Leitfaden

Datenschutz im Personalwesen

Herausgeber

DataSolution LUD GmbH
Isarstr. 13
D-14974 Ludwigsfelde

Ansprechpartner

Andreas Thurmann
T: +49 (0) 3378.202513
M: mail@ds-lud.de
W: www.datenschutzberater365.de

Titelbild

Fotolia # 102976939
Fotolia # 46742238

Copyright

Inhaltsverzeichnis

Einleitung

In der DSGVO findet sich keine besondere Regelung zum Datenschutz im Beschäftigungsverhältnis. Es gelten deshalb zunächst auch für den Datenschutz im Beschäftigungsverhältnis die allgemeinen Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO zur Verarbeitung von personenbezogenen Daten. Art. 88 Abs. 1 DSGVO enthält jedoch für die Datenverarbeitung im Beschäftigungskontext eine Öffnungsklausel mit dem Inhalt, dass die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen können.

Von dieser Öffnungsklausel hat der deutsche Gesetzgeber Gebrauch gemacht und in § 26 BDSG für die Bundesrepublik den Beschäftigungsdatenschutz wie folgt geregelt:

> Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies
>
> - für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses (Bewerbungsverfahren) oder
> - nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder
> - Beendigung oder
> - zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.
>
> Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Alle Informationen, die einem einzelnen Arbeitnehmer zugeordnet werden können, sind personenbezogene Daten.

Besondere Datenarten i. S. v. Art. 9 Abs. 1 DSGVO dürfen gem. § 26 Abs. 3 BDSG erhoben und verarbeitet werden, wenn die Verarbeitung zur Ausübung von Rechten oder zur Erfüllung von rechtlichen Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung überwiegt. Zum Schutz dieser Daten hat der Verantwortliche angemessene und spezifische Maßnahmen nach § 22 Abs. 2 BDSG einzurichten.

Unberührt und weiterhin gültig bleiben alle übrigen einschlägigen und bereichsspezifischen Datenschutzvorschriften, die eine Datenerhebung, -verarbeitung oder -nutzung erlauben oder anordnen. Dies gilt auch für die Regelungen zur Datenerhebung, -verarbeitung oder -nutzung auf der Grundlage einer freiwilligen Einwilligung. Es gelten deshalb unverändert alle von der Rechtsprechung auf der Grundlage des verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrechts entwickelten Grundsätze zum Datenschutz im Beschäftigungsverhältnis. Danach besitzt jeder Arbeitnehmer am Arbeitsplatz einen Anspruch auf den **Schutz seines Persönlichkeitsrechts.**

Beschäftigte im Sinne des BDSG sind

- Arbeitnehmerinnen und Arbeitnehmer, einschließlich Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
- Auszubildende,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- nach dem Jugendfreiwilligendienstgesetz Beschäftigte (Praktikanten),
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerbungsverfahren

Der Bewerberbegriff umfasst alle Arten von Beschäftigten i. S. v. § 26 Abs. 8 BDSG. Zur Begründung eines Beschäftigungsverhältnisses, d. h. im **Bewerbungsverfahren**, dürfen alle für eine Entscheidung über die Einstellung erforderlichen personenbezogenen Daten erhoben werden. Neben dem Allgemeinen Gleichbehandlungsgesetz (AGG) ist hier insbesondere die umfangreiche Rechtsprechung zum **Fragerecht des Arbeitgebers** zu berücksichtigen. Abzugrenzen ist zwischen Fragen, die für die Bewerberauswahl erforderlich sind, und solchen, die erst später bei der Einstellung zum Tragen kommen. So sind Fragen zu den sozialen Verhältnissen, zur Religionszugehörigkeit oder zur Krankenversicherung erst bei der Einstellung von Bedeutung und dürfen deshalb, von eng begrenzten Ausnahmen (z. B. Frage nach der Religionszugehörigkeit bei einer Bewerbung in einem sog. Tendenzunternehmen wie etwa einer kirchlichen Einrichtung) abgesehen, nicht schon im Bewerbungsverfahren erhoben werden.

Durchführung des Beschäftigungsverhältnisses

Zur Einstellung und nach der Einstellung darf der Arbeitgeber vom Beschäftigten alle Daten über Umstände und Sachverhalte erheben und speichern, die erforderlich sind, um seine Pflichten im Zusammenhang mit dem Beschäftigungsverhältnis erfüllen zu können.

Zulässig sind unter diesen Gesichtspunkten **alle Daten, die im Zusammenhang mit der Personalverwaltung**, zur Durchführung der Lohn- und Gehaltsabrechnung, zur Mitarbeiterführung, Personalplanung, zur betrieblichen Fortbildung und Personalentwicklung etc. **erforderlich sind**.

Der Arbeitgeber darf aber auch Mitarbeiterdaten erheben, speichern und nutzen, um seine Rechte im Zusammenhang mit dem Beschäftigungsverhältnis wahrnehmen zu können. Dazu gehören **Kontrollen zu Leistung und Verhalten des Beschäftigten** ebenso wie Informationen als Grundlage zur Wahrnehmung seines Weisungsrechts. Auch Maßnahmen und Kontrollen zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen im Beschäftigungsverhältnis sind nach der Gesetzesbegründung nach § 26 Abs. 1 Satz 1 BDSG zu beurteilen.

Beendigung des Beschäftigungsverhältnisses

Der Begriff der Beendigung umfasst die vollständige Abwicklung eines Beschäftigungsverhältnisses. Der Arbeitgeber darf hier alle zur Beendigung erforderlichen bzw. damit im Zusammenhang stehenden Mitarbeiterdaten erheben und speichern. Dazu gehören auch alle Daten zur Sozialauswahl im Rahmen betriebsbedingter Kündigungen und sonstige Daten, die eine Kündigung begründen, wie Abmahnungen oder Beweismittel zur Begründung einer Kündigung und im Falle eines Rechtsstreites auch alle im Zusammenhang mit der Durchführung des Rechtsstreits anfallenden Daten und Unterlagen.

Zu regeln ist auch die Frage der Aufbewahrungsdauer der **Personalakte** nach dem Ausscheiden eines Mitarbeiters. Es gibt hier keine definierte Aufbewahrungsfrist, sodass die Frist nach den individuellen Verhältnissen des jeweiligen Unternehmens festgelegt werden kann. Zweckmäßig ist es aber, die Personalakte bei Ausscheiden eines Mitarbeiters auszudünnen und nicht mehr erforderliche Unterlagen zu vernichten.

Erhebung und Speicherung von Bewerberdaten

Die Betrachtung des Arbeitnehmerdatenschutzes nimmt ihren Anfang bei den Fragen zur Zulässigkeit der Erhebung und Speicherung personenbezogener Daten. Der Arbeitnehmerdatenschutz beginnt deshalb mit dem Fragerecht des Arbeitgebers bzw. damit, welche Fragen der Arbeitgeber im Bewerbungsverfahren stellen darf und der Bewerber wahrheitsgemäß beantworten muss.

Das Datenschutzgesetz legt schon im allgemeinen Teil mit dem Grundsatz der Datenminimierung den Rahmen für den Umfang der Datenerhebung fest. Im Bewerbungsverfahren dürfen **nur diejenigen Fragen gestellt** und Daten erhoben werden dürfen, **die im Bewerbungsverfahren und zur Entscheidung über die Bewerbung erforderlich sind**. Der Abschluss des Arbeitsvertrags ist ein anderer Zweck.

Soweit Daten erfragt werden sollen, die Anhaltspunkte für eine Diskriminierung der Betroffenen ergeben können, greifen vorrangig die Vorschriften des Allgemeinen Gleichbehandlungsgesetzes. Fragen, die Indizien für eine **potenzielle Diskriminierung** liefern können *(Fragen nach Staatsangehörigkeit, Gesundheit, Behinderung, Religion und Weltanschauung, Rasse oder ethnische Herkunft, Geschlecht, Alter und sexuelle Identität)* sind deshalb grundsätzlich **unzulässig**.

Zusätzliche Daten, die erst für den Abschluss des Arbeitsvertrags erforderlich sind, dürfen erst zum Vertragsabschluss erhoben werden. Diese Differenzierung mag bezogen auf denjenigen Bewerber, der die Anstellung erhält, nicht von großer Bedeutung erscheinen. Sie schützt aber alle anderen Mitbewerber vor einer unnötigen Offenlegung persönlicher Informationen und Umstände, die für das Bewerbungsverfahren unwichtig sind.

Bewerberportal

Unternehmen gehen dazu über, Bewerbungen nicht mehr nur per Post oder E-Mail entgegenzunehmen, sondern setzen ein strukturiertes Online-Bewerberportal ein. Teilweise wird den Bewerbern dazu kommuniziert, Bewerbungen möglichst nur über das Bewerberportal einzureichen. Aus diesem Hinweis, Bewerbungen nur online abzugeben, können sich Probleme für eine belastbare Einwilligung in Speicherungen der Bewerbung ergeben, weil dem Bewerber als Alternative nur die Möglichkeit bleibt, von einer Bewerbung abzusehen. Damit besteht keine Wahlmöglichkeit für die Abgabe der Bewerbung und eine Freiwilligkeit ist nicht mehr gegeben.

Neben den unstreitig für beide Seiten damit verbundenen Vorteilen ergeben sich für die Unternehmen auch verschiedene Datenschutzanforderungen, die zwingend zu erfüllen sind.

Bewerberdaten enthalten neben Zeugnissen u. U. auch Gesundheitsdaten und unterliegen deshalb einem sehr hohen Schutzbedarf. Das Portal ist daher für die Bewerber möglichst transparent zu gestalten. Dem Portal muss deshalb eine ausführliche **Datenschutzerklärung** vorangestellt werden, die der Bewerber bei der Abgabe der Bewerbung zur Erfüllung der Informationspflicht gem. Art. 13 DSGVO zwingend zur Kenntnis nehmen und deren Kenntnisnahme er auch nachweisbar bestätigen sollte. In der Datenschutzerklärung ist er insbesondere über folgende Punkte zu unterrichten:

Einschaltung eines Personalberaters

Zur Abwicklung von Bewerbungsverfahren können Personalberater eingeschaltet werden. Die Beratungstätigkeit kann **je nach Ausgestaltung der Beauftragung** im Wege der Datenverarbeitung im Auftrag oder im Wege der **eigenen Verantwortlichkeit** geschehen.

Gelegentlich wird von Personalberatern der Wunsch nach Übermittlung einer Liste über die bereits vom Auftraggeber abgelehnten Bewerbungen geäußert, um eine nochmalige Ansprache dieser Personen zu vermeiden. Nach den Vorschriften des Allgemeinen Gleichbehandlungsgesetzes (AGG) müssen abgelehnte Bewerbungen bzw. Daten über abgelehnte Bewerbungen nach Ablauf der Rechtsmittelfristen zurückgegeben oder gelöscht werden. Eine Speicherung über den für die Abwicklung des Bewerbungsverfahrens erforderlichen Zeitraum hinaus wird als Verstoß gegen das allgemeine Persönlichkeitsrecht gewertet. Vor diesem Hintergrund muss eine Übermittlung einer Liste über bereits abgelehnte Bewerber an den Personalberater als unzulässig bewertet werden. Dies gilt auch unter dem Gesichtspunkt, dass sich zwischen dem Zeitpunkt der Ablehnung der Bewerbung und einer erneuten Nutzung der Daten die der Ablehnung zugrunde liegenden Verhältnisse geändert haben können und so dem Bewerber ein ungerechtfertigter Nachteil entstehen könnte.

Die Bewerber müssen über die Stellen, an die ihre Bewerbung übermittelt wird, unterrichtet werden, soweit sie nicht mit einer Übermittlung rechnen müssen. Mit der Einschaltung eines Personalberaters müssen die Bewerber nicht rechnen, deshalb **müssen** die Bewerber vor einer Weiterleitung an den Personalberater über diese Übermittlung **unterrichtet werden**, unabhängig davon, ob eine Datenverarbeitung im Auftrag oder eine Datenübermittlung stattfindet. Dabei genügt die grundsätzliche Information, dass ein Personalberater eingeschaltet wird. Der Name des Beraters bzw. der Firmenname muss dabei nicht mitgeteilt werden. Dies kann durch einen Hinweis in der Stellenausschreibung geschehen (z.B. „Mit der Bearbeitung/Aufbereitung der Bewerbungen wird ein Personalberater beauftragt.“).

Bewerberfragebogen

Um von den Bewerbern die relevanten Daten nach einem einheitlichen Muster zu erheben, werden häufig Fragebogen eingesetzt. Diese werden den Bewerbern z.T. mit der Einladung zum Bewerbungsgespräch zur Rücksendung oder Vorlage beim Bewerbungsgespräch oder zum Bewerbungstermin mitgebracht. Oft werden die Fragebogen dem Bewerber auch erst im Bewerbungsgespräch selbst übergeben. Für die Zulässigkeit der Fragen gelten die zum Fragerecht des Arbeitgebers entwickelten Grundsätze. Zu beachten ist aber, dass der Einsatz eines Bewerberfragebogens, wenn ein Betriebsrat eingerichtet ist, mitbestimmungspflichtig ist. Dies gilt sowohl für die Einführung des Fragebogens wie auch für die enthaltenen Fragen und auch für eventuelle spätere Änderungen der Fragen.

Wenn der Arbeitgeber die Beteiligungspflicht des Betriebsrats nicht beachtet, können die Bewerber daraus jedoch nicht das Recht ableiten, die im Bewerberfragebogen enthaltenen Fragen unwahr zu beantworten.

Ein Bewerber ist nicht verpflichtet, Informationen zu offenbaren, nach denen er nicht gefragt wird. Um alle für die Begründung eines Beschäftigungsverhältnisses notwendigen Informationen zu erhalten, empfiehlt es sich daher, Bewerberfragebogen zu verwenden. Um Rechtsprobleme zu vermeiden, sollten diese Frage-

bogen aber unbedingt mit dem Datenschutzbeauftragten und dem Betriebsrat abgestimmt werden.

Vorstellungsgespräch per Videokonferenz

Zur Abwicklung von Vorstellungsgesprächen und von Videointerviews werden auch Videokonferenzsysteme eingesetzt. Diese Systeme bieten den Vorteil, dass das Vorstellungsgespräch einfach durchgeführt werden kann und insbesondere bei größeren Entfernungen Reisezeiten und Reisekosten eingespart werden können

Videointerviews können in Bewerbungsverfahren zulässig sein, wenn sie in der eigenen Infrastruktur des Unternehmens ablaufen, andere Alternativen (persönliches Gespräch) zur Verfügung stehen und für die nötige Transparenz gesorgt ist. Insbesondere wenn Bewerber aus weiter Distanz anreisen müssen, kann eine digitale Lösung im beiderseitigen Interesse liegen. Für potentielle Bewerber kann ein Videointerview eine einfache, erste Möglichkeit sein, die schriftlich erfolgte Bewerbung ohne großen Aufwand zu vertiefen. Dies könnte dazu führen, dass mehr Bewerber die Möglichkeit haben, sich persönlich darzustellen, und der Arbeitgeber im Interesse beider Beteiligten dadurch eine qualifiziertere Auswahlentscheidung treffen kann.

Die Bewerber müssen über die Rahmenbedingungen des Videointerviews informiert werden. Da Videokonferenzsysteme wie z. B. Teams, Zoom, Skype u.a. Chat-Protokolle erstellen und je nach Anbieter u.U. auch in Drittländern speichern, ist für die Durchführung dieser Videointerviews eine Einwilligung der Bewerber erforderlich.

Videointerviews mit einer Erhebung und Speicherung von Bild- und Tonaufzeichnungen der Bewerber und einer zeitversetzten Auswertung der Videointerviews für eine Bewerberauswahl im Rahmen von Einstellungsverfahren werden als unverhältnismäßig beurteilt und sind unzulässig. Die zusätzliche Erhebung und Nutzung von Bild- und Tonaufzeichnungen über die Bewerber stellen einen wesentlich intensiveren Eingriff in deren informationelles Selbstbestimmungsrecht dar.

Soweit für das Bewerbungsverfahren festgelegt ist, dass Vorstellungsgespräche auch per Videokonferenz abgewickelt werden sollen, muss der Verantwortliche bereits bei der Stellenausschreibung darauf hinweisen, weil die Bewerber nicht damit rechnen müssen, dass für Vorstellungsgespräche ein Videokonferenzsystem eingesetzt wird. Für die Durchführung der **Videokonferenzsysteme** dürfen nur solche Systeme eingesetzt werden, die ihrerseits die **datenschutzrechtlichen Anforderungen** erfüllen, insbesondere hinsichtlich der vertraulichen Datenübertragung, des Verbots der Speicherung und Nutzung von personenbezogenen Daten durch den Anbieter des Videokonferenzsystems, von Datenübermittlungen in Drittländer u. a. Ebenso wie bei einem persönlichen Vorstellungsgespräch dürfen auch von einem mittels eines Videokonferenzsystems durchgeführten Vorstellungsgespräch keine Videomitschnitte und Gesprächsaufzeichnungen hergestellt werden. Hier ist auch eine Einwilligung wenig hilfreich, weil aufgrund der Abhängigkeit des Bewerbers vom Arbeitgeber im Bewerbungsverfahren und einer möglicherweise drohenden Ablehnung des Bewerbers bei einer Verweigerung der Einwilligung von einer Freiwilligkeit der Einwilligung nicht ausgegangen werden kann und die Einwilligung als unwirksam bewertet werden müsste. Selbstverständlich muss der Arbeitgeber das Online-Vorstellungsgespräch in einer vertraulichen Umgebung führen, in der eine Teilnahme unbeteiligter Personen und eine unbefugte Kenntnisnahme von Inhalten des Vorstellungsgesprächs ausgeschlossen ist.

Sprachgebrauchsanalyseverfahren

In einem Telefongespräch mit dem Computer spricht der Bewerber zu vorgegebenen Fragen. Analysiert wird nicht der Inhalt der Antwort, sondern die Sprache und die Sprechweise, so z.B. Wortwahl, Benutzung von Verben und Adjektiven, die Stimm- und Tonlage und Schwankungen, die Art des Sprechens, ob eher vorsichtig und zurückhaltend oder selbstsicher,

Sprachkomplexität, einfacher und logischer Satzaufbau, komplizierte Schachtelsätze, Flüssigkeit der Sprache, Sprechpausen, Wortschatz, Sprechtempo u. a.

Mit der Sprachgebrauchsanalyse kann nicht nur das Sprachniveau ermittelt werden, sondern es können mittels eines Persönlichkeitsprofils die Belastbarkeit in Stresssituationen, Selbstsicherheit, Risikobereitschaft, Einsatzbereitschaft, Teamfähigkeit u.a. für die Eignung des Bewerbers für eine bestimmte Stelle ermittelt werden.

Soweit lediglich das Sprachniveau oder der Grad der Beherrschung einer Fremdsprache ermittelt werden soll, z.B. für eine Stelle in einem Callcenter, was zulässig sein kann, müssen die Bewerber über den Zweck des Einsatzes dieser Instrumente und über die Auswertungsverfahren und über die Prinzipien der Auswertung informiert werden. Die Erstellung von Persönlichkeitsprofilen und die Ermittlung von Charakter- und Persönlichkeitseigenschaften allein auf der Grundlage von Sprachgebrauchsanalysen stellt einen massiven Eingriff in das informationelle Selbstbestimmungsrecht und das Persönlichkeitsrecht der Bewerber dar und ist mit den Zwecken eines Bewerbungsverfahrens nicht zu vereinbaren und damit als unzulässig zu beurteilen. Auch hier ist eine Einwilligung wenig hilfreich, weil aufgrund der Abhängigkeit des Bewerbers vom Arbeitgeber im Bewerbungsverfahren und einer möglicherweise drohenden Ablehnung des Bewerbers bei einer Verweigerung der Einwilligung von einer Freiwilligkeit der Einwilligung nicht ausgegangen werden kann und die Einwilligung als unwirksam bewertet werden müsste.

Fragerecht des Arbeitgebers und Beispiele zur Abgrenzung

Nach den vom Bundesarbeitsgericht entwickelten Grundsätzen darf der Arbeitgeber nur diejenigen Sachverhalte und Tatsachen erfragen, an denen er im Hinblick auf das zu begründende Beschäftigungsverhältnis ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat, welches das schutzwürdige Interesse des Bewerbers an der Geheimhaltung seiner persönlichen Verhältnisse übersteigt. Der Umfang des Fragerechts bzw. das Recht zur Stellung bestimmter Fragen bestimmt sich deshalb nach dem das ganze Datenschutzrecht beherrschenden Grundsatz der Erforderlichkeit. Welche Fragen gestellt werden dürfen und welche nicht, richtet sich an eventuellen Besonderheiten des vorgesehenen Arbeitsverhältnisses aus.

Im Bewerbungsverfahren dürfen nur Fragen gestellt werden, die nach objektiven Maßstäben zur konkreten Entscheidung über die Bewerbung erforderlich sind. Fragen, die erst zum Vertragsabschluss relevant werden, sind unzulässig (z.B. Fragen zur Religionszugehörigkeit).

Ein fehlendes Fragerecht darf auch nicht durch Verlangen eines amtlichen Führungszeugnisses oder durch die Vorlage einer Schufa-Auskunft umgangen werden.

Ebenso darf das Instrument der Einwilligung nicht dazu benutzt werden, das Spektrum der Fragen auf an sich unzulässige Fragen zu erweitern. Fragen, die nach den arbeits- und datenschutzrechtlichen Grundsätzen nicht gestellt werden dürfen, können auch nicht durch eine Einwilligung sanktioniert werden, sondern sind und bleiben unzulässig.

Alter

Nach § 1 Allgemeines Gleichbehandlungsgesetz (AGG) und § 75 Abs. 1 BetrVG sind Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität unzulässig. Eine unterschiedliche Behandlung wegen des Alters ist gemäß § 10 AGG nur zulässig, wenn sie objektiv und angemessen und durch ein legitimes Ziel gerechtfertigt ist.

Ansonsten ist eine unterschiedliche Behandlung wegen des Alters gem. § 7 Abs. 1 AGG untersagt.

Der Arbeitgeber darf das Alter deshalb nur dann erheben, wenn für die zu besetzende Stelle Kriterien des § 10 AGG zutreffen, z. B. wenn u. a. das Alter Zugangsvoraussetzung für eine bestimmte Beschäftigung oder Bildungsmöglichkeit oder für bestimmte Vorteile ist oder ein Höchstalter festgelegt ist, z. B. für bestimmte Ausbildungsanforderungen oder eine Mindestbeschäftigungszeit vor Eintritt in den Ruhestand. Ergibt sich jedoch aus vorgelegten Bewerbungsunterlagen das Alter des Bewerbers, dürfen diese Unterlagen und damit auch Daten über das Alter gespeichert werden.

Auch in der Stellenausschreibung kann ein auch nur mittelbarer Bezug auf das Alter einen Diskriminierungsverdacht nahelegen.

Alkohol- und Drogenabhängigkeit

Die Frage nach einer bestehenden Alkoholabhängigkeit oder Alkoholkonsum wird insbesondere dann für zulässig gehalten, wenn der Alkoholkonsum die Erfüllung der Arbeitsleistungen beeinträchtigen oder Sicherheitsrisiken verursachen kann (z.B. Kraftfahrer, Kranführer, Staplerfahrer). Ein Alkohol- oder Drogentest auf Verdacht oder nur vorsorglich ist nicht zulässig. Zulässig ist ein Alkohol- oder Drogentest nur, wenn objektive Anhaltspunkte für einen entsprechenden Verdacht bestehen. Wegen des Eingriffs in das Persönlichkeitsrecht des Betroffenen ist für einen derartigen Test die Einwilligung des Bewerbers erforderlich.

Berufserfahrungen und Qualifikationen

Berufserfahrungen und Qualifikationen **dürfen** erfragt werden, soweit sie in einem Zusammenhang mit der Stelle stehen. Weit zurückliegende und mit der fraglichen Stelle nicht mehr im Zusammenhang stehende Berufserfahrungen dürfen nicht mehr erfragt werden, weil sie keine Rückschlüsse auf die Eignung für die aktuelle Stelle mehr zulassen.

Betriebsratstätigkeit – frühere

Die Frage nach früheren Funktionen in Betriebsverfassungs- oder gleichgestellten Organen beim letzten Arbeitgeber ist unzulässig.

Besondere Arten von personenbezogenen Daten

Im Zusammenhang mit Bewerbungsverfahren sind insbesondere Gesundheitsdaten bzw. körperliche Umstände, Erkrankungen oder Eigenschaften von Bedeutung, die die Erfüllung der arbeitsvertraglichen Leistungen einschränken oder gefährden können. Das Datenschutzgesetz gestattet die Erhebung dieser Daten nur, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt.

In einem bestehenden Arbeitsverhältnis dürfen diese Daten im notwendigen Umfang erhoben werden, z.B. um die ordnungsgemäße Erfüllung der Arbeitspflicht geltend zu machen. Im Bewerbungsverfahren lässt sich diese Erhebung nicht begründen. Es kann aber davon ausgegangen werden, dass sich die Erlaubnis auf die Erhebung dieser Daten auch auf das Bewerbungsverfahren erstreckt, soweit sie benötigt werden, um das eventuelle Entstehen bzw. die ordnungsgemäße Erfüllung – potenzieller – zukünftiger Ansprüche auszuloten.

Bewerberfoto

Da aus dem Foto im Einzelfall eventuell diskriminierende Schlussfolgerungen gezogen werden können (z.B. über die ethnische Herkunft), darf nach den Vorschriften des Allgemeinen Gleichbehandlungsgesetzes ein Bewerberfoto **nicht** mehr verlangt werden. Unschädlich ist es dagegen, wenn ein Bewerber von sich aus seiner Bewerbung ein Foto beilegt.

Diskriminierungsrelevante Daten

Nach den Vorschriften des Allgemeinen Gleichbehandlungsgesetzes (AGG) sind folgende Kategorien von Daten als besonders schutzwürdig und diskriminierungsrelevant eingestuft:

- Rassische und ethnische Herkunft
- Religion oder Weltanschauung
- Geschlecht
- Behinderung
- Alter
- Sexuelle Identität

Das Datenschutzgesetz klassifiziert folgende Daten als besondere Datenarten, die wegen ihrer hohen Sensibilität und Schutzbedürftigkeit einem besonderen Schutz unterworfen sind:

- Rassische und ethnische Herkunft
- politische Meinungen
- religiöse und philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit oder Sexualleben

Die nach dem AGG diskriminierungsrelevanten Daten dürfen vom Arbeitgeber nur unter den im AGG geregelten Voraussetzungen erhoben werden. Die Erhebung dieser Daten ist im Bewerbungsverfahren dann zulässig, wenn diese Kriterien für den zu besetzenden Arbeitsplatz bei objektiver und sachlicher Beurteilung von ausschlaggebender Bedeutung sind. Trifft dies nicht zu, fallen diese Daten unter das Erhebungsverbot des Datenschutzgesetzes.

Politische Meinungen und die Gewerkschaftszugehörigkeit sind im Katalog des AGG nicht enthalten, aber im Datenschutzgesetz als besondere Daten definiert. Diese besonderen Daten dürfen nur unter den einschränkenden Vorschriften erhoben werden, wenn ihre Kenntnis zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt.

Zum Zeitpunkt der Bewerbung bestehen zwar noch keine derartigen Ansprüche; allerdings besteht mit der Aufnahme der Verhandlungen ein gesetzliches Schuldverhältnis mit sog. Sekundärpflichten zur gegenseitigen Sorgfalt und Rücksichtnahme. Nach der Regelungsabsicht des Gesetzgebers kann davon ausgegangen werden, dass sich die Erhebungserlaubnis nur auf solche Informationen erstreckt, die benötigt werden, um das eventuelle Entstehen bzw. die ordnungsgemäße Erfüllung (potenzieller) zukünftiger Ansprüche auszuloten.

Ehe und Familie

Die Frage nach dem Familienstand, verheiratet oder unverheiratet, oder nach einer beabsichtigten Eheschließung und Familienplanung betrifft die privaten Lebensverhältnisse des Bewerbers und ist **unzulässig**. Ebenso ist die Frage nach der Zahl der Kinder, dem eventuellen Status „alleinerziehendend“ und nach der Art und Weise einer eventuellen Kinderbetreuung unzulässig. Auch die Frage nach einer beabsichtigten Änderung des Wohnorts oder eines Umzugs ist unzulässig.

Fahrerlaubnis

Die Frage nach der Fahrerlaubnis und der Führerscheinklasse ist zulässig, wenn das Führen von Kraftfahrzeugen für die Erledigung der betrieblichen Tätigkeit erforderlich ist.

Finanzielle Verpflichtungen, Überschuldung

Fragen nach eventuellen finanziellen Verpflichtungen sind grundsätzlich **nicht** zulässig. Lediglich bei besonderen Vertrauensstellungen mit finanziellen Dispositionsbefugnissen oder Zugang zu und Verantwortung für Geldmittel dürfen hohe Unterhaltsverpflichtungen und Überschuldung erfragt werden. Dies geschieht unter dem Gesichtspunkt, dass sich auch der Arbeitgeber vor unangemessenen Risiken schützen können muss.

Nach **Lohn- und Gehaltspfändungen** darf **im Bewerbungsverfahren nicht** gefragt werden. Diese Frage ist erst bei der Einstellung wegen der Lohn- und Gehaltsabrechnung erlaubt.

Früheres Gehalt

Das frühere Gehalt darf **nicht** erfragt werden. Es kann dann einbezogen werden, wenn der Bewerber z.B. das frühere Gehalt als Forderung in die Verhandlung eingebracht hat.

Führungszeugnis

Der Arbeitgeber darf den Bewerber zwar nach einschlägigen, d.h. in einem konkreten Bezug zu der besetzenden Stelle stehenden Vorstrafen befragen, er darf aber **nicht** die Vorlage eines polizeilichen Führungszeugnisses verlangen. Denn darin können auch Einträge über Straftaten enthalten sein, die für die zu besetzende Stelle keine Bedeutung haben. Dadurch könnte der Arbeitgeber auch die Einschränkungen des Fragerechts umgehen und mehr Informationen erheben, als zulässig ist.

Eine Ausnahme gilt für Bewerber um Stellen mit Umgang mit Kindern und Jugendlichen. Von diesen Bewerbern kann ein erweitertes Führungszeugnis angefordert werden.

Das Führungszeugnis ist auch kein absolut sicherer Beweis dafür, dass der Betroffene strafrechtlich noch nicht auffällig geworden ist, denn es werden einerseits nicht alle Strafen eingetragen und andererseits nach Fristablauf wieder gelöscht. So werden Geldstrafen bis zu 90 Tagessätzen und Freiheitsstrafen bis zu drei Monaten, wenn keine Voreintragungen vorhanden waren, und Jugendstrafen von bis zu zwei Jahren auf Bewährung nicht eingetragen. Andererseits werden Einträge nach einer Frist von drei bis zehn Jahren wieder gelöscht.

Wenn eine Straftat nicht in das Führungszeugnis aufgenommen oder wieder gelöscht worden ist, darf sich der Betroffene wieder als straffrei bezeichnen und muss darüber auch keine Auskunft mehr geben.

Fremdsprachen

Nach Fremdsprachen **darf** der Arbeitgeber fragen, wenn die Beherrschung einer bestimmten Fremdsprache für das Arbeitsverhältnis von Bedeutung ist, z. B. bei Auslandseinsätzen oder wenn bestimmte Sprachkenntnisse für die Kommunikation im Unternehmen erforderlich sind. Die Frage nach Fremdsprachen ist auch zulässig, wenn Sprachkenntnisse zwar aktuell nicht relevant sind, aber betriebliche Planungen, mögliche Entwicklungen oder langfristige Strategien Auslandseinsätze oder einen Umgang mit ausländischen Geschäftspartnern u. U. erwarten lassen.

Gesundheitszustand und Behinderungen

Zu unterscheiden ist zwischen Fragen nach dem Gesundheitszustand und der gesundheitlichen Eignung des Bewerbers für die Stelle einerseits und der Anerkennung einer Behinderung andererseits.

Behinderungen, die mit der Stelle nicht in Zusammenhang stehen und die Eignung des Bewerbers nicht einschränken, darf der Arbeitgeber wegen des Diskriminierungsverbots nicht

erfragen. Dies gilt auch für alle Stufen der Behinderung. Ansonsten dürfen Körperbehinderungen im Bewerbungsverfahren nur dann und insoweit erfragt werden, als sie erfahrungsgemäß die Eignung des Bewerbers für die vorgesehene Tätigkeit beeinträchtigen oder die Vertragserfüllung durch den Arbeitnehmer gefährden.

Differenziert ist die Frage nach dem Gesundheitszustand zu beurteilen. Stellt die zu besetzende Stelle besondere Anforderungen an die Gesundheit oder an die Belastbarkeit des Stelleninhabers, z.B. in Laboratorien, kommt eine Einstellungsuntersuchung in Betracht. Die Untersuchung kann ein vom Arbeitgeber bestimmender Arzt oder auch der Betriebsarzt vornehmen. Der Arzt hat aber kein weitergehendes Fragerecht als der Arbeitgeber selbst. Er darf ebenso wie der Arbeitgeber nicht nach Krankheiten fragen, die für die zu besetzende Stelle nicht relevant sind oder inzwischen zumindest ohne für die Stelle relevante Folgen überwunden sind.

Ebenso ist ein HIV-Test zum Ausschluss einer HIV-Infektion oder die Frage nach einer HIV-Infektion i.d.R. unzulässig, es sei denn, es handelt sich um eine Tätigkeit mit einer erhöhten Ansteckungsgefahr, z.B. in der Nahrungsmittelbranche oder im medizinischen Bereich, oder die Erkrankung ist bereits ausgebrochen.

Darüber hinaus kann der Arbeitgeber nach dem Vorliegen von solchen gesundheitlichen Einschränkungen fragen, die erfahrungsgemäß die Eignung für die Stelle beeinträchtigen, die Vertragserfüllung gefährden oder sich unter der Belastung des Arbeitsplatzes sogar verschlimmern könnten.

Kuren, Heilverfahren

Nach einer beantragten Kur oder einem Heilverfahren darf **grundsätzlich nicht** gefragt werden. Allerdings besteht auf Seiten des Bewerbers eine Hinweispflicht, wenn er wegen einer bereits terminierten Kur das Beschäftigungsverhältnis nicht zum vertraglich vorgesehenen Termin antreten kann.

Lebenslauf

Ob der Arbeitgeber einen lückenlosen und vollständigen Lebenslauf verlangen kann, hängt von den Umständen des Bewerbers und der zu besetzenden Stelle ab. Handelt es sich um eine besondere Vertrauensposition oder um eine Stelle mit sicherheitsrelevanten Aufgaben, z. B. bei Sicherheits- und Bewachungsdiensten oder des Personenschutzes, u. a. mit Umgang mit Waffen, muss der Arbeitgeber genauer prüfen dürfen als bei einem Handwerker oder einem Angestellten in der Verwaltung. Auch das Alter des Bewerbers kann eine Rolle spielen und die Lage des Zeitraums, über den der Lebenslauf Auskunft geben soll sowie die Relevanz der Angaben für die zu besetzende Stelle. So muss nicht mehr über jede Einzelheit Auskunft gegeben werden, die u. U. schon viele Jahre zurückliegt und die für die zu besetzende Stelle bedeutungslos geworden ist. Andererseits dürfen wesentliche Angaben, die für den Arbeitgeber von Bedeutung sein können (z. B. mehrjährige Auslandsaufenthalte), um sich vom Bewerber ein zutreffendes Bild zu verschafften, nicht verschwiegen werden.

Motivation, Motivationsschreiben

Die Arbeitgeber verlangen bzw. erwarten zunehmend sogenannte Motivationsschreiben. Sie erfüllen den Zweck einer positiven Selbstpräsentation, i. d. R. mit einer Schilderung der Karriereerwartungen, der besonderen Qualifikationen und einer Selbsteinschätzung des Arbeits- und Leistungsvermögens des Bewerbers. Mit diesem Inhalt verstößt das Motivationsschreiben zwar nicht gegen datenschutzrechtliche Vorschriften. Zu beachten ist allerdings, dass sich hier der Bewerber bewusst positiv darstellt und Aussagen, z. B. über die Motive eines Arbeitsplatzwechsels, nicht verbindlich sein müssen. Der Bewerber unterliegt hier keiner Verpflichtung, seine individuelle Situation oder die tatsächlichen und persönlichen Motive offenzulegen, die zu dieser Bewerbung geführt hat. Er kann deshalb kreativ die Motive positiv gefärbt und geschönt darlegen. Bestätigen sich Aussagen im Motivationsschreiben später nicht, kann der Arbeitgeber deshalb den Arbeitsvertrag nicht anfechten.

Persönlichkeitsprofile, psychologische Tests, Intelligenztests

Zunehmend werden im Bewerbungsverfahren psychologische Tests durchgeführt, z. B., um die Reaktionen und die Belastbarkeit des Bewerbers und Verhaltensmuster in bestimmten Situationen herauszufinden. Da diese Testverfahren in besonderer Weise die Persönlichkeit des Bewerbers analysieren, ist ihr Einsatz nur bei besonderen beruflichen Anforderungen gerechtfertigt. Auch bei Anlegen strenger Maßstäbe an die Auswahl der zu testenden Personen ist eine informierte Einwilligung der Betroffenen und im Hinblick auf die Anforderungen an eine informierte Einwilligung auch eine ausführliche Information der Betroffenen über den Zweck und Ziel des Tests, über die Art der Ergebnisse und deren Nutzung sowie über die Art und Weise der Durchführung erforderlich.

Als Regelmaßnahme für sämtliche Bewerbungsverfahren sind derartige Tests als **unzulässig** zu beurteilen. Neben der Begrenzung des zu testenden Personenkreises auf Stellen mit besonderen Anforderungen ist auch eine ausreichende wissenschaftliche Absicherung der Testverfahren zu fordern.

Es dürfen nur die Eigenschaften und Fähigkeiten erfragt und erforscht werden, die am jeweiligen Arbeitsplatz auch relevant sind. Es sind auch die Grenzen des Fragerechts einzuhalten, d. h., es dürfen im Zusammenhang mit dem Test keine unzulässigen Fragen gestellt werden. Trotz Einwilligung kann das Fragerecht des Arbeitgebers nicht erweitert und auf unzulässige Fragen ausgedehnt werden.

Nur wissenschaftlich abgesicherte Testverfahren sind auch geeignet, objektive und sachgerechte Ergebnisse zu liefern. Zwar ist der Arbeitgeber nicht verpflichtet, seine Entscheidung nur auf wissenschaftlich basierte Erkenntnisse zu stützen, unzulässig ist es aber, im Zusammenhang mit derartigen Testverfahren schon von vornherein zweifelhafte und dubiose Fragen zu stellen oder Folgerungen zu ziehen.

Regelmäßig werden derartige Tests nicht selbst durchgeführt, sondern von Dienstleistungsunternehmen, z. T. auch aus Drittstaaten, angeboten. Die Datenerfassung erfolgt i.d.R. online durch das Dienstleistungsunternehmen und der Arbeitgeber erhält eine Analyse, nicht aber die Eingabedaten. Teilweise wird das Ergebnis auch nur an die Bewerber zu deren freien Verfügung ausgehändigt. Voraussetzung ist hier eine datenschutzgerechte Vertragsgestaltung, i. d. R. im Sinne einer Datenverarbeitung im Auftrag. Bei Auftragnehmern in einem Drittstaat sind die besonderen Voraussetzungen des Datenschutzgesetzes zu berücksichtigen.

Teilweise wird von den Analyseinstituten auch nach diskriminierungsrelevanten Daten gefragt, z.B. nach dem ethnischen Hintergrund der Bewerber. Diese Daten werden verwendet, um die Testergebnisse auf eventuell mögliche ethnisch bedingte Fehlinterpretationen hin zu überprüfen und zu korrigieren, teilweise auch für Forschungszwecke zur Verbesserung der psychometrischen Analyseverfahren. Diese Daten fließen nicht dem Auftraggeber zu und es entstehen für den Arbeitgeber auch keine auf diese Besonderheiten rückführbaren Erkenntnisse. Unter dem Aspekt der Freiwilligkeit dieser zusätzlichen Angaben, einer besonderen Information der Betroffenen über diese Nutzung und einer frühestmöglichen Löschung dieser Daten bzw. einer nicht umkehrbaren Anonymisierung mag diese zusätzliche Erhebung diskutabel sein.

Private Lebensverhältnisse

Grundsätzlich sind Fragen nach den privaten Lebensverhältnissen, sportlicher Betätigung einschließlich Risikosportarten, Raucher oder Nichtraucher, Aktivitäten in der Öffentlichkeit wie Demonstrationsteilnahme, Schreiben von Leserbriefen, ehrenamtliche Tätigkeiten etc. **unzulässig**. Ebenfalls unzulässig sind Fragen nach einer beabsichtigten Eheschließung, nach der Zahl der Kinder und nach der Familienplanung.

Religionszugehörigkeit

Die Angabe der Religionszugehörigkeit ist zwar beim Abschluss eines Arbeitsvertrags erforderlich, **im Bewerbungsverfahren** aber in aller Regel unbedeutend und darf **nicht** erfragt werden.

Ausnahme: Es sei denn, es handelt sich um eine Stelle in einem Tendenzunternehmen, z.B. in einer kirchlichen Organisation, in der eine bestimmte Religionszugehörigkeit erwartet wird. Unter diesen Gesichtspunkten darf z.B. auch ein Journalist, der sich bei einer Zeitung bewirbt, nach einer Parteimitgliedschaft gefragt werden.

Rückfrage beim bisherigen Arbeitgeber

Wenn der Bewerber noch in einem ungekündigten Arbeitsverhältnis steht, ist eine Rückfrage beim derzeitigen Arbeitgeber **nur mit Zustimmung des Bewerbers zulässig**, denn der derzeitige Arbeitgeber kann u.U. noch keine Kenntnis von den Wechselabsichten des Arbeitnehmers haben. Wenn der derzeitige Arbeitgeber auf diesem Weg von den Wechselabsichten seines Arbeitnehmers Kenntnis erhält, kann dies für den Bewerber bei einer Fortsetzung des bestehenden Beschäftigungsverhältnisses Nachteile mit sich bringen.

Selbst wenn das bisherige Arbeitsverhältnis bereits gekündigt ist, sind Rückfragen nur im engen Rahmen zulässig. So etwa zur Präzisierung von Aussagen im Arbeitszeugnis, wenn das Zeugnis des früheren Arbeitgebers so unbestimmt und unklar formuliert ist, dass sich der potenzielle neue Arbeitgeber kein Urteil über den Bewerber bilden kann und er bereits in konkrete Verhandlungen mit dem Bewerber eingetreten ist. Zulässig sind auch auf diesem Weg nur Fragen, an deren Beantwortung der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat. **Unzulässig** sind alle Fragen, die außerhalb des Fragerechts des Arbeitgebers liegen. Der frühere Arbeitgeber darf nur die Auskünfte erteilen, die auch in einem Zeugnis stehen dürften. Über das Ergebnis der Auskunft ist der Bewerber zu unterrichten.

Schwangerschaft, Elternzeit

Die Frage nach einer Schwangerschaft ist grundsätzlich **unzulässig**.

Ausnahme: Wenn die Tätigkeit ohne Gefährdung der Gesundheit für Mutter und Kind nach den Vorschriften des Mutterschutzgesetzes zum Beschäftigungsverbot gar nicht aufgenommen werden darf. So z.B. bei einer Tänzerin oder bei Haushaltshilfen, wenn der Bestand des Arbeitgeberbetriebes beeinträchtigt sein kann. Nach der aktuellen Rechtsprechung des Europäischen Gerichtshofes (EuGH) ist jedoch die Frage nach der Schwangerschaft nunmehr generell als unzulässig zu beurteilen. **Ausnahmen** davon sind unter der Prämisse des AGG für den Fall denkbar, wenn eine Stelle in Vertretung einer Arbeitnehmerin zu besetzen ist, die ihrerseits ihre Tätigkeit wegen einer Schwangerschaft nicht fortsetzen konnte.

Scientology

Die Scientology Kirche Hamburg e.V. ist nicht als Religions- oder Weltanschauungsgemeinschaft anzusehen. Wenn Scientology nicht als Kirche bzw. als kirchliche Organisation in diesem Sinne angesehen wird, fällt die Frage nach einer Mitgliedschaft zu dieser Vereinigung nicht unter das Diskriminierungsverbot des Allgemeinen Gleichbehandlungsgesetzes (AGG) und auch nicht unter die strengeren Regelungen für die Erhebung von besonderen Datenarten im Sinne des Datenschutzgesetzes. Nach dem Grundsatz, dass Daten nur insoweit erhoben werden dürfen, als sie zur Entscheidung über die Bewerbung erforderlich sind, ist aber die Frage nach einer Mitgliedschaft nur bei solchen Stellen als berechtigt anzusehen, bei denen ein besonderes Vertrauensverhältnis vorausgesetzt wird und bei denen sich Loyalitätskonflikte ergeben können.

Vorstrafen, strafrechtliche Ermittlungsverfahren, Antritt einer Freiheitsstrafe

Nach Vorstrafen darf nur gefragt werden, wenn diese für die zu besetzende Stelle relevant sind und am vorgesehenen Arbeitsplatz eine Wiederholungsgefahr bestehen könnte. So darf

ein Jugendbetreuer nach Sittlichkeitsdelikten und ein Finanzbuchhalter nach Vermögensdelikten oder ein Kraftfahrer, Kran- oder Staplerfahrer nach Alkoholdelikten gefragt werden. Der Bewerber muss darüber keine Auskunft mehr geben, wenn die Vorstrafe nicht in das Führungszeugnis aufgenommen werden darf oder aus dem Register zu tilgen ist. Vorstrafen dürfen deshalb auch nicht uneingeschränkt im Personalbogen erfragt werden, auch um die Resozialisierung nicht zu erschweren.

Nach strafrechtlichen Ermittlungsverfahren darf der Arbeitgeber nur fragen, soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert oder durch die Ermittlungen Zweifel an der persönlichen Eignung des Arbeitnehmers begründet werden.

Web-Recherche

Die Zulässigkeit der Web-Recherche wird unterschiedlich beurteilt. Einerseits wird argumentiert, dass diese Daten allgemein zugänglich zur Verfügung stehen, in aller Regel sogar von den Betroffenen selbst eingestellt worden sind und deshalb vom Arbeitgeber unter Beachtung des Erforderlichkeitsprinzips auch abgefragt werden dürfen. Gestützt wird diese Auffassung auf der als Ausnahmevorschrift vom Direkterhebungsgebot, die eine Erhebung von personenbezogenen Daten aus allgemein zugänglichen Quellen erlaubt. Dies ist aber nur dann der Fall, wenn das schutzwürdige Interesse des Betroffenen am Ausschluss der Erhebung nicht offensichtlich überwiegt.

Andererseits wird die Rechtsauffassung vertreten, dass die Vorschrift (die eine Erhebung von personenbezogenen Daten im Bewerbungsverfahren nur im Rahmen der Zulässigkeit erlaubt) für die Erhebung von Personaldaten für ein Beschäftigungsverhältnis nicht mehr greifen kann. Da dann diese Ausnahmeregelung vom Direkterhebungsgebot nicht mehr angewendet werden kann, verbleibt es beim Direkterhebungsgebot. Daraus folgt, dass allgemeine Web-Recherchen zur Beschaffung von Zusatzinformationen über den Bewerber unzulässig sind. Darüber hinaus soll sich ein Bewerber, wenn er sich in ein Anbahnungsverhältnis begibt, auch darauf verlassen können, dass diese vertragliche Beziehung auch den Rahmen der zulässigen Datenerhebung umreißt. Ein Rückgriff durch den Arbeitgeber auf andere Quellen würde sich vom gemeinsamen Willen der Beteiligten entfernen. Das Vertrauen darauf, dass dies nicht geschieht, ist schützenswert.

Zu berücksichtigen ist auch, dass durch Internetrecherchen keinesfalls die Einschränkungen des Fragerechts umgangen werden dürfen und das Fragrecht hierdurch auch keine Erweiterung erfährt.

Wettbewerbsverbote

Wegen der einschränkenden Wirkung eines Wettbewerbsverbots **darf** der Arbeitgeber den Bewerber danach fragen, ob vonseiten eines früheren Arbeitgebers ein wirksames Wettbewerbsverbot besteht und über welchen Zeitraum dieses Wettbewerbsverbot noch gültig ist. Vonseiten des Bewerbers besteht darüber nicht nur eine Auskunftspflicht bei einer entsprechenden Frage, sondern seinerseits eine **Hinweispflicht**.

Zeitliche Verfügbarkeit

Die zeitliche Verfügbarkeit, d.h. die zeitliche Unabhängigkeit des Bewerbers von bestimmten oder regelmäßigen Arbeitszeiten und seine diesbezügliche Flexibilität, **darf** bei Vorliegen entsprechender Anforderungen der Stelle, z.B. bei umfangreicherer Reisetätigkeit, erfragt werden. Das Fragerecht geht aber dann nicht so weit, dass auch nach den familiären Verhältnissen oder danach gefragt werden darf, wer in der Zeit der Abwesenheit ggf. die Kinder betreut oder sonstige familiäre Aufgaben wahrnimmt.

Zugehörigkeit zu politischen Parteien, Gewerkschaften und sonstigen Vereinigungen, Weltanschauung

Die Zugehörigkeit zu politischen Parteien, eine Mitgliedschaft in Gewerkschaften oder sonstigen Vereinigungen politischer oder unpolitischer Art oder Parteifunktionen darf grundsätzlich **nicht** erfragt werden.

Ausnahme**:** Wenn es sich um eine Anstellung bei einer Kirche, Partei oder Gewerkschaft handelt und wenn von dem Stelleninhaber eine Mitgliedschaft zu dieser Organisation erwartet wird (sog. Tendenzunternehmen).

Mitteilungs- und Offenbarungspflichten des Bewerbers

Neben dem Fragerecht des Arbeitgebers hat die Rechtsprechung auch **Mitteilungspflichten des Bewerbers** entwickelt. Demnach ist der Bewerber verpflichtet, **unaufgefordert** Umstände darzulegen, die für ihn erkennbar die Erfüllung des Vertrages bzw. die Ausübung der Tätigkeit unmöglich oder unzumutbar machen könnten oder wenn angemessene Leistungserwartungen des Arbeitgebers nicht erfüllt werden können bzw. andere Umstände von ausschlaggebender Bedeutung für die Besetzung des Arbeitsplatzes sind. Diese Mitteilungs- und Offenbarungspflichten sind jedoch im Hinblick auf den werbenden Charakter einer Bewerbung eng gefasst. Dem Bewerber soll nicht zugemutet werden, von sich aus über seine Person nachteilige und möglicherweise doch nicht relevante Aussagen zu machen. Unter diesem Gesichtspunkt werden die Mitteilungs- und Offenlegungspflichten des Bewerbers zurückhaltend gehandhabt.

Beispiele hierfür sind:

- Ein Bewerber um einen Arbeitsplatz als Berufskraftfahrer muss ungefragt auf eine bestehende Alkoholabhängigkeit hinweisen. Ebenso muss er auch offenlegen, wenn ihm der Führerschein entzogen wurde oder gravierende Mängel der Fahrpraxis bestehen.
- Erkrankungen muss der Bewerber von sich aus offenbaren, wenn die Erkrankung für ihn erkennbar die zu erwartende Arbeitsleistung einschränken wird.
- Hat der Bewerber eine Kur beantragt und ist zu erwarten, dass er sich zum Zeitpunkt des Arbeitsantritts in Kur befinden wird, besteht darüber eine Offenbarungspflicht.
- Ein Bewerber um ein zweckgebundenes befristetes Beschäftigungsverhältnis muss den Arbeitgeber über ein anstehendes Heilverfahren unterrichten.
- Der Bewerber muss den Arbeitgeber unaufgefordert über eine bevorstehende zu verbüßende Freiheitsstrafe unterrichten, unabhängig davon, ob die Straftat im Zusammenhang mit dem Beschäftigungsverhältnis steht. Der Hintergrund ist hier, dass der Bewerber wegen der zu verbüßenden Haftstrafe seine Arbeitsleistung nicht erbringen kann.
- Wenn aufgrund eines früheren Beschäftigungsverhältnisses ein Wettbewerbsverbot besteht, das die Erfüllung der Vertragsleistungen beeinträchtigt, muss der Bewerber den Arbeitgeber davon unterrichten.

Selbstverständlich besteht zu diesen Sachverhalten auch ein Fragerecht des Arbeitgebers.

Recht zur Falschauskunft

Korrekte Fragen des Arbeitgebers muss der Bewerber **vollständig** und **wahrheitsgemäß** beantworten. Unzulässige und rechtswidrige Fragen muss er nicht beantworten. Wenn aber der Arbeitgeber im Einstellungsgespräch unzulässige Fragen stellt, riskiert der Bewerber bei einer Verweigerung der Antwort u.U. die Ablehnung seiner Bewerbung. Beantwortet er die Fragen, legt er seine persönlichen Verhältnisse in einem Maße offen, dass es einer Verletzung seines

Persönlichkeitsrechts gleichkommt und läuft Gefahr, dass ihm die Antworten zum Nachteil gereichen.

Um hier die Rechte der Bewerber besser zu schützen, wurde in Rechtsprechung und Schrifttum sozusagen als Instrument der Notwehr das Recht zur Falschauskunft bzw. das Recht zur Lüge entwickelt. Dieses Recht zur Lüge ist für den Bewerber allerdings auch mit Risiken behaftet, denn die Rechtsprechung zum Fragerecht dürfte für die Bewerber in aller Regel inzwischen unüberschaubar geworden sein. Lügt der Bewerber an der falschen Stelle, schafft er einen Anfechtungsgrund für den Arbeitsvertrag. Wenn der Arbeitgeber zu einem späteren Zeitpunkt feststellt, dass der Bewerber im Bewerbungsgespräch eine zulässige Frage falsch beantwortet hat, kann er auch nach langer Zeit den Arbeitsvertrag wegen arglistiger Täuschung anfechten.

In Rechtsprechung und Schrifttum besteht Einigkeit darüber, dass die Regelungen des BGB über die Anfechtung eines Rechtsgeschäftes grundsätzlich auch für die Anfechtung eines Arbeitsvertrages gelten, soweit sie mit dem Wesen und dem Inhalt des Arbeitsverhältnisses als ein Rechtsgeschäft besonderer Art nicht unvereinbar sind. Im Falle einer berechtigten Anfechtung des Arbeitsverhältnisses durch den Arbeitgeber ist das angefochtene Arbeitsverhältnis von Anfang an nichtig. Für das Arbeitsverhältnis bedeutet dies, dass der Arbeitsvertrag mit sofortiger Wirkung und ohne Kündigungsschutz und ohne Kündigungsfrist endet.

Die Falschauskunft auf eine unzulässige Frage im Bewerbungsgespräch kann dem Bewerber nicht als arglistige Täuschung ausgelegt werden. Der Bewerber muss den Arbeitgeber nicht nur getäuscht haben, sondern er muss es auch arglistig getan haben. Nach der Rechtsprechung ist eine Täuschung dann nicht arglistig, wenn sich der Bewerber gegen eine unzulässige Frage des Arbeitgebers nicht anders als durch eine Lüge zu wehren weiß.

Ein Anfechtungsrecht des Arbeitgebers besteht, wenn:

1. die Frage des Arbeitgebers rechtmäßig und zulässig war,
2. der Bewerber gelogen, d.h. vorsätzlich falsch geantwortet hat,
3. der Bewerber wusste oder hätte wissen müssen, dass die von ihm verschwiegene Tatsache oder falsch beantwortete Frage für den Arbeitgeber von Wichtigkeit war und
4. die Lüge oder das Verschweigen für die Entscheidung des Arbeitgebers mitursächlich oder gar entscheidend war.

Das Anfechtungsrecht erlischt, wenn die verschwiegene Tatsache bzw. die unrichtige Antwort für die Fortsetzung des Beschäftigungsverhältnisses bedeutungslos geworden ist.

Direkterhebungsgebot

Personenbezogene Daten sind **vom Bewerber direkt** zu erheben, damit der Betroffene weiß, zu welchen Daten der Arbeitgeber über ihn Kenntnis erhält. Direkterhebung beim Betroffenen bedeutet, dass die personenbezogenen Daten **von ihm selbst erfragt** oder **mit seiner Kenntnis oder Mitwirkung** erhoben werden. Damit sind z.B. auch Eignungstests, Einstellungsprüfungen oder betriebsärztliche Untersuchungen zulässig. Ebenso sind Fragen nach Kindern und Ehepartner noch vom Direkterhebungsgebot sanktioniert, soweit diese Kenntnisse zur Gestaltung des Entgelts oder von bestimmten Zulagen erforderlich sind.

Ausnahmen von diesem Direkterhebungsgebot lässt das Datenschutzgesetz nur dann zu, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt. Als Ausnahme gilt auch, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht, oder wenn die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand erfordern würde und keine

Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Unter diesen Gesichtspunkten ist je nach Branche oder Art der zu besetzenden Stelle eine Datenerhebung über einen Bewerber zulässig, so auch Anfragen an Branchenauskunftsdienste (z.B. im Versicherungswesen) oder die Nutzung von Warndateien (z.B. im Zusammenhang mit Terrorismusabwehr).

Tests und Untersuchungen im Einstellungsverfahren

Die verbreiteten Einstellungstests sind weder genormt, noch ist die Vorgehensweise standardisiert. Die Ergebnisse und Rückschlüsse sind deshalb oft nicht nachvollziehbar und die Ergebnisse der verschiedenen Tests sind nicht vergleichbar. Zur Vereinheitlichung und Standardisierung der Einstellungstests hat das Deutsche Institut für Normung (DIN) im Jahr 2002 mit der DIN 33430 Standards für die Eignungsbeurteilung definiert.

Die Norm enthält im Wesentlichen Entscheidungshilfen zur Vorbereitung von Eignungsaussagen und -entscheidungen von Bewerbern und Maßstäbe zur Beurteilung und Auswahl von Dienstleistungen, die von Unternehmens- und Personalberatern angeboten werden. Die Norm stellt einheitliche Qualitätskriterien und -standards für berufsbezogene Eignungsbeurteilungen von Bewerbern zur Verfügung, mit deren Hilfe Fehlentscheidungen möglichst vermieden werden sollen.

Ärztliche Einstellungsuntersuchungen

Soweit bei der zu besetzenden Stelle **besondere gesundheitliche Anforderungen oder Auflagen** bestehen, kann der Arbeitgeber auch ärztliche Einstellungsuntersuchungen durch den betriebsärztlichen Dienst oder einen anderen beauftragten Arzt durchführen lassen. Für die Untersuchung ist eine **Einwilligung des Bewerbers** erforderlich. Der untersuchende Arzt hat kein erweitertes Fragerecht, d. h., der Arzt darf nur die Fragen stellen und Befunde erheben und Tests durchführen, die mit den Anforderungen der zu besetzenden Stelle im Zusammenhang stehen. Damit verbieten sich z. B. ungerechtfertigte und anlasslose Alkohol- und Drogentests. Der Arzt darf dem Arbeitgeber auch keine Befunde offenlegen, sondern nur mitteilen, ob der Bewerber für die Stelle, ggf. mit welchen Einschränkungen, geeignet oder nicht geeignet ist.

Assessmentcenter

Assessmentcenter besitzen in der Regel Testcharakter. Für die Zulässigkeit gelten die gleichen Voraussetzungen wie für psychologische Tests und Gutachten.

Grafologisches Gutachten

Der Arbeitgeber darf für die Beurteilung einer Bewerbung nur objektive und sachgerechte Informationen erheben. Ein grafologisches Gutachten darf deshalb nur **ausnahmsweise** und **mit Einwilligung des Bewerbers** eingeholt werden. Auch bei Vorliegen einer Einwilligung darf das Gutachten nach den Grundsätzen zur Verhältnismäßigkeit nur zu solchen Charaktereigenschaften Stellung nehmen, die für die auszuübende Tätigkeit von Bedeutung sind. Bei einfacheren Tätigkeiten sind graphologische Gutachten grundsätzlich unzulässig.

Intelligenz- und Kreativitätstests

Für Intelligenz- und Kreativitätstests gelten die gleichen Grundsätze wie für eine psychologische Begutachtung.

Persönlichkeitsprofile, psychologische Tests, Intelligenztests, Einstellungstests

Zunehmend werden im Bewerbungsverfahren psychologische Tests durchgeführt, z. B., um die Reaktionen und die Belastbarkeit des Bewerbers und Verhaltensmuster in bestimmten Situationen herauszufinden. Psychologische Tests oder Gutachten sind nur **sehr**

eingeschränkt bei der Besetzung von **besonderen Stellen**, und auch dann **nur mit Einwilligung** der Bewerber, zulässig. Die Bewerber müssen über Art und Umfang der Tests und der Begutachtung, über den voraussichtlichen Verlauf und die Reichweite des Tests vorher informiert werden. Zulässig sind auch dann nur Tests, die bestimmte, für den Arbeitsplatz relevante Eigenschaften und Fähigkeiten betreffen und nicht die gesamte Persönlichkeit des Bewerbers. Der Bewerber hat ein Recht auf Einsichtnahme in das Gutachten und wenn die Bewerbung nicht berücksichtigt wurde, muss der Arbeitgeber das Gutachten gegen Nachweis vernichten.

Behandlung der abgelehnten Bewerbungen

Die Speicherung von Bewerberdaten ist zulässig, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Die Kenntnis des Inhalts von nicht berücksichtigten Bewerbungen ist unter diesen Gesichtspunkten nicht mehr erforderlich. Nicht berücksichtigte Bewerbungen sind deshalb zurückzugeben.

Soweit Bewerbungen elektronisch gespeichert sind, ergibt sich eine Löschungsverpflichtung auch aus dem Datenschutzgesetz. Nach dieser Vorschrift sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Für Bewerbungen in Papierform greift die Löschungsverpflichtung zwar nicht, da aber Bewerbungen eine Vielzahl vertraulicher und z.T. auch sehr sensibler personenbezogener Daten enthalten, folgt die Verpflichtung zur Rückgabe aus dem allgemeinen Persönlichkeitsrecht des Bewerbers.

Gemäß dem Allgemeines Gleichbehandlungsgesetz (AGG) kann der Bewerber innerhalb einer Frist von zwei Monaten nach Kenntnis einer Benachteiligung einen Anspruch auf Schadensersatz erheben und binnen weiterer drei Monate einklagen. Werden vom abgelehnten Bewerber Indizien vorgelegt, die eine Benachteiligung nach den Vorschriften des AGG vermuten lassen, liegt die Beweislast dafür, dass kein Verstoß vorgelegen hat, beim Arbeitgeber. Um im Falle einer Klage den Entlastungsbeweis führen zu können, empfiehlt es sich deshalb, zumindest die entscheidungserheblichen Auszüge aus der Bewerbung, die Kriterien für das Auswahlverfahren und die Entscheidungsgründe über die Bewerbung für einen angemessenen Zeitraum aufzubewahren bzw. zu speichern. Die Frist für die Geltendmachung einer Benachteiligung beginnt mit der Kenntnis der Benachteiligung. Dies muss nicht immer der Zeitpunkt der Zustellung der Ablehnung sein, sondern es kann auch ein späterer Zeitpunkt sein. Unter Berücksichtigung von Postlaufzeiten und sonstigen eventuell möglichen Liegezeiten ist sicher kein Verstoß gegen das Allgemeine Gleichbehandlungsgesetz und den Datenschutz zu erkennen, wenn die Zweimonatsfrist als Mindestaufbewahrungsfrist gehandhabt und um einen angemessenen Zeitraum verlängert wird.

Es ist vertretbar, wenn ein Unternehmen die Bewerberunterlagen bis zu **sechs Monate ab Abschluss des Bewerbungsverfahrens** noch vorhält. Die Frist beginnt bei einer Bewerbung mit dem Zugang der Ablehnung.

Auch bei **Initiativbewerbungen** erscheint eine Speicherfrist von bis zu sechs Monaten ebenfalls als sachgerecht. Anders wäre es, wenn der Bewerber erklärt hat, mit einer längeren Speicherung einverstanden zu sein, bis das Unternehmen für ihn eine geeignete Stelle gefunden hat oder das Unternehmen eine solche Absicht dem Bewerber mitteilt und dieser damit einverstanden ist.

Eine **Weiterleitung** von Bewerbungen (z.B. innerhalb von konzernangehörigen Unternehmen) **an eine Schwestergesellschaft oder an die Muttergesellschaft** ist nur mit **Einwilligung des Bewerbers** zulässig. Ebenso ist eine Aufbewahrung der Bewerbung für eine später zu besetzende Stelle nur mit Einwilligung des Betroffenen zulässig. Sollte eine derartige Weiterleitung oder Aufbewahrung in Frage kommen, kann die Einholung der Einwilligung mit dem Ablehnungsschreiben dergestalt verbunden werden, dass dem Bewerber angeboten, wird, innerhalb einer zu setzenden Frist hierzu seine Einwilligung einzureichen. Ansonsten wird je nach Speicherungsform seine Bewerbung nach Ablauf der nach dem AGG angemessenen Frist gelöscht oder zurückgegeben.

Sollen die Bewerberdaten für eine später zu besetzende Stelle aufbewahrt werden, so ist dies nur mit ausdrücklicher, schriftlicher Einwilligung des Bewerbers zulässig.

Textbeispiel | Ihr Einverständnis vorausgesetzt würden wir gern Ihre Bewerbungsunterlagen noch länger behalten. Sollten wir nicht auf Sie zukommen, werden wir Ihre Unterlagen spätestens nach einem Jahr datenschutzgerecht vernichten. Teilen Sie uns bitte mit, wenn Sie der längeren Aufbewahrung widersprechen.

Personalakten

In der Privatwirtschaft gibt es keine Formvorschriften über die Führung von Personalakten. Form und Gestaltung der Personalakten obliegen deshalb der Gestaltungsfreiheit des Arbeitgebers.

Begriffsdefinition

Zunächst stellt sich die Frage nach dem Begriff der Personalakte oder elektronische Personalakte: Welche Unterlagen im Unternehmen gehören zur Personalakte und wie ist die Personalakte gegen andere Unterlagen abzugrenzen, die ebenfalls personenbezogene Daten über die Beschäftigten enthalten können? Diese Frage ist nicht nur theoretischer Natur, sondern gewinnt praktische Bedeutung, wenn ein Mitarbeiter Einsicht in die Personalakte verlangt und zu entscheiden ist, in welche Unterlagen Einsicht zu gewähren ist.

Zur **Personalakte gehören**, unabhängig von der Art und Weise ihrer Führung (d.h. sowohl manuell als auch automatisiert), **alle Informationen, Daten, Unterlagen und Vorgänge, die in einem unmittelbaren inneren Zusammenhang mit dem Beschäftigungsverhältnis stehen**.

Die Personalakte darf nur Daten enthalten, die für die Durchführung des Arbeitsverhältnisses erforderlich sind.

Demzufolge gehören zur Personalakte alle das Beschäftigungsverhältnis betreffenden Unterlagen und Daten unabhängig davon, an welcher Stelle, unter welcher Bezeichnung, in welcher Form und auf welchen Datenträgern sie geführt werden. Neben der als Personalakte bezeichneten Unterlagensammlung in der Personalabteilung gehören zur Personalakte auch alle Sonder- und Nebenakten sowie alle digital geführten oder auf Mikrofilm archivierten Unterlagen. Die klassische Personalakte kann in einer Akte geführt oder in Teilakten gegliedert sein. Zur Personalakte gehören auch Teilakten, die von Vorgesetzten außerhalb der Personalabteilung geführt werden.

Grundsatz der Erforderlichkeit

§ 26 Abs. 1 BDSG erlaubt die Verarbeitung von Beschäftigtendaten, wenn die Verarbeitung für die in § 26 BDSG genannten **Zwecke** erforderlich ist. Der Begriff der Erforderlichkeit ist ein unbestimmter Rechtsbegriff und bedarf deshalb der näheren Betrachtung und Interpretation. Grundsätzlich müssen Art und Umfang der personenbezogenen Daten und der Umfang der Verarbeitung gem. Art. 5 Abs. 1 lit. c DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**). Es dürfen also nicht mehr Daten erhoben, gespeichert und verarbeitet werden, als zur Erfüllung der Aufgabe bzw. der in § 26 BDSG genannten Zwecke benötigt werden. Es dürfen auch keine Daten auf Vorrat erhoben werden, z. B. unter dem Gesichtspunkt, dass die Daten

zu einem späteren Zeitpunkt für eine andere oder zusätzliche Nutzung vielleicht ganz nützlich wären. Eine Datenerhebung und Speicherung auf Vorrat oder ein vorsorgliches Datensammeln ist nicht zulässig. Es dürfen nur die Daten erhoben und gespeichert werden, die für die anstehende Aufgabe bzw. den jeweiligen Zweck, z. B. zur Entscheidung über die Einstellung oder zum Abschluss des Arbeitsvertrages, konkret benötigt werden. Welche Daten grundsätzlich und im Einzelfall konkret erforderlich sind, entscheidet der Arbeitgeber nach eigenem Ermessen.

Der Begriff selbst wird auch nicht einheitlich interpretiert. Es gibt eine strenge Interpretation, die eine Erforderlichkeit nur dann anerkennt, wenn die Aufgabe ohne Kenntnis der Daten überhaupt nicht wahrgenommen werden könnte bzw. der Zweck nicht erreicht werden könnte, die Daten also unverzichtbar sind. Eine etwas großzügigere Auslegung bejaht die Erforderlichkeit schon dann, wenn die Kenntnis der Daten die Erfüllung der Aufgabe bzw. die Erreichung des Zweckes fördert, erleichtert, unterstützt oder in kürzerer Zeit ermöglicht.

Ein zusätzliches Kriterium für die engere oder weitere Auslegung des Begriffes der Erforderlichkeit kann auch der Grad der Sensibilität der Daten sein. Handelt es sich um besondere Datenarten, sind einer Erhebung ohnehin enge Grenzen gezogen. Darüber hinaus ist mit der Erhebung, Verarbeitung und Nutzung umso mehr Zurückhaltung geboten je sensibler die Daten sind und je mehr in das Persönlichkeitsrecht des Betroffenen eingegriffen wird.

Informationspflichten bei der Datenerhebung

Bei der Datenerhebung ist der Betroffene gemäß Art. 13 DSGVO von der verantwortlichen Stelle (Arbeitgeber) über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung bei Datenübermittlungen auch über die Kategorien von Empfängern zu unterrichten. Die Identität des Arbeitgebers und die Zweckbestimmung der Datenerhebung sind i.d.R. offensichtlich bzw. ergeben sich aus dem Zusammenhang, sodass darüber keine gesonderte Unterrichtung mehr erforderlich ist.

Innerhalb einer Unternehmensgruppe kann sich diese Anforderung nach einer Unterrichtung über die Identität des Arbeitgebers ergeben, wenn die Personalhoheit bzw. Personalzuständigkeit an die Zentrale oder an eine andere bestimmte Gesellschaft im Gruppenverbund übertragen und dies bei der Einstellung für den Bewerber nicht erkennbar ist.

Über Kategorien von Empfängern muss der Betroffene unterrichtet werden, soweit er nach den Umständen des Einzelfalles nicht mit einer Übermittlung an diese rechnen muss. Unter diesem Gesichtspunkt entfällt eine Unterrichtungspflicht über Empfänger, an die im Arbeitsleben eine Datenübermittlung üblich ist, z.B. bei Übermittlungen an die Krankenkasse oder an das Bankinstitut zur Auszahlung des Gehalts oder bei Offenbarungen an den Betriebsrat. Eine Unterrichtungspflicht besteht dagegen, wenn zur Verarbeitung von Personaldaten im Wege der Datenverarbeitung im Auftrag Dienstleistungsunternehmen eingeschaltet werden oder wenn bestimmte personenbezogene Daten für konzernübergreifende Verarbeitungsverfahren an die Muttergesellschaft übertragen werden (insbesondere, wenn diese ihren Sitz im Ausland hat), soweit hierzu nicht ohnehin eine Einwilligung des Betroffenen erforderlich ist.

Der Arbeitnehmer ist im Vorfeld über die Nutzungen und Übermittlungen seiner Daten zu unterrichten, sofern er nicht bereits auf andere Weise Kenntnis davon erlangt hat. Diese Informationspflicht entfällt nur dann, wenn der Betroffene bereits über die Informationen verfügt.

Beschäftigtendaten in nichtautomatisierten Verfahren und Dateien (Akten)

Die Vorschriften der DSGVO gelten gem. Art. 2 Abs. 1 DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder

gespeichert werden sollen. Ein Dateisystem in diesem Sinne ist gem. Art. 4 Nr. 6 DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Damit ist auch künftig klargestellt, dass die Erhebung von Beschäftigtendaten und deren Speicherung in Personalakten, soweit sie im Zusammenhang mit der Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses stehen, unabhängig von der technisch-organisatorischen Form und dem Aufbau der Personalakten immer den Vorschriften des Datenschutzgesetzes unterliegen.

Werden im Rahmen eines **Bewerbungsverfahrens** vom Bewerber Informationen erfragt und manuell festgehalten oder bei der Einstellung ein Personalfragebogen ausgefüllt, fallen diese Unterlagen ebenfalls unter den Schutzbereich des Datenschutzgesetzes.

Datenschutzbelehrung der Beschäftigten

Neben der Informationspflicht, die immer dann greift, wenn der Arbeitgeber vom Beschäftigten personenbezogene Daten erhebt, muss der Arbeitgeber seine Beschäftigten auch über die **am jeweiligen Arbeitsplatz relevanten Datenschutzbestimmungen belehren**. Der Verantwortliche muss seine Beschäftigten über den Umgang mit personenbezogenen Daten und über die **Pflicht zur Wahrung der Vertraulichkeit belehren** und die Belehrung zum Nachweis der Wahrung der Rechenschaftspflicht auch **dokumentieren**. Die Art und Weise der Belehrung ist in der DSGVO nicht geregelt. Die Belehrung kann durch dokumentierte Schulungen geschehen und ergänzend durch aufgabenspezifische Arbeits- und Verfahrensanweisungen und Prozessbeschreibungen. Die Belehrung, die Arbeits- und Verfahrensanweisungen und Prozesse müssen so aufgabenspezifisch zugeschnitten sein, dass die Beschäftigten daraus klare Handlungsanweisungen für den Umgang mit personenbezogenen Daten an ihrem Arbeitsplatz entnehmen können. Wichtig sind insbesondere Belehrungen zur Zulässigkeit der Verarbeitung und zur Übermittlung von personenbezogenen Daten und zum Umgang mit den Rechten der Betroffenen. Im Hinblick auf die Rechenschaftspflicht sollte die Durchführung der Belehrung nachweisbar dokumentiert werden.

Abgrenzung der Personalakte gegen sonstige Unterlagen

Die Personalakten sind insbesondere gegen Betriebsakten und sonstige Sachakten sowie gegen persönliche Aufzeichnungen von Vorgesetzten abzugrenzen.

Betriebsdaten

Zu den Betriebsdaten gehören alle **Aufzeichnungen im Zusammenhang mit der Produktion** und dem Vertrieb von Produkten und Dienstleistungen. Aus dem Produktionsbereich sind dies z.B. Maschinenprotokolle zum Nachweis, wer wann welche Maschine für welches Produkt oder Werkstück benutzt hat, oder Qualitätsaufzeichnungen über die Herstellung und Abnahme von Produkten oder Teilprodukten zum Zwecke der Qualitätssicherung. Aufzeichnungen ähnlicher Art fallen im Bereich der Logistik, der Warenwirtschaft, der Lagerhaltung und des Controllings an. Diese Daten und Informationen stehen nicht in einem inneren Zusammenhang mit dem Beschäftigungsverhältnis. Sondern sie dienen Nachweisen im Zusammenhang mit der betrieblichen Leistungserstellung, Qualitätsnachweisen, Kostenzurechnungen u.a. Sie stehen nur in einem losen Zusammenhang mit dem eigentlichen Beschäftigungsverhältnis.

Auch **Akten** (z.B. über Personal- und Personalbedarfsplanungen, Nachfolgeplanungen, Personalentwicklungsmaßnahmen, Entwürfe von Zeugnissen und Beurteilungen) **und Aufzeichnungen von Vorgesetzten** zur Vorbereitung von Beurteilungen gehören zu den sog. Sachakten. Diese Akten und Unterlagen dienen der Vorbereitung von Personalentscheidungen und erzeugen für die Beschäftigten noch keine Rechtswirkungen.

Ebenfalls keine Personalaktendaten sind z.B. **Belege und Unterlagen aus dem internen Rechnungswesen**, wie Zahlungsanordnungen und alle sonstigen der Rechnungslegung dienenden Nachweise.

Persönliche Aufzeichnungen von Vorgesetzten

Wenn Vorgesetzte zur **Erfüllung ihrer fachlichen Führungsaufgaben** über ihre Mitarbeiter Aufzeichnungen anlegen, z.B. zur Planung von Schulungs- und Fortbildungsmaßnahmen oder als Materialsammlung für Beurteilungen, entstehen **Nebenakten**, die aber erst dann Bestandteil der Personalakte werden, wenn sie Verbindlichkeit erlangen.

Kein Personalaktencharakter habe diese Aufzeichnungen, wenn diese nicht zur Mitteilung an Dritte bzw. als Materialsammlung für dienstliche Beurteilungen angelegt sind und von vornherein nicht die Gefahr einer Verwechslung mit dienstlichen Vorgängen und auch kein Grund zu einem diesbezüglichen Misstrauen besteht.

Abmahnungen

Bei Störungen im Leistungsbereich eines Beschäftigungsverhältnisses ist die Abmahnung ein Mittel, um das Fehlverhalten eines Arbeitnehmers zu rügen. Darüber hinaus besitzt die Abmahnung für den Arbeitnehmer auch eine Warn- und Androhungsfunktion im Hinblick auf die Möglichkeit einer Kündigung bei Fortsetzung des gerügten Verhaltens. Damit die Abmahnung diese Funktion auch erfüllen kann, muss sie dem Betroffenen eröffnet und zu Beweiszwecken auch zur Personalakte hinzugefügt werden.

Je nach Art, Schwere und Bedeutung des gerügten Fehlverhaltens des Arbeitnehmers kann eine Abmahnung nach einer bestimmten Zeitspanne für das weitere Beschäftigungsverhältnis bedeutungslos geworden sein und sogar die künftige Entwicklung des Beschäftigten ungerechtfertigt negativ beeinträchtigen, z.B. wenn sie trotz ihrer tatsächlichen Bedeutungslosigkeit immer noch in Beurteilungen einfließt oder einfließen kann.

Vor diesem Hintergrund haben die Arbeitsgerichte bezüglich der Abmahnungen einen Entfernungsanspruch durch Zeitablauf erkannt. Ob eine Abmahnung durch Zeitablauf wirkungslos geworden ist, bemisst sich nach der Art der Verfehlung, deren Bedeutung für das weitere Beschäftigungsverhältnis, dem zwischenzeitlichen Verhalten des Arbeitnehmers und der Schwere der Vorwürfe. Ferner ist von Bedeutung, ob in der Zwischenzeit erneut eine Abmahnung ausgesprochen werden musste. In Rechtsprechung und Praxis wird vor diesem Hintergrund von einer Aufbewahrungsfrist von zwei Jahren ausgegangen.

Sobald eine Abmahnung für das weitere Beschäftigungsverhältnis bedeutungslos geworden ist, muss sie aus den Personalakten entfernt werden.

Dieser Grundsatz der Entfernung bei künftiger Bedeutungslosigkeit entspricht auch der datenschutzrechtlichen Regelung, wonach Daten über Beschäftigte nur solange gespeichert werden dürfen, als dies für die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Ebenso sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Hat die Abmahnung ihre Warnfunktion erfüllt und der Betroffene sein Verhalten entsprechend geändert, sodass die Abmahnung für die Zukunft keinerlei Funktion mehr besitzt, hat sich die Abmahnung erledigt und ist zu entfernen bzw. zu löschen. Der betroffene Mitarbeiter ist über die Löschung bzw. Entfernung der Abmahnung zu unterrichten.

Der gleiche Entfernungs- bzw. datenschutzrechtliche Löschungsanspruch besteht, wenn die Abmahnung oder die Androhung einer Abmahnung zu Unrecht ergangen ist.

Grundsätzliche Prinzipien zur Führung der Personalakten

Die Führung der Personalakten wird von folgenden Grundprinzipien bestimmt:

- Vertraulichkeit der Personalunterlagen
- Richtigkeit und Vollständigkeit
- Zulässigkeit und Zweckbindung der Informationen
- Transparenzgrundsatz

Vertraulichkeit der Personalunterlagen

Das Gebot der Vertraulichkeit verpflichtet den Arbeitgeber zur vertraulichen Behandlung der Inhalte sowohl innerhalb des Unternehmens als auch außenstehenden Dritten gegenüber. Kantinengespräche über Personalangelegenheiten verbieten sich damit.

Ebenso sind die **Personalakten sicher** zu **verwahren** und vor dem Zugriff unbefugter Personen zu schützen. Der **Kreis der zugriffsbefugten Personen** ist auch innerhalb der Personalabteilung auf den notwendigen Umfang zu **begrenzen**.

Gesundheitsdaten des Arbeitnehmers dürfen, soweit sie überhaupt als Inhalt der Personalakte erlaubt sind, nur besonders verschlossen geführt werden. Der Zugriff darf nur besonders befugten Personen erlaubt sein. Keinesfalls dürfen ärztliche Zeugnisse oder sonstige Unterlagen mit Informationen über die gesundheitlichen Verhältnisse des Mitarbeiters ungeschützt in der Personalakte abgelegt werden. Wenn sensible Gesundheitsdaten in die Personalakte aufgenommen werden dürfen, hat der Arbeitnehmer Anspruch darauf, dass dies unter Berücksichtigung seiner Interessen geschieht. Der Arbeitgeber ist verpflichtet, sensible Gesundheitsdaten, soweit sie überhaupt in die Personalakte aufgenommen werden dürfen, in besonderer Weise zu schützen und aufzubewahren. Dies ergibt sich aus dem Recht des Betroffenen auf Schutz des allgemeinen Persönlichkeitsrechts. Die zur Personalakte genommenen Gesundheitsdaten müssen durch Einschränkung des Kreises der Informationsberechtigten vor unbefugter zufälliger Kenntnisnahme geschützt werden.

Sofern sich Gesundheitsdaten des Mitarbeiters in der Personalakte befinden, sind diese getrennt, zum Beispiel in einem verschlossenen Umschlag oder einer gesonderten Akte, zu führen.

Richtigkeit und Vollständigkeit der Personalakten

Die Personalakte hat ein möglichst objektives und richtiges Bild von der Person, deren Tätigkeit und Leistungen zu vermitteln. Die Angaben müssen begründet und sachlich richtig sein und es dürfen Unterlagen nicht willkürlich hinzugefügt oder entfernt werden. Da für Unternehmen der Privatwirtschaft keine gesetzliche Verpflichtung zur Führung einer Personalakte besteht, existieren auch keinerlei Vorschriften darüber, welche Unterlagen in einer Personalakte enthalten sein müssen. Abgesehen von den gesetzlichen **Nachweispflichten** liegt es deshalb im Ermessen des Arbeitgebers, welche Unterlagen er neben diesen Nachweisdokumenten in die Personalakte aufnimmt. Grundsatz ist, dass der Arbeitgeber alle Beschäftigten gleich behandeln muss. Bei der Frage, welche Unterlagen in die Personalakte aufgenommen werden und welche nicht, ist somit bei allen Beschäftigten nach einheitlichen Grundsätzen zu verfahren.

Unzulässig ist es, durch die Aufnahme oder eine gezielte Nichtaufnahme bestimmter Unterlagen einzelne Mitarbeiter zu benachteiligen oder Vorteile zu gewähren. Ebenso sind unrichtige Daten zu berichtigen bzw. zu entfernen. Bestreitet der Beschäftigte die Richtigkeit der Daten, besteht ein **Recht auf Gegendarstellung**. Die Gegendarstellung ist in die Personalakte aufzunehmen und mit den bestrittenen Unterlagen zu verbinden.

Das **Gebot der Vollständigkeit** verlangt auch, dass die Sachverhalte vollständig, zutreffend und nicht lückenhaft aktenkundig gemacht werden. Sachverhalte müssen deshalb chronologisch und umfassend dargestellt sein. Unzulässig wäre es einzelne Unterlagen nicht aufzunehmen, den Sachverhalt damit lückenhaft darzustellen oder einzelne Unterlagen zu einem späteren Zeitpunkt ohne Wissen des Betroffenen wieder zu entfernen.

Bezüglich des Inhalts von Personalakten sind alle Mitarbeiter nach einheitlichen Grundsätzen zu behandeln. Die in der Personalakte gesammelten Daten müssen objektiv, richtig und vollständig sein.

Zulässigkeit und Zweckbindung der Informationen

Umfang und Inhalt der Personalakte ergeben sich zunächst aus den arbeits-, sozial-, steuer- und handelsrechtlichen Anforderungen unter dem Gesichtspunkt der Nachweispflichten des Arbeitgebers. Darüber hinaus wird der Inhalt durch den Anspruch des Arbeitnehmers auf Wahrung seines Persönlichkeitsrechts begrenzt. In die Personalakte bzw. in die Sammlung der Personalaktendaten dürfen deshalb nur solche Daten und Unterlagen aufgenommen werden, die in zulässiger Weise, d.h. unter Beachtung der Vorschriften zu Datenschutz und Arbeitsrecht, gewonnen worden sind.

Anhaltspunkte hierzu liefern auch die zum Fragerecht des Arbeitgebers entwickelten Grundsätze und die sich aus dem Allgemeinen Gleichbehandlungsgesetz ergebenden Anforderungen. Ebenso sind **Mitwirkungspflichten und Beteiligungsrechte der Mitarbeitervertretungen** zu beachten, wenn für die Erhebung von Bewerber- oder Mitarbeiterdaten Bewerber- bzw. Personalfragebögen eingesetzt werden. Ebenso dürfen Personaldaten nur für Zwecke der Personalarbeit genutzt und verwendet werden.

Unter dem Gesichtspunkt der Zulässigkeit ist auch die Frage der **Aufbewahrung der Personalakten** und der **Entfernung von Vorgängen** aus der Personalakte zu beurteilen. Für die steuer- oder sozialversicherungsrechtlich relevanten Unterlagen gelten die hierzu bestimmten **Aufbewahrungsfristen**. Für die sonstigen Unterlagen sind keine Aufbewahrungsfristen geregelt.

Die **Dauer der Aufbewahrung** regelt sich deshalb bei elektronisch gespeicherten Daten nach den Vorschriften des Datenschutzgesetzes. Manuell geführte Daten unterliegen zwar den Vorschriften zur Zulässigkeit der Erhebung, aber nicht den Löschungsvorschriften des Datenschutzgesetzes.

Bezüglich der manuell geführten Unterlagen greift das Recht der Betroffenen auf informationelle Selbstbestimmung. Dies hat zur Konsequenz, dass Unterlagen zu entfernen sind, wenn die Zweckbestimmung, welche die Aufnahme in die Personalakte rechtfertigte, weggefallen ist. Dieser **Entfernungsanspruch** gilt insbesondere für Vorgänge mit für den Betroffenen belastenden Inhalten, z.B. für Abmahnungen. Hier richtet sich die Aufbewahrungsfrist nach der Schwere des Vorgangs und der künftigen Bedeutung der Abmahnung. Sie ist nach der Rechtsprechung des Bundesarbeitsgerichts zu entfernen, wenn sie für den Arbeitnehmer belastend, aber für die Zukunft belanglos ist.

Inhalte, die den Betroffenen belasten, müssen aus der Personalakte entfernt werden, sobald der Grund für die Aufnahme entfallen ist und diese für die Zukunft nicht mehr erforderlich sind (z.B. Abmahnungen).

Für die Zeit **nach dem Ausscheiden eines Beschäftigten** existiert für die Personalakte als Ganzes ebenfalls keine Aufbewahrungsvorschrift. In Verbindung mit dem Ausscheiden können nicht mehr erforderliche Unterlagen entfernt werden. Für Unterlagen, die steuer- oder sozialversicherungsrechtlich von Bedeutung sind, müssen natürlich die jeweiligen **Aufbewahrungsfristen** beachtet werden. Vorgänge, aus denen die Betroffenen auch nach Beendigung

des Beschäftigungsverhältnisses noch Rechte herleiten könnten, sollten ebenfalls bis zum Ablauf von etwaigen Verjährungsfristen aufbewahrt werden. Da Unterlagen, insbesondere über Inhalt und Verlauf des Beschäftigungsverhältnisses, auch lange nach Beendigung des Beschäftigungsverhältnisses noch nachgefragt werden können, sind diese im Interesse der Betroffenen noch für einen angemessenen Zeitraum aufzubewahren. Ein Zeitraum von zehn Jahren gilt i. d. R. als ausreichend, kann aber nach Bedarf länger gestaltet werden.

Transparenzgrundsatz

Beschäftigte besitzen ein **Recht auf Einsichtnahme** in die vollständige Personalakte. Dieses Einsichtsrecht ist ein Kernbestandteil der Schutzrechte im Beschäftigungsverhältnis. Damit der Beschäftigte sein Einsichtsrecht auch umfassend geltend machen und der Arbeitgeber dieses Recht auch gewähren kann, muss für beide Seiten Umfang und Inhalt der Personalaktendaten definiert sein. Dies kann insbesondere dann unübersichtlich sein, wenn die Personalaktendaten auf mehrere Teilakten und Datenbestände an verschiedenen Orten (z.B. Personalabteilung, Niederlassung und Firmenzentrale oder Vorgesetzte) verteilt geführt werden.

Es ist unzulässig, neben den als offizielle Personalakte definierten Unterlagen weitere Personalakten zu führen, die dem betroffenen Mitarbeiter nicht zugänglich sind.

Bei komplexen Personaldatenstrukturen mit Haupt-, Sonder- und Nebenakten ist in die Hauptpersonalakte ein Hinweis auf die Sonder- und Nebenakten aufzunehmen, um dem Beschäftigten die Möglichkeit zur Realisierung seines Einsichtsrechts zu geben. Der Arbeitnehmer kann allerdings nicht verlangen, dass der Arbeitgeber der Personalakte ein vom Arbeitnehmer gefertigtes Inhaltsverzeichnis beifügt. Als Selbstverständlichkeit ergibt sich daraus auch das Verbot der Führung von Geheimakten, die dem Arbeitnehmer nicht bekannt sind und ihm nicht zugänglich gemacht werden.

Bei komplexen Personalaktenstrukturen, die für den Betroffenen nicht erkennbar sind (z.B. bei mehreren Teil- oder Nebenakten, Verteilung auf verschiedene Standorte oder Vorgesetzte), sollte ein **Personalaktenverzeichnis** angelegt und dem Beschäftigten bei der Einsichtnahme zugänglich gemacht werden. Damit können sich die Beschäftigten bei einer Einsichtnahme einen Überblick über die gesamte Personalakte bilden.

Einsichtsrecht in die Personalakten

Personalakten sind vertraulich zu führen und durch technische und organisatorische Maßnahmen **vor unbefugter Einsichtnahme zu schützen**, d. h., eine **Einsichtnahme in die Personalakten** darf den verschiedenen Stellen im Unternehmen nur bei **begründeten Anlässen** und nur im **erforderlichen Umfang** gewährt werden.

… durch den Beschäftigten selbst

Eine **unbeschränkte Befugnis zur Einsichtnahme** in seine eigene Personalakte einschließlich aller eventuell vorhandenen Teil- und Nebenakten besitzen nur Mitarbeiter, d.h. Arbeiter, Angestellte und zur Berufsausbildung beschäftigte Personen. Ein Einsichtsrecht besteht nur in diejenigen Unterlagen, die Bestandteil der Personalaktendaten sind. Sachakten oder Vorgänge, die sich erst im Planungsstadium befinden, gehören nicht dazu.

Das Einsichtsrecht umfasst auch das Recht des Arbeitnehmers, sich während der Arbeitszeit **Notizen oder Kopien aus der Personalakte** zu fertigen.

Soweit die Personalakte **kodierte Informationen** enthält, müssen dem Beschäftigten geeignete Hilfsmittel zur Verfügung gestellt werden (z.B. Schlüsselverzeichnisse), um diese Informationen verstehen zu können.

Der Betroffene kann zur Wahrnehmung seines Einsichtsrechts ein **Mitglied des Betriebsrats** hinzuziehen. Mit der Hinzuziehung erteilt der Beschäftigte dem Mitglied des Betriebsrats die erforderliche Zustimmung. Dem Mitglied des Betriebsrats ist dann die Einsicht in demselben Umfang zu gewähren wie dem Beschäftigten selbst. Das hinzugezogene Betriebsratsmitglied hat über den Inhalt der Personalakte Stillschweigen zu bewahren. Diese Schweigepflicht gilt auch gegenüber den anderen Mitgliedern des Betriebsrats.

… durch den Betriebsrat

Der Betriebsrat ist nicht Dritter im Sinne des Datenschutzgesetzes, sondern Teil des Unternehmens (und somit Teil der verantwortlichen Stelle). In dieser Eigenschaft besitzt der Betriebsrat **kein uneingeschränktes Einsichtsrecht** in die Personalakten, sondern lediglich ein Informationsrecht. Dies umfasst ein Recht auf Auskunft und Vorlage von Unterlagen in dem Umfang, wie es zur Erfüllung seiner Aufgaben erforderlich ist. Er besitzt deshalb auch **keine uneingeschränkten Zugriffsrechte** auf Personalverwaltungssysteme und Personaldaten.

… durch den Vorgesetzen

Vorgesetzte benötigen zur Wahrnehmung ihrer Führungsaufgaben ebenfalls Informationen über ihre Mitarbeiter. Dies rechtfertigt aber nicht eine uneingeschränkte Einsichtnahme in die Personalakten dieser Mitarbeiter. Den Vorgesetzten dürfen deshalb nur die für die **jeweiligen Führungsaufgaben erforderlichen, definierten und aufgabenbezogenen Informationen und Unterlagen** zur Verfügung gestellt werden. Eine Einsichtnahme in die gesamte Personalakte erfordert dagegen die Einwilligung des betroffenen Mitarbeiters.

Die nachfolgende Übersicht zeigt eine Übersicht der Kategorien von Personaldaten, die Vorgesetzten zur Verfügung gestellt werden dürfen bzw. auch Vorgesetzten gegenüber vertraulich zu behandeln sind.

- ☺ Abwesenheitszeiten (krankheitsbedingt oder wegen Urlaub)
- ☺ Beruflicher Werdegang im Unternehmen
- ☺ Beurteilungen durch frühere Vorgesetzte
- ☺ Bruttogehalt (fixe und variable Komponenten)
- ☺ Familienstand
- ☺ Gesundheitliche Einschränkungen (sofern relevant für die ausgeübte Tätigkeit)
- ☺ Qualifikationen (Aus- und Fortbildungen)
- ☺ Wohnort

Nicht erlaubt sind:

- ☹ Einsichten in Informationen über das familiäre und soziale Umfeld.
- ☹ Lohnpfändungen (sofern nicht relevant für die ausgeübte Tätigkeit)
- ☹ Mitgliedschaft in Berufsorganisationen, Verbänden etc.
- ☹ Nettogehalt
- ☹ Sozialdaten (Krankenkasse etc.)
- ☹ Unterhaltspflichten

Elektronische Personalakte

Neben den allgemeinen Anforderungen an eine Personalakte bestehen aus der Sicht des Datenschutzes an eine elektronische Personalakte folgende besonderen Anforderungen, um die Vertraulichkeit und Integrität der Beschäftigtendaten sicherzustellen:

Zugriffsschutz

Da die Personalakten einem besonderen Vertraulichkeitsschutz unterliegen, müssen die Zugriffsberechtigungen differenziert regelbar sein. Folgende Zugriffsberechtigungen müssen regelbar sein:

- uneingeschränkter Zugriff auf Unterlagen, z.B. für den jeweiligen Beschäftigten im Rahmen seines Einsichts-/Auskunftsrechtes
- eingeschränkter Zugriff auf ausgewählte Unterlagen, z.B. für die Fachvorgesetzten
- u.U. Differenzierung der Zugriffsberechtigungen auf Teile der Personalakte, z.B. für Personalsachbearbeiter mit bestimmten Teilzuständigkeiten (Lohnabrechnung, disziplinar- oder arbeitsrechtliche Angelegenheiten etc., soweit im HR-Bereich eine derartige Arbeitsteilung besteht)
- Unterlagen über Krankheiten oder sonstige besonders sensible Unterlagen, die einem besonderen Schutz unterliegen, müssen zusätzlich geschützt werden können

Erforderlich ist unter diesen Gesichtspunkten die Möglichkeit einer differenzierten Rechtegestaltung für bestimmte Personengruppen auf bestimmte Dokumentengruppen und die Möglichkeit, darüber hinaus zusätzlich einzelne Dokumente besonders zu schützen.

Verknüpfung von Dokumenten

Das Personalaktenrecht ermöglicht dem Mitarbeiter zu einem bestimmten Vorgang eine eigene Stellungnahme hinzuzufügen, z.B. zu einer disziplinarischen Maßnahme. Bei in Papierform geführten Personalakten muss diese Stellungnahme in einer solchen Form mit dem auslösenden Dokument verbunden werden, dass beide Dokumente nur gleichzeitig zur Kenntnis genommen werden können. Dies erfordert, dass bei einer elektronischen Personalakte beispielsweise eine Abmahnung mit einer nachträglichen Stellungnahme des Mitarbeiters so verknüpft werden muss, dass die Abmahnung nicht für sich allein aufgerufen werden kann.

Löschung oder Sperrung von Dokumenten

Da die **Dokumente** einer Personalakte **unterschiedlich lang aufbewahrt** werden müssen, müssen die Dokumente differenziert löschbar sein. Die Löschungsbefugnis muss aber an bestimmte Voraussetzungen bzw. Berechtigungen gebunden sein, d.h. es muss regelbar sein, wer nur lesen und wer auch Dokumente löschen können soll. Die Löschungsbefugnis sollte möglichst eingeschränkt werden.

Im Personalbereich ist nicht auszuschließen, dass Unterlagen anfallen, deren Richtigkeit vom Betroffenen bestritten wird und zumindest für einen bestimmten Zeitraum die Richtigkeit oder Unrichtigkeit nicht zuverlässig festgestellt werden kann. In einem solchen Fall verlangt das Datenschutzrecht, dass diese Daten gesperrt werden können, d.h. die Daten sind zwar gespeichert, dürfen aber nicht genutzt werden. Derartige Dokumente müssen mit einem Sperrvermerk versehen bzw. entsprechend gekennzeichnet werden können.

Protokollierung von Zugriffen

Aufgrund der besonderen Vertraulichkeit von Personalunterlagen sollten die **Zugriffe auf die Unterlagen vom System protokolliert** werden. Das Datenschutzgesetz verlangt hierzu, dass nachträglich festgestellt werden kann, von wem welche Daten in das System eingeben, verändert oder entfernt worden sind. Die Dokumentation des Systems sollte deshalb ein Konzept enthalten, das die Protokollierungen nachprüfbar beschreibt.

Download und Kopien

Ebenfalls aufgrund der besonderen Vertraulichkeit der Personaldaten sollte die Möglichkeit, von den gespeicherten Dokumenten Kopien herzustellen, **eingeschränkt** werden. Ideal wäre eine solche Einschränkung sowohl bezüglich bestimmter Dokumente als auch hinsichtlich bestimmter Benutzer des Systems. Die Herstellung von Kopien ist zu **protokollieren**.

Bei der Übertragung der Daten an den Datenserver sollten die Daten **verschlüsselt** werden. Ebenso sollten die Daten verschlüsselt gespeichert werden.

Zugriffsmöglichkeiten durch Administratoren

Zu beachten ist auch, welche **Rechte die Administratoren des IT-Systems** haben, in dem die elektronischen Personalakten verwaltet werden. Es ist insbesondere **nicht** zulässig, dass die Administratoren die einzelnen Personalakten kraft ihrer umfassenden Berechtigung einsehen oder gar verändern können. Schutz bieten hier z.B. eine Verschlüsselung der Daten oder das Vieraugenprinzip bei der Gestaltung der Rechte der Administratoren.

Information der Beschäftigten

Die Mitarbeiter **müssen** über die Einrichtung einer elektronischen Personalakte **unterrichtet werden**. Ferner muss für die Mitarbeiter eine Zugangsmöglichkeit zur elektronischen Personalakte eingerichtet werden, um dem Einsichtsrecht der Mitarbeiter nachkommen zu können.

Mitbestimmungspflicht

Je nach Ausgestaltung der elektronischen Personalakte und der Nutzungsmöglichkeiten der Daten kann die Einrichtung einer elektronischen Personalakte **mitbestimmungspflichtig** sein. Deshalb muss der **Betriebsrat** rechtzeitig beteiligt werden.

Verzeichnis für Verarbeitungstätigkeiten, Risikobewertung und Datenschutz-Folgenabschätzung

Mit der Einführung einer elektronischen Personalakte ist das Verzeichnis für Verarbeitungstätigkeiten anzupassen bzw. zu erstellen. Je nach Ausgestaltung des Verfahrens kann das Persönlichkeitsrecht der Beschäftigten in unterschiedlicher Weise berührt sein und eingeschränkt werden. Daher ist der Datenschutzbeauftragte rechtzeitig zu beteiligen, um eine Schutzbedarfsfeststellung und eventuell eine Datenschutz-Folgenabschätzung durchzuführen.

Allgemeine Anforderungen an die Archivierung

Zu dem Archivierungssystem muss eine **vollständige** und **aktuelle** Dokumentation vorhanden sein, die es erlaubt, jederzeit die Ordnungsmäßigkeit des Systems festzustellen. Insbesondere muss die gesamte Archivierung als Prozess so gestaltet sein, dass eine vollständige und nachvollziehbare Erfassung und unveränderbare Speicherung der Dokumente und eine inhaltliche bzw. bildliche Übereinstimmung mit dem Original gewährleistet ist. Diese allgemeinen Anforderungen ergeben sich aus steuer- und handelsrechtlichen Vorschriften und aus den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS).

Von der Ordnungsmäßigkeit dieses Prozesses hängt der Beweiswert gescannter Dokumente, d.h. insbesondere die Beweiskraft elektronischer Dokumente in einem gerichtlichen Verfahren ab. Jedes elektronische Dokument, das bei Gericht als Beweis vorgelegt wird, unterliegt der freien Beweiswürdigung des Gerichtes, d.h. der Richter entscheidet über dessen Beweisqualität. Die Beachtung dieser allgemeinen Anforderungen und deren Belegbarkeit durch eine nachvollziehbare Dokumentation sind deshalb eine notwendige Voraussetzung für die Beweiskraft der archivierten Dokumente.

Erhebung, Verarbeitung und Nutzung von Mitarbeiterdaten

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Beschäftigungsverhältnis sind zulässig, soweit dies für die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Für das Fragerecht im Beschäftigungsverhältnis gelten die gleichen Grundsätze wie im Bewerbungsverfahren.

Ein großer Teil der im Bewerbungsverfahren erhobenen Daten wird auch für die Durchführung des Beschäftigungsverhältnisses erforderlich sein. Andere im Bewerbungsverfahren erhobene Daten oder Dokumente sind nicht mehr von Bedeutung und müssen nach dem Grundsatz der Datenminimierung gelöscht werden. Darüber hinaus hat der Betroffene auch einen Anspruch auf Löschung dieser Daten. Unter diesen Gesichtspunkten wird z. B. eine weitere Aufbewahrung von Motivationsschreiben oder Ergebnissen von Einstellungstests oder Psychotests nicht mehr zu begründen sein.

Jeder Arbeitnehmer besitzt am Arbeitsplatz einen Anspruch auf Schutz seines Persönlichkeitsrechts. Dem stehen mit dem Recht auf Freiheit der Berufsausübung und mit dem Recht am Eigentum auch Grundrechte des Arbeitgebers gegenüber. Auf der Grundlage dieser Grundrechte besteht für den Arbeitgeber ein Organisations- und Direktionsrecht und als Konsequenz daraus ein berechtigtes Informationsbedürfnis über die Angelegenheiten seines Unternehmens. Daneben hat der Arbeitgeber Schutzpflichten (z.B. nach den Vorschriften des Jugendschutzgesetzes) wahrzunehmen, die ebenfalls eine Erhebung von personenbezogenen Daten erfordern können. Die zur Wahrung der berechtigten Arbeitgeberinteressen erforderliche Erhebung, Speicherung, Verarbeitung und Nutzung von Arbeitnehmerdaten einerseits und das Schutzbedürfnis des Arbeitnehmers sind gegeneinander auszugleichen. Seine Ausgestaltung findet dieses Rechtgebiet in kollektiven und in individualrechtlichen arbeitsrechtlichen Regelungen.

Die kollektivrechtlichen Regelungen ergeben sich für den privatwirtschaftlichen Bereich aus dem Betriebsverfassungsgesetz (BetrVG), hier insbesondere aus dem Recht zur Mitwirkung und Mitbestimmung der Arbeitnehmer. Zu nennen ist hier insbesondere die Grundsätze für die Behandlung der Betriebsangehörigen, der eine Behandlung der Betriebsangehörigen nach Recht und Billigkeit und insbesondere Gleichbehandlung vorschreibt. Arbeitgeber und Betriebsrat werden verpflichtet, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Aus datenschutzrechtlicher Sicht von Bedeutung sind auch die Vorschriften über die Mitbestimmung, weil deren Beachtung Voraussetzung für die datenschutzrechtliche Zulässigkeit der Erhebung, Speicherung, Verarbeitung und Nutzung der mit den mitbestimmungspflichtigen Verfahren zusammenhängenden personenbezogenen Daten ist.

Trotz der großen Bedeutung des Arbeitsrechts ist dieses Rechtsgebiet nicht in ein Gesetz gekleidet, sondern besteht aus Regelungen innerhalb einer Vielzahl von Gesetzen (z.B. BGB, Betriebsverfassungsgesetz, Allgemeines Gleichbehandlungsgesetz (AGG) oder Tarifverträge). Eine wichtige Ausgestaltung hat das Arbeitsrecht durch die Rechtsprechung gefunden, denn große Teile des geltenden Arbeitsrechts wurden durch Gerichte (insbesondere Arbeitsgerichte) entwickelt.

In einer Vielzahl unterschiedlicher Zusammenhänge werden vom Arbeitgeber über die Mitarbeiter personenbezogene Daten erhoben. Häufig sind diese Datenerhebungen für den Mitarbeiter nicht zu erkennen, z.B. im Zusammenhang mit Protokollierungen beim Betrieb von IT-Systemen. Hier sind, wenn die private Nutzung der Kommunikationseinrichtungen erlaubt ist, die Vorschriften des Telekommunikationsgesetzes (TKG) zum Telekommunikationsgeheimnis zu beachten.

Werden Mitarbeiterdaten in standardisierter, formularmäßiger und strukturierter Form erhoben, z.B. in Form von Personalfragebögen, ist die Mitbestimmungspflicht des Betriebsrates zu beachten. Die Nichtbeachtung der Mitbestimmungspflicht führt jedoch nach Auffassung des Bundesarbeitsgerichts nicht zu dem Recht des Arbeitnehmers, eine bestimmte Frage falsch

zu beantworten. Andererseits müssen Mitarbeiterdaten, die auf diesem Weg ohne Mitbestimmung erhoben worden sind, wegen der fehlenden Rechtsgrundlage der Speicherung auf Verlangen gelöscht werden. Gleiches gilt auch bei Mitarbeiterbefragungen im Rahmen von Ethikrichtlinien und damit verbundenen Selbstauskünften.

Personenbezogene Daten dürfen aber nur erhoben, gespeichert, verarbeitet und genutzt werden, soweit es für die Erreichung eines berechtigten Zwecks erforderlich ist. Die Gestaltung und die Auswahl von Datenverarbeitungssystemen haben sich dabei an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich (und nur so viel wie nötig) zu verarbeiten. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies machbar ist und der Aufwand in einem angemessenen Verhältnis zum Schutzzweck der Daten steht. ***Beispiele*** hierfür sind Zeiterfassungs- und Zutrittskontrollsysteme, Personalinformations- und Personalmanagementsysteme, Videoüberwachung und Protokollierungen im Zusammenhang mit dem Betrieb der IT sowie IT-gestützte Kommunikationssysteme wie E-Mail und Internet.

Zu beachten ist bei diesen Datenverarbeitungsverfahren, dass ihr Einsatz i.d.R. mitbestimmungspflichtig ist. Die in diesen Zusammenhängen erhobenen personenbezogenen Daten sind zumindest geeignet, eine unzulässige Leistungs- und Verhaltenskontrolle vorzunehmen. Wird die Mitbestimmungspflicht nicht beachtet, ist die Datenerhebung, Speicherung und Nutzung i.d.R. rechtswidrig. Dies hat zur Folge, dass die Daten nicht verarbeitet werden dürfen und die Betroffenen im Rahmen ihres Berichtigungs- und Löschungsrechts die Löschung der Daten verlangen können.

WICHTIG | Mitbestimmungspflichtig sind standardisierte Personalfragebogen sowie Datenverarbeitungsverfahren, die eine unzulässige **Leistungs- und Verhaltenskontrolle** ermöglichen können.

Personalstammdaten, Personalinformationssystem

Ob die für die Ausführung eines Beschäftigungsverhältnisses erforderlichen Personalstamm- und sonstige Personaldaten wie Vertrags-, Lohn-, Abrechnungs-, Sozialdaten etc. erhoben und gespeichert werden dürfen, bedarf grundsätzlich keiner Diskussion. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts darf aber dabei in die Privatsphäre des Arbeitnehmers nicht tiefer eingegriffen werden, als es der Zweck des Beschäftigungsverhältnisses erfordert.

Im Rahmen der **Zweckbestimmung** des Beschäftigungsverhältnisses ist für Umfang und Ausmaß der Datenspeicherung eine Interessenabwägung nach dem Grundsatz der Verhältnismäßigkeit vorzunehmen. Zulässig sind die Erhebung und Speicherung der Personaldaten im Rahmen der Erforderlichkeit. Abzugrenzen ist hier auch zwischen Daten, die im Bewerbungsverfahren erhoben worden sind, und solchen, die erst im laufenden Arbeitsverhältnis erforderlich sind bzw. im Laufe eines Arbeitsverhältnisses erst entstehen, denn nicht alle Daten, die im Bewerbungsverhältnis erhoben worden sind, sind auch im späteren Beschäftigungsverhältnis noch erforderlich.

Der Rahmen des Erforderlichen dürfen nur diejenigen Daten erhoben und gespeichert werden, die in der augenblicklichen Situation bzw. für den konkret anstehenden Zweck unverzichtbar sind. Es dürfen vielmehr auch solche Daten gespeichert werden, deren Kenntnis erst im Verlaufe eines Beschäftigungsverhältnisses erforderlich werden können. So ist z.B. die Speicherung des Geschlechts gerechtfertigt, denn die Arbeitgeber haben unter anderem die Pflicht, in bestimmten Abständen die Zahl der Arbeitnehmer nach Geschlecht zu melden.

Daten zum Familienstand können für Sozialleistungen, die soziale Auswahl bei Kündigungen und für Entscheidungen über Versetzungen und auswärtigen Arbeitseinsatz wichtig werden. Wenngleich es zutrifft, dass Kündigungen nicht zu jedem Zeitpunkt bevorstehen, so kann nicht von einer unzulässigen Vorratsspeicherung gesprochen werden.

In einem vernünftigen Umfang dürfen auch Mitarbeiterdaten gespeichert werden, die erst zu einem späteren Zeitpunkt benötigt werden. Auch diese Daten dürfen für einen schnellen Zugriff in automatisierten Verfahren oder Personalinformationssystemen gespeichert werden.

Unter den gleichen Gesichtspunkten dürfen z.B. Daten über Zusatzqualifikationen wie Ausbildungen in anderen Berufen, Sprachkenntnisse oder sonstige Spezialkenntnisse oder Fähigkeiten gespeichert werden, soweit sie bei späteren Personalplanungs- oder Einsatzentscheidungen eine Rolle spielen können.

Zu beachten ist, dass die erhobenen Mitarbeiterdaten nur für die Zwecke, für die sie erhoben worden sind, d.h. für Zwecke des Arbeitsverhältnisses verarbeitet und genutzt werden dürfen. Insbesondere ist es im Hinblick auf das Recht der Beschäftigten auf **informationelle Selbstbestimmung** nicht zulässig, durch Zusammenführung von Daten Persönlichkeitsprofile zu bilden.

Veröffentlichung von Beschäftigtendaten innerhalb des Unternehmens

Innerhalb eines Unternehmens ist eine Veröffentlichung bzw. Offenbarung personenbezogener Daten zu den Beschäftigten an diejenigen Stellen **zulässig**, für welche die Kenntnis der Daten **zur Aufgabenerfüllung wie z.B. Mitarbeiterplanung, Lohn- und Gehaltsbuchhaltung erforderlich** ist. Diesen Stellen dürfen aber Daten auch nur in dem Umfang offenbart werden, wie dies zur **Erfüllung ihrer Aufgaben** notwendig ist.

Jede Übermittlung an Stellen, deren Aufgabenerfüllung die Kenntnis der personenbezogenen Daten nicht erfordert, ist ebenso unzulässig, wie eine Offenbarung an eine an sich befugte Stelle über den zur Aufgabenerfüllung hinausgehenden Rahmen. Auch **Fachvorgesetzte** gehören zu den befugten Empfängern personenbezogener Daten über Mitarbeiter ihres Fachbereichs; aber nur bezüglich derjenigen Daten, deren Kenntnis erforderlich ist, um die jeweiligen Führungsaufgaben erfüllen zu können.

Personenbezogene Daten sind auch innerhalb des Unternehmens vertraulich zu behandeln. Sie dürfen nur in dem Maße offenbart werden, wie es für die Aufgabenerfüllung anderer Stellen (Betriebsrat, Vorgesetzte o.a.) notwendig ist.

Personalakten unterliegen einem besonderen Schutz und sind besonders vertraulich zu behandeln. Auf die Personalakten dürfen deshalb nur diejenigen Personen Zugriff besitzen, die mit Aufgaben der Personalsachbearbeitung betraut sind. Soweit innerhalb einer Personalabteilung unterschiedliche Zuständigkeitsbereiche bestehen (z.B. Disziplinarzuständigkeit, Lohn- und Gehaltsabrechnung u.a.), empfiehlt es sich, die Personalakte nach diesen Zuständigkeiten zu gliedern. Besonders sensible Unterlagen, z.B. über gesundheitliche Verhältnisse, sind in verschlossenen Umschlägen aufzubewahren.

Ebenso sind den Mitarbeitern alle **Ergebnisse der Personalsachbearbeitung**, insbesondere sensible Vorgänge wie Abmahnungen, nur in verschlossenen Umschlägen zuzustellen.

Eine besondere Form der Offenbarung innerhalb eines Unternehmens stellt die Veröffentlichung von Daten im Unternehmen dar, sei es unternehmensweit oder im Rahmen von Fachbereichen. Unter dem Gesichtspunkt des berechtigten Interesses sollten die innerbetrieblichen Veröffentlichungen auf den erforderlichen Umfang beschränkt werden, wobei das schutzwürdige Interesse der Mitarbeiter berücksichtigt werden muss.

Telefonverzeichnis

Eine Selbstverständlichkeit und datenschutzrechtlich unproblematisch ist die Veröffentlichung von Telefonverzeichnissen im Unternehmen, ggf. mit der betrieblichen E-Mail-Adresse und mit zusätzlichen Angaben über Aufgabengebiete und Zuständigkeiten, weil derartige Verzeichnisse für die innerbetriebliche Kommunikation erforderlich sind. Die Frage nach der Notwendigkeit stellt sich aber dann, wenn z.B. innerhalb eines Konzerns ein Telefonverzeichnis über die gesamte Belegschaft erstellt oder diese Informationen über alle Mitarbeiter über das Intranet zur Verfügung gestellt werden sollen, ohne dass auch eine entsprechende konzernweite Kommunikation stattfindet. Eine Einwilligung der Betroffenen ist zumindest dann erforderlich, wenn in das Verzeichnis private Verbindungsdaten aufgenommen werden sollen, selbst wenn sich dafür eine betriebliche Notwendigkeit ergibt.

Angaben in Telefon- und E-Mail-Verzeichnissen sind zunächst unproblematisch, sofern diese für die interne Kommunikation erforderlich sind. Die Weitergabe an Dritte sollte allerdings anlassbezogen geprüft werden, denn hier gibt es Risiken im Rahmen eines Missbrauchs der Daten. Insbesondere sei hier das Social Engineering erwähnt, also das Hacking des einzelnen Beschäftigten durch Nutzung interner Informationen = Manipulation.

Schwarzes Brett, Firmenzeitung

Zu den innerbetrieblichen Veröffentlichungen gehören auch Aushänge am schwarzen Brett, z.B. über Jubiläen von Mitarbeitern, Veröffentlichungen in Firmenzeitungen und sonstige Bekanntmachungen, z.B. über Verbesserungsvorschläge, Ausbildungsabschlüsse usw. Bei diesen unternehmensinternen Veröffentlichungen handelt es sich um eine Nutzung von personenbezogenen Daten über Mitarbeiter. Von der Zweckbestimmung des Arbeitsvertrages oder Anstellungsvertrages sind diese Veröffentlichungen nicht abgedeckt, weil sie zur Ausfüllung des Vertrages bzw. zur Wahrnehmung der Rechte und Pflichten aus dem Arbeits- bzw. Anstellungsvertrag nicht erforderlich sind. Die Zulässigkeit der Veröffentlichungen ist damit unter dem Gesichtspunkt des berechtigten Interesses des Unternehmens zu beurteilen, wobei gegen das schutzwürdige Interesse der Mitarbeiter abzuwägen ist. Die Art der Veröffentlichung, Schwarzes Brett oder in Listen, die an bestimmten Stellen eingesehen werden können, ist dabei unerheblich.

An einer **Veröffentlichung von Geburtsdaten, Jubiläen, Beförderungen** u.a. (soweit damit keine Änderung von Zuständigkeiten oder Befugnissen verbunden ist) ist kein berechtigtes Interesse des Arbeitgebers zu erkennen; ein Interesse der Mitarbeiter an einer vertraulichen Behandlung dieser Informationen ist nachvollziehbar. Je nach dem Umfang der Veröffentlichung (unternehmensweit bzw. für alle Mitarbeiter zugänglich oder nur innerhalb einer Abteilung oder Arbeitsgruppe) ist die **Einwilligung oder zumindest die Information des Mitarbeiters** erforderlich, damit ihm Gelegenheit zum Widerspruch gegeben wird. Von neu einzustellenden Beschäftigten sollte eine Einwilligung eingeholt werden. Gleiches gilt auch für Veröffentlichungen in der Firmenzeitung, z.B. für Gratulationen oder sonstige persönliche Mitteilungen. Bei erfolgreichen Ausbildungsabschlüssen sind innerbetriebliche Veröffentlichungen zulässig, jedoch ohne Prüfungsergebnis und Rangfolge. Unzulässig ist dagegen eine Veröffentlichung, wenn das Ausbildungsziel nicht erreicht wurde und eventuell eine Wiederholungsprüfung abgelegt werden soll. Hier besteht ein schutzwürdiges Interesse des Betroffenen daran, dass das Nichtbestehen einer Abschlussprüfung nicht im ganzen Unternehmen bekannt wird.

Vor der Offenbarung persönlicher Daten (beispielsweise am „Schwarzen Brett“ oder in einer Betriebszeitung) ist zu prüfen, ob eine die Einwilligung des Beschäftigten einzuholen ist.

Rennlisten (auch „Leistungsvergleiche“)

Um die Mitarbeiter zu motivieren, werden über erzielte Umsätze oder sonstige erfolgsrelevante Kriterien häufig sog. Rennlisten erstellt und bekannt gegeben. Diese Praxis ist grundsätzlich zulässig, jedoch kommt es auf die Ausgestaltung an. Unproblematisch, weil nicht mehr personenbezogen, ist eine Veröffentlichung einer anonymen Liste, in der die von den einzelnen Mitarbeitern (z.B. Außendienstmitarbeiter) erzielten Ergebnisse skaliert sind. Diese Liste reicht aus, damit sich der Einzelne einordnen und mit den von den Kolleginnen und Kollegen erreichten Ergebnissen vergleichen kann. Eine Zuordnung der Einzelergebnisse zu den Personen ist für diesen Zweck nicht erforderlich.

Problematisch ist es, die Namen der Mitarbeiter mit zu veröffentlichen. Häufig soll z.B. der Verkäufer des Monats oder des Jahres ausgezeichnet werden, um dadurch auch die anderen Mitarbeiter zu motivieren. Auch wenn für derartige Verfahren ein berechtigtes Interesse von Seiten des Arbeitgebers durchaus anerkannt werden kann, muss hier das schutzwürdige Interesse des einzelnen Mitarbeiters an einer personenbezogenen Bestenliste höher bewertet werden. Nicht jeder erfolgreiche Mitarbeiter will seine Arbeitsergebnisse im ganzen Unternehmen kommuniziert wissen und noch mehr hat der weniger erfolgreiche Mitarbeiter ein schutzwürdiges Interesse daran, dass seine Ergebnisse nicht allgemein bekannt werden. Zum einen werden nähere Umstände, die zu einem schlechten Ergebnis geführt haben und die der einzelne Mitarbeiter u.U. gar nicht zu vertreten hat, nicht dargestellt. Zum anderen ist die Befürchtung nicht unbegründet, bei schlechten Ergebnissen im Unternehmen diskriminiert zu werden. Unter diesen Gesichtspunkten sind personenbezogene Ergebnislisten nur mit einer freiwilligen Einwilligung der Betroffenen zulässig.

Datenschutzrechtlich unproblematisch sind Leistungsvergleiche in anonymisierter Form. Auch diese ermöglichen den Mitarbeitern eine Einschätzung ihrer individuellen Leistungen.

Freiwillige Einwilligungen können insbesondere in arbeitsrechtlichen Angelegenheiten wegen der sozialen Abhängigkeit der Arbeitnehmer problematisch sein. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Zur Freiwilligkeit in diesem Sinne gehört, dass der Betroffene eine echte Wahlmöglichkeit hat und seine Einwilligung auch verweigern kann, ohne Nachteile befürchten zu müssen. Wenn sich der Mitarbeiter einem gewissen Druck oder einer Erwartungshaltung von Seiten des Arbeitgebers ausgesetzt fühlt, ist er in seiner freien Entscheidung eingeschränkt. Einwilligungen, die unter derartigen Verhältnissen abgegeben werden, entbehren der echten Freiwilligkeit und sind deshalb nicht wirksam abgegeben.

Intranet

Werden personenbezogene Daten ins Intranet eingestellt, gelten grundsätzlich die gleichen Anforderungen wie bei vergleichbaren herkömmlichen Verfahren. Dies gilt aber nur, soweit das Intranet lediglich für Firmenangehörige zugänglich ist. So dürfen z.B. Telefonverzeichnisse, Organisationspläne u.a. ins Intranet eingestellt und denjenigen Personen zugänglich gemacht werden, die auch bei manuellen Verfahren Zugang zu diesen Unterlagen hätten. Auch Angaben über An-/Abwesenheit von Beschäftigten, z.B. zur Planung von Besprechungen, sind unbedenklich. Die Angabe weiterer Informationen wie Fehlzeitengründe, insbesondere Urlaub, Krankheit, Kur etc. ist aber dazu nicht erforderlich und deshalb unzulässig. Sollen von Mitarbeitern Fotos ins Intranet eingestellt werden, ist wegen des Rechts am eigenen Bild die freiwillige Einwilligung des Betroffenen erforderlich. Nicht erforderlich ist eine Einwilligung, wenn der Mitarbeiter die Veröffentlichung fotografischer Aufnahmen als Bestandteil der Arbeitspflicht akzeptiert hat. Werden personenbezogene Daten im Intranet vorgehalten, die in manuellen Verfahren nicht allgemein zugänglich sind, müssen auch im Intranet entsprechende Zugriffsbeschränkungen vorgesehen werden. Der Datenschutz darf durch die Nutzung des Intranets nicht verschlechtert werden.

Foto- und Filmaufnahmen von Mitarbeitern

Bei einer Nutzung oder Veröffentlichung von Bild- oder Filmaufnahmen greift als vorrangige Rechtsvorschrift für die Befugnis zur Nutzung oder Veröffentlichung der Aufnahmen die Regelung des Kunsturhebergesetzes:

> *„Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten."*

Diese Regelung gilt sowohl für Veröffentlichungen in Presse und Zeitschriften als auch für Filmaufnahmen, Werbefilme (z.B. für Firmen- und Produktpräsentationen), Firmenprospekte oder im Internet und Intranet sowie auf der Internetseite des Arbeitgebers.

Die Einwilligung sollte zu Beweiszwecken schriftlich eingeholt werden. In der Einwilligung sollten auch Art, Verwendungszweck, Dauer der Nutzung und das Trägermedium (Printerzeugnisse, Firmen- oder Werbeprospekt, Internetauftritt etc.) näher bezeichnet werden.

Auch für Bildveröffentlichungen auf der Internetseite, z.B. Kontaktdaten eines Ansprechpartners mit Foto, ist eine Einwilligung erforderlich. Gleiches gilt für eine Veröffentlichung im Intranet. Bei einer Vorstellung neuer Mitarbeiter im Intranet bietet es sich z.B. an, diese vom neuen Mitarbeiter selbst anfertigen zu lassen. Der Mitarbeiter kann dann selbst entscheiden, welche Informationen er mit oder ohne Foto einstellen will. Für Unterlagen, die über längere Zeit genutzt werden sollen, z.B. Firmenprospekte, empfiehlt es sich eventuell auch, in die Einwilligung eine Regelung für den Fall aufzunehmen, dass der Mitarbeiter das Unternehmen während der Dauer der Nutzung der Bildaufnahmen das Unternehmen wieder verlässt.

Ohne Einwilligung ist eine Nutzung nur zulässig, wenn diese Nutzung zur Erfüllung der Arbeitspflicht erforderlich ist, z.B. bei einem Fotomodell, oder wenn ein überwiegendes berechtigtes Interesse des Unternehmens besteht, z.B. für eine Abbildung des Beschäftigten in einem Werksausweis, weil hier ein besonderes Sicherheitsinteresse des Unternehmens an der jederzeitigen Identifizierbarkeit der Person besteht. Für alle weiteren Nutzungen, z.B. in Broschüren und Printmedien des Arbeitgebers oder im Intranet/Internet oder auch auf Visitenkarten, wird eine Einwilligung verlangt.

Auch bei nachträglichen Nutzungserweiterungen, z.B. für eine zusätzliche Abbildung des Beschäftigten auf einer Visitenkarte, ist eine neue bzw. erweiterte Einwilligung erforderlich. Dies ergibt sich aus dem Wesensgehalt der informierten Einwilligung. Zu diesem Wesensgehalt gehört, dass den Betroffenen der komplette Umfang der beabsichtigten Nutzungen offengelegt wird. Der Betroffene soll bei der Einwilligung den Umfang der Nutzungen eindeutig erkennen und beurteilen können. Dem Betroffenen ist bei der Abgabe der Einwilligung konkret darzulegen, für welche Zwecke sein Foto im Einzelnen genutzt werden soll. Auf diese dargelegten Zwecke bezieht sich die Einwilligung und an diese Zwecke ist der Arbeitgeber auch gebunden. Zweckerweiterungen sind grundsätzlich erneut einwilligungspflichtig. Unter diesem Gesichtspunkt verbieten sich nachträgliche Nutzungserweiterungen ohne erneute Einwilligung der Betroffenen. Auch die Regelungen im Kunsturheberrechtsgesetz und deren Strafbestimmung eröffnen hier keinen Spielraum für eine einwilligungsfreie Nutzungserweiterung.

Für die Nutzung von Foto- und Filmaufnahmen von Mitarbeitern ist grundsätzlich deren (schriftliche) Einwilligung notwendig.

Der Widerruf der Einwilligung ist zwar auch hier im Prinzipiell möglich, allerdings unterliegt er gewissen Einschränkungen. So besteht eine vertragliche Bindung, wenn die Veröffentlichung oder Nutzung der Bildaufnahmen Gegenstand des Vertrages mit dem Betroffenen ist, z.B. die Vorführung oder Präsentation von Produkten des Unternehmens, insbesondere gegen ein Honorar. Ansonsten greift hier der Grundsatz von Treu und Glauben, d.h. die Rücknahme der Einwilligung darf nicht willkürlich erfolgen, sondern hat sich an der Verkehrssitte zu orientieren. Eine Rücknahme ist z.B. dann zulässig, wenn wesentliche Grundlagen, auf die sich die Einwilligung gestützt hat, entfallen oder sich verändern.

Veröffentlichung von Personaldaten im Internet

Veröffentlichungen im Internet sind Datenübermittlungen an Dritte, wegen der grenzüberschreitenden Zugriffsmöglichkeiten sogar Übermittlungen in das Ausland. Hinzu kommt, dass Veröffentlichungen im Internet häufig lange zur Verfügung stehen und mit Suchmaschinen gezielt ausgewertet werden können. Diese Besonderheiten des Internets müssen bei der Beurteilung des schutzwürdigen Interesses der Betroffenen mit berücksichtigt werden.

Die Befugnis zur Veröffentlichung von personenbezogenen Daten in herkömmlichen Printmedien berechtigt unter diesen Gesichtspunkten nicht gleichzeitig auch zu einer Veröffentlichung im Internet, weil in Printmedien die Daten nur einem abgegrenzten Personenkreis, im Internet dagegen weltweit frei zur Verfügung stehen und auch automatisiert auswertbar sind. Eine Veröffentlichung im Internet setzt deshalb in aller Regel eine **Einwilligung der Betroffenen** voraus. Einer Einwilligung bedarf es nicht, wenn eine gesetzliche Veröffentlichungspflicht besteht, z.B. im Rahmen der allgemeinen Informationspflichten gemäß Telemediengesetz (Impressumpflicht).

Ausnahme: Auf eine Einwilligung kann auch bei Personen verzichtet werden, deren Aufgabe im Unternehmen es erfordert, für einen unbestimmten Kreis von außen ansprechbar zu sein, z.B. Außendienstmitarbeiter, Reklamationsbearbeiter oder Kundenberater. Allerdings dürfen nur die für eine Kontaktaufnahme erforderlichen Daten wie Name, Firmenanschrift, Telefonnummer und E-Mailadresse angegeben werden. Die Veröffentlichung von Fotos der betroffenen Mitarbeiter ist damit nicht abgedeckt. Für diese Veröffentlichung ist schon aufgrund des Rechts am eigenen Bild immer eine Einwilligung erforderlich. Auch wenn für diesen Personenkreis grundsätzlich von einer Befugnis zur Veröffentlichung der Kontaktdaten ausgegangen werden kann, ist die Verpflichtung zur Information des Betroffenen gemäß zu beachten.

Wegen der weltweiten Zugriffsmöglichkeit auf die im Internet veröffentlichten Daten, auch aus sog. Drittländern mit u.U. niedrigerem Datenschutzniveau, ist für die Betroffenen aufgrund der damit verbundenen erhöhten Gefährdung des Persönlichkeitsrechts ein Widerspruchsrecht anzuerkennen. Nach dieser Vorschrift ist eine Veröffentlichung im Internet dann unzulässig, wenn der Betroffene widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen Situation das Interesse des Arbeitgebers an dieser Veröffentlichung überwiegt. Die besondere Schutzwürdigkeit bzw. Betroffenheit muss der Betroffene darlegen.

Ist der Mitarbeiter mit der Nennung seines Namens nicht einverstanden, kann die Kontaktadresse z.B. folgendermaßen gestaltet werden: „Anfragen richten Sie bitte an unsere Telefonnummer … oder E-Mailadresse …“ Die E-Mailadresse muss in diesen Fällen namensneutral formuliert werden.

Rufbereitschaft und private Kontaktdaten

Private Telefon- und Mobiltelefonnummern sind dem Privatbereich zuzurechnen und dürfen vom Arbeitgeber grundsätzlich **nicht** erfragt werden.

Ausnahme: Soweit aber Beschäftigte aufgrund ihrer betrieblichen Aufgaben einer Rufbereitschaft unterliegen oder z.B. im Zusammenhang mit einem Katastrophen- oder Notfall-

Managementsystem in bestimmten Fällen erreichbar sein müssen, dürfen die privaten Kontaktdaten erhoben und gespeichert werden. Die Kontaktdaten dürfen aber dann auch nur für die erhobenen Zwecke, z.B. im Rahmen der Rufbereitschaft, genutzt werden.

Weitere persönliche Daten über Mitarbeiter

Telefon, E-Mail und Internetnutzung

Wenn die Nutzung der betrieblichen Kommunikationssysteme für private Zwecke erlaubt ist oder stillschweigend geduldet wird, wird der Arbeitgeber zum Diensteanbieter im Sinne des Telekommunikationsgesetzes. Dies hat zur Folge, dass die private Kommunikation unter den Schutz des Fernmeldegeheimnisses fällt und die für die Bereitstellung und den Betrieb des Dienstes eingerichteten Datenverarbeitungssysteme so zu gestalten sind, dass sie bezüglich Speicherung, Verarbeitung und Löschung der Daten die gesetzlichen Pflichten nach den Vorschriften des Telekommunikationsgesetzes (TKG) erfüllen können.

Ist die Nutzung der betrieblichen Kommunikationssysteme für private Zwecke erlaubt oder stillschweigend geduldet, so wird dadurch der Arbeitgeber zum Diensteanbieter (Provider) im Sinne des TMG (Telemediengesetz), TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz) TKG (Telekommunikationsgesetz) und die Mitarbeiter zu seinen Kunden.

Gemäß den gesetzlichen Grundlagen unterliegen der Inhalt der Kommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, dem Fernmeldegeheimnis. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Dies bedeutet, dass der Arbeitgeber sowohl bezüglich des Inhalts der privaten Kommunikationsvorgänge als auch der Verkehrsdaten, d.h. bezüglich der im Zusammenhang mit dem Kommunikationsvorgang entstehenden Protokolldaten in den IT-Systemen, das Fernmeldegeheimnis zu beachten hat. Eine Verletzung des Fernmeldegeheimnisses ist strafbar.

Ein Mithören von Telefongesprächen, das Aufzeichnen der Gespräche (abgesehen von besonderen Fällen mit Einwilligung der Betroffenen) oder eine Einsichtnahme in die Inhalte der E-Mail- oder Internetkommunikation ist unzulässig.

E-Mails unterliegen dem Schutz des Telekommunikationsgeheimnisses nur für die Dauer der Übertragung. Im Einzelfall ist genau zu prüfen, wann der Übermittlungsvorgang abgeschlossen ist. Dies ist spätestens dann der Fall, wenn die E-Mail im Postfach des Empfängers angekommen und der Übertragungsvorgang beendet ist. Das Fernmeldegeheimnis gilt nach Abschluss des Übertragungsvorgangs nicht mehr. Es schützt die Daten nur während des Kommunikationsvorgangs (während der Übermittlung), aber nicht mehr nach dessen Abschluss.

Nach Abschluss des Übertragungsvorgangs unterliegen die privaten E-Mails zwar nicht mehr dem starken Schutz des Telekommunikationsgeheimnisses, sondern dem Schutz des informationellen Selbstbestimmungsrechts als Ausfluss des Persönlichkeitsschutzes auf der Grundlage des Datenschutzgesetzes. Damit ist dem Arbeitgeber zwar grundsätzlich auch ein Zugriff auf die Inhalte versagt, es entfällt aber die Strafbarkeit eines unbefugten Zugriffes.

Nach einem Verbot der Nutzung der Kommunikationssysteme für private Zwecke greift zwar nicht mehr der Schutz des Telekommunikationsgeheimnisses, aber die Daten unterliegen dem allgemeinen Schutz des Datenschutzgesetzes. In diesem Rahmen sind eine Erhebung, Speicherung und Auswertung der Verkehrsdaten zulässig, soweit dies im Rahmen des Beschäftigungsverhältnisses oder im berechtigten Interesse des Arbeitgebers erforderlich und unter Berücksichtigung des schutzwürdigen Interesses des Mitarbeiters zulässig ist. Dass die

Beschäftigten die betrieblichen E-Mails zur Verfügung stellen müssen, ist unbestritten. Allerdings sollte dies in einer Form geschehen, dass die Beschäftigten darüber informiert sind, und nicht durch heimliche Kontrollen. Zu beachten ist trotz eines Verbots der privaten Nutzung, dass E-Mails der Mitarbeiter einem besonderen Vertrauensschutz unterliegen können, z.B. an Mitglieder des Betriebsrats oder sonstige Beauftragte (wie z.B. die Schwerbehindertenvertretung oder den betrieblichen Datenschutzbeauftragten). Diese E-Mails entziehen sich wegen ihrer besonderen Vertraulichkeit auch bei einem Verbot der privaten Nutzung einer Kontrolle durch den Arbeitgeber. Gleiches gilt auch für die Kommunikation von besonderen Vertrauenspersonen im Unternehmen, wie Betriebsarzt, Betriebsrat, Jugendvertreter, Datenschutzbeauftragter, Schwerbehindertenvertreter u.a. Um eine rechtssichere Lösung für den Einsatz der Kommunikationsmedien schaffen zu können, ist eine klare Entscheidung über Verbot oder Zulässigkeit der privaten Nutzung erforderlich. Die Entscheidung, ob eine private Nutzung gestattet wird oder nicht, ist nicht mitbestimmungspflichtig im Sinne des BetrVG.

Prinzipiell gilt zwar der Grundsatz „Was nicht erlaubt ist, ist verboten“. Wenn aber bei einem ungeregelten Zustand die private Nutzung der Kommunikationssysteme dem Arbeitgeber bekannt ist und hingenommen wird, entsteht ein Zustand der stillschweigenden Duldung, der im Ergebnis einer Erlaubnis der privaten Nutzung gleichkommt und für die privaten Kommunikationsvorgänge zur Anwendung des Telekommunikationsgeheimnisses führt.

Auch wenn die private Nutzung verboten ist, sollte die Einhaltung des Verbots regelmäßig angemessen überprüft werden. Werden über lange Zeit keine Kontrollen durchgeführt und auch das Verbot nicht gelegentlich erneuert (z.B. im Rahmen von Betriebsversammlungen), kann ein Zustand der betrieblichen Übung und stillschweigenden Duldung entstehen, was rechtlich einer Erlaubnis gleichkommt. In Abhängigkeit von dieser Entscheidung über die Zulässigkeit der privaten Nutzung ergibt sich für die Nutzung eine unterschiedliche rechtliche Ausgestaltung.

Wenn die private Nutzung der Kommunikationseinrichtungen nicht gestattet ist, muss auf dieses Verbot regelmäßig hingewiesen werden. Ansonsten kann eine stillschweigende Duldung entstehen.

Verbot der privaten Nutzung

Auch wenn eine private Nutzung des Kommunikationssystems verboten ist, ist der Abschluss einer Betriebsvereinbarung erforderlich, weil anhand der aufgezeichneten Verkehrsdaten eine Leistungs- und Verhaltenskontrolle der Mitarbeiter möglich und damit die Mitwirkungspflicht des Betriebsrats gegeben ist. Wird ein Call Center betrieben, müssen die Einzelheiten des Telefonbetriebs ebenfalls in einer Betriebsvereinbarung geregelt werden. Besteht kein Betriebsrat, müssen mit den Mitarbeitern einzelvertragliche Regelungen getroffen werden. Wenn keine Betriebsvereinbarung und auch keine Einzelvereinbarung mit den Mitarbeitern abgeschlossen wird, werden personenbezogenen Daten teilweise rechtswidrig gewonnen und es fehlt die Rechtsgrundlage als Zulässigkeitsvoraussetzung für die Speicherung und Verarbeitung der Daten.

Von diesen Rechtsfolgen ausgenommen sind nur diejenigen Protokolldaten, die keinen Personenbezug besitzen, d.h. entweder von Anfang an keine Datenelemente enthalten, die eine Identifizierung der Benutzer ermöglichen oder vor ihrer Auswertung in einer nicht mehr rückgängig zu machender Weise anonymisiert worden sind. Unter dem Gesichtspunkt des Schutzes vor unzulässigen Leistungs- und Verhaltenskontrollen und des Schutzes des Persönlichkeitsrechts der Arbeitnehmer sind lediglich bei Vorliegen von rechtfertigenden Umständen, z.B. zur Gewährleistung der technischen Datensicherheit, der Ordnungsmäßigkeit oder Datenverarbeitung, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle, insbesondere bei Gefahr im Verzug oder bei konkreten Hinweisen auf eine Straftat, Auswertungen im Rahmen der Verhältnismäßigkeit als zulässig anzusehen.

Durch den Abschluss einer Betriebsvereinbarung oder einer Einzelvereinbarung mit den Mitarbeitern kann die Befugnis der Auswertung der aufgezeichneten Daten näher geregelt werden. Die Aufzeichnungen und Auswertungen sind zulässig, soweit diese im berechtigten Interesse des Unternehmens erforderlich sind und überwiegende schutzwürdige Interessen der Betroffenen nicht verletzt werden.

In einer Güterabwägung auf der Grundlage des Verhältnismäßigkeitsprinzips sind die berechtigten Interessen des Unternehmens (Betriebssicherheit, Schutz des Eigentums, Gewährleistung der technischen Datensicherheit, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle, Missbrauchsschutz etc.) ebenso einzubringen wie die schutzwürdigen Interessen der Betroffenen (Persönlichkeitsschutz, Recht auf informationelle Selbstbestimmung, Recht auf freie Entfaltung am Arbeitsplatz, unzulässige Leistungs- und Verhaltenskontrolle u.a.). Diese Interessen sind gegeneinander abzuwägen und in der Betriebsvereinbarung zum Ausgleich zu bringen. In diesem Rahmen sind Protokollierungen zur Fehleranalyse, Abwehr von Angriffen, Gewährleistung der Betriebssicherheit, Missbrauchskontrolle und Kontrolle einer rechtswidrigen Nutzung zulässig.

Diese Aufzeichnungen sind zweckgebunden und dürfen nur für die dort genannten Zwecke genutzt werden. Art und Umfang der Kontrollen und Auswertungen, die Nutzung der Ergebnisse, Beteiligung der Mitarbeitervertretung, Information der Betroffenen usw. werden in der Betriebsvereinbarung festgelegt.

Erlaubte private Nutzung

Bei einer erlaubten privaten Nutzung fallen nicht nur die Inhalte, sondern auch die näheren Umstände der Kommunikation, also die Verkehrs- und Abrechnungsdaten, die von der Telefonanlage bzw. dem Kommunikationssystem aufgezeichnet werden, unter das Telekommunikationsgeheimnis gemäß Telekommunikationsgesetz. Da i.d.R. auf technischem Weg nicht zwischen der privaten und der betrieblichen Kommunikation unterschieden wird, ist bei den Verkehrs- und Abrechnungsdaten oft nicht ohne weiteres erkennbar, ob eine private oder betriebliche Kommunikation zugrunde gelegen hat. Diese fehlende Unterscheidbarkeit der privaten und betrieblichen Kommunikation schafft für das Personal der IT-Administration eine Risikosituation, denn jede unbefugte Kenntnisnahme der durch das Telekommunikationsgeheimnis geschützten Daten (geschützt sind die Daten der privaten Kommunikation) verletzt das Telekommunikationsgeheimnis und löst eine Strafbarkeit aus.

Um sich bei einer erlaubten privaten Nutzung vor strafrechtlichen Folgen zu schützen, ist jedes Telefongespräch bzw. jede E-Mail als ein möglicherweise privater Kommunikationsvorgang zu behandeln und dem Schutz des Telekommunikationsgesetzes zu unterwerfen.

Dadurch werden aber die aus betrieblichem Interesse notwendigen Kontroll- und Auswertungsmöglichkeiten der aufgezeichneten Protokolldaten erheblich reduziert und der Umgang mit den Daten gestaltet sich rechtlich sehr problematisch. Um diese rechtlichen Probleme zu beseitigen, sind eine klare Entscheidung über die Zulässigkeit oder das Verbot einer Nutzung der Kommunikationssysteme für private Zwecke und der Abschluss einer Betriebsvereinbarung mit einer Regelung der erforderlichen Kontrollen dringend erforderlich.

Zusätzlich zur Betriebsvereinbarung sollte von jedem einzelnen Mitarbeiter eine schriftliche Erklärung darüber gefordert werden, ob er unter den in der Betriebsvereinbarung festgelegten Kontrollbefugnissen die Telefonanlage bzw. E-Mail und Internet für private Zwecke nutzen will und dass er dann die vereinbarten Kontrollen auch für die privaten Kommunikationsvorgänge (Telefongespräche und Nutzung von Internet und E-Mail) anerkennt. Diese Erklärung ist deshalb erforderlich, weil das Brief- und

Fernmeldegeheimnis ein Grundrecht ist und nicht durch eine kollektivrechtliche Vereinbarung mit Bindungswirkung für den einzelnen Mitarbeiter eingeschränkt werden kann. Eine derartige Einschränkung ist nur durch Gesetz (z.B. TKG) oder Einwilligung des Betroffenen zulässig, wobei bei einer Einwilligung das Grundrecht nicht in seiner Substanz eingeschränkt werden kann. Gibt der Mitarbeiter diese Erklärung nicht ab, ist für ihn die private Nutzung des Systems verboten. Nutzt er das System trotzdem für private Zwecke, handelt es sich um eine verbotene private Nutzung und er kann sich nicht auf den Schutz des Telekommunikationsgeheimnisses berufen. Es gelten dann die Regelungen der Betriebsvereinbarung.

Um nicht für alle vorhandenen und künftig verfügbaren Kommunikationssysteme (Telefon, E-Mail, Mobiltelefon, Internet etc.) getrennte Betriebsvereinbarungen abschließen zu müssen, empfiehlt es sich, eine Grundsatzvereinbarung über die Nutzung von elektronischen Medien abzuschließen.

Da die grundsätzlichen Regelungen für verschiedene Einrichtungen, in denen Protokollierungen anfallen, in gleicher Weise gelten, z.B. PC, Netzwerk, Server, Firewall etc. bietet es sich an, diese Einrichtungen in diese Betriebsvereinbarung einzubeziehen. So kann die Anzahl der erforderlichen Vereinbarungen reduziert werden. Wenn in einem Unternehmen kein Betriebsrat besteht, muss mit jedem Mitarbeiter eine entsprechende Einzelvereinbarung geschlossen werden. Eine Möglichkeit besteht auch darin, im Unternehmen eine Policy mit einem einer Betriebsvereinbarung vergleichbaren Inhalt zu erlassen. Die Mitarbeiter können dann eine entsprechende Erklärung abgeben, ob sie unter den in der Policy geregelten Voraussetzungen das System privat nutzen wollen.

Eine Policy ist erforderlich unabhängig davon, ob die Nutzung der Einrichtungen für private Zwecke zulässig ist oder nicht. Lediglich die inhaltlichen Regelungen sind teilweise unterschiedlich. Die Regelungen der Policy müssen genauso wie eine Betriebsvereinbarung das Persönlichkeitsrecht der Mitarbeiter beachten, d.h. die Kontrollen dürfen das Persönlichkeitsrecht der Mitarbeiter nicht in einer unzulässigen Weise einschränken, unabhängig davon, ob eine private Nutzung der Einrichtungen erlaubt ist oder nicht. Kontrollen dürfen deshalb nur in dem Ausmaß eingerichtet werden, wie sie zur Wahrung des berechtigten Kontrollinteresses des Unternehmens erforderlich sind und nicht überwiegende schutzwürdige Interessen der Mitarbeiter verletzen. Bei einer zulässigen privaten Nutzung der Einrichtungen dürfen die Kontrollen das Telekommunikationsgeheimnis nicht in unzulässiger Weise einschränken.

Gibt es einen Betriebsrat, ist die Mitbestimmungspflicht zu beachten. Dieser kann durch eine Betriebsvereinbarung zur Nutzung der betrieblichen Kommunikationssysteme entsprochen werden. In Unternehmen ohne Betriebsrat empfiehlt sich der Erlass einer Policy, welche die Nutzung der betrieblichen Kommunikationssysteme individualrechtlich regelt.

Im Falle einer erlaubten oder geduldeten privaten Nutzung ist wegen des Vertrauensschutzes aus dem Telekommunikationsgeheimnis heraus eine personenbezogene Auswertung von Verkehrsdaten nur sehr eingeschränkt zulässig. Zulässig sind Auswertungen lediglich für bestimmte Zwecke, z.B. Gebührenabrechnung, soweit diese überhaupt durchgeführt wird. Weitere Ausnahmen hiervon erlaubt das Telekommunikationsgesetz nur zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen und zur Missbrauchsbekämpfung. Danach kann die Erhebung (d.h. Protokollierung) von Daten zur Gewährleistung der technischen Datensicherheit, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle oder insbesondere bei Gefahr im Verzug (z.B. bei konkreten Hinweisen auf eine Straftat) im Rahmen der Verhältnismäßigkeit als zulässig angesehen werden. Wird eine Betriebsvereinbarung abgeschlossen, darf dieser Rahmen in der Betriebsvereinbarung in

einem angemessenen und für das Unternehmen erforderlichen Umfang unter Beachtung des Persönlichkeitsrechts der Betroffenen ausgestaltet werden. Die Zulässigkeit der Kontrollen richtet sich dann nach den Regelungen in der Betriebsvereinbarung.

Verlangt der Arbeitgeber einen Einzelverbindungsnachweis, ist dieser gemäß TKG nur zulässig, wenn der Arbeitgeber in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und dass der Betriebsrat (oder die Personalvertretung) entsprechend der gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. Auch im Hinblick auf diese Informations- und Beteiligungspflicht ist der Abschluss einer Betriebsvereinbarung bzw. einer Vereinbarung mit den Beschäftigten erforderlich. Gemäß TKG entscheidet der Teilnehmer, ob ihm die von ihm gewählten Rufnummern ungekürzt oder um die letzten drei Stellen gekürzt mitgeteilt werden sollen. Insbesondere bei einer erlaubten privaten Nutzung muss auf die Mitteilung der vollständigen Rufnummer verzichtet werden.

Es empfiehlt sich mit der Erlaubnis einer privaten Nutzung eine klare Kennzeichnung der privaten E-Mails zu regeln, z.B. durch den Zusatz „privat“ im Betreff, damit im Falle eines notwendigen Zugriffes durch den Arbeitgeber private E-Mails möglichst sicher zu erkennen sind. Ferner empfiehlt es sich, den Zugriff nur im Vieraugenprinzip, z.B. im Beisein eines Mitgliedes des Betriebsrates oder des Datenschutzbeauftragten vorzunehmen.

Zugriffsrecht des Arbeitgebers auf das E-Mail-Konto von Beschäftigten

Bei Abwesenheit eines Beschäftigten, insbesondere bei längerer Abwesenheit wegen Urlaub oder Krankheit, kann eine Einsichtnahme in betriebliche E-Mails des Beschäftigten erforderlich werden. Grundsätzlich hat der Arbeitgeber, z.B. zur Aufrechterhaltung der Bearbeitung von Posteingängen, ein berechtigtes Interesse an der Kenntnis der betrieblichen Posteingänge auch während einer Abwesenheit des Beschäftigten. Der Arbeitgeber hat zu diesem Zweck das Recht, die Erledigung der betrieblichen Aufgaben und der Arbeitsabläufe durch die Beschäftigten zu kontrollieren und ggf. durch Einsichtsbefugnisse und entsprechende Anweisungen zu steuern. Insoweit gilt für die elektronische Korrespondenz nichts anderes als für den herkömmlichen Postverkehr. Die Rechtsgrundlage dazu ergibt sich aus § 26 Abs. 1 Satz 1 BDSG. Andererseits muss der Beschäftigte unabhängig von der Erlaubnis einer privaten Nutzung des E-Mail-Systems keine uneingeschränkten Kontrollen dulden.

Private E-Mails und E-Mail-Account bei Ausscheiden des Beschäftigten

Scheidet ein Beschäftigter aus dem Unternehmen aus, sind auf Wunsch private E-Mails herauszugeben. Eine einfache Löschung ohne Abstimmung mit dem Betroffenen ist problematisch, denn nach Auffassung der Gerichte darf der betriebliche E-Mail-Account erst gelöscht werden, wenn der ehemalige Inhaber an der Nutzung des Accounts kein Interesse mehr hat. Werde im Zusammenhang eines Vertragsverhältnisses dem Beschäftigten ein E-Mail-Account zur Verfügung gestellt, auf dem dieser auch private E-Mails abspeichern darf, entspreche es den vertraglichen Nebenpflichten, den Account nach Beendigung der Zusammenarbeit solange nicht zu löschen, bis klar sei, dass der Beschäftigte kein Interesse mehr an der Nutzung des Accounts hat. Dem Betroffenen sollte deshalb Gelegenheit gegeben werden, seine privaten E-Mails für sich zu sichern. Dies gilt auch für andere private Daten auf dem PC. Anschließend sollte von ihm eine Erklärung verlangt werden (z. B. in einer Austrittscheckliste), dass an den verbleibenden Daten seinerseits kein Interesse mehr besteht und die Daten gelöscht werden können bzw. dass es sich bei diesen Daten nur noch um betriebliche Daten handelt, die der Verfügungsgewalt des Arbeitgebers unterliegen. Wann der Account gelöscht werden soll, ist Vereinbarungssache mit dem Betroffenen. Zweckmäßig ist es, für eine angemessene Übergangszeit eine Abwesenheitsnachricht zu schalten, dass der Betroffene über diese Adresse nicht mehr erreichbar ist. Eine Frist von einigen

Monaten wird hier als angemessen beurteilt. Im Anschluss daran kann der Account gelöscht werden.

Private E-Mails bei Tod des Beschäftigten

Wie mit den E-Mails eines verstorbenen Mitarbeiters zu verfahren ist, ist ebenso komplex wie sensibel. Da das **Datenschutzrecht nur für lebende Personen** gilt, fällt diese Frage nicht mehr unter die Datenschutzvorschriften. Es gelten vielmehr die **Grundsätze zum postmortalen Persönlichkeitsschutz**. Dem stehen die Ansprüche der Erben gegenüber. E-Mails können aber auch höchstpersönlicher Natur sein und Dinge betreffen, die auch die Erben nichts angehen, z. B. nicht erbberechtigte Personen, eine heimliche Liebschaft usw. Es stellt sich dann die Frage der Vererbbarkeit überhaupt und auch die Frage nach einer Offenbarungsbefugnis den Erben gegenüber. Auch Angehörigen gegenüber kann dieser postmortale Persönlichkeitsschutz des Betroffenen greifen und eine Offenbarungsbefugnis infrage stellen. So sind Konstellationen denkbar, in denen der Erblasser gar nicht möchte, dass die jeweiligen Erben umfassende Verfügungsgewalt über alle Accounts erhalten, z. B. wenn verhindert werden soll, dass die Erben höchstpersönliche E-Mail-Korrespondenz zur Kenntnis nehmen. Auch kann gewollt sein, dass der digitale Nachlass (oder Teile davon) an andere Personen geht als an die regulären Erben. Fehlen Regelungen in Betriebsvereinbarungen, ist deshalb ein Zugriff auf möglicherweise wichtige geschäftliche E-Mails schwierig und zunächst nicht gestattet, weil diese mit privaten Nachrichten vermischt sein könnten. Andererseits kann dem Arbeitgeber auch nicht zugemutet werden, wegen dieser Zugriffsbeschränkungen einen u. U. hohen wirtschaftlichen Schaden zu riskieren, weil er wichtige betriebliche E-Mails nicht zur Kenntnis nehmen kann.

Da in den allermeisten Fällen zu diesem Fragenkomplex keine betrieblichen Regelungen vorhanden sind, ist nach einem einigermaßen rechtssicheren Weg zu suchen, wie der Arbeitgeber unter Wahrung eines hinreichenden Schutzes der privaten E-Mails die betrieblichen Vorgänge zur Kenntnis nehmen kann. Denkbar wäre etwa, dass beim Zugriff ein fachkundiger Mitarbeiter der IT-Abteilung, der betriebliche Datenschutzbeauftragte und ein Vertreter der Fachabteilung des betroffenen Mitarbeiters und des Betriebsrats anwesend sind und über den Vorgang ein schriftliches Protokoll angefertigt wird. Als privat zweifelsfrei erkennbare E-Mails dürfen nicht geöffnet werden und sollten auf einem externen Datenträger gespeichert und ggf. den Erben übermittelt werden, wobei deren Legitimation und Empfangsbefugnis zu prüfen ist. Dieser Weg ist aber auch nur eine Notlösung mit allen rechtlichen Risiken, um ein akutes Problem zu lösen, und kann eine belastbare Lösung mittels Betriebsvereinbarung oder Vereinbarung mit den Beschäftigten nicht ersetzen.

Personen mit besonderen Berufsgeheimnissen

Zu diesem Personenkreis gehören z.B. Betriebsärzte und die Mitglieder des Betriebsrats sowie der Schwerbehindertenvertreter. Diese Personen unterliegen besonderen Vertraulichkeitsverpflichtungen. Diese Verpflichtungen umfassen auch Informationen darüber, wann sie mit welchen Personen im Unternehmen über die betrieblichen Kommunikationssysteme Kontakt hatten. Als Auswirkung dieser besonderen Verschwiegenheitsverpflichtungen ergibt sich für den Arbeitgeber das Verbot, auf diese Kommunikationsdaten zuzugreifen und diese auszuwerten.

Mitbestimmung bei Telefon, E-Mail, Internet

Bei der Nutzung der betrieblichen Kommunikationssysteme entsteht eine Vielzahl von Protokolldaten, z.B. wer wann mit wem telefoniert hat, an wen eine E-Mail versandt wurde, ggf. mit welchen Anhängen (Art und Größe der Datei) und welche Seiten im Internet besucht worden sind. Diese Daten, u.U. in Kombination mit personenbezogenen Daten aus anderen Datenverarbeitungssystemen (z.B. Zeiterfassungssystemen),

ermöglichen je nach Art und Umfang der Aufzeichnungen eine unzulässige Verhaltens- und Leistungskontrolle.

Gemäß BetrVG besteht für derartige Datenverarbeitungsverfahren eine Mitbestimmungspflicht von Seiten des Betriebsrats. Bei der Beurteilung der Mitbestimmungspflicht kommt es nicht darauf an, ob der Arbeitgeber diese Kontrollen auch tatsächlich ausübt. Entscheidend ist die Frage, ob aufgrund der technischen Konzeption des Verfahrens und der Art der erfassten Daten eine Leistungskontrolle möglich ist.

Schon die bloße Möglichkeit reicht aus, um die Mitbestimmungspflicht zu begründen. Bei der Ausgestaltung der Mitbestimmung, d.h. bei den in der Betriebsvereinbarung zu treffenden Regelungen, ist zu beachten, dass das Schutzniveau der Datenschutzgesetze nicht unterschritten und das Persönlichkeitsrecht der Betroffenen nicht unzulässig beeinträchtigt wird.

Personenbezogene Daten in Form von Protokolleinträgen fallen nicht nur im Zusammenhang mit der Nutzung von betrieblichen Kommunikationssystemen, sondern auch mit der Nutzung von IT-Systemen (z.B. auf Netzwerk-, Server- und Applikationsebene) an. Da ein weitgehend identischer Regelungsbedarf besteht, empfiehlt es sich anstelle einer Vielzahl von speziellen Betriebsvereinbarungen für die einzelnen Systeme eine übergreifende Betriebsvereinbarung über die Nutzung von elektronischen Medien abzuschließen. Dadurch wird die Anzahl der Betriebsvereinbarungen und der hierfür erforderliche Aufwand erheblich reduziert und Doppelregelungen vermieden.

Heimliches oder offenes Mithören von Telefongesprächen, auch im Call Center

Ein offenes Mithören ist vom Bundesarbeitsgericht während eines Anlernprozesses in der Probezeit für zulässig gehalten worden. Ein heimliches Mithören oder Aufzeichnen von Telefongesprächen ist unabhängig von Verbot oder Erlaubnis der Nutzung für private Zwecke grundsätzlich unzulässig. Dies gilt nach der Rechtsprechung auch für betriebliche Telefongespräche im Verhältnis zwischen Arbeitgeber und Arbeitnehmer.

Das Aufzeichnen von Telefongesprächen berührt auch das Recht am gesprochenen Wort beider Gesprächsteilnehmer als Auswirkung des Persönlichkeitsrechts. Ein Aufzeichnen von Telefongesprächen (und dazu gehören auch die im Rahmen der betrieblichen Aufgabenerfüllung geführten Gespräche, z.B. mit einem Kunden), stellt deshalb einen Eingriff in das Persönlichkeitsrecht aller beteiligten Gesprächspartner dar.

Mithören ist nur für sehr eng begrenzte Zwecke zulässig. Und dies auch nur, wenn beide Gesprächspartner eingewilligt haben.

Andererseits besteht aber auch ein anerkanntes Interesse der Unternehmen, Kundengespräche einem laufenden Kontroll- und Verbesserungsprozess zu unterwerfen. Dass der Arbeitgeber zu diesem Zweck die Arbeit der Call Center-Agenten (und somit die Telefongespräche) kontrollieren können muss, um Mängel im Arbeits- und Gesprächsverhalten der Agenten feststellen und beheben zu können, ist in der Rechtsprechung anerkannt. Das Mithören und ggf. die Aufzeichnung von Telefongesprächen ist aber unter dem Gesichtspunkt der Verhältnismäßigkeit auf den unbedingt erforderlichen Umfang zu begrenzen, z.B. auf die Dauer der Einarbeitungsphase von Mitarbeitern oder auf einen von vorneherein für Schulungs- oder Coachingzwecke begrenzten Zeitraum.

Bei der Ausgestaltung der Maßnahmen müssen im Hinblick das Persönlichkeitsrecht der Gesprächsteilnehmer folgende Gesichtspunkte berücksichtigt werden:

- Für die Gesprächskontrolle ist das mildeste geeignete Mittel zu wählen. Das mildeste Mittel ist das Mithören ohne Gesprächsaufzeichnung. Ist dieses Mittel ausreichend, z.B. wenn im unmittelbaren Anschluss an das Telefonat das Coaching-Gespräch stattfindet und wegen der unmittelbaren Aufarbeitung des Gesprächs keine Aufzeichnung erforderlich ist, ist eine Aufzeichnung nicht notwendig und dann auch nicht zulässig.
- Aufzeichnungen sind zulässig, wenn z.B. aufgrund des Arbeitsablaufs oder der Art und Weise des Coachings das Coaching-Gespräch sinnvoll erst später geführt werden kann oder aufgrund der Art des Coachings oder aus anderen berechtigten Gründen grundsätzlich Aufzeichnungen erforderlich sind.
- Neben der Frage, ob nur Mithören oder auch Aufzeichnen zulässig ist, ist auch die Frage der Auswertung der Gespräche erheblich. Im einfachsten Fall kann sich ein Coach die Aufzeichnungen anhören. Auch die Auswertungen müssen auf das für das Coaching-Ziel erforderliche Maß beschränkt werden. Unzulässig ist es, die Aufzeichnungen beliebig auszuwerten.
- Durch das Aufzeichnen der Gespräche darf für die Mitarbeiter kein unzumutbarer Überwachungsdruck entstehen, d.h. es sind nur Stichprobenkontrollen zulässig, aber keine totale Kontrolle aller Gespräche. Art und Umfang der Stichproben und der Auswertungen sind festzulegen und den Betroffenen offenzulegen. Den Mitarbeiter soll die Möglichkeit geboten werden, im Einzelfall eine Aufzeichnung auch zu verhindern.
- Die Tatsache des Mithörens bzw. der Aufzeichnung muss beiden am Gespräch beteiligten Personen bekannt sein, denn das Recht am gesprochenen Wort gilt für den Anrufer genauso wie für den Mitarbeiter. Beide müssen vorher darüber informiert werden und der Anrufer muss die Möglichkeit besitzen, das Mithören oder die Aufzeichnung des Gespräches zu blockieren. Hierzu können bestimmte Zeiträume festgelegt oder die Tatsache der Aufzeichnung auf technischem Weg erkennbar gemacht werden
- Die Befugnis zur Aufzeichnung der Telefongespräche setzt eine Einwilligung aller Gesprächsteilnehmer, nicht nur des Mitarbeiters, voraus.
- Über das ganze Verfahren ist eine Betriebsvereinbarung erforderlich.

Gewerkschaftszugehörigkeit

Die Gewerkschaftszugehörigkeit fällt unter die **besonderen Datenarten**. Die Zugehörigkeit zur Gewerkschaft darf deshalb vom Arbeitgeber **nicht** erfragt werden. Der Arbeitgeber erhält aber von der Mitgliedschaft zur Gewerkschaft z.B. im Rahmen der Lohnabrechnung dann Kenntnis, wenn der Mitarbeiter den Gewerkschaftsbeitrag direkt abführen lässt. Dies ist auch rechtlich unproblematisch, weil der Beschäftigte in die direkte Abführung eingewilligt hat und die Kenntnis der Gewerkschaftszugehörigkeit zur Geltendmachung rechtlicher Ansprüche genutzt wird. Allerdings dürfen diese Daten dann auch nur zu Abrechnungszwecken genutzt werden.

Die Tatsache der Kenntnis der Gewerkschaftszugehörigkeit berechtigt aber den Arbeitgeber nicht zu Datenübermittlungen an die Gewerkschaften. So ist die Übergabe von Lohnlisten an Gewerkschaften, um deren Zustimmung zu Kostensenkungsmaßnahmen im Personalbereich zu erzielen, in personenbezogener Form nicht erforderlich und daher unzulässig. Das BetrVG berechtigt zwar bestimmte betriebliche Ausschüsse und Betriebsratsmitglieder zur Einsichtnahme in die Listen über die Bruttolöhne und Gehälter, nicht aber gewerkschaftliche Tarifkommissionen. Bei Verhandlungen über Firmentarifverträge dürfen grundsätzlich nur Lohnlisten ohne Namensnennung verwandt werden. Im Einzelfall kann die Pseudonymisierung der Beschäftigtendaten genügen.

Die Mitgliederwerbung durch Gewerkschaften über die betriebliche E-Mailadresse muss der Arbeitgeber dulden, wenn dadurch keine unzumutbare Beeinträchtigung des Betriebsablaufes verursacht wird.

Krankenrückkehrgespräche

Rückkehrgespräche sollten grundsätzlich bei jeder Art von Rückkehr, nicht nur bei Krankheit, sondern auch nach Urlaub, Mutterschaft etc. geführt werden. Sie sollten formalisiert werden, d.h. es sollte ein geregelter Prozess eingerichtet werden, der einen formalisierten Ablauf und eine Gleichbehandlung aller Mitarbeiter gewährleistet. Dazu gehört auch ein standardisiertes Protokoll, das auch dem Mitarbeiter ausgehändigt wird. Ein derartiges formalisiertes Verfahren ist aber auch mitbestimmungspflichtig. Diese Maßnahmen tragen dazu bei, Rückkehrgespräche zu einem normalen Bestandteil des Arbeitslebens zu machen.

Eine Untermenge der Rückkehrgespräche ist das Krankenrückkehrgespräch. Diese Gespräche werden je nach Stand und Schwere der vorliegenden Umstände (Dauer, Häufigkeit der Erkrankungen) meist in abgestuften Formen (3 bis 5 Stufen) geführt, wobei sich die Stufen in ihrer Art und in ihren Zielen unterscheiden. Die Stufen reichen vom Motivationsgespräch bis zum sehr ernsthaften Fehlzeitengespräch mit einer Darlegung eventueller Sanktionen.

Krankenrückkehrgespräche können als Bestandteil eines betrieblichen Gesundheitsmanagements sinnvoll sein und datenschutzrechtlich korrekt abgewickelt werden. Wenn es beispielsweise Anzeichen dafür gibt, dass die Erkrankung auf die Arbeitsbedingungen zurückzuführen sein könnte, können Informationen des Arbeitnehmers aus einem derartigen Gespräch sehr nützlich sein. Das Gespräch muss dann aber darauf ausgelegt sein, mögliche betriebsbedingte Krankheitsursachen zu erforschen und die Arbeitsbedingungen zu verbessern. Wie Krankenrückkehrgespräche geführt werden sollten, ist allerdings nicht geregelt.

Zu den problematischen Fragen, die nicht gestellt werden dürfen bzw. nicht beantwortet werden müssen, gehören folgende Fragenkategorien:

- Abwesenheitsgründe und Fragen nach dem persönlichen Umfeld
- Diagnosen (Teilweise wird die Meinung vertreten, dass die Frage zwar erlaubt ist, der Mitarbeiter aber nicht zur Beantwortung verpflichtet ist. Erlaubt ist die Frage, ob die Erkrankung möglicherweise auf betriebsbedingte Umstände zurückzuführen ist.)
- Fragen nach dem erwarteten künftigen Verlauf der Krankheit und nach eventuellen weiteren zu erwartenden Fehlzeiten
- Zusammenhänge zwischen früheren Krankheiten und der aktuellen Fehlzeit bzw. weiteren zu erwartenden Fehlzeiten (gleiche oder unterschiedliche Erkrankungen) wegen der Möglichkeit der Ableitung einer negativen Gesundheitsprognose
- Ausforschende Fragen zum Hintergrund der Krankheit sind nicht erlaubt. Auch die Frage, ob die Krankheit die gleiche Ursache hat wie frühere Krankheiten, sollte nicht gestellt werden.

Im Krankenrückkehrgespräch dürfen Fragen nach der Diagnose und dem Verlauf der Krankheit **nicht** gestellt werden. Fragen nach dem Befinden, ob die Erkrankung vollständig überwunden ist, ob und ggf. welche betrieblichen Ursachen möglicherweise die Erkrankung verursacht haben und was getan werden kann, um diese Ursachen abzustellen, dürfen gestellt werden.

Der Mitarbeiter kann die Aushändigung eines Protokollexemplars verlangen, muss es aber nicht mitunterzeichnen.

Betriebliches Eingliederungsmanagement (BEM)

Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, klärt der Arbeitgeber mit der zuständigen Interessenvertretung im Sinne (Betriebsrat), bei schwerbehinderten Menschen außerdem mit der Schwerbehindertenvertretung, mit **Zustimmung und Beteiligung der betroffenen Person** die Möglichkeiten, wie die

Arbeitsunfähigkeit möglichst überwunden werden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann (betriebliches Eingliederungsmanagement).

Weil der Arbeitgeber kein Sozialleistungsträger ist, verlangt es der Zustimmung des Betroffenen. Da es sich um **besondere Datenarten (Gesundheitsdaten)** handelt, sind die zusätzlichen Anforderungen an die Einwilligung mit dem ausdrücklichen Bezug der Einwilligung auf die besonderen Datenarten zu beachten. Verlangt wird die informierte Einwilligung, d.h. der Betroffene ist über alle Stufen des Verfahrens und über die Möglichkeit des jederzeitigen Widerrufs der Einwilligung zu unterrichten.

Die Einwilligung muss sich auch die Mitwirkung der beteiligten Stellen (Betriebsrat, Betriebsarzt und ggf. Schwerbehindertenvertretung) beziehen, weil deren Beteiligung von der Einwilligung des Betroffenen abhängig ist.

Die anfallenden Daten, Aufzeichnungen und Schriftstücke unterliegen deshalb der besonderen Zweckbindung dieser Vorschrift und müssen auch **getrennt** von der Personalakte geführt werden. Zulässig ist natürlich ein Vermerk in der Personalakte, dass eine BEM-Akte vorhanden ist. Eine Aufbewahrungsfrist für die BEM-Unterlagen ist nicht geregelt. Aus Datenschutzsicht richtet sich die Aufbewahrung nach den allgemeinen Vorschriften. Danach sind die Daten zu löschen bzw. zu vernichten, wenn sie für die Erfüllung des Zweckes, für den sie gespeichert worden sind, nicht mehr erforderlich sind.

Blutuntersuchungen

Blutuntersuchungen, z.B. zur Durchführung eines Alkohol- oder Drogentests bzw. zur Klärung einer Abhängigkeit mit anschließender Offenbarung des Ergebnisses an den Arbeitgeber, sind ein Eingriff in die Intimsphäre des Arbeitnehmers und unterliegen dem Schutz des Grundgesetzes. Blutentnahmen sind grundsätzlich auch ein Eingriff in die körperliche Unversehrtheit, den der Arbeitnehmer im Hinblick auf sein Recht auf körperliche Unversehrtheit nicht dulden muss. Routineuntersuchungen im laufenden Arbeitsverhältnis, die vorbeugend klären sollen, ob der Arbeitnehmer alkohol- bzw. drogenabhängig ist, sind deshalb regelmäßig **unzulässig**.

Ausnahme: Blutuntersuchungen können dann zulässig sein, wenn aufgrund besonderer Risiken des Arbeitsplatzes (z.B. durch Umgang mit besonders gefährlichen Maschinen oder Geräten, mit Waffen oder Sprengstoff etc.) von einem Alkohol- oder Drogenkonsum besondere Gefährdungen ausgehen oder besonderer Umstände bzw. eines Anlasses, die eine berechtigte Sorge begründen, dass ein Alkohol- oder Drogenproblem bestehen könnte. In diesen Fällen besteht auch eine Fürsorgepflicht auf Seiten des Arbeitgebers, die ihn berechtigen oder sogar verpflichten kann, durch Einholung einer geeigneten ärztlichen Untersuchung die gesundheitliche Tauglichkeit des Arbeitnehmers zur Ausübung der vereinbarten Beschäftigung abzuklären.

In jedem Fall muss aber das schutzwürdige Interesse des Betroffenen an der Wahrung seiner körperlichen Unversehrtheit und seiner Intimsphäre gegen das Interesse des Arbeitgebers an der Untersuchung abgewogen werden. Zulässig sind in diesem Rahmen nur diejenigen Untersuchungen, die zur Klärung erforderlich sind. Auch dürfen z.B. bei Blutuntersuchungen nur diejenigen Laborauswertungen und Tests vorgenommen werden, die zur Klärung der arbeitsrechtlichen Situation erforderlich sind. Überschüssige bzw. weitergehende Ergebnisse dürfen nicht erzielt werden.

Krankheitsstatistiken

Anonyme Statistiken über Abwesenheiten von Mitarbeitern durch Krankheit oder unentschuldigtes Fehlen sind datenschutzrechtlich zulässig. Diesem Interesse kann und konnte zwar in der Vergangenheit auch dadurch genügt werden, dass solche Aussagen und Erkenntnisse ohne Einsatz technischer Hilfsmittel erarbeitet wurden. Es ist aber auch ein berechtigtes Interesse des Arbeitgebers, sich diejenigen Kenntnisse, die er berechtigterweise benötigt, in wirtschaftlich sinnvoller Weise schnell und kostengünstig zu verschaffen.

Schutzwürdige Belange der Arbeitnehmer machen eine solche Datenverarbeitung noch nicht unzulässig. Zwar werden dadurch auch schutzwürdige Belange der Arbeitnehmer berührt, da der Arbeitgeber Erkenntnisse gewinnen kann, die ihnen – wenn auch berechtigterweise – zum Nachteil gereichen können. Das allein macht die Datenverarbeitung noch nicht unzulässig. Die Grenze für die Zulässigkeit einer Datenverarbeitung ergibt sich vielmehr erst aus einer Abwägung der berechtigten Interessen des Arbeitgebers und der schutzwürdigen Belange des Arbeitnehmers. Würde jede Berührung schutzwürdiger Belange des Arbeitnehmers eine Datenverarbeitung unzulässig machen, wäre diese nur in wenigen Ausnahmefällen zulässig.

Diese Interessenabwägung führt vorliegend dazu, dass eine solche Datenverarbeitung zulässig ist. Der Arbeitgeber hat – auch außerhalb der Lohn- und Gehaltsabrechnung – ein berechtigtes Interesse daran zu erfahren, ob, wann, wie oft und wie lange ein Arbeitnehmer unentschuldigt gefehlt und damit seine Vertragspflicht verletzt hat. Das bedarf keiner näheren Darlegung. Berechtigte Belange des Arbeitnehmers, dem Arbeitgeber diese Erkenntnisse zu verwehren, bestehen nicht.

Da diese Verfahren eine Verhaltens- und Leistungskontrolle der Mitarbeiter ermöglichen, ist die Mitbestimmungspflicht des Betriebsrates zu beachten.

Führerscheinbesitz (Kontrolle des Führerscheinbesitzes)

Wenn Beschäftigte ein Firmenfahrzeug führen, muss der Arbeitgeber regelmäßig prüfen, ob der Beschäftigte eine gültige Fahrerlaubnis besitzt. Diese Kontrolle kann elektronisch unterstützt werden, z.B. durch Aufbringen von elektronisch lesbaren Aufklebern (RFID-Chip) und maschineller Lesung und auch in Form einer Datenverarbeitung im Auftrag vergeben werden. Zulässig ist die Erfassung des Namens des Beschäftigten sowie der Führerscheindaten wie Führerscheinklasse, ausstellende Behörde und Datum der Ausstellung. Zu beachten ist die Mitwirkungspflicht des Betriebsrates und eine ausreichende Information der Betroffenen über den Zweck der Datenspeicherung und über Art und Umfang der Datenerhebung und -verarbeitung. Bei Ausscheiden des Mitarbeiters oder bei Entzug des Firmenfahrzeuges müssen die Daten gelöscht bzw. falls diese zu Nachweiszwecken noch gespeichert werden müssen, für eine weitere Verarbeitung oder Nutzung gesperrt werden.

Mitarbeiterbefragungen

Mitarbeiterbefragungen werden mit unterschiedlichen Zielen durchgeführt, z.B. im Rahmen der Organisationsentwicklung, zur Verbesserung des Betriebsklimas oder der Arbeitszufriedenheit.

Solange die Befragung **anonym** durchgeführt wird, ist die Maßnahme datenschutzrechtlich unproblematisch, weil keine personenbezogenen Daten entstehen. Dann sollten aber Fragen wie z.B. nach dem Alter, nach der Dauer der Betriebszugehörigkeit, nach Voll- oder Teilzeitbeschäftigung etc. unterlassen werden, weil diese Fragen insbesondere bei kleineren Einheiten u.U. wieder Rückschlüsse auf die Person des Befragten zulassen. Ebenso ist darauf zu achten, dass bei gruppenbezogenen Befragungen die Gruppen ausreichend groß gewählt werden (ca. sieben Personen), damit Rückschlüsse auf einzelne Gruppenmitglieder ausgeschlossen werden. Soll allerdings das Ergebnis der Befragung hinterher mit den Betroffenen besprochen werden, ist eine Einwilligung erforderlich.

Werden Mitarbeiterbefragungen durch ein externes Unternehmen durchgeführt, so handelt es sich i.d.R. um eine Datenverarbeitung im Auftrag. Die Voraussetzungen für eine Auftragsdatenverarbeitung sind dann einzuhalten. Die Beauftragung eines externen Unternehmens bietet die Gewähr, bei einer entsprechenden Vertraulichkeitsverpflichtung die Anforderungen an eine anonymisierte Durchführung der Befragung zu erfüllen. Um eine tragfähige Vertrauensbasis für eine Befragung zu schaffen, sollten allerdings Ziel und Zweck der Befragung, die Art und Weise der Durchführung und die Maßnahmen zur Gewährleistung des Vertrauensschutzes der Mitarbeiter diesen erläutert werden.

Wird die Befragung online durchgeführt, ist darauf zu achten, dass keine personenbezogenen Daten (z.B. die IP-Adresse des Mitarbeiter-PCs, Protokolldaten oder sonstige Daten wie Kennungsinformationen etc.) gespeichert werden, die eine Identifikation des Mitarbeiters ermöglichen.

In die Planung und Vorbereitung des Vorhabens sollte der Betriebsrat mit einbezogen und seine Zustimmung eingeholt werden.

Konsumverhalten im Betrieb

Informationen über das Konsumverhalten der Beschäftigten, über Ernährungsgewohnheiten (auch, soweit sie sich auf den Arbeitsplatz beziehen, z.B. die Auswahl des Kantinenessens) oder über Personaleinkäufe sind dem privaten Lebensbereich des Beschäftigten zuzurechnen und dürfen ggf. nur für Bestell- und Abrechnungszwecke genutzt werden. Ebenso dürfen Informationen über seine privaten Lebensgewohnheiten, seine Lebens- und familiären Umstände, sportliche Betätigungen und sonstige Freizeitbeschäftigungen weder erhoben noch gespeichert oder genutzt werden. Auch ob der Betroffene raucht oder Nichtraucher ist, gehört zum privaten Lebensbereich und darf nicht erhoben werden.

Leistungsvergleiche

Zur Leistungsabrechnung oder für Steuerungs-, Vergleichs- und Benchmarkingzwecke werden die Ergebnisse von Verkaufs-, Vertriebs- und Außendienstmitarbeitern erfasst und aufbereitet. Personenbezogene Auswertungen und Ergebnisübersichten, Ranglisten usw. dürfen den verantwortlichen Vorgesetzten zur Erfüllung ihrer Planungs-, Führungs- und Steuerungsaufgaben zugänglich gemacht werden. Insoweit besteht eine Rechtsgrundlage, weil die Kenntnis der Leistungsdaten der Mitarbeiter durch die Vorgesetzten für die Ausführung des Beschäftigungsverhältnisses erforderlich ist.

Weitere Nutzungen und Offenbarungen im Unternehmen, z.B. für Vergleiche von verschiedenen Vertriebsbereichen sowie für internes oder externes Benchmarking etc. sind im Rahmen einer Interessenabwägung zu beurteilen. Diese sind nur dann zulässig, wenn von Seiten des Unternehmens ein berechtigtes Interesse besteht und das schutzwürdige Interesse des Betroffenen am Ausschluss der Offenbarung nicht überwiegt. Für Nutzungen im Rahmen eines internen und externen Benchmarking reichen auch Ranglisten in anonymisierter Form aus, sodass sich für diese Zwecke der Einsatz von personalisierten Ranglisten verbietet.

Gleiches gilt auch für die interne Veröffentlichung von sog. Bestenlisten oder Rennlisten, um den einzelnen Mitarbeitern einerseits Vergleichsmöglichkeiten zu bieten und sie andererseits zu mehr Leistung zu motivieren. Für diese Zwecke ist eine anonymisierte Liste durchaus ausreichend, denn sie ermöglicht den einzelnen Mitarbeitern, ihr eigenes Leistungsniveau und ihre Ergebnisse in das gesamte Leistungsgefüge einzuordnen und daraus persönliche Leistungsziele abzuleiten. Zu bedenken ist auch, dass bei einer personenbezogenen Offenbarung dieser Bestenlisten bei denjenigen Mitarbeitern, die unterdurchschnittliche Ergebnisse erzielt haben, das Ansehen im Unternehmen möglicherweise geschädigt wird und so eine diskriminierende Wirkung entstehen kann. In diesen Fällen ist das schutzwürdige Interesse der Betroffenen höher zu bewerten als das Interesse des Unternehmens; eine Offenbarung ist nur mit Einwilligung der Betroffenen zulässig. Dies kann umso mehr der Fall sein, wenn Umstände für ein niedrigeres Ergebnis vorliegen, die der Betroffene nicht zu vertreten hat, die aber im Kollegenkreis unbekannt sind. Auch die Mitarbeiter, die besonders gut abgeschnitten haben, sind oft nicht daran interessiert, dass ihre Ergebnisse im Unternehmen offengelegt werden.

Die Veröffentlichung von personenbezogenen Leistungsvergleichen ist nur mit Zustimmung der Mitarbeiter erlaubt.

Ethikregelungen

Soweit Ethikregelungen die arbeitsvertraglichen Pflichten des Arbeitnehmers (z.B. die arbeitsvertraglichen Treuepflichten) regeln, handelt es sich um Maßnahmen auf dem Boden des Direktionsrechts des Arbeitgebers. Auf der Grundlage seiner Treuepflicht ist der Arbeitnehmer gehalten, Schaden vom Arbeitgeber fernzuhalten. Datenerhebungen von den Beschäftigten, die im Rahmen dieser Maßnahmen anfallen, sind zulässig. Erhoben werden dürfen aber nur diejenigen Daten, die mit der arbeitsvertraglichen Tätigkeit des Beschäftigten im Zusammenhang stehen.

Werden personenbezogene Daten erhoben, z.B. mittels Interessenkonflikt-Fragebogen, ist folgendes zu beachten:

1. Personenkreis

Befragt werden dürfen nur diejenigen Personen im Unternehmen, die von ihrer Stellung her (Vertrauensstellung, Entscheidungsbefugnisse, Informationsstand über vertrauliche betriebliche Informationen etc.) für die hinterfragten Sachverhalte überhaupt in Frage kommen. Personen, die von ihrer Stellung her nicht in diese Loyalitäts- bzw. Interessenkonflikte kommen können, dürfen auch nicht befragt werden.

2. Zulässigkeit der Fragen

Die Zulässigkeit der Fragen bestimmt sich nach allgemeinen arbeitsrechtlichen Grundsätzen und beurteilt sich an der Position des Befragten. Je vertraulicher die Position ist und je höher in der Führungsebene der Befragte angesiedelt ist und je mehr Entscheidungsbefugnisse der Befragte hat, umso umfassendere Fragen sind erlaubt. Dies aber nur, soweit der Arbeitgeber im Hinblick auf die Tätigkeit und den Arbeitsplatz ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Beantwortung hat. Fragen nach den persönlichen Verhältnissen und insbesondere zu seinen Vermögensverhältnissen sind nur dann zulässig, wenn es sich um besondere Vertrauensstellungen handelt, z.B. mit finanziellen Entscheidungsbefugnissen oder der Gefahr der Bestechung oder des Geheimnisverrats.

3. Umfang der Fragen

Man kann zwischen Fragen zu den persönlichen Verhältnissen des Befragten und zu denen seiner Angehörigen unterscheiden. Zu seinen persönlichen Verhältnissen darf natürlich mehr gefragt werden als zu den Verhältnissen seiner Angehörigen. Auch bei einem hohen Missbrauchspotenzial, d.h. bei Führungskräften auf hoher Ebene ist das Hinterfragen von Verhältnissen von Angehörigen sehr problematisch und auf besondere Ausnahmefälle beschränkt. Aber auch in diesen Fällen ist eine undifferenzierte Einbeziehung von Angehörigen in die Befragung unzulässig und auf Personen mit einem besonderen Näheverhältnis beschränkt.

4. Mitbestimmungspflicht

Die Datenerhebungen werden meist in Form von Fragebögen (Personalfragebögen) durchgeführt. Diese Fragebögen sind sowohl bezüglich der Grundfrage der Einführung als auch des Inhalts mitbestimmungspflichtig

Whistleblower-Regelungen

Whistleblower-Regelungen stellen häufig bei der Abwägung des Schutzes der Beteiligten (Whistleblower und Beschuldigter) den Schutz des Whistleblowers deutlich in den Vordergrund. Unter Effektivitätsgesichtspunkten betrachtet (und zum Schutz des Whistleblowers) ist dies zwar nachvollziehbar, das Datenschutzrecht stellt aber ebenso auf den Schutz der Betroffenen ab. Im Spannungsfeld zwischen diesen beiden Schutzbedürfnissen müssen deshalb auch wirksame Maßnahmen zum Schutz des Beschuldigten eingerichtet werden.

Dem allgemeinen Grundsatz des „in dubio pro reo“ (im Zweifel für den Angeklagten) folgend hat auch in einem Whistleblowing-System der Beschuldigte so lang als unschuldig zu gelten,

solange ein Fehlverhalten nicht bewiesen ist. Für das Whistleblowing-System bedeutet dies, dass das gesamte Verfahren an diesem Grundsatz auszurichten ist, dass an jeder Stelle des Verfahrens bis zum Beweis des Gegenteils von der Unschuldsvermutung auszugehen ist und dass die Meldungen im kleinstmöglichen Kreis streng vertraulich zu behandeln sind. Damit wird ein Durchsickern von Hinweisen, Gerüchte im Unternehmen und Nachteile des Betroffenen bei möglicherweise unberechtigten Anschuldigungen vermieden. Dazu gehört auch, dass die Stelle, die die Meldungen entgegennimmt, unabhängig organisiert ist, ein faires und objektives Verfahren betrieben wird und Konsequenzen erst dann gezogen werden dürfen, wenn ein Fehlverhalten bewiesen ist.

Whistleblowing-Verfahren müssen streng vertraulich behandelt werden. Solange kein Fehlverhalten nachgewiesen wurde, gilt für den Betroffenen die Unschuldsvermutung.

Ferner ist zu fordern, dass das zu meldende Fehlverhalten schwerwiegend sein muss und somit also nur solches Verhalten betreffen darf, zu dem der Arbeitgeber ein Weisungsrecht besitzt und an dessen Kenntnis er ein berechtigtes Interesse hat. Damit sind Sachverhalte, die die Privat- oder Intimsphäre der Mitarbeiter betreffen, in einem Whistleblowing-System nicht darstellbar.

Da die Informationen über mögliches Fehlverhalten anonym und ohne Wissen des Betroffenen erhoben werden, gewinnt die Bestimmung des Datenschutzgesetzes zur Benachrichtigungspflicht besondere Bedeutung. Nach dieser Bestimmung muss der Betroffene über die Tatsache der Erhebung und Speicherung der Daten unterrichtet werden. Eine Ausnahme von dieser Unterrichtungspflicht besteht solange, wie durch die Unterrichtung die Geschäftszwecke des Arbeitgebers gefährdet würden und ein schutzwürdiges Interesse des Betroffenen an einer Unterrichtung nicht überwiegt. Wenn also ein begründeter Anfangsverdacht für ein relevantes Fehlverhalten besteht, darf die Unterrichtung des Betroffenen unterbleiben, solange eine Behinderung der Aufklärung (z.B. durch eine Entfernung oder Veränderung von Beweismitteln) zu befürchten ist. Wann die Benachrichtigung durchzuführen ist muss im Einzelfall entschieden werden; sie ist aber im Interesse des Betroffenen, auch unter dem Gesichtspunkt von möglicherweise ungerechtfertigten Anschuldigungen, zum frühestmöglichen Zeitpunkt durchzuführen.

Wird das Whistleblowing-System ausgelagert (z.B. die Hotline), handelt es sich zumindest dann, wenn der Auftragnehmer die technische Plattform zur Verfügung stellt und diese im Wesentlichen darauf beschränkt ist, die Meldungen entgegenzunehmen und aufzubereiten, um eine Datenverarbeitung im Auftrag. In diesem Fall ist der Abschluss einer Datenschutzvereinbarung erforderlich.

Potentialanalyse

Mitarbeiterdaten werden nicht nur zum Zwecke der Personalverwaltung und der Lohn- und Gehaltsabrechnung erhoben und verarbeitet, sondern vielfach auch zum Zwecke der Personalentwicklung und der Förderung des Führungskräftenachwuchses. Es werden in diesen Zusammenhängen oftmals Potentialanalysen erstellt und Mitarbeiterdaten in sog. Förderdateien gespeichert und für Weiterbildungszwecke verarbeitet.

Obwohl man die Erhebung und Verarbeitung der Mitarbeiterdaten für diese Zwecke durchaus im wohlverstandenen Interesse der Mitarbeiter sehen kann, ist im Hinblick auf die hohe Sensibilität der Daten eine **Einwilligung der betroffenen Mitarbeiter erforderlich** (siehe auch Kap. Persönlichkeitsprofile, psychologische Tests, Intelligenztests).

Terrorismuslisten

Zur Bekämpfung des Terrorismus hat die EG zwei „Antiterrorismusverordnungen“ ((EG) Nr. 2580/2001 und (EG) Nr. 881/2002) erlassen. Diese Verordnungen sind, anders als Richtlinien,

unmittelbar geltendes Recht und müssen, weil sie gegenüber dem Datenschutzgesetz Vorrang besitzen, angewendet werden. Diese Verordnungen enthalten Sanktionslisten mit Daten über terrorverdächtige Personen. Nach den Vorschriften dieser Verordnungen müssen juristische Personen, also auch Unternehmen, die Daten von Kunden, Lieferanten, Beschäftigten und sonstigen Geschäftspartnern, an die finanzielle Transaktionen durchgeführt werden, mit diesen Listen abgleichen. So kann die Erteilung eines AEO–Zertifikats von der Bedingung abhängig gemacht werden, dass antragstellende Unternehmen ihre in sicherheitsrelevanten Bereichen tätigen Beschäftigten einer Sicherheitsüberprüfung anhand der sogenannten Terrorismuslisten der Anhänge der o.g. Verordnungen unterziehen. Unzulässig ist ein Abgleich mit außereuropäischen Listen, z.B. mit Listen von Stellen der USA, weil für diese Listen ein rechtsstaatliches Zustandekommen nicht belegt ist.

Andererseits enthalten die Antiterror-Verordnungen nach Ansicht der Aufsichtsbehörden für den Datenschutz nur eine allgemeine Handlungspflicht und verpflichten nicht zu den Screenings. Ein Datenscreenings ist nicht pauschal und anlasslos durchzuführen. Ein Screening der Beschäftigten ist beispielsweise nicht für geboten anzusehen, weil die Banken im Zusammenhang mit der Lohnzahlung gem. Kreditwesengesetz ohnehin Abgleiche mit den Terrorlisten vornehmen.

Technische Kontrollsysteme

Die Möglichkeiten technischer Kontrollsysteme beschränken sich schon lange nicht mehr nur auf Zeiterfassungs-, Zutrittskontroll- oder Videoüberwachungssysteme. Die Unterstützung von Prozessen aller Art durch IT-Technik und die zunehmende Ausstattung von Arbeitsmitteln mit Mikroelektronik hat nicht nur zwangsläufig die Speicherung bestimmter, zur Prozessgestaltung erforderlicher Daten zu Folge. Oft ermöglicht sie – und das ohne Kenntnis der Betroffenen – auch eine Erhebung und Speicherung von überschießenden Daten und deren Nutzung für Zwecke, die im Einzelfall z.T. als grenzwertig bezeichnet werden und in der Summe den Rahmen der Zulässigkeit übersteigen können. Dies gilt insbesondere, wenn Daten aufgrund der vorhandenen technischen Plattformen zusammengeführt und ausgewertet werden können.

Als Beispiele seien der Einsatz von RFID-basierten Systemen in Firmenausweisen, Kantinenabrechnungssystemen (über die mühelos z.B. alle Vegetarier und Rohkostler ermittelt werden könnten), Mobiltelefone, Fahrzeugnavigationssysteme und deren Einsatz im Flottenmanagement, elektronische Fahrtenbücher und Fahrtenschreiber genannt. Hinzu kommen Protokollierungen bei der Benutzung von IT-Systemen und Datenverarbeitungsverfahren sowie bei der Nutzung von E-Mail, Internet und Intranet, über die sich nicht nur das Kommunikationsverhalten der Mitarbeiter ermitteln lässt. Damit eröffnen sich dem Arbeitgeber umfassende technische Kontroll- und Auswertungsmöglichkeiten bis hin zur Erstellung von umfassenden Persönlichkeitsprofilen. Diese können den Rahmen des im Beschäftigungsverhältnis Erforderlichen weit übersteigen und unabhängig von ihrer tatsächlichen Nutzung das Persönlichkeitsrecht der Betroffenen in unzumutbarer Weise beeinträchtigen. Dies umso mehr, als die Betroffenen Art und Ausmaß der möglichen Erhebungen und der Kontrollmöglichkeiten kaum erkennen können.

Ziel aus datenschutzrechtlicher Sicht ist es nicht, den Einsatz dieser Technologien und Systeme zu verhindern, sondern so zu gestalten, dass sie einerseits der Erreichung der berechtigten Zwecke des Unternehmens Genüge tun und andererseits in allen Phasen der Erhebung, Speicherung, Verarbeitung und Nutzung dieser Daten das Persönlichkeitsrecht der Betroffenen und deren berechtigte schutzwürdige Interessen nicht unzumutbar eingeschränkt werden.

Der Einsatz von bestimmten technischen Systemen wie der Videoüberwachung oder von mobilen Speicher- und Verarbeitungsmedien ist im Datenschutzgesetz selbst geregelt. Für den Einsatz von Kommunikationssystemen wie Telefon, E-Mail und Internet sind, soweit eine Nutzung für private Zwecke zugelassen ist, Regelungen im Telekommunikationsgesetz (TKG) zu finden. Der Einsatz anderer Technologien ist unter dem Gesichtspunkt der Erforderlichkeit abzuwägen und auszugestalten. Die Überwachung der IT-Infrastruktur rückt im Hinblick auf die Gewährleistung und Optimierung der Systemverfügbarkeit und der IT-Sicherheit immer mehr

in den Fokus der IT-Administratoren und Sicherheitsverantwortlichen. Zunehmend wird spezielle Software für die Live-Überwachung der technischen Systeme und zur Erkennung aktueller Bedrohungen eingesetzt. Der Einsatz derartiger Software ist einerseits im berechtigten Sicherheitsinteresse des Unternehmens erforderlich, andererseits ermöglicht ein unkontrollierter Einsatz eine beinahe beliebige Kontrolle der Beschäftigten. Für einen in beiderlei Hinsicht angemessenen Einsatz empfiehlt sich deshalb die Erstellung eines Sicherheitskonzepts bzw. einer Protokollierungs- und Überwachungsrichtlinie und deren Abstimmung mit dem Betriebsrat und dem Datenschutzbeauftragten. Da diese Systeme eine Leistungs- und Verhaltenskontrolle ermöglichen, besteht eine Mitbestimmungspflicht und es ist eine Betriebsvereinbarung erforderlich.

Für alle Überwachungssysteme gilt, dass wegen der Möglichkeit einer unzulässigen Verhaltens- und Leistungskontrolle eine Betriebsvereinbarung abgeschlossen werden muss.

Bild- und Videoaufzeichnungen

Datenschutzrelevant ist ein Videoüberwachungssystem nur dann, wenn von der Überwachung natürliche Personen betroffen sind. Werden z.B. nur Produktionsvorgänge an Maschinen ohne Betroffenheit von Personen überwacht, ist das System nicht Gegenstand des Datenschutzes. In allen anderen Fällen verursachen Videoüberwachungssysteme häufig schwerwiegende Eingriffe in das Persönlichkeitsrecht der Mitarbeiter.

Bei der Beurteilung des Einsatzes von Videoüberwachungsanlagen ist zunächst zu unterscheiden, ob öffentlich zugängliche Räume oder unternehmensinterne Bereiche überwacht werden. Zur Aufgabenerfüllung öffentlicher Stellen werden Überwachungssysteme zur Überwachung von öffentlichen Anlagen und Gebäuden, insbesondere im Zusammenhang mit der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, eingesetzt.

Aber auch bei nichtöffentlichen Stellen, z.B. Privatunternehmen, sind öffentlich zugängliche Bereiche vorhanden, z.B. Verkaufsräume, Ausstellungsräume, Hausmessen etc. Bei diesen öffentlich zugänglichen Bereichen kommt es wiederum darauf an, ob Arbeitsplätze überwacht werden bzw. ob es Zweck des Verfahrens ist, die Arbeitsplätze zu überwachen oder zumindest mit zu überwachen oder ob die Mitüberwachung der Arbeitsplätze bzw. deren Einbeziehung in den überwachten Bereich lediglich ein – möglicherweise sogar unvermeidbarer – Nebeneffekt ist und die Überwachung anderen Zwecken dient.

Bei der Videoüberwachung ist grundsätzlich zu unterscheiden, ob es sich bei der Überwachung um öffentlich zugängliche oder unternehmensinterne Räume handelt.

Die Videoüberwachung von öffentlich zugänglichen Räumen ist im Datenschutzgesetz geregelt und ist zulässig

- zur Aufgabenerfüllung öffentlicher Stellen,
- zur Wahrnehmung des Hausrechts oder
- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.

Im Bereich der Privatwirtschaft und dem Mitarbeiterdatenschutz greift das Datenschutzgesetz bei der Überwachung von öffentlich zugänglichen Betriebseinrichtungen, zur Wahrung des Hausrechts oder zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke.

Öffentlich zugänglich sind Räume, die von ihrer Bestimmung und von ihrem Zweck her für die Öffentlichkeit eingerichtet sind, z.B. Verkaufs- oder Ausstellungsräume. Nicht öffentlich

zugänglich sind Räume oder Unternehmensbereiche, für die ein Zugang für betriebsfremde Personen nicht vorgesehen ist bzw. die nicht für den öffentlichen Zutritt bestimmt sind. Dazu gehört das interne Betriebsgelände und auch die Gebäude des Unternehmens. Es spielt dabei keine Rolle, ob diese Bereiche durch einen Zaun umfriedet sind. Es muss aber schon erkennbar sein, dass es sich hier um ein Firmengelände handelt. Das Datenschutzgesetz spricht zwar von öffentlich zugänglichen Räumen, dies ist aber im Sinne von Bereichen zu verstehen. Entscheidend ist deshalb nicht die räumliche Abgeschlossenheit, sondern eine für den Benutzer erkennbare berechtigte öffentliche Zugänglichkeit. Dies ist z.B. in Museen oder Kaufhäusern, Verkaufsräumen, Tankstellen, aber auch bei Messen und Ausstellungen der Fall. Sind in derartigen öffentlich zugänglichen Bereichen Arbeitsplätze von Mitarbeitern eingerichtet oder bewegen sich Mitarbeiter in diesen Bereichen, können bezüglich der Videoüberwachung und der Nutzung der Videoaufzeichnungen nur die Vorschriften des Arbeitnehmerdatenschutzes Anwendung finden.

Wahrung des Hausrechts

Im Rahmen des Hausrechts kann eine Videoüberwachung sowohl zum Schutz der betrieblichen Anlagen als auch zum Schutz der Beschäftigten gegen Einwirkungen, Eindringen und Schädigungen von außen zulässig sein. Rechtsgrundlage für die Anwendung des Hausrechts ist das Bürgerliche Gesetzbuch. Danach kann derjenige, der das Recht hat, die Räumlichkeiten zu nutzen, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen. Dieses Hausrecht kann auch dann ausgeübt werden, wenn die Bereiche allgemein zugänglich sind. Allerdings darf das Hausrecht nicht willkürlich ausgeübt werden. Besteht ein Grund für die Ausübung des Hausrechts, darf der Berechtigte die Einhaltung des Hausrechts auch mit geeigneten Mitteln überwachen und nach den zum Einsatz von Videoüberwachungsanlagen entwickelten Grundsätzen auch eine Videoüberwachungsanlage einsetzen. Anwendung kann das Hausrecht finden z.B. zur Abwehr von Einbrüchen, bei drohendem Vandalismus und sonstigen Übergriffen von außen, z.B. bei Unternehmen, die im kritischen Fokus der Öffentlichkeit stehen.

Räumlich reicht das Hausrecht bis an die Grundstückgrenze bzw. an die Grenze des unter das Verfügungsrecht des Eigentümers bzw. Pächters reichenden Bereiches. Bereiche außerhalb des Firmenbereiches, z.B. vorgelagerte allgemein zugängliche Bereiche wie Gehsteige, Straßen oder Nachbargrundstücke fallen nicht mehr unter das Hausrecht und können deshalb mit einer Berufung auf die Ausübung des Hausrechts nicht bzw. nur in extremen Ausnahmefällen bei Vorliegen besonderer Risiken überwacht werden. Das Hausrecht kann sich auch während der Arbeitszeit nicht gegen Mitarbeiter richten, weil sich diese befugt in den geschützten Bereichen aufhalten und sich i.d.R. zur Erfüllung ihrer Arbeitsleistung auch dort aufhalten müssen.

Berechtigtes Interesse

Das berechtigte Interesse des Arbeitgebers zur Videoüberwachung kann sich aus Sicherheitsinteressen, der Diebstahlüberwachung bzw. Diebstahlprävention oder zur Wahrnehmung sonstiger berechtigter Interessen für konkret festgelegte Zwecke ergeben. Bei den sonstigen berechtigten Interessen müssen zwei Voraussetzungen erfüllt sein:

1. Es muss sich um berechtigte Interessen des Unternehmens, z.B. vor dem Hintergrund einer objektiv anzuerkennenden Gefährdungslage, handeln. Diese Interessen können sowohl ideeller, rechtlicher als auch wirtschaftlicher Natur sein.
2. Die konkreten Zwecke, für die die Überwachungsanlage eingerichtet werden soll, müssen vor ihrer Inbetriebnahme festgelegt und dokumentiert werden.

Das berechtigte Interesse als Rechtsgrundlage für eine Videoüberwachung greift nur für nichtöffentliche Stellen. Nach dem Willen des Gesetzgebers, den Einsatz der Videotechnik aufgrund des Überwachungscharakters und der damit verbundenen Grundrechtsrelevanz möglichst einzuschränken, ist der Umfang des berechtigten Interesses jedoch eng auszulegen. Der Einsatz lässt sich deshalb insbesondere im Zusammenhang mit

Diebstahlschutz und konkreter Diebstahlprävention und zur Gefahrenabwehr, z.B. in Banken, begründen.

Erforderlichkeit

Voraussetzung für die Zulässigkeit einer Videoüberwachungsanlage ist in allen Fällen nicht nur, dass es sich bei dem verfolgten Zweck um einen von unserer Rechts- und Gesellschaftsordnung anerkannten legitimen Zweck handeln muss. Die Videoüberwachung muss zur Erreichung dieses Zweckes auch erforderlich sein. Das Kriterium der Erforderlichkeit bedeutet, dass kein anderes geeignetes Mittel zur Zweckerreichung zur Verfügung stehen darf, dass weniger tief in das Persönlichkeitsrecht der Betroffenen eingreift. Dieses Kriterium der Erforderlichkeit ist auch an die einzelnen Ausstattungsmerkmale des Überwachungssystems anzulegen.

Eine Videoüberwachung ist nur dann zulässig, wenn kein anderes, milderes Mittel zur Verfügung steht, mit dem derselbe Zweck in angemessener Weise erreicht werden kann.

Kennzeichnung der Überwachung

Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Bei den Aufnahmekameras selbst (oder bei größeren Bereichen mit mehreren Kameras an den Eingängen) muss an gut sichtbarer Stelle ein Hinweis auf die Videoüberwachung angebracht werden. Der Hinweis muss die für die Überwachung verantwortliche Stelle mit Anschrift angeben und eine Kontaktmöglichkeit (z.B. eine Telefonnummer) enthalten, unter der sich die Betroffenen über die Zwecke und die näheren Umstände der Videoüberwachung informieren können. Eine verdeckte Videoüberwachung ist grundsätzlich unzulässig und wurde bisher von den Gerichten nur in besonderen Ausnahmefällen und als vorübergehende Maßnahme für zulässig gehalten, z.B. wenn die verdeckte Überwachung das letzte und einzige noch verfügbare Mittel war, um Diebstähle aufzuklären.

Zuordnung zu einer Person

Werden die Videoaufnahmen einer bestimmten Person zugeordnet, d.h. die Aufzeichnungen werden ausgewertet und die betroffenen Personen werden nicht nur zufällig und beiläufig, sondern gezielt identifiziert, müssen diese Personen über die anschließende Verarbeitung oder Nutzung dieser konkret personenbezogenen Aufzeichnungen unterrichtet werden. Die Benachrichtigung ist vorzunehmen, wenn die betroffene Person identifiziert wird und sich daran eine personenbezogene Verarbeitung oder Nutzung der Aufzeichnungen anschließt. Sie ist zum frühestmöglichen vertretbaren Zeitpunkt vorzunehmen, wobei es im berechtigten Interesse der verantwortlichen Stelle liegt, den Zweck der Beobachtung und Aufzeichnung nicht durch eine zu frühe Benachrichtigung zu gefährden. Die in einer eventuellen Betriebsvereinbarung getroffenen Regelungen sind zu beachten.

Löschung der Aufzeichnungen

Die Daten (d.h. Videoaufzeichnungen) sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Wird die Anlage z.B. zur Gewährleistung der Sicherheit der Firmenanlagen betrieben und war der vergangene Tag unauffällig, besteht keine Legitimation für eine weitere Speicherung und die Aufzeichnungen sind zu löschen. Sind nur einzelne Aufnahmen verdächtig, dürfen auch nur diese solange gespeichert werden, bis der Vorgang aufgeklärt ist oder die Aufzeichnungen in einem anschließenden Verfahren nicht mehr als Beweismittel benötigt werden.

Biometrische Daten

Biometrische Daten oder biometrische Muster werden zunehmend zur Authentifizierung von Berechtigten an Computersystemen oder anstelle von Magnetkarten zur Identifizierung im Rahmen von Zutrittskontrollsystemen eingesetzt. Zu den biometrischen Daten bzw. Verfahren gehören z.B. Stimm- und Gesichtserkennung, Fingerabdruck, Iris- und Venenerkennung, Erkennung von Unterschriften und Tippmuster.

Die biometrischen Daten gehören zu den besonderen Datenarten im Sinne des Datenschutzgesetzes. Dies erklärt sich daraus, dass je nach Verfahren und Art der Daten auch Rückschlüsse auf Rasse und Gesundheit gezogen werden können. So kann z.B. bei der Gesichtserkennung auf die Rasse und bestimmte gesundheitliche Umstände und bei der Stimm-, Venen- oder der Iriserkennung auch auf bestimmte gesundheitliche Einschränkungen geschlossen werden, was z.B. beim Fingerabdruckverfahren wieder nicht möglich ist. Diese Rückschlussmöglichkeiten stellen noch dazu sog. überschießende Informationen dar, die für die Erreichung des Unternehmenszwecks überhaupt nicht erforderlich sind, aber ausgewertet werden könnten. Hinzu kommen die Dauerhaftigkeit und Unveränderbarkeit dieser Daten, denn sie ermöglichen auch nach Jahrzehnten noch eine Identifikation der betroffenen Personen.

Die Zulässigkeit von biometrischen Verfahren ist zu prüfen; ein solches ist zulässig, wenn es zur Durchführung des Arbeitsverhältnisses erforderlich ist. Im Rahmen der Erforderlichkeit ist das Interesse des Arbeitgebers (z.B. an der höheren Sicherheit der biometrischen Verfahren) gegen das schutzwürdige Interesse der Betroffenen abzuwägen. Dabei ist genau das Verfahren zu wählen und nur dieses zulässig, dass im Hinblick auf die Erforderlichkeit des Einsatzes von biometrischen Verfahren den geringstmöglichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verursacht. Unter diesen Gesichtspunkten sind folgende Kriterien als Zulässigkeitsvoraussetzungen für biometrische Verfahren zu beachten bzw. anzustreben:

- Es darf kein anderes, milderes Mittel geben, mit dem sich der angestrebte Zweck mit dem gleichen Erfolg und der gleichen oder angemessenen Sicherheit erreichen lässt. Gibt es ein derartiges Verfahren und ist es mit vertretbaren Mitteln einsetzbar, verbieten sich biometrische Verfahren schon unter dem Gesichtspunkt der Erforderlichkeit.
- Eine verdeckte Überwachung bzw. Personenerkennung lediglich im Vorbeigehen (z.B. bei einer Gesichtserkennung oder bei Speicherung von Biometriedaten auf einem RFID-Chip möglich) ist unzulässig. Der Betroffene muss durch eine aktive Handlung mitwirken, denn nur so ist für ihn der Vorgang der Identifizierung erkennbar.
- Überschießende Informationen, die Rückschlüsse oder vermeintliche Rückschlüsse auf sonstige Verhältnisse der Person (z.B. auf Rasse oder Gesundheit) erlauben, dürfen nicht erhoben und gespeichert oder genutzt werden.
- Soweit möglich, sollten die biometrischen Daten nicht im Klartext, sondern anonymisiert als Referenzdaten gespeichert werden.
- Biometrische Daten (z.B. der Fingerabdruck) sollten nach Möglichkeit auf dem Datenträger des Betroffenen und nicht in einem zentralen System des Arbeitgebers gespeichert werden. Beim Ausscheiden oder einer Änderung des Verfahrens kann dann der Betroffene diesen Datenträger und damit seine biometrischen Daten selbst vernichten.
- Das Verfahren muss transparent gestaltet werden, d.h. die Betroffenen müssen über die Funktionsweise des Verfahrens, die Art und Weise der Datenerfassung und über die Art der gespeicherten Daten unterrichtet werden. Die Beteiligungsrechte der Mitarbeitervertretung müssen beachtet werden.

RFID-Einsatz

Mittels der RFID-Technik (Radio Frequency Identification) können anhand von Funksignalen aus miniaturisierten Transpondern, die z.B. in Ausweisen für Zutrittskontrollsysteme, in Hausausweisen oder auch in Etiketten von Produkten eingebaut sind, Daten ausgelesen werden. Werden entsprechende Lesegeräte installiert, können damit auch engmaschige Bewegungsprofile erzeugt werden (ohne dass die Betroffenen dies erkennen können), die dann den Rahmen des eigentlich berechtigten Zweckes übersteigen. Dies kann z.B. bei der Steuerung von Zutrittsberechtigungen oder im Rahmen eines Zeiterfassungssystems der Fall sein.

Vor einem Einsatz von RFID-Systemen müssen deshalb die Verarbeitungszwecke, die Art der erhobenen und gespeicherten Daten sowie deren Nutzung beschrieben werden. Da diese Systeme auch eine unzulässige Leistungs- und Verhaltenskontrolle ermöglichen, ist die Mitbestimmungspflicht des Betriebsrats zu beachten. Die Systeme sind so zu gestalten, dass die Kontrollen nur durch Mitwirken der Mitarbeiter oder sonst erkennbar und nicht heimlich stattfinden und die Mitarbeiter keiner Totalkontrolle unterworfen werden. Da technisch auch die Möglichkeit besteht, betriebsfremde RFID-Chips zu lesen und damit unzulässige Daten zu erheben, muss auch gewährleistet sein, dass nur die zulässigen Etiketten gelesen werden können.

Soweit auf den Transpondern eine Verarbeitung stattfindet, also Daten nicht nur gelesen, sondern auch geändert oder neue Daten gespeichert werden können, sind die Vorschriften des Datenschutzgesetzes zu mobilen Datenträgern zu beachten. Danach müssen die Beschäftigten in allgemein verständlicher Form über die Funktionsweise des Mediums, über ihre Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrechte und über Maßnahmen bei Verlust oder Zerstörung unterrichtet werden. Ferner müssen Kommunikationsvorgänge, die auf dem Medium eine Verarbeitung auslösen, für die Betroffenen erkennbar sein und es müssen unentgeltlich in einem angemessenen Umfang Lesegeräte zur Verfügung gestellt werden, damit die Betroffenen durch Auslesen des Inhalts ihr Auskunftsrecht wahrnehmen können.

GPS-Geräte und Handyortung

Mobiltelefone und GPS-Navigationsgeräte ermöglichen es, den Standort der Betroffenen festzustellen. Damit besteht zumindest die technische Möglichkeit, z.B. über Außendienstmitarbeiter oder Fahrpersonal durch Übertragung der Standortdaten Bewegungsprofile zu erzeugen, aber auch Zündstatus, Sensorzustände, Fahrtrichtung und hausnummerngenaue Position des Fahrzeuges ließen sich überwachen. Diese Funktionen werden z.B. von Speditionen in Flottenmanagementsystemen zur Ortung von Fahrzeugen genutzt aber auch Lenk- und Standzeiten.

Die datenschutzrechtliche Zulässigkeit der Ortung mittels GPS-Technik ist nach den Regelungen des Datenschutzgesetzes zu beurteilen; d.h. die Erfassung und Verarbeitung dieser Daten ist zulässig, wenn sich die Notwendigkeit aus den Anforderungen des Beschäftigungsverhältnisses ergibt. Eine Zulässigkeit dieser Überwachung lässt sich z.B. bei Geld- und Werttransporten begründen oder zur Überwachung von Fuhrparks zur Verfolgung von Autodiebstählen. Aber auch hier ist keinesfalls eine Totalüberwachung zulässig, d.h. der Betroffene muss die Überwachung auch ausschalten können, ohne Nachteile befürchten zu müssen. Ferner muss der Betroffene über die Art und Weise der Überwachung, die Überwachungsintervalle und die Speicherung und Nutzung der Daten unterrichtet werden. Heimliche und überraschende Kontrollen sind unzulässig; es sei denn, sie sind ausnahmsweise zur Aufdeckung vermuteter Straftaten erforderlich.

Ähnliche Grundsätze sind auch bei der Ortung von Mobiltelefonen anzuwenden. Auch hier muss sich die Notwendigkeit einer Ortung aus den Anforderungen des Beschäftigungsvertrags ergeben. Die Überwachung muss für den Betroffenen erkennbar sein und er muss über die Art und Weise der Überwachung und über die Zwecke, für die die Daten genutzt werden sollen, unterrichtet werden. Eine besondere Unterrichtungspflicht ergibt sich bezüglich der Ortung von Mobilfunkgeräten aus dem Telekommunikationsgesetz, wonach der Teilnehmer (d.h. der Arbeitgeber) die Mitbenutzer (d.h. die Arbeitnehmer) über die erteilte Einwilligung zur Erfassung

von Standortdaten unterrichten muss. Eine Totalüberwachung ist wegen des unzumutbar hohen Überwachungsdrucks auch hier unzulässig und wohl auch nur in den seltensten Fällen (z.B. bei Geld- und Werttransporten) erforderlich. Selbstverständlich unterliegt der Einsatz derartiger Systeme auch der Mitbestimmung. Soweit kein Betriebsrat eingerichtet ist, sind andere Regelungen, z.B. in der Form von Richtlinien über den Einsatz dieser Systeme erforderlich.

Bei beiden Überwachungssystemen müssen Funktionen vorhanden sein, die eine vollständige Abschaltung der Ortungsfunktion ermöglichen, um eine Überwachung in der Freizeit und bei einer Nutzung für private Zwecke auszuschließen. Dies ist z.B. der Fall, wenn ein Firmenfahrzeug oder ein Mobiltelefon auch in der Freizeit für private Zwecke genutzt werden darf.

Ist die Privatnutzung von Fahrzeugen oder Mobiltelefonen gestattet, muss eine Deaktivierung der Ortungsfunktion im Privatbereich vorgenommen werden können.

Offenbarungen an den Betriebsrat

Der Betriebsrat hat nach den Vorschriften des Betriebsverfassungsgesetzes umfangreiche Aufgaben, Schutzaufträge, Förderungspflichten und Mitbestimmungsrechte wahrzunehmen. Um diese Aufgaben wahrnehmen zu können, ist der Arbeitgeber verpflichtet, den Betriebsrat rechtzeitig und umfassend zu unterrichten und auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Der Betriebsausschuss hat auch das Recht, in die Listen über Bruttolöhne und Gehälter Einsicht zu nehmen.

Vor diesem Hintergrund besteht für das Unternehmen die Pflicht, den Betriebsrat rechtzeitig und umfassend, soweit zur Durchführung seiner Aufgaben, Rechte und Kontrollfunktionen oder des Mitbestimmungsrechts erforderlich – zu informieren. Dies entspricht auch den Grundsätzen des Datenschutzgesetzes, nach denen bei jeder Übermittlung bzw. Offenbarung von personenbezogenen Daten nur diejenigen Daten offengelegt werden dürfen, die zur Erfüllung der jeweiligen Aufgaben, hier der Aufgaben des Betriebsrates erforderlich sind. Die Unterrichtung durch den Arbeitgeber muss so umfassend sein, dass der Betriebsrat in eigener Verantwortung prüfen kann, ob sich für ihn Aufgaben ergeben, und ob, ggf. inwiefern er tätig werden muss, um seine Aufgaben und Rechte nach den Vorschriften des Betriebsverfassungsgesetzes wahrzunehmen.

Nach diesen Grundsätzen kann der Betriebsrat eine Übersicht über alle Datenverarbeitungsverfahren bzw. Dateien verlangen, in denen Daten über die Beschäftigten gespeichert sind, einschließlich eventueller Auftragnehmer, von denen diese Daten im Wege einer Datenverarbeitung im Auftrag verarbeitet werden. Dazu gehören auch Informationen über technische und organisatorische Maßnahmen zum Datenschutz. Hier bietet es sich an, dem Betriebsrat Zugang zum internen Verfahrensverzeichnis zu gewähren.

Sonstige rechtliche Rahmenbedingungen

Der Betriebsrat ist dem Unternehmen gegenüber nicht Dritter i.S.d. der Datenschutzgesetze, sondern Teil des Unternehmens. Als solches Unterliegt der Betriebsrat genauso wie andere Stellen im Unternehmen den Vorschriften des Datenschutzgesetzes, d.h. er darf personenbezogene Daten nur in dem Umfang erheben (vom Unternehmen verlangen) wie es zur Erfüllung seiner Aufgaben erforderlich ist und er darf diese Daten auch nur in diesem Rahmen speichern, verarbeiten, nutzen und offenbaren. Da der Datenfluss vom Unternehmen an den Betriebsrat häufig zumindest in Form von Auszügen aus automatisiert geführten Datenbeständen geschieht, fallen diese Daten unter den Schutz des Datenschutzgesetzes. Aus der Sicht des Unternehmens handelt es sich bei diesen Weitergaben um eine Nutzung der Daten. Einerseits unterliegt der Betriebsrat dem Datengeheimnis, andererseits gelten für die Mitglieder des Betriebsrates auch besondere Verschwiegenheitspflichten nach dem Betriebsverfassungsgesetz.

Auskunftsanspruch des Betriebsrates bei Abmahnungen

Der Betriebsrat hat zur Wahrnehmung seiner Aufgaben nach dem Betriebsverfassungsgesetz keinen Anspruch auf Vorlage aller Abmahnschreiben bzw. auf eine Unterrichtung über alle erteilten oder beabsichtigten Abmahnungen, weil nicht bei allen Abmahnungen ein Mitbestimmungsrecht des Betriebsrates gegeben ist. So sind etwa bei Arbeitsvertragsverletzungen wie Tätlichkeiten oder Beleidigungen Mitbestimmungsrechte des Betriebsrats offensichtlich nicht berührt.

Personalratsanhörung bei Kündigung

Der Arbeitgeber hat dem Betriebsrat die Personalien des zu kündigenden Arbeitnehmers, die Kündigungsgründe, die Kündigungsart (ordentliche oder fristlose Kündigung) und die Beschäftigungsdauer mitzuteilen.

Einstellungen

Der Arbeitgeber muss den Betriebsrat bei allen mitbestimmungspflichtigen Einstellungen unterrichten. Dazu gehören u.a. unbefristete und befristete Beschäftigungsverhältnisse, Ausbildungsverhältnisse, Umwandlungen von befristeten in unbefristete Beschäftigungsverhältnisse, Übernahme von Auszubildenden in ein Beschäftigungsverhältnis, Übernahme von Leiharbeitnehmern u.a. Auch ein kurzfristiger Einsatz eines Leiharbeitnehmers ist mitbestimmungspflichtig. Der Arbeitgeber muss dem Betriebsrat auch hier deren Namen mitteilen.

Vorlegen muss der Arbeitgeber die Bewerbungsunterlagen aller Bewerber. Zu den Bewerbungsunterlagen zählen Bewerbungsschreiben, Zeugnisse, Teilnahmebestätigungen, Lebenslauf, Angaben über den Gesundheitszustand u.ä., ebenso Personalfragebögen, Ergebnisse von Eignungs- und Einstellungstests oder Einstellungsprüfungen und auch solche Unterlagen, die der Arbeitgeber anlässlich der Bewerbung über die Person des Bewerbers erstellt hat, sowie Angaben zur vorgesehenen Eingruppierung. Der Betriebsrat kann nicht die Teilnahme an Einstellungsgesprächen verlangen, wenn jedoch das Einstellungsgespräch ausschlaggebend für die Einstellung ist, kann der Betriebsrat eine Darlegung verlangen, warum dieser Bewerber nach seiner Einschätzung besser ist als die anderen Bewerber anderen.

Sozialauswahl bei Kündigungen

Der Betriebsrat kann keine vollständige Auflistung der Sozialdaten aller objektiv vergleichbaren Beschäftigten verlangen, vorlegen muss er jedoch die Personaldaten der von ihm für vergleichbar gehaltenen Beschäftigten und die von ihm praktizierten Abwägungskriterien. Dazu gehören die Dauer der Betriebszugehörigkeit, das Lebensalter, eventuelle Unterhaltspflichten und Schwerbehinderung.

Daten über Jubiläen, Geburtstage etc.

Betriebsräte wünschen von der Personalabteilung des Öfteren Daten über Geburtstage oder Jubiläen der Beschäftigten, um gratulieren zu können. Für eine Offenbarung dieser Daten an den Betriebsrat ist keine Rechtsgrundlage vorhanden, weil diese Offenbarung zur Durchführung des Beschäftigungsverhältnisses nicht erforderlich ist. Andererseits wird hierfür keine formelle Einwilligung für erforderlich gehalten. Es genügt, wenn die Beschäftigten über die Tatsache von Offenbarungen aus diesen Anlässen unterrichtet ist und ihnen Gelegenheit gegeben ist, gegen solche Offenbarungen zu widersprechen.

Daten über Ausscheiden von Beschäftigten

Termine über das Ausscheiden von Beschäftigten aus dem Beschäftigungsverhältnis dürfen dem Betriebsrat offenbart werden. Diese Offenbarungen sind im Rahmen der Durchführung des Beschäftigungsverhältnisses vertretbar.

Verzeichnis über alle Beschäftigten, die die Voraussetzungen für ein betriebliches Eingliederungsmanagement erfüllen

Der Betriebsrat kann quartalsmäßig ein Verzeichnis über alle Mitarbeiter verlangen, die im zurückliegenden Jahr die Voraussetzungen für ein betriebliches Eingliederungsmanagement erfüllt haben. Die Einwilligung der Betroffenen ist dafür nicht erforderlich. Für die Ausübung seines gesetzlichen Überwachungsrechts muss der Betriebsrat diesen Personenkreis kennen; einer namentlichen Benennung stehen weder datenschutzrechtliche Gründe entgegen.

Aufdeckung von Straftaten

Gemäß § 26 Abs. 1 Satz 2 BDSG dürfen personenbezogene Daten eines Beschäftigten zur Aufdeckung von Straftaten erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung oder Nutzung nicht überwiegt und insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Nach dem Wortlaut des Gesetzes muss es sich um eine Straftat handeln. Das Vorliegen einer Ordnungswidrigkeit im Sinne des Ordnungswidrigkeitengesetzes reicht für die Anwendung dieser Vorschrift nicht aus. Ferner muss es sich bei dem Verdacht um eine Straftat im Arbeitsverhältnis handeln, z. B. um Diebstahl oder Korruption. Eine außerhalb des Beschäftigungsverhältnisses begangene Straftat, z. B. im privaten Lebensbereich, rechtfertigt keine Datenerhebung durch den Arbeitgeber.

Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten Beschäftigter ist nur zulässig, wenn der Verdacht besteht, dass die Straftat bereits begangen worden ist, also die Tat vollendet ist. Präventivmaßnahmen zur Verhinderung möglicher Straftaten lassen sich auf diese Bestimmung nicht stützen, können aber nach § 26 Abs. 1 Satz 1 BDSG zulässig sein. Es müssen tatsächliche Anhaltspunkte vorliegen, die einen Verdacht begründen. Personenbezogene Daten dürfen deshalb zur Aufdeckung von Strafdaten nur dann erhoben werden, wenn der begründete Verdacht besteht, dass die betroffene Person im Arbeitsverhältnis eine Straftat begangen hat. Bloße Verdächtigungen, Gerüchte oder vage Hinweise ohne jeden tatsächlichen Anhaltspunkt zumindest für die konkrete Möglichkeit des Vorliegens einer Straftat reichen nicht aus, um einen Verdacht in diesem Sinne zu begründen.

Auch im Zusammenhang mit der Aufdeckung von Straftaten darf immer nur das mildeste geeignete Mittel gewählt werden, d. h. sowohl von der Art der Kontrolle und der Erhebung der personenbezogenen Daten als auch vom Umfang der Daten her sind nur die Mittel und Erhebungen mit der geringsten Eingriffstiefe in das Persönlichkeitsrecht der Betroffenen zulässig, die für die Zwecke der Aufdeckung der Straftat erforderlich sind.

Als tatsächliche Anhaltspunkte werden zwar nicht schon konkrete Beweise verlangt, aber es müssen hinreichende Anhaltspunkte vorhanden sein, die für die Wahrscheinlichkeit des Vorliegens einer Straftat sprechen. Solche Hinweise können sich z. B. aus Hinweisen aus einem Whistleblowing- Verfahren oder aus Hinweisen aus IT-Protokollen auf sicherheitsrelevante Vorgänge ergeben.

Liegen derartige tatsächliche Anhaltspunkte vor, müssen diese vor Beginn der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Beschäftigtendaten zum Zweck der Aufdeckung der Straftat dokumentiert werden.

Da diese Dokumentation die Rechtfertigung und der Ausgangspunkt für die Überwachungs- bzw. Ermittlungstätigkeit ist, sollten nicht einfach nur die Verdachtsmomente aufgeschrieben, sondern bezüglich ihres Beweiswertes für das Vorliegen einer Straftat auch beurteilt und konkretisiert werden. Nur wenn diese Hinweise dokumentiert und ausreichend konkret und belastbar sind, dürfen weitere Datenerhebungen, Verarbeitungen und Nutzungen vorgenommen werden. Eine unvollständige Dokumentation der Verdachtsmomente führt aber nicht dazu, dass die aus den Überwachungsmaßnahmen gewonnenen Beweise vor Gericht nicht verwertbar sind.

An der Schwere und des Konkretisierungsgrads des Anfangsverdachts sind die weiteren Maßnahmen zur Aufklärung zu messen, denn die Aufklärungsmaßnahmen müssen sich auch im Rahmen der Verhältnismäßigkeit bewegen. So wird z. B. bei einem nur schwachen Verdacht auf eine Straftat eine umfangreiche heimliche Videoüberwachung als unverhältnismäßig zu beurteilen sein.

Auch für die weitere Vorgehensweise ist das Verhältnismäßigkeitsprinzip zu beachten. Nach diesem Grundsatz ist eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten nur zulässig, wenn diese geeignet, erforderlich und angemessen ist. § 26 Abs. 1 Satz 2 BDSG konkretisiert dieses allgemeine Verhältnismäßigkeitsprinzip: Die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Beschäftigungsdaten ist nur zulässig, wenn

die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung der Straftat erforderlich ist,

das schutzwürdige Interesse des Beschäftigten am Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt und

insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Aufnahme von Kontrollen oder Einleitung von Überwachungsmaßnahmen ist grundsätzlich ein Vorgang, der tief in das Persönlichkeitsrecht des oder der Betroffenen eingreift. Dies gilt insbesondere unter dem Gesichtspunkt, dass es sich bei den einzuleitenden Kontrollen in aller Regel um verdeckte Maßnahmen handeln wird. Diese verdeckten Überwachungsmaßnahmen sind nach der ständigen Rechtsprechung der Gerichte der Arbeitsgerichtsbarkeit nur zulässig, wenn keine anderen Maßnahmen zur Verfügung stehen, die weniger tief in das Persönlichkeitsrecht des Betroffenen eingreifen und mit denen der Zweck der Kontrolle ebenfalls erreicht werden kann. Entsprechend eng ist der Handlungsspielraum des Arbeitgebers bei der Bemessung der Maßnahmen auszulegen.

Unter dem Gesichtspunkt der Erforderlichkeit sind solche Maßnahmen nur dann zulässig, wenn kein anderes, milderes Mittel zur Verfügung steht. So sind z. B. anonymisierte Überwachungen immer einer personenbezogenen Überwachung vorzuziehen. Ein Personenbezug darf erst hergestellt werden, wenn die Möglichkeiten einer anonymisierten Überwachung ausgeschöpft sind. Der Einsatz einer Videoüberwachungsanlage ist z. B. nur dann zulässig, wenn sich das Ziel nicht mit einem milderen Mittel erreichen lässt. Beim Einsatz müssen Art, Umfang und Ausmaß der Überwachung auf den notwendigen Umfang beschränkt werden.

Der Umfang des Eindringens in die Privatsphäre des Betroffenen muss in einem angemessenen Verhältnis zu Art und Schwere der möglicherweise begangenen Straftat stehen.

In diese Abwägung ist einerseits die Schwere der Straftat einzubringen, d. h. der Unrechtsgehalt des Rechtsverstoßes, die Höhe des entstandenen Schadens, ob erstmalige Straftat oder Wiederholung; auch das Motiv der Straftat kann eine Rolle spielen. Andererseits ist in diese Güterabwägung die Schwere des Eingriffs der Maßnahme in das Persönlichkeitsrecht des Betroffenen einzubringen. Dabei sind auch die Folgen für den Betroffenen für den Fall zu beurteilen, dass sich am Ende der Verdacht auf eine Straftat nicht bestätigt. Unter diesen Gesichtspunkten sind z. B. Maßnahmen, die tief in das Persönlichkeitsrecht des Betroffenen

eingreifen, einen hohen Überwachungsdruck erzeugen oder schwerwiegende Folgen für den Betroffenen nach sich ziehen können, nur bei entsprechend schweren Straftaten gerechtfertigt.

Ebenso in die Abwägung einzubeziehen sind das Maß, das Gewicht bzw. die Beweiskraft der tatsächlichen Anhaltspunkte. Sind diese Anhaltspunkte zwar für das Vorliegen einer Straftat hinreichend konkret, der Bezug auf einen bestimmten Beschäftigten aber noch relativ unbestimmt, verbieten sich ebenso schwerwiegende oder zu frühzeitige auf eine bestimmte Person ausgerichtete Überwachungsmaßnahmen. Es muss also auch die zu überwachende Person bzw. der zu überwachende Personenkreis mit hinreichender Sicherheit eingegrenzt werden können, um personenbezogene Überwachungsmaßnahmen zu rechtfertigen. Nicht zuletzt muss auch hier der Grundsatz gelten, dass der Betroffene bis zum Beweis einer Straftat als unschuldig zu gelten hat.

Falls Hinweise auf eine unerlaubte Handlung auftreten, sollte, soweit geeignete Mittel zur Verfügung stehen, die weitere Aufklärung anonymisiert durchgeführt werden. Dies ist im Einzelfall z. B. über IT-Systemprotokolle oder Protokolle von Datenbanksystemen möglich. Sind die Hinweise soweit konkret, dass ein Verdacht auf eine rechtswidrige Handlung begründet ist, ist die Rechtsnatur des Verstoßes zu ermitteln. Es ist festzustellen, ob es sich um eine Straftat im Sinne des Strafgesetzbuches handelt oder nicht. Nur wenn eine Straftat vorliegt, sind weitere Maßnahmen auf der Grundlage des § 26 Abs. 1 Satz 2 BDSG zulässig. Handelt es sich um eine Ordnungswidrigkeit, greift § 26 Abs. 1 Satz 2 BDSG nicht. Allerdings können Kontrollen hinsichtlich der Einhaltung von betrieblichen Vorschriften, z. B. von Compliance-Regelungen oder zur Aufklärung von Verstößen gegen derartige Regelungen oder von Ordnungswidrigkeiten auf § 26 Abs. 1 Satz 1 BDSG gestützt werden.

Auch im Zusammenhang mit der Aufdeckung möglicher Straftaten gilt der Grundsatz, dass die anonymisierte Erhebung Vorrang vor einer personalisierten Datenerhebung hat.

Bei Vorliegen einer Straftat müssen vor der Einleitung weiterer Maßnahmen die tatsächlichen Anhaltspunkte, die den Verdacht auf eine Straftat begründen, dokumentiert werden. Folgende Feststellungen sollten getroffen werden:

- Welcher Schaden (Art und Höhe) ist festgestellt worden?
- Um welchen konkreten Rechtsverstoß handelt es sich? Feststellung, dass es sich um eine Straftat im Sinne des StGB handelt und dass die Straftat im Beschäftigungsverhältnis begangen wurde.
- Welche tatsächlichen Anhaltspunkte bzw. Indizien bestehen für die Begründung eines Verdachts?
- Gegen welchen oder welche Mitarbeiter bzw. Kreis von Mitarbeitern richtet sich der Verdacht?
- Welche Mittel, Verfahren oder Methoden sollen zur weiteren Aufklärung angewandt werden, insbesondere welche Daten sollen erhoben und auf welche Weise verarbeitet oder genutzt werden?
- Dabei ist die Abwägung der Mittel gegen das schutzwürdige Interesse des oder der Betroffenen zu dokumentieren. Aus der Abwägung muss hervorgehen, dass auch tatsächlich die mildesten geeigneten Mittel eingesetzt werden.
- Wenn ein Betriebsrat eingerichtet ist, ist der Betriebsrat zu informieren und an den Überwachungsmaßnahmen zu beteiligen.
- Sobald sich herausstellt, dass der Verdacht unbegründet ist, sind alle erhobenen Daten zu löschen und die gesammelten Unterlagen zu vernichten. Dem Transparenzgebot des Datenschutzrechts folgend, sollte der Betroffene über die Maßnahme und über das Ergebnis der Kontrollen unterrichtet werden.

Übermittlung von Personaldaten

Nach der Definition der Datenschutzgesetze liegt eine Datenübermittlung oder Bekanntgabe von personenbezogenen Daten vor, wenn die Daten an einen Dritten weitergegeben werden oder der Dritte Daten, die zur Einsicht oder zum Abruf bereitgehalten werden, einsieht oder abruft. Dritter ist jede Stelle oder Person außerhalb des Unternehmens, z.B. Bankinstitut oder Versicherungsunternehmen. In großen Unternehmen können auch andere Unternehmensbereiche Dritte in diesem Sinne sein.

Nicht Dritte, sondern dem Unternehmen zuzurechnen, sind der Betriebsrat oder auch Unternehmen, die personenbezogene Daten im Auftrag verarbeiten (z.B. ein Steuerberater, wenn er die Lohnabrechnung im Service erledigt oder ein Auftragsrechenzentrum, das die automatisierten Datenverarbeitungsverfahren abwickelt). Bei dieser Auftragsdatenverarbeitung bleibt das Unternehmen Herr der Daten, während bei einer Übermittlung die Daten in den Verantwortungs- und Herrschaftsbereich des Dritten übergehen.

Wird dagegen die Datenverarbeitung im Ausland in einem sog. Drittstaat (Staat außerhalb der EU und des Europäischen Wirtschaftsraumes) durchgeführt, stellt dies immer auch eine Datenübermittlung dar. Die Befugnis zur Datenverarbeitung im Auftrag in Drittländern ist deshalb auch unter den Zulässigkeitsvoraussetzungen einer Datenübermittlung zu beurteilen. Die Art und Weise, wie die Datenübermittlung technisch vorgenommen wird, ist unerheblich. Es spielt also unter rechtlichen Gesichtspunkten keine Rolle, ob die Übermittlung mündlich, telefonisch, schriftlich, durch Übergabe eines elektronischen Datenträgers oder im Wege der Datenübertragung oder Einsichtnahme in einen elektronischen Datenbestand erfolgt.

Die Übermittlung von personenbezogenen Mitarbeiterdaten ist zulässig, soweit sie zur Ausführung des Arbeits- oder Anstellungsvertrags erforderlich ist. Dazu gehören Übermittlungen an Geldinstitute zur Auszahlung des Gehalts, an die Sozialversicherungsträger, Finanzbehörden und andere Stellen, soweit gesetzlich geregelte Meldepflichten bestehen. Unter dem Gesichtspunkt der Wahrnehmung von Rechten und Pflichten aus dem Arbeitsvertrag ist auch eine Offenbarung im erforderlichen Umfang gegenüber Gerichten zulässig.

Datenübermittlungen, für die keine gesetzliche Ermächtigung bzw. Verpflichtung besteht, z.B. zur Wahrung des berechtigten Interesses des Arbeitgebers oder Auskünfte an Versicherungen, sind sehr zurückhaltend zu beurteilen, denn der Arbeitnehmer genießt aus dem Arbeitsvertrag heraus einen hohen Vertrauensschutz. Man wird deshalb in aller Regel zu dem Ergebnis kommen müssen, dass bei Fehlen einer gesetzlichen Übermittlungsbefugnis das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung höher einzuschätzen und eine Einwilligung der betroffenen Mitarbeiter erforderlich ist.

Auskünfte bzw. Übermittlungen sind auch im berechtigten Interesse eines Dritten zulässig. Häufig werden in diesem Rahmen Anfragen und Auskunftsersuchen von Gläubigern und Inkassounternehmen an die Arbeitgeber gerichtet. Bei derartigen Anfragen besteht grundsätzlich keine Auskunftspflicht des Arbeitgebers. Eine Auskunft könnte lediglich dann in Betracht kommen, wenn über die Forderung ein Vollstreckungstitel vorliegt und ohne die Auskunft die Rechtsverfolgung vereitelt oder erheblich erschwert würde, z.B. wenn der Arbeitnehmer unbekannt verzogen ist und der Arbeitgeber Informationen über den Aufenthalt oder den neuen Arbeitgeber besitzt.

Die Übermittlung von personenbezogenen Mitarbeiterdaten ist nur zulässig, soweit dies im Rahmen des Beschäftigungsverhältnisses erforderlich ist. Eine Übermittlung an Dritte zum Zwecke der Werbung oder Marktforschung ist unzulässig.

Die Übermittlung von Mitarbeiterdaten an Branchenauskunftsdienste ist unzulässig. Für Werbung, Markt- und Meinungsforschung dürfen Mitarbeiterdaten im Gegensatz zu Kundendaten ebenfalls nicht übermittelt werden, weil diese Übermittlungen zur Ausführung des

Beschäftigungsverhältnisses nicht erforderlich sind. Damit ist z.B. die Übermittlung von Arbeitnehmerdaten an Versicherungen unzulässig. Dies gilt auch dann, wenn die Versicherung z.B. auf der Grundlage eines Gruppenversicherungsvertrags vorteilhafte Angebote unterbreiten würde. Hier besteht für den Arbeitgeber die Möglichkeit, nach dem Lettershop-Prinzip unter Nutzung seiner Adressdaten den Arbeitnehmern Informationsmaterial zukommen zu lassen. Aber auch dieses Verfahren ist unter dem Gesichtspunkt einer Interessenabwägung zu beurteilen und zurückhaltend zu praktizieren.

Datenübermittlungen innerhalb von Unternehmensgruppen

Innerhalb von Unternehmensverbünden, z.B. innerhalb von Unternehmensgruppen oder Konzernstrukturen, gewinnt die Übermittlung von Mitarbeiterdaten aufgrund der zunehmenden Verflechtung, auch der internationalen Verflechtung, immer mehr an Bedeutung. Innerhalb eines Konzernverbundes sind die einzelnen Unternehmen als verantwortliche Stellen im Sinne des Datenschutzgesetzes anzusehen.

Da das Datenschutzgesetz **kein Konzernprivileg** kennt, sind auch die Unternehmen innerhalb einer Unternehmensgruppe im Verhältnis zueinander als Dritte anzusehen. Auch hinsichtlich der Mitarbeiterdaten besteht insofern keine Privilegierung für eine Datenübermittlung. Da Mitarbeiterdaten als sensible Daten zu beurteilen sind, bedarf es deshalb auch innerhalb von Unternehmensgruppen für eine Datenübermittlung stets einer Rechtsgrundlage. Aufgrund des fehlenden Konzernprivilegs bleibt nur der Rückgriff auf die allgemeinen Rechtsgrundlagen des Datenschutzgesetzes.

Folgende Rechtsgrundlagen stehen für eine Datenübermittlung innerhalb von Unternehmensgruppen zur Verfügung:

- Arbeitsvertrag oder das Anbahnungsverhältnis
- Vorrangige Rechtsvorschriften, ggf. auch eine Betriebsvereinbarung
- Überwiegende berechtigte Interessen der übermittelnden Stelle
- Überwiegende berechtigte Interessen des Datenempfängers
- Eine freiwillige, informierte Einwilligung

Arbeitsvertrag oder Anbahnungsverhältnis

Grundsätzlich kann ein konzernweiter Arbeitsvertrag abgeschlossen werden, der als Grundlage für eine konzernweite Datenübermittlung auf der Grundlage Datenschutzgesetzes dient. Voraussetzung ist allerdings, dass im Arbeitsvertrag bereits der Konzernbezug hergestellt wird. Dies kann dadurch geschehen, dass die Konzernmutter selbst für den Beschäftigten klar erkennbar als Arbeitgeber auftritt oder im Arbeitsvertrag ein konzernweiter Einsatz oder ein Einsatz über die Anstellungsgesellschaft hinaus vereinbart wird. Auf diese ausdrückliche vertragliche Vereinbarung eines konzernweiten Arbeitsvertrages kann bei höherrangigen Führungskräften oder bei sog. High-Potential Mitarbeitern verzichtet werden, wenn sich erkennbar aus ihrem Aufgabengebiet eine konzernweite Tätigkeit ergibt.

Betriebsvereinbarung

Eine Betriebsvereinbarung kann im Einzelfall die Rechtsgrundlage für eine Datenübermittlung innerhalb eines Konzerns bilden. Voraussetzung ist, dass es sich um eine konzernweite Betriebsvereinbarung handelt oder zumindest diejenigen Gesellschaften des Konzerns erfasst, an die Daten übermittelt werden sollen. Eine einseitige Betriebsvereinbarung einer einzelnen Gesellschaft kann ein anderes Unternehmen im Konzern nicht binden. Zu beachten ist auch hier, dass sich die Betriebsvereinbarung im Korridor der grundsätzlichen Zulässigkeit der Datenübermittlung bewegen muss, weil eine rechtlich unzulässige Datenübermittlung auch durch eine Betriebsvereinbarung nicht sanktioniert werden kann. Würde eine Betriebsvereinbarung,

in der Regel unter der Zuständigkeit des Konzernbetriebsrats, im Interesse des Unternehmens oder des Konzerns Datenverarbeitungen oder Datenübermittlungen gestatten, die den Zulässigkeitsrahmen der Datenschutzgesetze überschreiten, wären diese Regelungen unwirksam und könnten keine tragfähige Grundlage für eine Datenverarbeitung oder Datenübermittlung bilden.

Berechtigtes Interesse

Die Möglichkeit einer Datenübermittlung im berechtigten Interesse des Arbeitgebers wird unterschiedlich beurteilt. So scheidet das Vorliegen eines berechtigten Interesses des Arbeitgebers im Sinne Datenschutzgesetzes als Rechtsgrundlage einer Datenübermittlung schon deshalb aus, weil wegen des Fehlens der Erforderlichkeit vom Vorliegen eines überwiegend schutzwürdigen Interesses der Betroffenen am Ausschluss der Verarbeitung auszugehen ist. Eine unternehmensübergreifende Datenverarbeitung sei deshalb nur möglich, wenn eine Einwilligung vorliege.

Andererseits kann ein Personaldatenfluss bei Einhaltung bestimmter Voraussetzungen zulässig sein. Als Grundvoraussetzung ist dabei davon auszugehen, dass durch die Begründung eines berechtigten Interesses, sei es des Arbeitgebers oder (i.d.R.) des Mutterunternehmens, nicht das vom Gesetzgeber ausdrücklich nicht gewollte Konzernprivileg durch die Hintertür eingeführt wird. Das berechtigte Interesse muss deshalb schon mehr enthalten als ein sicher in vielen Fällen und Zusammenhängen vorhandenes allgemeines Informationsinteresse oder ein aus wirtschaftlichen und organisatorischen Gegebenheiten ableitbares Interesse an einer arbeitsteiligen Zusammenarbeit der beteiligten Stellen. Dieses Interesse der Gruppenunternehmen dürfe nicht höher anzusetzen sein als das Interesse der Beschäftigten an der Vertraulichkeit ihrer Daten.

Ein allgemeiner Bedarf an Informationen oder der Wunsch nach arbeitsteiliger Zusammenarbeit der beteiligten Stellen bedingen noch kein berechtigtes Interesse.

Andererseits kann der Anspruch auf Datenschutz der Betroffenen nicht grundsätzlich einer Personaldatenübermittlungen erfordernden, konzerninternen Organisation von Zuständigkeiten im Personalbereich entgegenstehen. Jedenfalls dann, wenn das die Personaldaten empfangende Unternehmen nicht mehr Funktionen erhält, als sie auch dem Arbeitgeber zustehen. Wenn z.B. durch vertragliche Abrede – wie auch bei einer Datenverarbeitung im Auftrag – sichergestellt ist, dass darüberhinausgehende, sich aus dem Interesse der Unternehmensgruppe ergebende Verwendungen nicht vorgenommen werden, können die schutzwürdigen Interessen der Beschäftigten zurücktreten.

Selbstverständlich ist bei dieser Abwägung auch auf die individuelle Schutzbedürftigkeit der Daten abzustellen und zu prüfen, ob der beabsichtigte Übermittlungszweck nicht auch mit anonymisierten oder pseudonymisierten Daten erreicht werden kann.

Angesichts der zunehmenden Globalisierung und internationalen Vernetzung auch von mittelständischen Unternehmen sind innerhalb von Unternehmensstrukturen ein übergreifender Personaleinsatz und eine Zentralisierung von Zuständigkeiten und Datenverarbeitungsverfahren nicht mehr aufzuhalten. Diese Entwicklung zieht nicht nur ein allgemeines organisatorisches und/oder technisches und wirtschaftliches Interesse an bestimmten Datenübermittlungen nach sich, sondern erfordert aus vitalen Unternehmensinteressen heraus auch eine gewisse Flexibilität bei der Übermittlung von personenbezogenen Daten. Diese Entwicklung wird auch nicht mit dem Hinweis auf eine grundsätzliche datenschutzrechtliche Unzulässigkeit von Datenübermittlungen oder auf datenschutzrechtliche Bedenken aufzuhalten sein.

Eine sorgfältige Abwägung des berechtigten Interesses der beteiligten Unternehmen und Berücksichtigung des schutzwürdigen Interesses der betroffenen Mitarbeiter unter Einbeziehung

der Sensibilität der zu verarbeitenden bzw. zu übermittelnden Daten ist ein durchaus gangbarer Weg zum Ausgleich der gegensätzlichen Interessenlage. Selbstverständlich ist die Lösung zu bevorzugen, die den geringstmöglichen Eingriff in das Persönlichkeitsrecht der Betroffenen verursacht. Unter diesen Gesichtspunkten ist einer anonymisierten Übermittlung der Vorzug vor einer personenbezogenen Übermittlung zu geben.

Ein berechtigtes Interesse des Unternehmens, das schutzwürdige Interesse der betroffenen Mitarbeiter und die Sensibilität der Daten sind stets gegeneinander abzuwägen, um eine passende Lösung für die Übermittlung zu finden. Es ist daher immer zunächst zu prüfen, ob der beabsichtigte Übermittlungszweck auch mit anonymisierten oder pseudonymisierten Daten erreicht werden kann.

Selbstverständlich sollten auch die Beachtung der Mitbestimmungs- bzw. Mitwirkungspflichten der Mitarbeitervertretung und deren rechtzeitige Information sein, um die Mitarbeiterinteressen entsprechend zu berücksichtigen. Wo keine Mitarbeitervertretung besteht, müssen die Betroffenen schon im Hinblick auf die Unterrichtungspflicht unterrichtet werden.

Für die übermittelten Daten ist die Zweckbindung zu beachten, d.h. die empfangende Stelle ist darüber zu informieren, dass die übermittelten personenbezogenen Daten nur für den Zweck verarbeitet und genutzt werden dürfen, für den sie übermittelt worden sind. Das Datenschutzgesetz enthält zwar eine Öffnungsklausel für eine Verarbeitung oder Nutzung der übermittelten Daten durch den Empfänger für andere Zwecke, und zwar im Rahmen eines dann anders gelagerten, aber auch im berechtigten Interesse des Empfängers liegenden Zwecks. Da das Datenschutzgesetz keine Einschränkung dieser Öffnungsklausel enthält, ist jeder Datenempfänger trotz Zweckbindung befugt, die Daten wieder für andere berechtigte Zwecke zu verarbeiten und zu nutzen.

Es empfiehlt sich, mit der Zweckbindung einen klaren Rahmen für die zulässige Verarbeitung oder Nutzung der Daten zu schaffen, um diese Endlosschleife für eine Übermittlung zu verhindern.

Mit einer eindeutigen Zweckbindung ist ein klarer Rahmen für die zulässige Verarbeitung und Nutzung der übermittelten Daten zu schaffen.

Datenübermittlung an Behörden, Polizei, Staatsanwaltschaft und Gerichte

Eine Datenübermittlung an Dritte ist zur Durchführung des Beschäftigungsverhältnisses erforderlichen Fällen zur Wahrung berechtigter Interessen Dritter und zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit oder zur Verfolgung von Straftaten zulässig. Für eine Übermittlung an Behörden, Polizei, Staatsanwaltschaft und Gerichte (Rechtsanwälte, Detekteien, Inkassobüros etc. sind nicht einbezogen) kommt diese Vorschrift als Auffangregelung nur zum Zuge, wenn keine spezialgesetzlichen Regelungen für eine Auskunftspflicht vorgehen, z.B. Vorschriften des Sicherheitsüberprüfungsgesetzes, der Gewerbeordnung, der Strafprozessordnung u.a. Neben diesen gesetzlich geregelten Auskunftsansprüchen handelt es sich häufig um Anfragen von Gläubigern, Fürsorgeämtern oder Familiengerichten nach Wohnort, Anstellungsverhältnis im Unternehmen und pfändbaren Gehaltsanteilen. Hier hat der Arbeitgeber das berechtigte Interesse der anfragenden Stelle gegen das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung oder Nutzung abzuwägen.

Da auch bei einer für die anfragende Stelle günstig ausgehenden Abwägung keine Auskunftspflicht besteht, sollte der Arbeitgeber aufgrund seiner Fürsorgepflicht den Arbeitnehmer

darüber unterrichten, seine Einwilligung einholen und die Auskunft auf die unbedingt erforderlichen Angaben beschränken. Eine Auskunft kann beispielsweise in Betracht kommen, wenn über die Forderung ein Vollstreckungstitel vorliegt und die Rechtsverfolgung ohne die Auskunft vereitelt oder gravierend erschwert würde, etwa wenn der Arbeitnehmer mit unbekannter Anschrift verzogen ist, dem Arbeitgeber aber Informationen über die neue Anschrift oder den neuen Arbeitgeber vorliegen.

Die Rechtsgrundlage für das Auskunftsverlangen sollte sich der Arbeitgeber eindeutig belegen lassen und Auskünfte nur aufgrund einer schriftlichen Anfrage erteilen.

Beendigung des Beschäftigungsverhältnisses

Für die Inhalte der Personalakten gelten unterschiedlichste Aufbewahrungsfristen nach steuerlichen, sozialversicherungsrechtlichen und einer Vielzahl einzelrechtlicher Vorschriften. Eine generelle gesetzliche Vorschrift über die Aufbewahrung von Personalunterlagen besteht jedoch nicht.

Soweit keine Aufbewahrungsfristen bestehen, erlaubt das Datenschutzgesetz eine Speicherung von Beschäftigtendaten nur in dem Umfang, wie es zur Durchführung und zur Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Demzufolge sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zweckes ihrer Speicherung nicht mehr erforderlich ist. Andererseits dürfen personenbezogene Daten dann nicht gelöscht werden, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden. In diesen Fällen müssen die Daten gesperrt werden.

Es besteht keine generelle gesetzliche Vorschrift zur Aufbewahrungsfrist von Personalunterlagen.

Innerhalb dieses Erlaubnisrahmens kann der Arbeitgeber die Aufbewahrung der Personalunterlagen nach eigenem Ermessen und Bedarf festlegen. Bei der Regelung der Aufbewahrungsfristen muss aber der Arbeitgeber die Gleichbehandlung aller Arbeitnehmer gewährleisten. Beurteilungskriterien für die Aufbewahrung von Unterlagen kann der Ablauf von Verjährungsfristen von eventuellen Ansprüchen ausgeschiedener Mitarbeiter, die Erforderlichkeit von Unterlagen für außerbetriebliche Rentenansprüche oder zur Ausstellung von Zeugnissen oder sonstigen Bescheinigungen sein.

Grundsätzlich besteht für den Arbeitgeber eine sog. nachwirkende Betreuungspflicht, die bei der Bemessung der Aufbewahrung der Personalunterlagen zu berücksichtigen ist. Unter diesen Gesichtspunkten hat sich in der Praxis eine Aufbewahrung von Personalunterlagen über einen Zeitraum von mindestens zehn Jahren herausgebildet. Diese Frist ist aber nicht pauschal für alle Unterlagen anzuwenden, sondern nur für diejenigen Vorgänge, die noch längerfristig von Interesse sein können. Für Unterlagen ohne jegliches Aufbewahrungsinteresse und ohne Aufbewahrungsfrist gilt die Löschungsverpflichtung.

Ein Anspruch auf Herausgabe der Personalunterlagen nach Beendigung des Beschäftigungsverhältnisses besteht nicht. Art. 15 DSGVO gewährt ein Recht auf Auskunft und auf Erteilung von Kopien der zur Person des Beschäftigten gespeicherten Daten, aber keinen Herausgabeanspruch von Originalunterlagen.

Personenbezogene Daten über Beschäftigte für die Nutzung betrieblicher Kommunikationssysteme, im Internet oder im Intranet wie z.B. Kontaktdaten oder Fotos sind mit dem Ausscheiden zu löschen. Soweit aus betrieblichen Gründen oder Organisationsgründen erforderlich, kann in einzelnen Systemen für eine bestimmte Zeit eine Nachricht hinterlegt werden, dass

diese Person nicht mehr erreichbar ist. Fotos müssen aber aus den Kommunikationsverzeichnissen gelöscht werden, weil sie für diese Informationszwecke nicht mehr erforderlich sind.

Die Speicherung und Nutzung von Fotos oder Videoaufzeichnungen nach dem Ausscheiden stellt sich differenziert dar. Soweit Fotos oder Videoaufnahmen im Zusammenhang mit der **Ausübung der betrieblichen Tätigkeit** hergestellt wurden, z. B. Fotos oder Aufzeichnungen eines Vortrags, den ein Beschäftigter bei einer Firmenveranstaltung gehalten hat, oder Beschäftigte haben bei einer Firmenveranstaltung Gäste bedient, sind diese Tätigkeiten Teil ihrer betrieblichen Tätigkeit und die Aufnahmen stützen sich auf § 26 Abs. 1 Satz 1 BDSG. Zur Vermeidung von Streitigkeiten empfiehlt es sich immer, im Zusammenhang mit einer Einwilligung in die Herstellung von Fotos und Videoaufnahmen, die Nutzungsrechte für den Fall eines Ausscheidens der betroffenen Person aus dem Unternehmen zu regeln. Hat die betroffene Person mit der Einwilligung auch die Befugnis zur Nutzung nach einem Ausscheiden aus dem Unternehmen erklärt, steht diese Einwilligung zumindest dann, wenn keine objektiv berechtigten Gründe für einen Widerruf der Einwilligung bestehen, einer Löschungspflicht und einem Löschungsverlangen entgegen.

Sind personenbezogene Daten, insbesondere Fotos oder Videoaufnahmen eines ausgeschiedenen Beschäftigten, im Zusammenhang mit **Repräsentations- oder Werbezwecken** im Internet veröffentlicht, besteht für die weitere Nutzung meist keine Rechtsgrundlage mehr. Wenn in der Einwilligungserklärung über die weitere Nutzung dieser Fotos oder Videoaufnahmen keine Regelungen getroffen worden sind, müssen diese Fotos oder Videoaufnahmen zumindest dann gelöscht werden, wenn mit diesen Aufnahmen eine Zugehörigkeit zum Unternehmen zum Ausdruck gebracht wird. Daneben kann die Einwilligung ggf. widerrufen und ein Anspruch auf Löschung gem. Art. 17 DSGVO geltend gemacht werden. Allerdings darf dieses Recht nicht schikanös ausgeübt werden und orientiert sich an dem Grundsatz nach Treu und Glauben.

Aufbewahrungsfristen für Daten in der Personalverwaltung und Lohnabrechnung

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Personal			
Arbeitsanweisungen	u.a. Datenschutzanweisungen	10	
Ab- und Anwesenheitsmeldungen		10	
Ab- und Anwesenheitsmeldungen	soweit zur Dokumentation von Zuschlägen für Wochenend- und Nachtarbeit notwendig	6	
Abkürzungs- oder Schlüsselverzeichnisse	 soweit zum Verständnis der Buchführung erforderlich	6 10	
Ablaufdiagramme	soweit zum Verständnis der Buchführung erforderlich	10	
Ablaufprotokolle	soweit steuerlich relevant	6	
Abmahnungen		2	Abmahnungen sind der Personalakte nach Ablauf der Frist zu entnehmen bzw. zu löschen.
Abschlagslisten		10	
Abschlagszahlungen	Unterlagen über z.B. Lohnabschlagszahlungen	10	
Abschlussbuchungsbelege		10	
Abschlussvergütungen (auch Provisionsabrechnungen)	z.B. Zahlung für Abschluss eines Vertrags (z.B. Versicherung)	10	
Abtretung von Forderungen		10	
Aktenvermerke		10	
An-, Ab- und Ummeldungen der Krankenkasse und Ersatzkasse		6	
Anforderrungen für Arbeitskräfte		-	
Anschriftenänderungsmitteilungen		6	
Anstellungsverträge		6	nach Vertragsende
Anwesenheitslisten		10	
Arbeitnehmerversicherungsunterlagen	soweit Buchungsbelege	10	bes. Pflichten im Rahmen der betriebl. Altersversorgung (§5 LStDV)
Arbeitsgerichtvorgänge		10	

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Arbeitsplatzbeschreibung und -bewertungen		-	
Arbeitsunfähigkeitsbescheinigung		4	§ 6 AAG (Aufwendungsausgleichsgesetz)
Arbeitszeitdaten		2	
Arbeitszeitnachweise	Dokumentation der Arbeitszeit, die über die werktägliche Arbeitszeit von 8 Stunden hinausgehen	2	§ 16 Abs. 2 ArbZG (Arbeitszeitgesetz)
Arbeitszeitnachweis (Minijobber und kurzfristig Beschäftigte)	Dokumentation Beginn, Ende und Dauer der täglichen Arbeitszeit spätestens bis zum Ablauf des 7. auf den Tag der Arbeitsleistung folgenden Kalendertages	2	
Arbeitszeitstatistiken	mögl. anonymisiert bzw. pseudonymisiert	-	
Arbeitszeugnis, Beurteilung		3	Arbeitsrecht
Aufenthaltserlaubnis / Beschäftigungserlaubnis	Das Aufenthaltsgesetz verpflichtet Arbeitgeber dazu, sich vor Aufnahme der Beschäftigung zu vergewissern, dass ihre ausländische Mitarbeiterin oder ihr Mitarbeiter dazu berechtigt ist. Arbeitgeber sind verpflichtet, für die Dauer der Beschäftigung eine Kopie des Aufenthaltstitels, der Duldung oder der Aufenthaltsgestattung in elektronischer oder in Papierform aufzubewahren. Bei einem Versäumnis beträgt das Bußgeld bis zu 500.000 Euro.	-	§ 4 Abs. 2 AufenthG
Aufklärung nach Jugendarbeitsschutzgesetz		10	§ 199, Abs. 3, Nr. 1 BGB
Auflösungs-, Aufhebungsvertrag		10	nach Vertragsende
Außendienstabrechnungen		10	
Autokostenabrechnungen		10	
Ausweis (Kopie)	möglich, Kopie auf Grundlage berechtigte Interesse nach Art. 6 Abs. 1 lit. f) DSGVO in Branchen, wo deren Mitarbeiter eine Mitführungspflicht von Personaldokumenten gemäß § 2a Abs. 1 SchwarzArbG prüfen. Bei begründetem Zweifel kann bei Auskunftsanfragen nach Art. 15 DSGVO ein Nachweis über die Identität des Anfragenden verlangt werden.	-	Das Ablichten von Ausweisen, Reisepässe bzw. ID-Cards ist nur mit formgerechter Einwilligung zulässig (§ 20 Abs. 2 PAuswG, § 18 Abs. 3 PaßG) zulässig.
Beitragsabrechnungen zu Sozialversicherungen	Soweit Buchungsbelege (bzgl. der Verjährung sind verschiedene Vorschriften des SGB zu beachten, z.B. bis zum Ablauf des auf die letzte Betriebsprüfung des Rentenversicherungsträgers folgende Kalenderjahr gem. § 28 f I SGB IV)	10	

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Belegschaftsstatistiken		10	
Befristungsvereinbarungen	Als Vertragsbestanteil	10	
Beschäftigungsverzeichnis		10	
Berufsgenossenschaftsunterlagen	soweit Buchungsbelege	10	Die Satzung der jeweiligen Berufsgenossenschaft kann andere Fristen vorschreiben). Nach § 28 f I SGB IV auch bis Ablauf des auf die Prüfung folgenden Kalenderjahres.
Betriebliche Altersvorsorge	Diese Frist gilt, wenn der Versorgungsfall für den Arbeitnehmer **während** des aktiven Arbeitsverhältnisses eintritt oder bis spätestens sechs Jahre nach der letzten Lohnzahlung.	6	
Betriebliche Altersvorsorge	Diese Frist gilt, wenn der Versorgungsfall für den Arbeitnehmer **nach** dem aktiven Arbeitsverhältnis eintritt.	30	
Betriebsunfallunterlagen	Soweit Buchungsbeleg (z.B. bei Betriebsrentenzahlung als Folge des Unfalls)	1	
Betriebliches Eingliederungsmanagement (BEM)	Dokumente, die im Zusammenhang mit dem BEM vorgelegt bzw. in die Akte übernommen oder in einem BEM-Gespräch erstellt werden Für jeden Beschäftigten ist eine eigene, separate BEM-Akte anzulegen (getrennt von der Personalakte).	3	In Absprache und mit Einwilligung des Beschäftigten sollte die Frist festgelegt werden, um bei etwaigen Folgeerkrankungen auf Wunsch des Beschäftigten zugreifen zu können.
Bewerbungsunterlagen, Bewerbungskorrespondenz	Empfohlen wird eine Frist von 6 Monaten, damit ggf. Schadensersatzansprüche aufgrund Ungleichbehandlung nach dem AGG abgewehrt werden können.	-	Bewerbungsunterlagen aus der Personalakte können dem ausscheidenden Mitarbeiter übergeben werden. Alternativ sind sie datenschutzgerecht zu vernichten.
Bezugs- und Lohnbelege, intern		10	
Bonusunterlagen		10	
Bruttolohnlisten		6	
Bruttolohnsammellisten		6	
Bruttolohnstreifen		6	
Beschäftigungsverzeichnis		10	
Code-Pläne	z.B. Schlüsselverzeichnisse	10	
Darlehnsunterlagen, Darlehnsverträge		10	nach Vertragsende
Dauervorschüsse		10	

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Detailfunktionsbeschreibungen		10	
Dienstpläne	Dienstpläne mit handschriftlichen Abänderungen + Unterschriebene Dienstpläne	2	§ 16 (2) ArbZG § 2a Schwarzarbeitbekämpfungsgesetz und das Mindestlohngesetz (MiLoG) sind zu beachten. Nach dem MiLoG muss die tägliche Arbeitszeit aufgezeichnet werden (Dokumentationspflicht), wobei diese Aufzeichnungen zwei Jahre aufzubewahren sind.
Dokumentationen für IT-Programme und -Systeme	An- und Abmeldung von Mitarbeitern an die IT bzw. Änderungen von Benutzerrechten	10	
Doppelbesteuerungsunterlagen, ausländische Steuerbescheide		10	
Einbehaltekonten für Arbeiter und Angestellte		10	
Eingliederungsverträge		10	nach Vertragsende
Erklärungen, eidesstattliche		10	
Fahrgelderstattungsunterlagen		10	
Fahrtenbücher (Geschäftsfahrten)		10	
Fehlerjournale, Fehlerlisten		10	
Fehlerprotokolle		10	
Fehlermeldungen (s. auch Anwesenheitslisten und Fehlzeitenmeldungen)	soweit Lohnbelege	10	
Fehlermeldungen (s. auch Anwesenheitslisten und Fehlzeitenmeldungen)	soweit allgemeiner Teil des Lohnkontos	6	
Forderungsverzicht		10	
Führerschein (Kopie)	Nutzung von Dienstfahrzeugen durch Beschäftigte	-	Anfertigung einer Kopie des Führerscheins ist nicht zwingend erforderlich und zulässig. Zu Nachweiszwecken kann ein Vermerk in der Personalakte hinterlegt werden.

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Führungszeugnis (polizeiliches)	Vorstrafen sind nur dann relevant und Daten hierüber dürfen nur dann erhoben werden, wenn sie einen Bezug zur Tätigkeit des Arbeitnehmers haben. Das wäre vorstellbar bei Mitarbeitern im Bereich von Kassiertätigkeiten und Diebstahl oder bei Kraftfahrern und Verkehrsdelikten. Verkehrsdelikte interessieren aber bei einem Büromitarbeiter nicht. Nur nach solchen für die Tätigkeit relevanten Vorstrafen darf überhaupt gefragt werden.	-	
Führungszeugnis (erweitertes)	*Beispiel:* Träger der öffentlichen Jugendhilfe dürfen keine Personen hauptamtlich beschäftigen oder vermitteln, die einschlägig vorbestraft sind. Auch muss vom Träger sichergestellt werden, dass unter seiner Verantwortung nur neben- oder ehrenamtliche tätige Personen Kinder oder Jugendliche beaufsichtigen, betreuen, erziehen oder ausbilden oder einen vergleichbaren Kontakt haben, die nicht einschlägig vorbestraft sind.	-	Einsichtnahme bzw. Ablage bedarf einer Gesetzesgrundlage, bspw. § 72a SGB VIII
Fürsorgeunterlagen (Arbeiter-Unterstützungskasse, Notstandsbeihilfe etc.)		6	
Geburtsurkunde	Kopie nur mit Einwilligung zulässig	-	§ 10 PStG (Auskunfts- und Nachweispflicht)
Gehalts- und Lohnstrukturerhebungen		-	
Gehaltsabrechnungen		10	
Gehaltsbescheinigungen		10	
Gehaltsbücher	soweit Buchungsbelege	10	
Gehaltsempfängerstammdaten mit Unterlagen		10	
Gehaltsfestsetzungsunterlagen		6	
Gehaltsjournale	soweit Grundbuchfunktion oder Buchungsbelege	10	
Gehaltslisten	Gehaltslisten einschließlich Liste für Sonderzahlungen	10	
Gehaltspfändungsunterlagen		10	
Gehaltsübersichten		-	
Gehaltsverteilung nach Kostenstelle		-	
Gehaltsvorschusskonten		10	
Gesundheitsausweis / Nachweis Belehrung	Die Bescheinigung und die letzte Dokumentation der Belehrung sind beim Arbeitgeber aufzubewahren.	-	§§ 42 f. IfSG (Infektionsschutzgesetz)
Gleitzeitunterlagen		10	

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Gratifikationen	soweit Buchungsbelege	10	
Eheurkunde	Kopie nur mit Einwilligung zulässig	-	§ 10 PStG (Auskunfts- und Nachweispflicht)
Jahreslohnnachweise für Berufsgenossenschaften		6	
Kilometergeldabrechnungen		6	
Kindergeldunterlagen für Angestellte und Arbeiter		6	
Kostenstatistiken		-	
Kostenträgerpläne		-	
Krankengeldzuschussunterlagen		10	
Krankenkassenbeitragsabrechnung	Sozi, Beitragsnachweise für Krankenkasse (personenbezogen Abrechnung der MA)	10	Aufbewahrungspflichtig auch nach DEÜV
Krankenversicherungskarte / elektronische Gesundheitskarte (Kopie)	Kopie nur mit Einwilligung zulässig	-	
Kurzarbeitergeldanträge		6	an Agentur für Arbeit
Kurzarbeitergeldlisten		6	
Leihverträge		10	nach Vertragsende
Lohn- und Gehaltsstatistiken		-	
Lohnabrechnungen		10	
Lohn und Gehalt, Unterlagen zu …		10	
Lohnaufteilungsblätter	Berufsausbildungsbeihilfe	-	
Lohnvorkalkulationsunterlagen		-	
Lohnvorschüsse, Anträge		-	
Mehrarbeitsstundennachweise	soweit Buchungsbeleg	10	
Mehrarbeit, Verzeichnis der Arbeitnehmer die in eine Verlängerung der Arbeitszeit gemäß § 7 Abs. 7 ArbZG eingewilligt haben.		2	§ 16 (2) ArbZG
Monatsberichte, intern		-	
Mutterschaftsgeldunterlagen		10	

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Nettolohnberechnungen		10	
Niederschriften, Gewährung von Prämien für Verbesserungsvorschläge	als Lohnbeleg	10	
Pensionskassenunterlagen		10	
Pensionsrückstellungsermittlungen		10	
Pensionszahlungen, Unterlagen	Es empfiehlt sich eine von der Personalakte getrennte Aufbewahrung	30	Geht es um Ansprüche der Altersvorsorge in Bezug auf eine Pensionskasse, beträgt die Verjährungsfrist 30 Jahre. Solange sollten die dazu bestehenden Unterlagen aufbewahrt werden. Entscheidend zur Ermittlung des exakten Fristendes ist § 199 BGB.
Personalakten, Personalunterlagen	Arbeitsverträge, MA bezogene gesetzliche vorgeschriebene Unterlagen Unterlagen, die keinen der aufgelisteten Aufbewahrungsfristen unterliegen, sind zu entfernen	10	Eine Aufbewahrungsfrist von 6 Jahren ist bindend, wenn in der Personalakte Dokumente zum Steuerrecht zu finden sind. Ratsam ist die Aufbewahrung von Personalakten von mindestens 10 Jahren. Und auch wenn der Gesetzgeber nicht für alle Personalunterlagen eine verpflichtende Archivierungsfrist festlegt, so ist es dennoch sinnvoll, die Personalakte solange aufzubewahren, bis sämtliche juristischen Ansprüche verjährt sind.
Personalstandsmeldungen	Für die Berichterstattung im Anhang (Bestandteil des Jahresabschlusses), Aufbewahrungspflicht hier nach Stichtagsmeldung	10	
Prämien, Niederschriften über Gewährung	als Lohnbelege	10	
Protokolle einer DEÜV-Meldung		3	
Provisionsabrechnungen mit Unterlagen		10	
Provisionsgutschriften		10	
Provisionsverträge		6	

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Prozessakten	soweit für Rechnungswesen relevant	6	
Qualitätsbelohnungen i.S. von Prämien		10	
Reiseauslagenbelege		10	
Reisekostenabrechnung		10	
Schichtzettel für Bruttolohnverrechnungen	soweit Lohnbelege	10	
Schwerbehindertenausweis (Kopie)	Gesundheitsdaten nach Art. 9 DSGVO sind mit einer besonderen Vertraulichkeit zu handhaben. Kopie nur mit Einwilligung zulässig.	-	SGB IX, §§ 123, 241 Abs. 2 BGB, §§ 1, 3, 7, 8, 13 bis 15, 22 AGG
Sondergratifikationen		10	
Sozialleistungsunterlagen		10	
Sozialpläne einschl. Errechnungsunterlagen		10	
Sozialversicherungsausweis	Sozialversicherungsnummer notwendig für die Gehaltsabrechnung	-	Arbeitgeber muss sich den Sozialversicherungsausweis oder das entsprechende Schreiben zu Beginn einer Beschäftigung vorlegen lassen.
Sozialversicherungsbeitragskonten, Nachweis		6	
Sozialversicherungsunterlagen		10	
Steuererklärung, elektronisch übermittelte	Aufbewahrungsfrist endet nicht vor Ende der Festsetzungsverjährung gem. AO; Aufbewahrung der originär digitalen Daten erforderlich	6	
Steuererklärung, elektronisch übermittelte	Soweit Buchungsbeleg (z.B. Kapitalertragssteueranmeldung), Aufbewahrungsfrist endet nicht vor Ende der Festsetzungsverjährung gem. AO; Aufbewahrung der originär digitalen Daten erforderlich	10	
Stundenlohnzettel		6	
Stundenlohnzettel als Buchungsbeleg		10	
Stundungsbelege		10	
Tageslohnscheine		10	
Überstundengenehmigungen		6	
Überstundenlisten	soweit Lohnbelege	10	
Überstundenmeldungen	soweit Lohnbelege	10	
Urlaubsanträge		-	empfohlen 3 Jahre Kontrollfunktion

Name	Inhalt	Dauer (Jahre)	Bemerkungen
Urlaubslisten	soweit Unterlagen zur Ermittlung von Rückstellungen oder zur Abrechnung	10	
Verdienstbescheinigungen für Arbeiter und Angestellte		-	