anhand von

erfassten Verbindungsdaten ausgewertet (oder kontrolliert) werden soll, so muss im Vorfeld eine Interessenabwägung zwischen Arbeitgeber und Beschäftigten stattgefunden haben. Erst wenn die Interessen der Arbeitgeberseite nach einer Kontrolle (z. B. hinsichtlich einer missbräuchlichen Nutzung der Telefonanlage) gegenüber den Persönlichkeitsrechten der Beschäftigten deutlich überwiegen, sind Kontrollen auch erlaubt. Und nur wenn es keine andere zumutbare Form der Kontrolle gibt, kann dies auch auf dem Weg von Datenauswertungen erfolgen. Zu berücksichtigen bleibt außerdem: Es darf keine Totalüberwachung geben und der jeweilige Beschäftigte muss auch darüber in Kenntnis sein, dass Kontrollen unternommen werden (können). Und: Personenbezogene Daten, die für diesen bestimmten Zweck erhoben wurden, dürfen auch ausschließlich für diesen verwandt werden und sind nach der Erfüllung des Zweckes (nach der Kontrolle) wieder zu löschen.

Private Telefonnutzung am Arbeitsplatz

Im Beschäftigungsverhältnis dreht sich häufig vieles um die Frage: Ist auch eine private Nutzung des dienstlichen Telefonanschlusses erlaubt? Grundsätzlich gilt: Es gibt von Seiten des Arbeitnehmers keinen Anspruch auf die Verwendung des dienstlichen Anschlusses in privaten Zusammenhängen. Insbesondere deshalb sollten Beschäftigte immer auch im Auge behalten, dass eine Privatnutzung des dienstlich bereitgestellten Telefons zwar durchaus sozialüblich sein kann, jedoch auch in bestimmten Zusammenhängen als Verstoß gegen die arbeitsvertraglichen Pflichten ausgelegt werden kann. Insbesondere gilt dies, wenn die Privatnutzung ein bestimmtes Ausmaß überschritten hat und die Erbringung der Arbeitsleistung dadurch negativ beeinflusst wird. In Fällen übermäßigen Privattelefonierens am Arbeitsplatz, können also durchaus Abmahnungen oder Kündigungen gerechtfertigt sein.

Dennoch erlauben viele Arbeitgeber eine Nutzung des Telefons – meist in geringem Umfang – auch für private Zwecke. Damit ergeben sich unterschiedliche Folgen, insbesondere auch hinsichtlich des Umgangs mit personenbezogenen Daten.

Erlaubt ein Arbeitgeber seinen Mitarbeitern, privat zu telefonieren, so wird er – juristisch betrachtet – gemäß der Bestimmungen des Telekommunikationsgesetzes

(TKG) zu einem Anbieter von Telekommunikationsdienstleistungen. Damit darf er – sofern dies notwendig ist – personenbezogene Gesprächsdaten nur zur Sicherstellung der Funktionsfähigkeit der Telefonanalage oder zu Zwecken der kostenmäßigen Abrechnung der Gespräche erheben und verarbeiten. Ausnahme: Der Beschäftigte hat ausdrücklich erklärt, dass er mit darüber hinausgehenden Datenerhebungen oder -verarbeitungen einverstanden ist.

Kontrollen durch den Arbeitgeber anhand der angefallenen personenbezogenen Nutzungsdaten sind damit in nur sehr engen Grenzen möglich. Soll etwa auch eine Kontrolle hinsichtlich einer möglichen missbräuchlichen Nutzung erfolgen, so müssen in der Regel die Beschäftigten eine Einverständniserklärung zu dieser weitergehenden Kontrolle abgeben. Weigert sich der Betroffene, so ist ihm dann meist die private Nutzung nicht gestattet.

Verbietet ein Arbeitgeber die Privatnutzung ausdrücklich, so ist er für eine etwaige Datenerhebung immer noch an die Vorgaben der Datenschutzgesetze (BDSG, SDSG, DSG-EKD, KDO) gebunden. Zwar benötigt er in diesem Fall für entsprechende Missbrauchskontrollen nicht unbedingt ein Einverständnis des Betroffenen, jedoch sind die Verhältnismäßigkeit des eingesetzten Verfahrens und der Schutz der Persönlichkeitsrechte auf jeden Fall zu berücksichtigen. Und auch hier gilt: Totalüberwachung oder heimliche Kontrollen bleiben verboten.

Neben den bereits beschrieben Daten über Telefongespräche und -verbindungen lassen sich auf technischem Wege häufig weitere Informationen über den Telekommunikationsvorgang erlangen. Insbesondere über die Voice-Over-IP-Technik (Telefonieren über das Internet) ergeben sich heute zahlreiche und auch neue Auswertungsmöglichkeiten. So kann etwa die Anzahl nicht angenommener Gespräche erfasst werden, die Dauer vom Eingehen des Anrufes bis zum Entgegennehmen, die Anzahl weitergeleiteter Gespräche und vieles mehr.

Diese Auswertungsmöglichkeiten können im Arbeitsverhältnis zu vielen kritischen Situationen führen: Beschäftigte und ihre Arbeitsleistung können anhand der gesammelten Daten beurteilt und gemessen werden. Eine solche „Leistungs- und Verhaltenskontrolle“ über die mittels einer

Telefonanlage erhobenen personenbezogenen Daten ist grundsätzlich nicht erlaubt. Ähnlich wie das Mithören oder Aufzeichnen von Gesprächen ist auch dies nur nach einer erteilten individuellen Erlaubnis der Betroffenen oder einer entsprechenden innerbetrieblichen Regelung (Betriebsvereinbarung) gestattet. Und auch hier gilt: Eine derartige Regelung darf nicht den datenschutzrechtlichen Mindeststandard des Telekommunikationsgesetzes (bei einer mindestens in Teilen erlaubten Privatnutzung) bzw. der Datenschutzgesetze unterlaufen.

Betriebs- und Dienstvereinbarungen

Am Arbeitsplatz gelten nicht nur Gesetze, Verordnungen, Arbeitsanweisungen oder Arbeitsverträge. Es gelten häufig auch Betriebs- oder Dienstvereinbarungen. Diese Verträge zwischen Arbeitnehmervertretung (Betriebsrat, Personalrat oder Mitarbeitervertretung) und Arbeitgeber gelten für alle Beschäftigten. Niemand kann ohne Weiteres davon ausgenommen werden. In solchen betrieblichen Vereinbarungen kann unter anderem auch der Umgang mit der Telekommunikations-Infrastruktur also konkret auch der Telefonanlage festgelegt werden. Die Bestimmungen sind bindend.

Sofern es Betriebs- oder Dienstvereinbarungen gibt, ist in ihnen meist auch festgehalten, welche Technik (Telefonanlage selbst) eingesetzt wird, ob und wenn ja in welchem Rahmen eine mögliche Privatnutzung erlaubt ist, wie Kontrollen der Nutzung erfolgen und welche personenbezogenen Daten hierfür verwendet werden dürfen. Hierbei sind die bereits erläuterten gesetzlichen Regelungen zu beachten. Zwar ermöglichen Betriebs- oder Dienstvereinbarungen als „sonstige Rechtsvorschriften“ auch die Erhebung und Verarbeitung personenbezogener Daten, jedoch muss auch diese immer im Rahmen der Wahrung der Persönlichkeitsrechte der betroffenen Arbeitnehmer erfolgen.

Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar.

Fotografieren und Filmen von Mitarbeitern

Inhalt:

Worum geht es?

Immer häufiger möchten Unternehmen und Einrichtungen Fotos von ihren Mitarbeitern auf Webseiten einstellen oder auf Informationsmaterial abdrucken, um eine besondere Servicefreundlichkeit nach außen hin zu demonstrieren. Das Weisungsrecht des Arbeitgebers geht so weit, dass er die dienstlichen Kontaktdaten z. B. E-Mail-Adresse und Durchwahl von Mitarbeitern bekannt geben kann, wenn sie als Ansprechpartner fungieren.

Oft ist allerdings unklar, ob der Arbeitgeber eigenmächtig entscheiden kann, ob Fotos von Mitarbeitern veröffentlicht werden, vor allem aber wie man sich als Mitarbeiter in solchen Fällen verhalten kann. Ähnliches gilt für das Erstellen von Filmen am Arbeitsplatz zu Werbezwecken, für Schulungen oder Ähnliches, in denen Mitarbeiter als Darsteller abgebildet werden.

Durch die rasanten Entwicklungen der Verbreitung im Internet können unerwünschte Effekte entstehen. Besonders durch die Ausweitung automatischer Gesichtserkennung sind die Risiken des Missbrauchs stark gestiegen und müssen im Zusammenhang mit biometrischen Verfahren bewertet werden. Hinzu kommt die Problematik der Urheber- und Nutzungsrechte.

Rechtlicher Hintergrund:

Bei Fotos und Filmen, auf denen Mitarbeiter zu erkennen sind, handelt es sich eindeutig um personenbezogene Daten. Bei der Verwendung personenbezogener Daten sichern uns die Datenschutzgesetze zu, selbst darüber zu entscheiden, ob wir das möchten oder nicht, außer eine Rechtsvorschrift geht dieser Regel vor. Das ist hier der Fall - es gibt ein „vorgeschaltetes“ Gesetz, das Kunsturheberrechtsgesetz. Für die Beschäftigten ist das günstig.

Das Recht am eigenen Bild ist ein durch das Grundgesetz verbürgtes allgemeines Persönlichkeitsrecht. Es gilt auch für das Filmen von Personen. Das Recht am eigenen Bild wird allerdings nicht durch die Datenschutzgesetze geregelt, sondern über das Kunsturheberrechtsgesetz (KunstUrhG). Das Kunsturheberrechtsgesetz sichert in § 22 jeder Person zu, selbst darüber zu entscheiden, ob sie fotografiert oder gefilmt werden möchte. Ausnahmen sind Personen der Zeitgeschichte, die es quasi als Zugeständnis an ihre Bedeutsamkeit und ihre Prominenz hinnehmen müssen, auch ungewollt abgelichtet zu werden. Die zweite Ausnahme entsteht, wenn für das Aufnehmen ein Honorar ausgehandelt wird wie zum Beispiel bei Models und Schauspielern. Auch wenn auf Versammlungen und Aufzügen (gemeint sind Umzüge in der Öffentlichkeit) fotografiert wird, gibt es eine Ausnahmeregel. Der Arbeitsplatz ist keine öffentliche Veranstaltung, an der man nach Belieben teilnehmen kann und damit auch in Kauf nehmen muss fotografiert zu werden. Für Beschäftigte treffen die Ausnahmeregelungen nicht zu.

Je nach Arbeitsplatz gelten unterschiedliche Datenschutzgesetze. Das Kunsturheberrechtsgesetz hingegen gilt auf dem gesamten Staatsgebiet der Bundesrepublik Deutschland und somit genauso für Mitarbeiter kirchlicher Einrichtungen, Beamte im Staatsdienst oder Mitarbeiter in Unternehmen. Allen Beschäftigten steht es zu, frei darüber zu entscheiden, ob sie abgebildet werden möchten oder nicht.

Das Direktionsrecht des Arbeitgebers wird in der Gewerbeordnung (GewO) formuliert und ist ein weniger starkes Recht, als das allgemeine Persönlichkeitsrecht. Der Bezug von Lohn/Gehalt erfolgt auf der Erbringung einer Arbeitsleistung und ist nicht als Honorar im Sinne des Kunsturheber-

rechts anzusehen. Insofern ist es dem Arbeitgeber - rechtlich - nicht möglich, über die Köpfe der Betroffenen hinweg zu entscheiden, dass sie fotografiert und die Fotos gewerblich genutzt werden.

Die Entscheidung, ob man als Mitarbeiter sein Bild auf der Webseite des Unternehmens finden möchte, kann man selbst treffen.

Sonderfall Werksausweise

> *Zur Zutrittskontrolle werden in Unternehmen und Einrichtungen Mitarbeiterausweise ausgestellt. Es liegt weitgehend im Direktionsrecht des Arbeitgebers, ob er dies möchte oder nicht. Wenn diese Ausweise Fotos des Inhabers enthalten sollen, kommt das Kunsturheberrecht zum Tragen und konkurriert mit dem Direktionsrecht. Ob ein Mitarbeiter über die Verwendung seines Bildes auf einem Werksausweis entscheiden kann, hängt erheblich davon ab, ob die Werksausweise aus sicherheitsrelevanten Gründen tatsächlich notwendig sind.*
>
> *Als Mitarbeiter eines Atomkraftwerks muss man das sicher hinnehmen. Die Gefahren, die durch einen unkontrollierten Zutritt für die Allgemeinheit ausgehen, sind zweifellos höher zu bewerten, als das Recht am eigenen Bild, zumal der Verwendungszweck die Veröffentlichung nicht beinhaltet. Ob dieses Sicherheitsbedürfnis objektiv so hoch ist, dass das Recht am eigenen Bild nicht mehr greift, muss an jeder Betriebsstätte im Einzelfall geklärt werden. Auf bloßen Wunsch hin können keine Persönlichkeitsrechte außer Kraft gesetzt werden. Nur Behörden können „zum Zwecke der Rechtspflege und der öffentlichen Sicherheit“ (§ 24 KunstUrhG) Fotografien ohne Erlaubnis verwenden.*

Rolle der Arbeitnehmervertreter

Da dieses Persönlichkeitsrecht abschließend im Kunsturheberrechtsgesetz formuliert ist, ist es auch nicht möglich, eine Betriebs- oder Dienstvereinbarung zu diesem Thema abzuschließen. Betriebsräte, Per-

sonalräte und Mitarbeitervertretungen spielen dennoch eine wichtige Rolle bei diesem Thema.

Beim Kunsturheberrecht handelt es sich um ein Gesetz zugunsten der Beschäftigten. Die Arbeitnehmervertreter haben die Aufgabe darüber zu wachen, dass dieses Recht umgesetzt wird, dass also sicher gestellt wird, dass kein Mitarbeiter unter Druck gesetzt wird, sondern seine Entscheidung frei treffen möchte. Und diese Entscheidung sollte man sich reiflich überlegen.

Risiken für die Beschäftigten

Wenn heute Fotos und Filme im Internet dargestellt werden, muss man davon ausgehen, dass man nicht mehr kontrollieren kann, was daraus entsteht. Ein effektiver Schutz gegen ungewünschtes Kopieren ist nicht möglich. Es ist auch kaum möglich, Fotos zu löschen, die anschließend in unerwünschten Zusammenhängen im Internet auftauchen oder gar zum Identitätsdiebstahl genutzt werden können.

Objektiv gesehen birgt ein Mitarbeiterbild im Intranet, also im Firmennetzwerk des Unternehmens dieselben Risiken. Jeder, der die Fotos ansehen kann, kann sie auch mit wenigen Handgriffen kopieren und ins Internet stellen.

Allein die Bildersuche nach Namen des betroffenen Mitarbeiters in den bekannten Suchmaschinen macht solche Bilder für jeden verfügbar und ermöglicht es, sie zu kopieren. Seit geraumer Zeit werden auch spezielle Personen-Suchmaschinen betrieben (z. B. yasni.com oder 123people.com), die alle im Internet vorhandenen Informationen über eine Person zusammenstellen und für jedermann kostenlos verfügbar machen. Das erfolgt automatisch, ungeachtet dessen, ob die Informationen wahr oder falsch sind oder der Betroffene eingewilligt hat. Denn es werden natürlich nicht nur Selbstauskünfte des Betroffenen sondern auch Informationen Dritter über die betroffene Person hinzu gezogen. Problematisch ist auch, dass sich die Betreiber auf US-amerikanisches Recht berufen und Einsprüche der Betroffenen schwierig bis unmöglich sind.

Mitarbeiterfotos auf Unternehmensseiten in Sozialen Netzwerken:

Gesichtserkennung und Biometrische Profile von Beschäftigten

Besonders kritisch wird es, wenn solche Mitarbeiterfotos - von wem auch immer - in sozialen Netzwerken eingestellt werden. Jedes Foto, das bei facebook eingestellt wird, durchläuft automatisch eine Gesichtserkennung. Werden Menschen auf Fotos erkannt, werden ihre Gesichter vermessen (Augenabstand, Kopfform). Diese Daten ergeben ein nahezu unverwechselbares biometrisches Profil einer Person. Man braucht nur noch die Unterstützung der Mitglieder, den biometrischen Merkmalen einen Namen zuzuordnen. facebook fordert derzeit (2012) alle Mitglieder auf, sich an der Gesichtserkennung zu beteiligen und bei Fotos die Personen zu benennen, die man erkennt. Name und biometrische Merkmale der Person sind fortan bei facebook gespeichert, ohne dass es die betroffene Person weiß.

Die Zuordnung von Gesicht und Name können alle Nutzer von facebook vornehmen, die diese Person kennen. Es spielt keine Rolle, ob die abgebildete Person auf einem (Gruppen-)Foto Mitglied von facebook ist oder nicht. Die Person wird biometrisch vermessen und von Mitgliedern mit einem Namen versehen. Für welche Geschäftsmodelle die gespeicherten biometrischen Merkmale von Personen herhalten werden, kann nur spekuliert werden. Fakt ist, die biometrischen Profile werden erstellt und gespeichert.

Facebook ist wie so oft Vorreiter, hat allerdings kein Monopol auf diese Technik. Die Gesichtserkennung funktioniert erschreckend gut und verbreitet sich rasant im Alltag. Wer digitale Bilder von sich veröffentlicht oder es anderen überlässt das zu tun, setzt sich diesem Risiko aus. Ein Foto im Intranet - zum Beispiel von der Betriebsfeier - ist mit wenigen Mausklicks bei facebook eingestellt, der Name ist zugeordnet und die biometrischen Merkmale sind gespeichert. Das ist Alltag, keine Zukunftsvision.

Weiteres Problem: Nutzungsrechte

Ein weiteres Problem kann entstehen, wenn Mitarbeiter gebeten werden Fotos für betriebliche Zwecke (Internet, Intranet, Werkszeitung…) zur Verfügung zu stellen,

die für andere Zwecke angefertigt worden sind. Gerne wird auf sogenannte Beauty-Fotos oder Bewerbungsfotos zurückgegriffen, die professionelle Fotografen erstellt haben. Auch wenn diese Fotos von den abgebildeten Personen bezahlt wurden, haben sie damit nicht automatisch auch das Recht erworben, diese Bilder zu scannen, digitale Kopien zu erstellen oder dem Arbeitgeber Nutzungsrechte einzuräumen. Will man dem Arbeitgeber ein Foto für betriebliche Zwecke überlassen, muss man sich beim Fotografen versichern, dass dies im Preis eingeschlossen ist. Findet ein Fotograf ein solches Foto im Internet z. B. auf der Webseite des Unternehmens, kann er eine Nutzungsgebühr verlangen, die sich nach Verbreitungsgrad und Nutzungsdauer berechnet. Für Fotos, die ohne Nutzungsrechte im Internet veröffentlicht werden, entstehen schnell Nutzungsgebühren im vierstelligen Bereich.

Ein anderes Problem taucht auf, wenn Unternehmen, Behörden und sogar Ministerien eigene Seiten in sozialen Netzwerken betreiben. Ein Auftritt bei facebook ist heute alltäglich. Werden dort Fotos von Mitarbeitern eingestellt, hat man nicht nur das bereits geschilderte Problem mit biometrischen Daten. In den umfangreichen Nutzungsbedingungen von sozialen Netzwerken werden den Betreibern oft uneingeschränkte Nutzungsrechte eingeräumt für alles, was dort veröffentlicht ist. Also auch für Fotos. Für die Netzwerke spielt es letztlich keine Rolle, ob man diese Rechte tatsächlich besitzt, denn in den Nutzungsbedingungen wird vorausgesetzt, dass man nur einstellen darf, wofür man auch die Nutzungsrechte hat. Damit haben sich die Betreiber der Netzwerke abgesichert. Das Schadensrisiko bleibt bei dem, der das Foto eingestellt hat.

Fazit:

Das Recht am eigenen Bild ist ein allgemeines Persönlichkeitsrecht. An allen Betriebsstätten gilt das Kunsturhebergesetz. Es regelt in § 22, dass Mitarbeiter ohne ihre ausdrückliche Erlaubnis nicht fotografiert oder gefilmt werden dürfen. Der Zweck des beabsichtigten Fotografierens oder Filmens spielt dabei keine Rolle, außer bei außerordentlich sicherheitsrelevanten Anlagen für Sicherheitsüberprüfungen. Hier kann es Ausnahmen geben.

Das Direktionsrecht des Arbeitgebers geht nicht so weit, dass er über das Fotografie-

ren von Mitarbeitern und die Verwendung der Fotos entscheiden kann.

Der Mitarbeiter kann frei entscheiden, ob er einverstanden ist oder nicht. Betriebsräte, Personalräte und Mitarbeitervertretungen können zwar zu diesem Thema keine Betriebsvereinbarung abschließen, sie sind aber dazu verpflichtet zu kontrollieren, dass geltendes Recht umgesetzt und kein Mitarbeiter unter Druck gesetzt wird.

Auch wenn der Arbeitgeber ein durchaus legitimes Anliegen hat, so ist es ihm beim Abbilden von Mitarbeitern in Intranet und Internet überhaupt nicht möglich, die abgebildeten Mitarbeiter vor Schäden zu bewahren, die durch den Missbrauch entstehen.

Inzwischen sind die Missbrauchsrisiken außerordentlich groß geworden. Speziell durch den Einsatz von Gesichtserkennungssystemen, die in soziale Netzwerke integriert sind und biometrische Merkmale der Abgebildeten speichern, ganz gleich, ob sie Mitglied in dem Sozialen Netzwerk sind, oder ob sie nur auf einem Foto erscheinen, das ein Mitglied eingestellt hat. Daneben stellen sich auch urheberrechtliche Fragen im Hinblick auf die Übertragung von Nutzungsrechten der Fotos auf den Arbeitgeber und ggf. die sozialen Netzwerke.

Das Risiko für das Unternehmen oder die Einrichtung ist relativ gering. Das Risiko, das Beschäftigten durch das Einstellen von Mitarbeiterfotos in Unternehmensauftritten bei facebook und anderen sozialen Netzwerken entsteht, ist hingegen nicht abzuschätzen. Auch wenn die Risiken letztlich nicht vom Arbeitgeber ausgehen, sollte man sich als Mitarbeiter der persönlichen Risiken bewusst sein, die der Arbeitgeber auch bei bestem Willen nicht verhindern kann.

Diese Entscheidung darf nicht durch das Ausüben von Druck herbeigeführt werden. Wer dies tut oder Fotos von Mitarbeitern ohne deren explizites Einverständnis anfertigt oder veröffentlicht, riskiert nach § 33 KunstUrhG eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe.

Kann der Arbeitgeber das Einverständnis des Mitarbeiters nicht nachweisen, gilt es als nicht erteilt. Ein bereits - vielleicht in Unkenntnis der Situation - gegebenes Einverständnis des Mitarbeiters kann jeder-

zeit ohne Angabe von Gründen widerrufen werden.

Sofern ein Arbeitgeber dem nicht nachkommt, sollten sich betroffene Mitarbeiter an ihren Betriebsrat, Personalrat oder Mitarbeitervertretung wenden, da dieses Problem höchstwahrscheinlich noch weitere Mitarbeiter betrifft. Wird diese Praxis nicht abgestellt, ist es bei dieser Sachlage aussichtsreich einen Juristen einzuschalten.

Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden. Kontaktadresse im Anhang.

Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktadresse im Anhang.

GPS, Ortungssysteme und Flottenmanagement - Ortung mit Smartphones

Inhalt:

Worum geht es?

Navigationssysteme sind in viele Dienst- und Firmenfahrzeuge eingebaut und sind ein geschätztes Hilfsmittel, um ohne Umwege zum Ziel zu gelangen. Verschiedene Navigationssysteme verfügen zusätzlich über einen Rückkanal, über den die aktuellen Standortpositionen an den Arbeitgeber gesendet werden. Das kann dazu benutzt werden, um einen Außendienst oder Lieferfahrzeuge zu steuern (Flottenmanagement), oder um die Fahrer permanent zu kontrollieren. Wenn es um eine „einfache“ Standortverfolgung geht, lassen sich auch GPS-Sender (Track-Logger) installieren. Diese werden oft (aber nicht ausschließlich!) in Nutzfahrzeugen installiert, um sie nach Diebstählen wieder aufzufinden. Da Smartphones auch über GPS-Sensoren verfügen, lassen sich auch darüber sehr einfach solche Bewegungsprofile der Nutzer erstellen.

Risiken für Beschäftigte

Die verbesserten Möglichkeiten Fahrtrouten des Außendienstes zeitnah zu steuern sind unbestritten. Allerdings stellen Ortungssysteme für Beschäftigte ein beträchtliches Risiko dar: Erste Kündigungen, die mithilfe von GPS-Daten begründet wurden, hat es bereits gegeben. Weiter verbreitet sind jedoch Leistungsbeurteilungen, Ermahnungen und Abmahnungen wegen unerwünschten Fahrverhaltens (zu langsam, zu schnell, zu hoher Spritverbrauch usw.). Flottenmanagementsysteme bringen ab Werk bereits viele Überwachungs- und Kontrollmechanismen mit, die in Deutschland unzulässig sind, wenn sie auf Beschäftigte angewendet werden.

Wenn dienstliche Smartphones auch privat genutzt werden können, und die Ortungsfunktion aktiviert ist, ergibt sich aus Standortdaten ein detailliertes Protokoll des Sozialverhaltens. Ein mitgeführtes Smartphone registriert, ob man sich in einer Arztpraxis, in einer Apotheke, einer Gaststätte, im Fitnessstudio, in der Wohnung eines Kollegen oder in einem Etablissement mit eher zweifelhaftem Ruf aufhält. Alles höchstprivate Angaben, die in keiner Beziehung zum Arbeitsverhältnis stehen.

Bei Ortungssystemen, Flottenmanagement und der Ortung über Smartphones ist es nicht immer bekannt, dass die gesamten Wegstrecken mitverfolgt werden, geschweige denn, was mit den Daten passiert.

Im Folgenden geht es um die Fragen:

- ***Was ist zulässig?***
- ***Wie kann man als Beschäftigter auf Ortungssysteme Einfluss nehmen?***

Rechtliche Situation:

- Eine verdeckte Ortung ist unzulässig. Für Navigationssysteme mit Rückkanal zum Flottenmanagement handelt es sich im Sinne der Datenschutzgesetze um sogenannte mobile personenbezogene Speicher- und Verarbeitungsmedien im Sinne von § 3 Abs. 10, § 6c BDSG und § 3 Abs. 9, § 18 SDSG.

- Für Ortungsgeräte oder Smartphones, die mit den Nutzern in fester Beziehung stehen, gelten die Vorgaben der Datenschutzgesetze (§§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD, § 3 KDO). Bei Smartphones gilt zusätzlich die Bildschirmarbeitsplatzverordnung (BildschArbV, Anhang Nr. 22), die ebenfalls eine verdeckte Ortung verbietet.

- Eine erkennbare Ortung kann üblicherweise nicht aus den arbeitsvertraglichen Pflichten des Mitarbeiters abgeleitet werden. Selbst bei Fahrern ist eine Totalüberwachung aufgrund der Datenschutzgesetze (§§ 4, 32 BDSG, §§ 4, 31 SDSG,

§§ 4, 24 DSG-EKD, § 3 KDO) unverhältnismäßig und damit unzulässig. Der Arbeitgeber kann so etwas nicht eigenmächtig veranlassen.

- Eine erkennbare, begrenzte Ortung zu festgelegten Zwecken kann unter Einhaltung gesetzlicher Vorgaben zulässig sein.

Handlungsmöglichkeiten

- Wer ein dienstliches Smartphone erhält, sollte sich erkundigen, ob die Standortfunktion aktiviert ist. Das ist für den Nutzer nicht mehr ersichtlich, wenn hierzu vom Arbeitgeber bereits eine entsprechende App installiert wurde. In vielen Fällen nützt es wenig, den GPS-Sensor auszuschalten, da er von der App wieder eingeschaltet werden kann. Deshalb sollte man sich diese Aussage nach Möglichkeit schriftlich geben lassen. Jeder Beschäftigte hat das Recht, Auskunft zur Erhebung und Verarbeitung seiner Daten zu verlangen (§ *34 BDSG,* § 20 SDSG, § 15 DSG-EKD und § 13 KDO).
- Das Gleiche gilt für Navigations- oder Ortungssysteme. Man sollte sich erkundigen, ob Wegstrecken aufgezeichnet und an den Arbeitgeber gesendet werden. Bei Flottenmanagementsystemen ist das offensichtlich und ein wesentlicher Einsatzzweck. Aber auch hier sollte man sich zunächst einen Überblick verschaffen, welche Daten zu welchen Zwecken ausgewertet werden können. Die üblichen Auswertungsmöglichkeiten selbst „einfacher“ Flottenmanagementsysteme sind sehr umfangreich und offenbaren ungeahnte Details. Eine schriftliche Antwort ist wichtig, und man sollte selbst einen Blick in die Auswertungsmöglichkeiten nehmen. Das kann man als Beschäftigter mit Verweis auf das Auskunftsrecht der Datenschutzgesetze verlangen (§ *34 BDSG,* § 20 SDSG, § 15 DSG-EKD und § 13 KDO).
- Sofern es eine Interessenvertretung gibt, ist es sinnvoll anzuregen, eine Betriebs- oder Dienstvereinbarung abzuschließen. Das ermög-

licht eine ausgewogene und einheitliche Lösung und verhindert, dass einzelne Mitarbeiter zu freiwilligen Einwilligungen überredet werden.

- Sofern es keine Interessenvertretung gibt, sollte man sich als Mitarbeiter über die wesentlichen Punkte mit dem Arbeitgeber verständigen und dies schriftlich festhalten. Dieses Vorgehen entspricht einer freiwilligen Einwilligung des Beschäftigten. Ohne eine solche freiwillige Einwilligung darf der Arbeitgeber keine Ortung von Mitarbeitern vornehmen (außer eine Betriebs-/Dienstvereinbarung wurde abgeschlossen).

  Aber auch hier kann keine vollständige Überwachung vereinbart werden. Auch wenn es keine „Gegenleistung“ des Arbeitgebers für die Benachteiligung durch die Überwachung für den Beschäftigten gibt, ist eine solche Vereinbarung rechtlich unwirksam. Es widerspricht dem gesunden Menschenverstand, als Beschäftigter einem solchen Überwachungsdruck ohne Gegenleistung zuzustimmen. Es muss davon ausgegangen werden, dass die Einwilligung nicht wie rechtlich gefordert freiwillig gegeben wurde. Sie ist somit unwirksam.

- Eine freiwillige Einwilligung sollte nicht ohne guten Grund erfolgen. Zur Einwilligung gehört auch, dass schriftlich festgehalten wird, zu welchen Zwecken die Daten verwendet werden. Eine anderweitige Nutzung ist ausgeschlossen.

- Hat man als Mitarbeiter den Eindruck, dass man auf unzulässige Art überwacht wird, sollte man dies möglichst lückenlos dokumentieren, Indizien und Beweise sammeln und Aussagen protokollieren. Sonst läuft man Gefahr, dem Arbeitgeber etwas zu unterstellen. Es kann hilfreich sein, in Erfahrung zu bringen, ob es anderen genauso geht. Sofern vorhanden, sollte man die Interessenvertretung informieren. Diese kann sich gemeinsam mit dem Beauftragten für Datenschutz um die Angelegenheit kümmern.

- Gibt es keine Interessenvertretung und auch keinen Beauftragten für Datenschutz oder bestehen Zweifel an seinem Engagement, kann man sich auch an die Aufsichtsbehörde für den Datenschutz wenden.

- Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saarlandes wenden. Kontakt im Anhang.

Was können Interessenvertreter tun?

- Beim Einsatz von Ortungssystemen oder Geräten, die zur Ortung benutzt werden können, sind die Rechte der Interessenvertreter zu beachten. Betriebsräte, Personalräte und Mitarbeitervertretungen haben mitzubestimmen in Fragen der Ordnung und des Verhaltens im Betrieb und bei der Nutzung von technischen Einrichtungen, die dazu geeignet sind, die Leistung oder das Verhalten von Mitarbeitern zu kontrollieren.

  Ziel einer solchen Vereinbarung sollte sein, den Schutz der Beschäftigten zu konkretisieren und Möglichkeiten der Überwachung zu verhindern, die über das gesetzliche Maß hinaus gehen. Hier muss man aufpassen, denn durch eine ungeschickte Formulierung kann das Gegenteil erreicht werden - die Beschäftigten werden dann legal überwacht.

- Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktdaten im Anhang.

Chipkarten und RFID

Inhalt:

Worum geht es?

In vielen Betrieben und Einrichtungen werden Chipkarten (oder Karten mit Magnetstreifen) ausgegeben, um Türen zu öffnen und gelegentlich auch um in Kantinen bargeldlos zu bezahlen. Diese Technik ist vielerorts schon abgelöst durch sogenannte RFID-Tags - die oft aussehen wie Pfandchips für Einkaufswagen im Supermarkt. RFID steht für **R**adio **F**requency **ID**entification, einfach übersetzt handelt es sich um Funketiketten.

RFID-Tags können alles, was mit Chip- oder Magnetkarten möglich war und noch viel mehr. Sie funktionieren als winzige Sender und können kontaktlos über Distanzen von wenigen Zentimetern bis zu einigen Metern automatisch identifiziert werden.

RFID-Tags lassen sich sehr preiswert herstellen, dadurch entstehen einerseits neue industrielle Anwendungen. Sie lösen den Barcode ab und bieten auch neue Möglichkeiten, da jedes Etikett einen einmaligen Identifikationscode hat und mit dem Objekt in Bezug gesetzt wird, dass es trägt.

Wenn Mitarbeiter mit solchen Karten ausgestattet werden, können sie nicht nur zum aktiven Öffnen von Türen eingesetzt werden, sondern auch dazu, Aktivitäten von Mitarbeitern zu kontrollieren. Ein Schlüssel erlaubt es nicht, festzustellen, wer wann eine Tür geöffnet hat. Chipkarten und RFID-Tags schon. Oft ist jedoch nicht bekannt, ob solche Speicherungen erfolgen und was mit diesen Daten im Anschluss passiert. Aus diesem Grund besteht das Risiko, dass verdeckt Bewegungs- oder Aktivitätsprofile von Beschäf-

tigten angelegt werden können, ohne dass sie etwas davon merken.

Im Folgenden geht es um die Fragen:

- ***Zu welchen Zwecken dürfen Chipkarten und RFID-Tags am Arbeitsplatz genutzt werden?***
- ***Was müssen Beschäftigte wissen, wenn Chipkarten und RFID-Tags zum Einsatz kommen?***

Rechtlicher Hintergrund:

Bei Chipkarten, Magnetkarten und RFID-Tags handelt es sich um Gegenstände auf denen personenbezogene oder -beziehbare Daten gespeichert sind. Anhand der Daten lässt sich zweifelsfrei feststellen, wer der Besitzer der Karte ist und das ist schließlich auch der Sinn.

Die Erhebung und Verarbeitung von personenbezogenen Daten von Beschäftigten wird geregelt in den Datenschutzgesetzen (§§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD, § 3 KDO).

Chipkarten, Magnetkarten und RFID-Tags sind mobile personenbezogene Speicher- und Verarbeitungsmedien im Sinne von § 3 Abs. 10, § 6c BDSG und § 3 Abs. 9, § 18 SDSG.

- Der Arbeitgeber kann die Einführung eines Chipkartensystems zur Zutrittskontrolle mit seinem Weisungsrecht (§ 106 GewO) begründen. Für die Umsetzung hat er Datenschutzrecht und die Rechte der Interessenvertreter zu wahren.
- Das Erheben von Beschäftigtendaten mit Chipkartensystemen oder RFIDs ist fest an den Zweck gebunden, z. B. Öffnen von Türen oder Bezahlen in Kantinen (Abrechnungszwecke)
- Grundsätzlich ist es unzulässig, die Beschäftigtendaten aus einem Chipkartensystem zu speichern, auszuwerten oder anders zu nutzen.
- Nur wenn eine Erforderlichkeit juristisch nachgewiesen werden kann, ist die Speicherung (unter der Auflage der Zweckbindung) erlaubt. Kann die rechtliche Erforderlichkeit nicht nachgewiesen wer-

den, bleibt das Speichern der Beschäftigtendaten verboten.

- Der Arbeitgeber muss die Beschäftigten unaufgefordert in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten informieren.
- Der Arbeitgeber muss die Beschäftigten darüber informieren, wie sie ihre Rechte auf Auskunft, Berichtigung, Sperrung und Löschung ihrer Daten ausüben können.
- Der Arbeitgeber muss die Beschäftigten dahingehend unterrichten, wie bei Verlust oder Zerstörung des Mediums zu verfahren ist.
- Der Arbeitgeber hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.
- Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.
- Wenn Karten oder RFID-Tags als Bezahlsystem in Kantinen eingesetzt werden: Die Verwendung der Daten ist nur für Abrechnungszwecke zulässig und nicht, um festzustellen, wie gesund sich ein Beschäftigter ernährt.
- Der Arbeitgeber ist verpflichtet, für das System ein Verfahrensverzeichnis anzulegen. Verfahrensverzeichnisse geben verbindlich Auskunft über den gesamten Prozess von der Datenerhebung, -verarbeitung bis zur Löschung; sie benennen verantwortliche Personen und die eingesetzte Technik. (Diese Anforderung besteht nicht für kirchliche Einrichtungen).
- Es ist in jedem Fall unzulässig, verdeckt Bewegungs- und Aktivitätsprofile über Chipkarten, Magnetkarten oder RFID-Tags herzustellen.

Handlungsmöglichkeiten für Beschäftigte

- Wer am Arbeitsplatz mit einem Chipkarten oder RFID-System arbeiten muss, sollte sich darüber informieren, welche Daten auf dem Chip sind, ob Daten gespeichert werden oder nicht.

- Wenn Daten gespeichert werden sollen, muss es hierfür eine Rechtsgrundlage geben. Der Arbeitgeber muss (nach §§ 4, 32 BDSG, §§ 4, 31 SDSG, §§ 4, 24 DSG-EKD, § 3 KDO) begründen, dass er die Daten speichern darf. Er kann die Begründung nicht verweigern.

- Als Beschäftigter kann man Einblick in das Verfahrensverzeichnis verlangen, um zu erfahren ob und wenn ja wo, welche Daten von wem verarbeitet werden. Liegt kein Verfahrensverzeichnis vor, darf das System nicht betrieben werden. Die Auflagen der Datenschutzgesetze sind nicht erfüllt (gilt nicht bei kirchlichen Einrichtungen)! Das Verfahrensverzeichnis wird vom Arbeitgeber oder vom Beauftragten für Datenschutz gepflegt und kann dort eingesehen werden. Dort steht auch die Rechtsgrundlage für eine eventuelle Speicherung.

- Als Beschäftigter hat man das Recht auf Auskunft über alle Daten aus dem System, die die eigene Person betreffen. Bei fehlerhaften Daten hat man das Recht auf Korrektur; bei Daten die unzulässig gespeichert sind, hat man das Recht auf Löschung.

- Gibt es Zweifel an der Umsetzung des Datenschutzes, sollte man Beweise für diese Zweifel sammeln und die Interessenvertretung einschalten. Existiert keine Interessenvertretung oder führt das nicht zum Erfolg, dann kann man sich an die Rechtsberatung der Arbeitskammer wenden oder direkt an die Landesbeauftragte für Datenschutz.

- Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos an die Rechtsberatung der Arbeitskammer des Saar-

landes wenden. Kontaktdaten finden sich im Anhang.

Handlungsmöglichkeiten für die Interessenvertretung

- Wenn ein Chipkartensystem oder RFID-Tags für Mitarbeiter eingeführt werden soll, haben Betriebsräte, Personalräte und Mitarbeitervertretungen starke Mitbestimmungsrechte zum Schutz ihrer Kollegen. Die Interessenvertretungen haben nicht nur die Pflicht, zu kontrollieren, ob die Datenschutzgesetze eingehalten werden.

- Betriebsräte, Personalräte und Mitarbeitervertretungen haben auch das Recht, für den Betrieb des Systems den Abschluss von Betriebs- und Dienstvereinbarungen zu verlangen. Darin wird für alle Beteiligten verbindlich geregelt, was zulässig ist, was unterbleibt, wie mit dem System gearbeitet wird und wer verantwortlich ist. Alle Beschäftigten und der Arbeitgeber sind gesetzlich verpflichtet, Betriebs- und Dienstvereinbarungen einzuhalten.

- Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V. einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktdaten finden sich im Anhang.

Smartphones am Arbeitsplatz

Inhalt:

Worum geht es?

Smartphones haben in vielen Betrieben und Einrichtungen die Mobiltelefone ersetzt. Die praktischen Vorteile liegen auf der Hand, trotzdem erweisen sie sich im betrieblichen Einsatz zunehmend als kritisches Thema.

Smartphones vereinigen die kritischen Aspekte von Mobiltelefonen mit denen von PCs, E-Mail, Internetanwendungen, Ortungsgeräten sowie dem Fotografieren und Filmen am Arbeitsplatz. Hinzu kommt die Tatsache, dass es die Smartphone-Betriebssysteme dem Benutzer kaum ermöglichen wahrzunehmen, welche Apps zu welchem Zeitpunkt welche Daten (an den Arbeitgeber?) senden.

Im Folgenden geht es darum:

- ***Was ist zu beachten, wenn das private Smartphone am Arbeitsplatz genutzt wird?***
- ***Was müssen Arbeitgeber und Beschäftigte beachten, wenn Smartphones als Arbeitsmittel bereitgestellt werden?***

Rechtliche Situation

Allgemeine Vorgaben:

- Ob mit Smartphone oder anderen Geräten: Generell dürfen keine Fotos, Filme und Tonaufzeichnungen von Personen gemacht werden, ohne deren vorheriges Einverständnis. Zuwiderhandlungen kön-

nen mit Freiheitsstrafen geahndet werden. (§ 201 StGB, § 35 KunstUrhG)

- Smartphones legen die Kommunikation in sozialen Netzwerken nahe. Auch wenn ein Mitarbeiter als Privatperson kommuniziert, so ist üble Nachrede über den Arbeitgeber in den Netzwerken ein Kündigungsgrund. Auch bei Affekthandlungen nach einem unangenehmen Gespräch mit dem Vorgesetzten (§§ 186, 187 StGB).

Privates Smartphone am Arbeitsplatz

Wer sein persönliches Smartphone an den Arbeitsplatz mitbringt, muss dafür sorgen, dass es keinen störenden Einfluss auf Betriebsabläufe hat. Hierzu kann der Arbeitgeber Regeln aufstellen oder er kann im Einzelfall von seinem Weisungsrecht Gebrauch machen.

- Der Arbeitgeber kann das Mitbringen von Mobiltelefonen und Smartphones mit Kamerafunktion grundsätzlich verbieten, wenn er dadurch den Verrat von Betriebsgeheimnissen verhindern will. Eine Nutzung in den Pausen, außerhalb der geschützten Bereiche oder ausschließlich in Sozialräumen kann er hingegen nicht verbieten.

- Der Arbeitgeber muss nicht dulden, dass während der bezahlten Arbeitszeit privat telefoniert wird, soziale Netzwerke oder das Internet genutzt werden. Er kann dies während der Arbeitszeit verbieten, auch wenn es sich um ein privates Gerät handelt und ihm darüber keine Kosten entstehen.

- Sofern es nicht ausdrücklich erlaubt ist, darf ein Mitarbeiter keine betrieblichen Ressourcen für sein Privatvergnügen nutzen. Es ist nicht zulässig, mit einem privaten Smartphone ein betriebliches W-LAN und Internetzugänge zu nutzen. Auch nicht in den Pausen. Sollte durch Zuwiderhandlungen Schadsoftware (Viren) eindringen, kann der Arbeitgeber den Mitarbeiter haftbar machen.

Smartphone als Betriebsmittel

- Smartphones, die vom Arbeitgeber bereitgestellt werden, gehen nicht in den Besitz des Benutzers über, außer das ist vereinbart.
- Der Arbeitgeber kann im Rahmen seines Weisungsrechts (§ 106 GewO) festlegen, wofür ein Smartphone genutzt wird. Eine Nutzung zu privaten Zwecken ist nur dann zulässig, wenn sie ausdrücklich erlaubt ist. Ist nichts festgelegt, muss davon ausgegangen werden, dass die Privatnutzung verboten ist.
- Sofern nichts Abweichendes geregelt ist, ist der Benutzer eines dienstlichen Smartphones nicht berechtigt, es zu verändern z. B. durch download oder Deinstallation von Apps.
- Wenn ein Mitarbeiter ein Smartphone zu dienstlichen Zwecken erhält, ergibt sich daraus nicht zwangsläufig eine Rufbereitschaft. Das muss separat mit Betriebsrat, Personalrat oder Mitarbeitervertetung vereinbart werden. Ist keine Interessenvertretung vorhanden, muss die Rufbereitschaft einzelvertraglich geregelt werden.
- Smartphones verfügen über GPS-Sensoren zur Standortbestimmung. Über Apps können Smartphones zur Ortung der Mitarbeiter eingesetzt werden. Eine verdeckte Ortung ist unzulässig (§ 4 BDSG, BildschArbV Anhang Nr. 22). Eine erkennbare Ortung kann üblicherweise auch nicht aus den arbeitsvertraglichen Pflichten des Mitarbeiters abgeleitet werden. Der Arbeitgeber kann so etwas nicht eigenmächtig veranlassen (§ 4 BDSG).
- Smartphones verfügen über die Möglichkeit per E-Mail zu kommunizieren. Es gelten dieselben Grundsätze wie bei der stationären E-Mail am Arbeitsplatz. Kontrollen aus Gründen der Systemwartung sind jedoch immer möglich.
- Auch bei Smartphones wird der Zugriff auf das Internet registriert. Der Arbeitgeber hat als Besitzer

des Smartphones Zugriff auf die sogenannten Logfiles des Providers und kann den Mitarbeiter kontrollieren. Wie weit diese Kontrollen gehen dürfen, wird in der Rechtsprechung unterschiedlich bewertet. Deshalb sollten die Nutzungsbedingungen innerbetrieblich in Betriebs-/Dienstvereinbarungen festgelegt werden, oder, wo das nicht möglich ist, einzelvertraglich zwischen Arbeitgeber und Mitarbeiter. Ungeregelte Situationen sind oft ungünstig für Mitarbeiter.

- Private Informationen sind für den Arbeitgeber auch dann tabu, wenn eine Privatnutzung verboten ist. Er kann jedoch ungeachtet des Inhalts arbeitsrechtliche Schritte z. B. eine Abmahnung vornehmen, wenn er (z.B. an Überschrift und Absender) erkennen kann, dass das Verbot der Privatnutzung überschritten wurde.

Anwendbarkeit der Gesetze

Oft wird die Privatnutzung zwar offiziell verboten. Da es aber in Zeiten der Flatrates nicht mit Kosten für den Arbeitgeber verbunden ist, wird es gleichzeitig stillschweigend geduldet. Das hat folgenden Hintergedanken: Wenn privates Telefonieren gestattet wird, gilt das Telekommunikationsgesetz (TKG). Dieses hebt das Datenschutzniveau an; der Arbeitgeber wird in seinen Kontrollrechten (Einzelverbindungsnachweise u. ä.) eingeschränkt. Das möchten viele Arbeitgeber mit einem Verbot der Privatnutzung umgehen.

Diese Argumentation greift jedoch nicht, denn auch wenn der Besitzer des Diensttelefons/Smartphones nur dienstlich telefoniert, ist es nicht auszuschließen, dass er einen privaten Anruf erhält. Hier ist das TKG anzuwenden. Insofern sind personenbezogene Kontrollen durch den Arbeitgeber über den reinen Abrechnungszweck hinaus nur sehr eingeschränkt möglich.

Smartphones dürfen nicht zur Ortung und Überwachung der Mitarbeiter eingesetzt werden. Da Smartphones als mobile Bildschirmgeräte dienstlich und damit regelmäßig genutzt werden, greift die Bildschirmarbeitsplatzverordnung. Diese untersagt eine verdeckte Kontrolle. Im Übrigen werden verdeckte Kontrollen über die Grundsätze der Datenerhebung in den

Datenschutzgesetzen (§ 4 BDSG, § 4 SDSG, § 4 DSG-EKD, § 3 KDO) verboten.

Auch wenn es sich bei einem Smartphone um ein neues Gerät handelt, so führt es letztlich eine Reihe bekannter Technologien zusammen und macht sie mobil verfügbar. Bereits abgeschlossene Betriebs- und Dienstvereinbarungen (z. B. zur Internetnutzung, zu E-Mail, zur Telefonnutzung) gelten vollständig oder in Teilen auch für Smartphones.

Handlungsmöglichkeiten

Wer ein dienstliches Smartphone erhält, sollte sich erkundigen, ob es Betriebsvereinbarungen, Dienstvereinbarungen oder Anweisungen gibt, die zu beachten sind. Aus einer geduldeten Übertretung ergibt sich auch auf Dauer kein Gewohnheitsrecht.

Wenn es keine Regelungen gibt, sollte er den Betriebsrat bzw. Personalrat oder die Mitarbeitervertretung informieren, damit dieser gemeinsam mit dem Arbeitgeber eine rechtssichere Vereinbarung schließt, die die Mitarbeiter vor Überwachung schützt.

Sofern es keine Interessenvertretung und keine verbindliche Nutzungsrichtlinie gibt, sollte man sich als Mitarbeiter über die wesentlichen Punkte mit dem Arbeitgeber verständigen und dies schriftlich festhalten.

Hat man als Mitarbeiter den Eindruck, dass man auf unzulässige Art überwacht wird, dass Gespräche aufgezeichnet, vertrauliche (dienstliche) E-Mails gelesen werden oder Ähnliches, sollte man dies möglichst lückenlos dokumentieren, Indizien und Beweise sammeln und Aussagen protokollieren. Sonst läuft man Gefahr, dem Arbeitgeber etwas zu unterstellen. Es kann hilfreich sein, in Erfahrung zu bringen, ob es anderen genauso geht. Sofern vorhanden, sollte man die Interessenvertretung informieren. Diese kann sich gemeinsam mit dem Beauftragten für Datenschutz um die Angelegenheit kümmern.

Gibt es auch keinen Beauftragten für Datenschutz oder bestehen Zweifel an seinem Engagement, kann man sich auch an die Aufsichtsbehörde für den Datenschutz wenden.

Alle sozialversicherungspflichtig Beschäftigten im Saarland können sich kostenlos

an die Rechtsberatung der Arbeitskammer des Saarlandes wenden. Kontakt im Anhang.

Bei der dienstlichen Nutzung von Smartphones sind die Rechte der Interessenvertreter zu beachten. Betriebsräte, Personalräte und Mitarbeitervertretungen haben mitzubestimmen in Fragen der Ordnung und des Verhaltens im Betrieb und bei der Nutzung von technischen Einrichtungen, die dazu geeignet sind die Leistung oder das Verhalten von Mitarbeitern zu kontrollieren. Wenn Smartphones betrieblich genutzt werden sollen, kann (und sollte!) eine Betriebs- bzw. Dienstvereinbarung abgeschlossen werden, die die Regeln für Arbeitgeber und die Mitarbeiter rechtsverbindlich festlegt (ordnungsgemäßer Umgang, Kontrollen, Privatnutzung…). Auch die Rufbereitschaft ist ein mitbestimmungspflichtiger Tatbestand.

Betriebsräte, Personalräte und Mitarbeitervertretungen erhalten im Saarland Unterstützung durch BEST e. V., einer Tochtereinrichtung der Arbeitskammer und des DGB Saar. Kontaktdaten im Anhang.

Social Media, Soziale Netzwerke

Inhalt:

Worum geht es?

Das Internet eröffnet heute sowohl im Rahmen des Privatgebrauchs als auch bei der beruflichen Nutzung vielfältige Möglichkeiten. Es lässt sich als Medium zur Information, für die Telekommunikation (E-Mail, Voice-Over-IP-Telefonie) oder als Mittel der Selbstdarstellung (z. B. mit privaten oder Firmenwebsites) nutzen. Ein besonderes Angebot bieten seit einiger Zeit die sogenannten „Social-Media"-Anwendungen. Zu Social Media (engl. für soziale Medien) zählen unter anderem die sozialen Netzwerke. Diese bilden eine internetbasierte technische Plattform für den aktiven „sozialen" Austausch von Informationen zwischen den Nutzern. Sie heißen facebook, Xing oder Wer-kennt-wen, Twitter oder Flickr. Mittlerweile gibt es eine fast unüberschaubare Anzahl derartiger Internet-Angebote und -Anwendungen. Sie eröffnen den Anwendern innerhalb dieses Web 2.0, dem „Mitmach-Internet", die Möglichkeit, sich zu vernetzen, zu kommunizieren, Fotos oder Videos zu veröffentlichen oder auch Meinungen zu äußern. Die Nutzer sind damit nicht mehr nur ausschließlich Konsumenten von Inhalten im Netz, sondern gestalten diese selbst mit.

Problembereiche bei der Nutzung von Social Media

Social Media-Anwendungen beinhalten zahlreiche, für die Nutzer auch kritische Aspekte: Unabsichtlich eingestellte Beiträge, die im Nachhinein nicht mehr erwünscht erscheinen, sind oft nur schwer oder gar nicht von den jeweiligen Seiten zu entfernen. Meist wird es dadurch behindert, dass die meist kommerziellen Be-

treiber der sozialen Netzwerke – ob gewollt oder ungewollt – dies technisch erschweren. Vielen Nutzern ist es darüber hinaus auch nicht bewusst, dass einmal veröffentlichte Beiträge leicht von Dritten vervielfältigt und andernorts neu veröffentlicht werden können (so z. B. Fotos). Darüber hinaus ist oft in den Nutzungsbedingungen vermerkt, dass man das jeweilige Nutzungsrecht auch an den Betreiber des Netzwerkes abtritt.

Ebenfalls häufig kommt es vor, dass die Veröffentlichung bestimmter Informationen in manchen Zusammenhängen aus Nutzersicht zwar angemessen erscheint (Fotos der letzten Party auf einer Internetseite, zu der nur die engsten Freunde Zugang haben), diese in anderen Kontexten aber höchst problematisch sein kann. Etwa, wenn die gleichen Fotos plötzlich auf der hochseriösen Seite eines „Business"-Netzwerkes erscheinen.

Auch im Rahmen des sogenannten Cyber-Mobbings (z. B. Beleidigungen oder Bedrohungen, begünstigt durch die vermeintliche Anonymität im Netz) und bei bestimmten Formen der Internet-Kriminalität (wie z. B. das sogenannte Phishing, das Ausspähen sensibler persönlicher Daten mittels manipulierter Internetseiten) werden Social-Media-Anwendungen gezielt missbraucht. Eine besondere Qualität gewinnen derartige Aktivitäten, wenn sie im beruflichen Zusammenhang geschehen (z. B. Mobbing) oder über die technische Infrastruktur am Arbeitsplatz abgewickelt werden. Dies kann zum Teil höchst folgenreich für die davon Betroffenen sein.

Recherchen des Arbeitgebers im Internet und in sozialen Netzwerken

Auch bereits vor Aufnahme eines Beschäftigungsverhältnisses gibt es zahlreiche kritische Aspekte. So ist es heute fast schon gängige Praxis, dass Personalverantwortliche innerhalb von Personalauswahlverfahren Informationen über Bewerber aus dem Internet (z. B. über Suchmaschinen) und den sozialen Netzwerken sichten und für ihre Entscheidungen heranziehen.

Dies ist auf der Grundlage der Datenschutzgesetzgebung ohne Einverständnis des Betroffenen allerdings grundsätzlich nicht erlaubt. Nach den Datenschutzgesetzen ist eine Datenerhebung, -nutzung oder -verarbeitung grundsätzlich nur erlaubt, wenn sie unmittelbar beim Betroffe-

nen und mit dessen Wissen erfolgt (Grundsatz der Direkterhebung gemäß § 4 Abs. 2 BDSG; § 12 Abs. 1 SDSG; § 4 Abs. 2 DSG-EKD; § 9 Abs. 2 KDO). Abweichungen hiervon sind nur erlaubt, wenn die Persönlichkeitsrechte und schutzwürdigen Interessen des Betroffenen nicht tangiert werden. Dies ist angesichts eines (in Aussicht stehenden) Beschäftigungsverhältnisses sicher nicht der Fall. Insbesondere angesichts der Tatsache, dass Informationen aus dem Internet (die vielleicht auch z.B. von Dritten erstellt wurden) kein verlässliches und schon gar kein vollumfängliches Bild über einen Beschäftigten oder einen Bewerber liefern.

Außerdem gilt: Im Beschäftigungsverhältnis (im Bewerbungsverfahren gilt dies auch) ist eine Datenerhebung oder -verarbeitung und -nutzung nur erlaubt, wenn sie maßgeblich für die Durchführung des Beschäftigungsverhältnis bzw. für die Erfüllung der Aufgaben der Dienststelle ist (vgl. § 32 Abs. 1 BDSG; § 31 Abs. 1 SDSG; §§ 4 Abs. 1, 5 Abs. 1 DSG-EKD; §§ 9 Abs. 1, 10 Abs.1 KDO). Dies ist bei einer Internet-Recherche in der Regel wohl nicht der Fall. Eine Ausnahme besteht nur, wenn der Bewerber innerhalb seiner Bewerbung selbst auf bestimmte Internetseiten verwiesen hat oder wenn er selbst Daten zum Zweck der Arbeitssuche in speziellen Netzwerken (z. B. XING, stepstone.de, monster.de) eingestellt hat.

Bewerber und auch Arbeitnehmer, die in einem Beschäftigungsverhältnis stehen, sollten sich dennoch immer bewusst darüber sein, dass der (zukünftige) Vorgesetzte bei öffentlich zugänglichen Informationen natürlich auch in deren Kenntnis gelangen kann. Von großer Bedeutung ist es daher, als Nutzer zu wissen, wie die Privatsphäre im Internet auch über technische Vorkehrungen (Einstellungen der Profile in den sozialen Netzwerken) am besten geschützt werden kann.

Soziale Netzwerke am Arbeitsplatz

Auch im bestehenden Beschäftigungsverhältnis können sich im Hinblick auf die Nutzung von Social-Media-Anwendungen viele Probleme ergeben. Gerade soziale Netzwerke gelten als Internetanwendungen, auf die ein großer Teil (erlaubter oder nichterlaubter) Privatnutzung entfällt. So kommt es nicht selten vor, dass der Zugang zu diesen Seiten technisch verhin-

dert oder der Besuch der entsprechenden Seiten eingeschränkt oder verboten wird. Dies ist grundsätzlich statthaft, sollte jedoch so transparent wie möglich erfolgen. Den Nutzern sollte also bekannt sein, warum und in welchem Umfang Internetseiten gesperrt werden.

Arbeitsrechtlich betrachtet stellt sich die Nutzung sozialer Netzwerke am Arbeitsplatz nicht anders dar als die Nutzung anderweitiger Internetangebote. Die jeweilige betriebliche Internet- bzw. E-Mail-Nutzungsregelung ist also zu beachten. Dies betrifft auch die Kontrolle des Nutzungsverhaltens. Dabei ist zu berücksichtigen: Bei sozialen Netzwerken wird es durch deren Betreiber Dritten oft recht einfach gemacht, personenbezogene Auswertungen anzustellen. Zum Beispiel dann, wenn Daten wie Nutzungszeitpunkte (etwa der Zeitpunkt eines „Postings“, einer Mitteilung bei Facebook) öffentlich zugänglich gemacht werden. Diese freiwillig veröffentlichten personenbezogenen Daten können schnell als vermeintlicher Beweis für eine eigentlich verbotene Privatnutzung des Internets am Arbeitsplatz herangezogen werden – und zwar ohne, dass dafür eine zusätzliche Datenauswertung in offener oder verdeckter Form stattfinden muss.

Nicht nur der Zugang zu Informationen aus der eigentlichen Privatsphäre des Beschäftigten kann im Beschäftigungsverhältnis zu Problemen führen. Es können sich weitere kritische, im Einzelfall ebenfalls auch arbeitsrechtliche Folgen ergeben. Und zwar beispielsweise dann, wenn Beschäftigte sie sich in ihren Online-Beiträgen zum Unternehmen oder zu anderen Mitarbeitern und Vorgesetzten (vor allem kritisch) äußern.

Für eine rechtliche Bewertung derartiger Äußerungen sind mehrere Sachverhalte zu berücksichtigen. Zum einen ist jeder Arbeitnehmer an die sogenannten Haupt- und Nebenpflichten aus seinem Arbeitsvertrag gebunden (gemäß § 612 BGB). Zu den Hauptpflichten zählt für den Arbeitnehmer vor allem die Erbringung der arbeitsvertraglich geschuldeten Arbeitsleistung. Wer diese nicht erbringt, zum Beispiel weil ihn eine übermäßige private Internetnutzung davon abhält, muss selbstverständlich mit Sanktionen oder gar arbeitsrechtlichen Schritten des Arbeitgebers (Abmahnung bis hin zur Kündigung) rechnen.

Daneben bestehen die in diesem Zusammenhang die oft ebenso wichtigen Nebenpflichten. Zu diesen zählt die Pflicht zur Verschwiegenheit über Betriebs- oder Geschäftsgeheimnisse oder auch eine allgemeine Treuepflicht gegenüber seinem Arbeitgeber. Damit wird bereits bei der Unterzeichnung des Arbeitsvertrages eine Verpflichtung zur besonderen Loyalität gegenüber dem Arbeitgeber begründet. Wer gegen diese verstößt, handelt vertragswidrig und muss im schlechtesten Fall mit einer Abmahnung oder gar der Kündigung rechnen.

Betriebs- oder Geschäftsgeheimnisse

Bei der Nutzung sozialer Netzwerke werden manchmal auch Inhalte erstellt, die in einem direkten oder indirekten Zusammenhang zur eigenen Arbeit stehen. Man vernetzt sich mit Arbeitskollegen und tauscht mit diesen Neuigkeiten aus, gibt in seinem Netzwerkprofil an, dass man Mitarbeiter der Firma XY ist oder wird von anderen Netzwerkmitgliedern als ein solcher „markiert“. Man tritt also, je nach Sichtbarkeit des Netzwerk-Profils für Unbeteiligte, mal in größerem, mal in geringerem Maße in die Öffentlichkeit und nimmt Bezug zu seinem Arbeitgeber. Und man äußert sich auf diese Weise auch als Mitarbeiter der jeweiligen Firma. Dessen sollte man sich stets bewusst sein. Denn unbedachte Äußerungen können folgenreich sein. Insbesondere dann, wenn bei Aktivitäten in sozialen Netzwerken Betriebs- oder Geschäftsgeheimnisse verbreitet werden.

Betriebs- oder Geschäftsgeheimnisse sind jede auf einen Betrieb bzw. ein Geschäft bezogene Tatsache

- die der Geschäftsinhaber (Arbeitgeber) erkennbar geheim hält,
- die nur ein begrenzter Personenkreis kennt und
- die anderen Personen nicht einfach zugänglich sind.

Das können im Einzelnen sein:

- alle wirtschaftlichen Daten eines Betriebes, die Außenstehenden nicht ohne weiteres zugänglich sind,
- Kunden- und Preislisten,
- Bilanzen,
- Konstruktions-, Herstellungsverfahren,
- technisches Know-how und
- Personalangelegenheiten.

Arbeitnehmer sind zur Verschwiegenheit über Betriebsgeheimnisse verpflichtet. Dies gilt selbstverständlich auch bei Äußerungen in sozialen Netzwerken. Die Verschwiegenheitspflicht beginnt mit Abschluss des Arbeitsvertrags und wird über das Ende des Arbeitsverhältnisses hinweg fortgeführt. Auch beim Ausscheiden aus dem Unternehmen ist man also weiterhin zur Verschwiegenheit verpflichtet.

Der Verrat eines Geschäftsgeheimnisses durch einen Arbeitnehmer während des Arbeitsverhältnisses kann nicht nur arbeitsrechtlich von Bedeutung sein. Er ist unter Umständen auch strafrechtlich zu ahnden und verpflichtet darüber hinaus zu Schadensersatz. Dies ist der Fall, wenn das Geheimnis aufgrund des Arbeitsverhältnisses anvertraut war und der Arbeitnehmer aus Eigennutz, das bedeutet zu Wettbewerbszwecken, gehandelt hat (§ 17 Gesetz gegen den unlauteren Wettbewerb, UWG).

Entsprechende Regelungen gibt es auch für die Geheimhaltungspflichten öffentlicher Amtsträger (Verletzung des Dienstgeheimnisses gemäß § 353b Strafgesetzbuch, StGB; Verletzung des Steuergeheimnisses gemäß § 355 StGB).

Einer besonderen Pflicht zur Wahrung fremder Geschäftsgeheimnisse unterliegen unter anderen folgende Berufsgruppen:

- Ärzte, Apotheker, Angehörige eines anerkannten Heilberufs,
- Psychologen,
- Rechtsanwälte, Notare,
- Wirtschaftsprüfer, Steuerberater, Buchhalter,
- Sozialarbeiter und Sozialpädagogen sowie deren Mitarbeiter und Auszubildenden,
- Angehörige einer privaten Kranken-, Unfall- oder Lebensversicherung oder privatärztlichen Verrechnungsstelle und
- Amtsträger im öffentlichen Dienst.

Die Verletzung von Privatgeheimnissen, die einem dieser sogenannten Berufsgeheimnisträger anvertraut sind, ist nach § 203 des Strafgesetzbuches (StGB) strafbar.

Neben der Veröffentlichung von Betriebs- oder Geschäftsgeheimnissen, müssen Arbeitnehmer vor allem dann mit negativen Konsequenzen (Abmahnung, Kündi-

gung) rechnen, wenn in Beiträgen in sozialen Netzwerken, in Online-Blogs oder -Foren die Grenzen der freien Meinungsäußerung überschritten und etwa ruf- oder kreditschädigende Äußerungen gegenüber dem Arbeitgeber geäußert werden. Zu beachten ist dabei immer: Es gibt kaum eine klar zu ziehende Grenzlinie zwischen Erlaubtem und Verbotenem. Auch Arbeitsgerichte entscheiden in der Regel auf der Grundlage einer Einzelfallprüfung und der Abwägung zwischen der Loyalitätspflicht gegenüber dem Arbeitgeber und dem Recht auf freie Meinungsäußerung.

Social Media-Richtlinien

Neben der individual-arbeitsrechtlichen Bewertung von Äußerungen sowie einer Bewertung der allgemeinen Gewohnheiten im Betrieb, spielt bei einer solchen Einzelfallprüfung vor allem auch das Vorhandensein oder Nicht-Vorhandensein betrieblicher Kollektivregelungen eine Rolle. Gibt es dienstliche Anweisungen oder gar eine Betriebs- oder Dienstvereinbarung zum Verhalten der Beschäftigten beim Umgang mit Social Media-Anwendungen, so sind diese natürlich für die Beschäftigten bindend. Aber auch hier gilt: Sie dürfen nicht das Grundrecht der freien Meinungsäußerung in Frage stellen.

Gibt es solche „Social Media-Guidelines“, also Richtlinien zum Umgang mit Social Media-Anwendungen, so können diese zum Inhalt haben:

- Erlaubnis oder Verbot zur Nutzung von sozialen Netzwerken während der Arbeitszeit,
- Verhältnis zwischen privater und dienstlicher Nutzung,
- Kanäle/Verantwortlichkeit/Zuständigkeit für unterschiedliche betriebliche Themen,
- Beteiligungsrechte des Betriebs- oder Personalrats bzw. der Mitarbeitervertretung,
- Wahrung der Vertraulichkeit, Schutz vor Verrat von Betriebsgeheimnissen,
- zulässige und unzulässige Inhalte,
- Eigenwerbung bzw. Kritik an Wettbewerbern,
- Umgang mit negativer Kritik und rechtswidrigen Posts,
- Umgang mit betriebsinterner Kritik.

Betriebsrat, Personalrat oder Mitarbeitervertretung haben bei der Erstellung sol-

cher Richtlinien ein Mitbestimmungsrecht, da die Inhalte auch Fragen der Ordnung des Betriebes und des Verhaltens der Arbeitnehmer im Betrieb betreffen. Ein Mitbestimmungsrecht besteht demnach gemäß § 87 (1) Nr. 1 Betriebsverfassungsgesetz (BetrVG), § 78 (1) Nr. 14 Saarländisches Personalvertretungsgesetz (SPersVG), § 40 k MVG-EKD.

Anhang

Anschriften

Beratung für Arbeitnehmer

Arbeitskammer des Saarlandes
Haus der Beratung, Trierer-Straße 22, 66111 Saarbrücken
Arbeitsrecht-Hotline (0681) 4005-111
Online: https://arbeitskammer.beranet.info/

Beratung für Betriebs- und Personalräte

BEST e. V. c/o Arbeitskammer des Saarlandes
Fritz-Dobisch-Straße 6 - 8, 66111 Saarbrücken
Telefon: (0681) 4005-249
Mail: best@best-saarland.de

Die Aufsichtsbehörden für den Datenschutz im Saarland

Unabhängiges Datenschutzzentrum Saarland
Judith Thieser - Landesbeauftragte für Datenschutz und Informationsfreiheit
Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Telefon: (0681) 94781-0
Mail: poststelle@datenschutz.saarland.de

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit
Husarenstraße 30, 53117 Bonn
Telefon: (0228) 99 77 99-0
Mail: poststelle@bfdi.bund.de

Datenschutzbeauftragter der Katholischen Kirche Diözese Trier und Speyer
Hartmut Junkes - Katholisches Büro Saarland
Ursulinenstraße 67, 66111 Saarbrücken
Telefon: (0681) 906 82 21

Datenschutzbeauftragter der ev. Kirche im Rheinland
Kirchenkreis Völklingen, Ottweiler, Saarbrücken
Dr. Herbert Ehnes
Rathausuferstraße 23, 40213 Düsseldorf
Telefon: (0211) 136 36 27

Datenschutzbeauftragter der ev. Kirche Pfalz
Kirchenkreis Homburg, Zweibrücken
Ludwig Buchert
Domplatz 5, 67346 Speyer
Telefon: (06232) 667 156

Weiterführende Informationen

arbeitskammer.de

Informationsportal der Arbeitskammer des Saarlandes. Beratung für Arbeitnehmer, reichhaltiges Informationsmaterial online verfügbar, z. B. dieses Handbuch.

best-saarland.de

BEST e. V. ist eine Tochtereinrichtung der Arbeitskammer des Saarlandes und des DGB Saar. BEST berät und qualifiziert Betriebs- und Personalräte zu Fragen des Datenschutzes und der Gestaltung von Arbeit. BEST hat dieses Handbuch erstellt.

www.datenschutz.saarland.de

Webseite der Landesbeauftragten für Datenschutz und Informationsfreiheit. Vielfältiges und einzigartiges Informationsangebot mit Arbeitshilfen zur Umsetzung des Saarländischen Datenschutzgesetzes.

bfd.bund.de

Webseite des Bundesbeauftragten für Datenschutz mit Download von Informationsmaterialien, Arbeitshilfen und umfangreichen Kommentaren.

datenschutz.de

Virtuelles Datenschutzbüro - Umfangreiches und verlässliches Informationsportal, getragen von zahlreichen offiziellen Datenschutzinstitutionen Deutschlands, der Kirchen und ausländischen Partnerinstitutionen.

gesetze-im-internet.de

Kostenloser Download aller Bundesgesetze in ihrer offiziellen Fassung, offizielles Internet-Angebot der Bundesregierung.

datenschutz-kirche.de

Informationsportal zum Datenschutz in der katholischen Kirche

www.ekd.de/datenschutz/4650.html

Informationsportal zum Datenschutz in der evangelischen Kirche

bsi.bund.de

Die Webseite des Bundesamtes für Sicherheit in der Informationstechnik. Seriöse und herstellerneutrale Informationen zur (technischen) Datensicherheit. Kostenloser Download des renommierten IT-Grundschutzhandbuches.

Stichwortverzeichnis