Datenschutz und neue Medien in der Personalabteilung

Datum: 2009-09-30
Kurzbeschreibung: Der neue Beitrag erläutert den datenschutzkonformen Umgang mit Internet, E-Mail und Telekommunikation im Unternehmen. Er geht auch auf den Umgang mit Gesundheitsdaten von Arbeitnehmern (speziell bezogen auf das betriebliche Eingliederungsmanagement) ein.
Autor: Thilo Märtin, Rechtsanwalt und Partner, Nürnberg

[Beginn Überblick]

Überblick

Durch moderne Medien wie Internet, E-Mail und Telefon sind heute so viele Daten über die eigene Person im Umlauf, dass sie kaum noch zu kontrollieren sind. Arbeitgeber tragen hier insbesondere Verantwortung für den Umgang mit den Daten ihrer eigenen Mitarbeiter. Ist erst der Eindruck entstanden, dass die Daten nicht vor Zugriffen Unberechtigter geschützt sind, entsteht schnell ein Klima des Misstrauens, das für das Unternehmen schädlich sein kann. Dies gilt umso mehr in besonders sensiblen Bereichen, bei denen es zum Beispiel um Gesundheitsdaten geht.
Im Folgenden soll der datenschutzkonforme Umgang mit modernen Medien wie Internet, E-Mail und Telekommunikation erläutert und umsetzbar gemacht werden. Neben den Rechtsgrundlagen werden konkrete Beispiele und Checklisten angeführt, die die Umsetzung in die Praxis erleichtern. Auf Grundlage der aktuellen Rechtsprechung und technischen Entwicklung der vergangenen Jahre und unter Berücksichtigung der Anfang 2011 verabschiedeten Änderungen zum Beschäftigtendatenschutz ist damit ein rechtssicherer und aktueller Umgang möglich.

[Ende Überblick]

[Beginn Gesetze, Vorschriften und Rechtsprechung]

Gesetze, Vorschriften und Rechtsprechung

Die wichtigsten Rechtsgrundlagen stellen das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz, das Strafgesetzbuch und das Telekommunikationsgesetz (TKG) dar. Im Zusammenhang mit der Mitbestimmung des Betriebsrats sind die Vorschriften des Betriebsverfassungsgesetzes (BetrVG) zu beachten.

[Ende Gesetze, Vorschriften und Rechtsprechung]

Persönlichkeitsschutz des Mitarbeiters

Der im Grundgesetz verankerte Schutz des Persönlichkeitsrechts wirkt über das Bundesdatenschutzgesetz (BDSG), das Betriebsverfassungsgesetz (BetrVG) und verschiedene Einzelgesetze in das Arbeitsverhältnis hinein.[1] Über das vom Bundesverfassungsgericht definierte **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** sind hiervon insbesondere die neuen Medien betroffen.[2]
Deshalb steht es dem Arbeitgeber grundsätzlich zwar frei, ob und in welcher Form er seinen Mitarbeitern Zugang zu Medien wie Internet, E-Mail oder Telefon gewährt. Hierbei ist das Persönlichkeitsrecht des Arbeitnehmers mit den Unternehmerinteressen des Arbeitgebers in Einklang zu bringen, was angesichts der geltenden Gesetze teilweise schwierig bis unmöglich ist.

Rechtsgrundlagen – ein Überblick

Die Arbeitnehmerrechte im Hinblick auf den Schutz seiner Daten resultieren aus einigen wenigen, grundsätzlichen gesetzlichen Regelungen, die in Detailgesetzen näher ausgestaltet wurden. Die für die Arbeitnehmer wichtigsten Regelungen sollen im Folgenden kurz erläutert werden.

---

1 § 1 Abs. 1 BDSG und § 75 Abs. 2 BetrVG.
2 BVerfG, Urteil v. 27.2.2008, 1 BvR 370/07, 1 BvR 595/07.

Das gesprochene Wort

Das Recht am gesprochenen Wort entspringt dem Freiheitsgrundrecht des Art. 2 GG und bestimmt, dass jedermann selbst darüber bestimmen kann, ob der Inhalt einer Kommunikation einem anderen zugänglich gemacht werden soll oder nicht.
Dies gilt aber nur für das ausschließlich gesprochene Wort und nicht für schriftliche Kommunikation wie z. B. E-Mails. Einer Ausweitung hierauf, wie sie in der Literatur teilweise vertreten[3] wird, kann nicht gefolgt werden, da das geschriebene Wort und die neuen Medien eigene Schutzrechte erfahren. Ein allgemeines Grundrecht auf kommunikative Selbstbestimmung gibt es nicht.
Das Recht am gesprochenen Wort ist damit nicht identisch mit dem Grundrecht auf informationelle Selbstbestimmung, welches den Art. 1 Abs. 1 und Art. 2 Abs. 1 GG entspringt, und die Umstände, die die Gesamtheit einer Persönlichkeit ausmachen, schützt. Darüber hinaus kann sich hierauf grundsätzlich auch eine juristische Person des Privatrechts, also z. B. ein Unternehmen berufen.[4]

Das Fernmeldegeheimnis

Eine spezielle Ausprägung in einem eigenen Grundrecht erfährt der Schutz des gesprochenen Worts durch die Verankerung des Fernmeldegeheimnisses in Art. 10 Abs. 1 GG. Das Fernmeldegeheimnis schützt die Integrität des Übermittlungswegs der Kommunikation.[5] Das bedeutet insbesondere, dass sich in die Übertragung der Daten keine Dritten einschalten dürfen, um von den Inhalten Kenntnis zu erlangen. Dies können sowohl gesprochene Worte, wie auch andere Daten (z. B. E-Mails) sein.
Das **Fernmeldegeheimnis endet** aber **mit der Ankunft des Inhalts beim Empfänger** – sozusagen an der Datenbuchse in der Wand bzw. im Computer des Arbeitnehmers. Wenn also jemand sich nach der Übermittlung in die Übertragung einschaltet – z. B. durch heimliches Mithören oder Mitlesen der Daten über eine technische Vorrichtung, so unterliegt dies nicht mehr dem Schutz des Fernmeldegeheimnisses. Geschützt wird hierdurch also lediglich das Übertragungsmedium, hier z. B. das Kabel.
Eine spezialgesetzliche Ausprägung erfährt das Fernmeldegeheimnis durch § 88 TKG. Die Norm unterstellt alle Inhalte der Telekommunikation dem Fernmeldegeheimnis. Sie sanktioniert es, wenn sich der Diensteanbieter von Inhalten oder näheren Umständen Kenntnis verschafft.
§ 88 TKG gilt für alle Anbieter, die Telekommunikationsdienste geschäftsmäßig gegenüber Dritten erbringen.
Für Arbeitgeber bedeutet dies, dass er seinen Mitarbeitern gegenüber dann die Vorgaben des Fernmeldegeheimnisses grundsätzlich beachten muss, wenn er ihnen die **private Nutzung der betrieblichen Telekommunikationsanlagen** gestattet. Denn im Rahmen der privaten Nutzung werden die Mitarbeiter gegenüber dem Arbeitgeber zu Dritten im Sinne des § 88 TKG, weil der Arbeitgeber den Mitarbeitern Telekommunikationsdienste anbietet.
Adressaten und damit Verpflichtete des Fernmeldegeheimnisses sind nicht nur der Arbeitgeber, sondern auch alle verantwortlich mit der Betreuung der Telekommunikationsanlagen Befassten, die Zugang zu den Daten bzw. Inhalten der Kommunikation haben. «Telekommunikationsanlagen» im Sinne des TKG sind «technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können».[6]
Die für Unternehmen relevanten Anlagen sind damit Telefonanlagen und jegliche Programme zur Übertragung von elektronischer Post (E-Mails) oder Programme zur Datenübertragung in das Internet.

Strafbarkeit bei Verstoß gegen das Fernmeldegeheimnis

Eine Verletzung des Fernmeldegeheimnisses wird im Strafgesetzbuch mit Strafe bedroht. § 206 StGB sanktioniert 2 Tatbestände: **Ein Verstoß gegen die Schweigepflicht** der durch das Fernmeldegeheimnis Verpflichteten wird dann bestraft, wenn sie ihre Kenntnisse über Inhalte aus der Telekommunikation Dritten mitteilen. Dies können auch Personen im eigenen Unternehmen sein, wenn z. B. Vorgesetzte unterrichtet werden, die diese Information nicht schon in ihrer Funktion als Betreiber der Anlage erhalten.

---

3 Vgl. *Däubler*, Internet und Arbeitsrecht, Rn. 248 f.
4 BVerfG, Beschluss v. 9.10.2002, 1 BvR 1611/96, 1 BvR 805/98.
5 Vgl. BVerfG, Urteil v. 14.7.1999, 1 BvR 2226/94, 2420/95 und 2437/95.
6 Vgl. § 3 Zf. 23 TKG.

Erlangt ein Arbeitgeber auf diesem Wege Informationen, kann daraus ein Verwertungsverbot im Rahmen einer Verhältnismäßigkeitsabwägung bei einer Kündigung entstehen, d. h. diese Information darf unter Umständen nicht zum Grund der Kündigung gemacht werden[7];.[8]
Als zweites sanktioniert § 206 StGB das «**Unterdrücken von Sendungen**». Hiervon sollen nach der wohl überwiegenden Meinung in der Literatur[9] auch sog. nicht verkörperte Sendungen – also z. B. E-Mails – erfasst sein, weil ansonsten der Schutz des Fernmeldegeheimnisses leerlaufen würde.
Für das Unterdrücken einer E-Mail muss diese zunächst dem Diensteanbieter (hier z. B. dem Arbeitgeber) durch vorschriftsmäßiges Inverkehrbringen «anvertraut» werden. Das bedeutet, dass der Diensteanbieter die Gewalt über die E-Mail ausüben können muss und dass sie auf den objektiv üblichen Umständen auf den Weg gebracht wurde. Unterdrückt wird eine E-Mail, wenn sie durch einen technischen Eingriff ihren Empfänger nicht, nicht vollständig oder verspätet erreicht.
Diese Unterdrückung kann konkret z. B. über **E-Mail -Filter** geschehen, die die Zustellung von z. B. Spam-E-Mails vollständig verhindern. Eine Information des Empfängers über derartige Vorgänge kann zu einer Einwilligung führen.[10] Eine Unterdrückung liegt aber dennoch weiter vor und erfüllt damit den Tatbestand des § 206 Abs. 2 Nr. 2 StGB. Ob das grundsätzliche Löschen von Spam-E-Mails dennoch zulässig ist, ist derzeit nicht abzusehen. Rechtsprechung liegt hierzu noch nicht vor.
Damit ist zu empfehlen, dass die **Beschäftigten** im Rahmen einer **Betriebs- oder Dienstvereinbarung** umfassend **über** einen solchen **Prüf- und Löschvorgang informiert** werden. Weiterhin sollten die angelegten Löschkriterien sehr weit gefasst werden, um das Löschen relevanter Mails zu verhindern. Spam-verdächtige E-Mails sollten dem Benutzer in einen **speziellen Ordner** zugestellt werden, aus dem er diese selbstständig löschen kann. Eine globale Löschung der Inhalte dieses Ordners ist nur nach vorheriger Einwilligung zulässig.[11]
Diese Problematik gilt unabhängig davon, ob der private E-Mail-Verkehr im Unternehmen im gewissen Umfang erlaubt oder grundsätzlich verboten ist, da selbst bei einem Verbot privater Mails der Empfang derselben vom Beschäftigten nicht umfassend kontrolliert werden kann.

Das geschriebene Wort – Anforderungen an E-Mails

Auch das geschriebene Wort ist durch das Gesetz in einem gewissen Umfang geschützt. Bei Arbeitnehmern wird hier ein besonderes Augenmerk auf die Unterscheidung zwischen privater und geschäftlicher Nutzung gelegt werden müssen.[12]
Der Schutz des Briefgeheimnisses in § 202 StGB ist nicht auf E-Mails und Faxe anwendbar, weil die bei beiden Medien verwendeten Daten nicht als «verschlossenes» und «verkörpertes Schriftstück» im Sinne des Gesetzes angesehen werden können.
Anders hingegen der **Schutz gegen das Ausspähen von Daten und der Schutz gegen Veränderung von Daten** in §§ 202a, 303a StGB: Hier wird der Schutz des klassischen Briefgeheimnisses zumindest teilweise auf Daten ausgedehnt. Der unbefugte Zugriff auf oder die Veränderung von elektronisch gespeicherten oder übermittelten Daten wird, wenn sie gegen unberechtigten Zugang gesichert sind, mit Geldstrafe oder Freiheitsstrafe von bis zu 3 Jahren bestraft. Der Versender einer E-Mail, die diesen Schutz genießen soll, muss also besondere Vorkehrungen gegen einen unbefugten Zugriff getroffen haben, damit § 202a StGB greift.
Für die Praxis stellt sich nun die Frage, wann eine E-Mail gegen unbefugten Zugriff so geschützt ist, dass bei einem Durchbrechen dieser Sicherung § 202a StGB greift.

[Beginn Tipp]

Praxis-Tipp

---

7 LAG Hamm, Urteil v. 25.1.2008, 10 Sa 169/07, RDV 2008, S. 211.

8 Vgl. hierzu auch Abschn. 2 Beweisverwertungsverbote im Kündigungsfall sowie Abschn. 5.2.2 Mithören und Aufzeichnen.

9 *Lenckner* in Schönke/Schröder, Kommentar zum StGB, § 206, Rn. 20; *Fischer*, Kommentar zum StGB, § 206, Rn. 15; *Schmidl* in DuD 2005, S. 267;OLG Karlsruhe, RDV 2005, S. 67; a. A. *Kühl* in Lackner/Kühl, Kommentar zum StGB § 206, Rn. 8, *Barton* in CR 2003, S. 839.

10 Problematisch und insoweit noch ungeklärt ist, ob nicht auch der Absender in diese Unterdrückung einwilligen müsste, da auch er sich noch im Schutzbereich des Fernmeldegeheimnisses befindet. Für massenhaft versendete Spam-Mails wird dies aber abgelehnt, vgl. dazu im Einzelnen Schmidl a. a. O., S. 269.

11 Näher zu dem Thema: *Michael Würtz,* TU Darmstadt, Hochschulrechenzentrum, E-Mail-rechtliche Aspekte, Vers. 1.4.

12 Vgl. dazu im Detail Abschn. 1.3 Private Nutzung von Internet und E-Mail.

Anforderungen an E-Mails

Diese Anforderungen müssen Ihre Mails erfüllen, damit sie gegen unbefugtes Ausspähen geschützt sind:

- Die E-Mail – kann nicht unbefugt verändert werden (Integrität)
- Die E-Mail – kann von keinem unbefugten Dritten gelesen werden (Vertraulichkeit)
- Die E-Mail – wird wirklich vom Sender an den Empfänger verschickt (Authentizität)

[Ende Tipp]

Um diese Kriterien zu erfüllen, wird derzeit **ausschließlich eine Verschlüsselung** des E-Mailverkehrs anerkannt. Selbst diese erfüllt nicht genau die Kriterien, die im Gesetz gefordert werden. Anerkannt wird sie deshalb, weil sonst ein Schutz der Daten während der Übermittlung nach dem heutigen Stand der Technik über § 202a StGB gar nicht möglich wäre.

[Beginn Tipp]

Praxis-Tipp

Mindestanforderungen an die Verschlüsselung

Eine Verschlüsselung sollte folgende Mindestanforderungen erfüllen:

- Verschlüsselung mit 2448 Bit oder mehr
- RSA- oder Elgamal-Algorythmus[13]
- Asynchrone «Public Key»-Verschlüsselung[14]
- Kostenfreie OpenSource-Lösung: GnuPG für Windows[15]

Nicht ausreichend sind

- ein Lese- und Nutzungsverbots-Text am Ende der E-Mail
- eine elektronische Signatur bzw. Zertifizierung

[Ende Tipp]

Der bloße **Ausspruch eines Lese- und Nutzungs-Verbots**, wie man ihn häufig am Ende von E-Mails liest und auch eine **elektronische Unterschrift** (Zertifizierung), reichen nicht aus, um den Schutz des § 202a StGB zu erlangen, da dieser Hinweis lediglich sicherstellt, dass der Inhalt der E-Mail nur vom Empfänger genutzt werden darf. Er bewirkt damit nur in Verbindung mit einer Verschlüsselung den Schutz durch § 202a StGB.

Unabhängig von einer Kenntnisnahme durch unbefugte Dritte **darf jede dienstliche E-Mail auch inhaltlich vom Arbeitgeber eingesehen und kontrolliert werden**. So wie die dienstliche Post in Papierform, unterliegen auch dienstliche E-Mails dem Organisationsrecht des Arbeitgebers. Dass es hierbei immer wieder zu Konflikten bei der privaten Nutzung dieses Mediums kommt, ist voraussehbar und bedarf deshalb gewisser Regeln.[16]

Videoüberwachung - das Recht am eigenen Bild

Das Recht am eigenen Bild ist als Bestandteil des Persönlichkeitsrechts aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ein Teil der Grundrechte jedes Menschen. Dies hat zur Folge, dass grundsätzlich jeder Mensch selbst darüber bestimmen kann, wann Bilder von ihm gemacht werden dürfen und wann nicht. Für den Bereich der Beschäftigtenverhältnisse sind deshalb insbesondere Regelungen für Überwachungen mit Videokameras notwendig.

Wie in anderen Bereichen, muss auch hier ein Ausgleich zwischen den berechtigten Kontrollinteressen des Arbeitgebers und dem Persönlichkeitsrecht der Beschäftigten gefunden werden. § 6b Abs. 1 Nr. 2 und 3 BDSG legen deshalb fest, dass eine Videoüberwachung gerechtfertigt ist zur **Wahrnehmung des Hausrechts** oder zur **Wahrnehmung berechtigter Interessen für konkret festzulegende Zwecke**. Eine ständige Überwachung von Mitarbeitern erzeugt aber regelmäßig einen kaum zu rechtfertigenden Überwachungsdruck, der mit dem

---

[13] So verwendet z. B. in Rahmen der OpenSource-Verschlüsselung GnuPG.

[14] Näheres dazu beim BSI: https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesseltkommunizieren/Grundlagenwissen/AsymmetrischeVerschluesselung/asymmetrische_verschluesselung_node.html (zuletzt abgerufen am 30.5.2014).

[15] Zu finden mit User-freundlicher Anleitung unter www.gpg4win.de (zuletzt abgerufen am 30.5.2014).

[16] Näheres dazu in Abschn. 1.3 «Private Nutzung von Internet und E-Mail».

Persönlichkeitsschutz nicht vereinbar ist. Sicherheitsinteressen des Arbeitgebers müssen an dieser Stelle in den meisten Fällen hinter der freien Entfaltung der Persönlichkeit zurücktreten.[17]
Eine Rechtfertigung einer **ständigen Überwachung** kann nur eintreten, wenn die Sicherheitsinteressen des Arbeitgebers so überwiegend sind, dass der Überwachungsdruck, unter dem die Beschäftigten arbeiten müssen, gerechtfertigt werden kann. Dies ist beispielsweise der Fall in **Banken** oder Unternehmen, die äußerst wertvolle Gegenstände herstellen oder verkaufen (Gelddruckereien, Juweliere).
Liegt ein Missbrauchsverdacht gegen Beschäftigte vor und will der Arbeitgeber dagegen mit einer Videoüberwachung vorgehen, so muss er zuvor eine (sicherheitshalber dokumentierte) Interessenabwägung mit dem Persönlichkeitsschutz der Beschäftigten durchführen.[18]
Allerdings dürfen sogenannte Zufallsfunde durch eine Videoüberwachung dennoch in manchen Fällen vor Gericht benutzt werden, um eine Kündigung zu rechtfertigen. D. h., bloß weil eine Videoüberwachung im Arbeitsbereich heimlich stattgefunden hat und damit ggf. rechtswidrig war, bedeutet dies nicht gleichzeitig ein Verwertungsverbot dieser Beweise vor Gericht. Das Bundesarbeitsgericht (BAG) hat zu Beweisverwertungsverboten, die aus Datenschutzverletzungen resultieren, im Jahr 2013 ein wegweisendes Urteil gesprochen (vgl. dazu unten Abschn. 2 Beweisverwertungsverbote im Kündigungsfall), das die Nutzung von Beweisen, die unter Verstoß gegen das Persönlichkeitsrecht erlangt wurden, in bestimmten Fällen untersagt. In Bezug auf Beweise, die durch eine heimliche und damit rechtswidrige Videoüberwachung entstanden sind, hat das BAG jedoch nach dem obigen Urteil noch einmal klargestellt, dass es auf eine genaue Interessensabwägung ankommt, ob die rechtswidrig erlangten Beweise auch tatsächlich zu einem Beweisverwertungsverbot führen.[19] Zur Klarstellung nachfolgend ein Leitsatz aus diesem Urteil zur Videoüberwachung:
«Informationen und Beweismittel, die der Arbeitgeber mittels einer heimlich durchgeführten Videoüberwachung gewonnen hat, unterliegen nicht allein deshalb einem prozessualen Verwendungs- und Verwertungsverbot, weil der Zweck der Beobachtung nicht auf ihre Gewinnung gerichtet war. Auch bezogen auf einen sog. Zufallsfund muss aber das Interesse des Arbeitgebers an der prozessualen Verwendung und Verwertung der Daten und/oder Beweismittel höher zu gewichten sein als das Interesse des Arbeitnehmers an der Achtung seines durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährleisteten, allgemeinen Persönlichkeitsrechts. Davon kann nur ausgegangen werden, wenn es um den Nachweis eines strafbaren Verhaltens oder einer ähnlich schwerwiegenden Pflichtverletzung des Arbeitnehmers geht und die Informationsbeschaffung und -verwertung selbst dann nicht unverhältnismäßig ist.»

Rechtsgrundlagen des Beschäftigtendatenschutzes

Der bereits seit Jahren diskutierte Regelungsbedarf zum Arbeitnehmerdatenschutz hat noch immer nicht zu umfassenden Regelungen hierzu geführt. In Anbetracht dessen, dass möglicherweise in 2015 eine neue EU-Datenschutz-Grundverordnung folgt, wird mit einer nationalen Regelung auch gar nicht mehr oder jedenfalls nicht so bald zu rechnen sein. Die geplante Datenschutz-Grundverordnung lässt jedoch gerade im Bereich des Arbeitnehmerdatenschutzes den nationalen Staaten einen eigenen Spielraum, sodass diese Entwicklung noch abgewartet werden muss.
In der letzten Novelle des Bundesdatenschutzgesetzes (BDSG) vom Sommer 2009 wurden jedoch einige Normen in das Gesetz eingeführt, die für den Arbeitnehmerdatenschutz eine Grundlage bilden.

Definition des Beschäftigten

Im neuen eingefügten Absatz 11 zu § 3 BDSG wird der Begriff des Beschäftigten definiert. Dieser orientiert sich zwar weitgehend am Arbeitnehmerbegriff, weitet ihn aber darüber hinaus auf alle abhängig Beschäftigten aus. So werden hiervon beispielsweise **auch Bewerber und Scheinselbstständige, aber auch** «**Personen, deren Beschäftigungsverhältnis beendet ist**»**, erfasst**.
Die Definition dient der Konkretisierung des neuen § 32 BDSG (vgl. näher dazu Abschn. 1.2.3), der die Zweckbindung von Beschäftigtendaten konkreter fasst.

---

[17] § 75 Abs. 2 BetrVG.
[18] BAG, Beschluss v. 26.8.2008, 1 ABR 16/07.
[19] Vgl. BAG, Urteil v. 21.11.2013, 2 AZR 797/11.

Kündigungsschutz des Datenschutzbeauftragten

§ 4f Abs. 3 BDSG regelt den besonderen Kündigungsschutz für den betrieblich bestellten Datenschutzbeauftragten (DSB). Dieser darf hiernach während der Zeit seiner Bestellung und noch ein Jahr nach seiner Abberufung nicht gekündigt werden. Einzige Ausnahme ist das Vorliegen von Gründen für eine außerordentliche, fristlose Kündigung. Das bedeutet, dass ein wichtiger Grund vorliegen muss. Das Bundesarbeitsgericht (BAG) hat diese Grundsätze zwischenzeitlich bestätigt und den Kündigungsschutz des Datenschutzbeauftragten gestärkt. So hat das BAG klargestellt, dass ein solcher wichtiger Grund für eine Kündigung gegeben sein kann, wenn die weitere Ausübung der Funktion und Tätigkeit als Datenschutzbeauftragter unmöglich oder sie zumindest erheblich gefährdet erscheint, beispielsweise weil der betriebliche Datenschutzbeauftragte (DSB) die erforderliche Fachkenntnis und Zuverlässigkeit nicht (mehr) besitzt.[20] Weiterhin hat das Gericht hier klargestellt, dass der interne DSB nicht abberufen werden darf, nur um ihn durch einen externen DSB zu ersetzen, und eine Mitgliedschaft im Betriebsrat steht der Tätigkeit als DSB nicht entgegen.[21]
Mit § 4f Abs. 3 BDSG wurden die Rechte des DSB auf **Qualifikation gestärkt**. Schon bei der letzten Novelle aus dem Jahr 2006 wurde die erforderliche Fachkenntnis der DSB konkretisiert. Nach der nun neuen, systematisch etwas deplatzierten Regelung ist der Arbeitgeber zur Ermöglichung der Fortbildung des DSB verpflichtet und muss auch die Kosten dafür übernehmen.

Konkrete Zweckbindung von Beschäftigten-Daten (§ 32 BDSG)

Die umfänglichste Neuerung zum Arbeitnehmerdatenschutz stellt **der 2009 eingefügte** § 32 BDSG dar. Er regelt den Umfang der erlaubten Nutzung von Arbeitnehmerdaten – oder genauer: Beschäftigtendaten. Die Norm bezieht sich auf die in § 3 Abs. 11 BDSG neu eingeführte Definition eines Beschäftigten und betrifft damit alle dort geregelten Beschäftigtenverhältnisse.
§ 32 BDSG legt fest, dass Daten von Beschäftigten ausschließlich

- zur Begründung
- Durchführung und
- Beendigung

des Beschäftigungsverhältnisses

- erhoben
- verarbeitet oder
- genutzt

werden dürfen.
Zur **Aufdeckung einer Straftat** dürfen personenbezogene Daten über den verdächtigen Arbeitnehmer erst nach einer Interessenabwägung erhoben (verarbeitet oder genutzt) werden. Hierbei sind folgende Voraussetzungen zu beachten:

- zu dokumentierende Anhaltspunkte für eine Straftat, begangen im Beschäftigungsverhältnis müssen vorliegen. (Wichtig: Präventive Maßnahmen sind hiervon nicht erfasst!)
- Die Daten müssen erforderlich sein für die Aufdeckung und
- im Rahmen einer Interessenabwägung ist zu entscheiden, ob nicht das (rechtmäßige) schutzwürdige Interesse des Betroffenen das Aufklärungsinteresse des Arbeitgebers überwiegt, mithin also ein unverhältnismäßig tiefer Eingriff in den Persönlichkeitsschutz des Beschäftigten vorliegt.

§ 32 BDSG ersetzt, so die Gesetzesbegründung, die bisher oft im Arbeitnehmerbereich angewandte Interessenabwägung des **§ 28 Abs. 1 Nr. 1 BDSG** und versucht, diese zu konkretisieren.
Die angedeutete Ersetzung von § 28 Abs. 1 Nrn. 2 und 3 BDSG ist, so wurde mittlerweile klargestellt, ausdrücklich nicht gewollt, sodass insbesondere die Nr. 2 auch weiterhin auf Sachverhalte mit Beschäftigten-Bezug Anwendung finden kann.
Nachfolgend einige Klarstellungen in Bezug auf Datenverwendungen im Lichte des § 32 BDSG:

- Die **Aufbewahrung von Bewerberunterlagen** zum Abwarten der Klagefristen nach dem AGG für die Dauer von 6 Monaten ist zulässig und vom überwiegenden Interesse des Arbeitgebers gem. § 28 Abs. 1 Nr. 2 BDSG gedeckt.
- Die Recherche von **Bewerberdaten in sozialen Netzwerken** ist wohl zulässig, insoweit die Daten allgemein zugänglich und nicht auf einen bestimmten Nutzerkreis beschränkt sind. Allein die Tatsache, dass ein eigener Benutzer-Account mit Login beim Anbieter des Netzwerkes

[20] BAG, Urteil v. 23.3.2011, 10 AZR 562/09.
[21] Vgl. BAG, Urteil v. 23.3.2011, 10 AZR 562/09.

erforderlich ist, stellt noch keine Einschränkung des Nutzerkreises in diesem Sinne dar.[22] Allerdings muss klargestellt werden, dass die sogenannten Background-Checks von Bewerbern in sozialen Netzwerken rechtlich noch umstritten sind. Nach der hier vertretenen Ansicht und ohne weitere gesetzliche Regelungen hierzu ist jedoch eine Recherche in allen sozialen Netzwerken nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG zulässig. Abschließend ist anzumerken, dass allerdings viele Netzwerke die Recherche und Nutzung der Daten für gewerbliche Zwecke untersagen, sodass regelmäßig ein Verstoß gegen die Nutzungsbedingungen vorläge, der zivilrechtlich zu ahnden wäre.

- Weiterhin ist die Erlaubnis zur Datennutzung beim Verdacht von Straftaten auf repressive Maßnahmen beschränkt. Was mit Datenerhebungen passieren darf, **die der Vorbeugung und damit Verhinderung von Straftaten dienen,** wie beispielsweise das Loggen von besuchten Internetseiten zur Missbrauchskontrolle oder präventiven Maßnahmen zur **Korruptionsbekämpfung** hat mittlerweile durch die Rechtsprechung einen gewissen Rahmen erfahren. Hier war insbesondere das schon erwähnte Urteil des BAG vom Juni 2013[23] wegweisend.[24] Die Anforderungen an die in § 32 BDSG geforderte Interessenabwägung, insbesondere im Rahmen der dort geforderten Erforderlichkeit der Maßnahme, sollten vom Arbeitgeber künftig genau dokumentiert werden. Dabei sollte die Dokumentation für ggf. gerichtliche Maßnahmen sowohl auf unternehmerische Schadens- wie auch Compliance-Aspekte abzielen. Dies betrifft etwa die gesetzliche Verpflichtung zur Durchführung von Aufsichtsmaßnahmen aus §§ 130, 30, 9 OWiG oder die möglichen Folgen des Bekanntwerdens von Gesetzesverstößen im Unternehmen, insbesondere auch Ansehens- und Rufschäden. Neben Straftaten wie Diebstählen kommen durch gesetzliche Aufsichtspflichten außerdem noch einige weitere mögliche Pflichtverletzungen mit Unternehmensbezug in Betracht, wie z. B. Korruptionsdelikte, Untreue, Verrat von Geschäftsgeheimnissen oder Kartellverstöße.[25]

ungeklärt. Es spricht allerdings einiges für die Auffassung, dass das Verbot von Screenings nicht für präventive Maßnahmen gilt.

Privatenutzung von Internet und E-Mail

Die Frage, ob und in welchem Umfang ein Arbeitgeber seinen Mitarbeitern die private Nutzung von Internet, E-Mail und Telefon erlauben soll, ist eine der meistgestellten Fragen. Einerseits hat der Arbeitgeber bei privater, elektronischer Kommunikation die Vorgaben des Fernmeldegeheimnisses gegenüber seinen Mitarbeitern zu beachten und darf damit E-Mail und Internet-Verkehr nicht mehr überwachen. Andererseits jedoch ist er als Unternehmer aus einer Vielzahl von Vorschriften zur Überwachung seines Unternehmens und Einschätzung möglicher Risiken verpflichtet. Der sich hieraus ergebende Konflikt wurde mittlerweile durch die Rechtsprechungspraxis in eine Lösung gezwängt, die zwar dem Gesetz widerspricht, jedoch aufgrund der gesetzgeberischen Untätigkeit von allen Beteiligten anerkannt wird[26]

Compliance-Anforderungen des deutschen Gesetzgebers

Um dies zu verdeutlichen werden im Folgenden die wichtigsten gesetzlichen Anforderungen erläutert und der jeweilige Konflikt aufgezeigt, der zwischen Arbeitgeberpflichten und Arbeitnehmerrechten entsteht.

Der rechtliche Rahmen für jede Tätigkeit eines Unternehmers wird durch das Prinzip der Organisationsverpflichtung gesetzt. Nach dem Prinzip der **Organisationsverpflichtung** haben Unternehmen

- rechtskonform zu handeln,
- erforderliche Strukturen für rechtskonformes Handeln bereitzustellen.

Verstöße gegen diese Organisationsverpflichtung führen zu einem Organisationsverschulden der Organe des Unternehmens und der darunterliegenden Stabstellen, jeweils **mit persönlicher Haftung**

---

[22] So auch Forst, NZA 2010, S. 427 (431); Hoormann, DSRI-Tagungsband, 2011, 577.

[23] BAG, Urteil v. 20.6.2013, 2 AZR 546/12.

[24] S. dazu Abschn. 2 Beweisverwertungsverbote im Kündigungsfall.

[25] Vgl. hierzu umfassend: Brink/Wybitul: Der «neue Datenschutz» des BAG - Vorgaben zum Umgang mit Beschäftigtendaten und Handlungsempfehlungen zur Umsetzung, ZD 2014 S. 225.

[26] S. Compliance .

für diese Personen. Um rechtskonformes Handeln gewährleisten zu können, muss der Unternehmer seinen Betrieb daraufhin kontrollieren können.

- **Konflikt mit dem Fernmeldegeheimnis:** Gewährt der Unternehmer seinen Mitarbeitern eine private Nutzung neuer Medien wie E-Mail oder Internet, darf er in diesem privaten Bereich seiner Mitarbeiter aufgrund der oben aufgezeigten Persönlichkeitsrechte wie dem Fernmeldegeheimnis gar nicht mehr oder nur sehr beschränkt kontrollieren. Je nachdem wie intensiv dieser Bereich ausgestaltet ist, wird man zu der Erkenntnis gelangen müssen, dass das Unternehmen Teile seiner IT-Anlage nicht beherrscht, weil es diese wegen Verstoß gegen Gesetze nicht kontrollieren kann.
- **Kennzeichnungspflicht von E-Mails**: Seit 1.1.2007 hat der Gesetzgeber festgelegt, dass E-Mails, die Bezug zum Geschäft des Unternehmens haben, mit den gleichen Angaben zu kennzeichnen sind wie der typische Geschäftsbrief. Dies führt dazu, dass jede E-Mail, die über eine Domainkennung verschickt wird, die auf ein Unternehmen registriert ist, mit den entsprechenden Angaben zu versehen ist. Bei fehlender Angabe führt dies zu einem Bußgeld und es besteht das Risiko, dass das Unternehmen abgemahnt wird. Hierdurch entsteht bei jeder E-Mail mit der Domainendung des Unternehmens nach außen der **Rechtsschein, dass das jeweilige Unternehmen handelt**. Zieht man eine Parallele zur physikalischen Post, wird dies schnell deutlich: Kein Mitarbeiter würde für einen privaten Brief das Briefpapier des Unternehmens verwenden, um z. B. private Bestellungen vorzunehmen. Dementsprechend fordert die Organisationspflicht des Arbeitgebers einen **Gleichlauf zwischen elektronischer und physikalischer Post.** Dies hat zur Folge, dass der Gesetzgeber damit faktisch die privaten E-Mails in Unternehmen abgeschafft hat.
- **Compliance mit KonTraG:** Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) definiert erweiterte Pflichten der Unternehmensleitung bezüglich des Risikomanagements und der Risikosteuerung. Wesen des mit dem KonTraG bezweckten Risikomanagements ist, dass ein Unternehmen keine Geschäfte betreiben soll, die nicht in seinen unmittelbaren Kernbereich gehören. Das Unternehmen wird dann in einem Bereich tätig, in dem es über kein unmittelbares Know-how verfügt. **Die Folge**: Bei einer privaten Zulassung von E-Mailnutzung erbringt das Unternehmen gefälligkeitshalber kostenlose Providerdienstleistungen für Dritte, die Mitarbeiter. Das Unternehmen gibt hier offensichtlich zu erkennen, dass es plötzlich in einem Bereich tätig ist, in dem es, anders als etwa ein professioneller Provider, über kein Fachwissen verfügt. Eine solche riskante Tätigkeit darf deshalb – um nicht gegen das KonTraG zu verstoßen – nicht erfolgen.

Aus diesen Gründen stellt die Zulassung einer privaten Nutzung von Internet, E-Mail und Telefon ein nicht unerhebliches Risiko für den Arbeitgeber dar. Nur im Rahmen einer vollständigen Untersagung privater Kommunikation ergeben sich **angemessene Kontrollmöglichkeiten** für den Arbeitgeber, die dennoch immer am Persönlichkeitsschutz des Arbeitnehmers zu messen sind (vgl. hierzu auch Abschn. 1.3.4).

Fürsorgepflicht des Arbeitgebers

Das Dienstverhältnis verpflichtet nicht nur zu Arbeit, Beschäftigung und Entgelt, sondern zu gegenseitiger Rücksichtnahme und Interessenförderung.[27] Aus der Fürsorgepflicht des Arbeitgebers und deren Gegenstück – der Treuepflicht des Arbeitnehmers – lässt sich ablesen, dass es einen schützenswerten Bereich gibt, den der andere Teil respektieren muss.

Im Rahmen seiner Fürsorgepflicht hat der Arbeitgeber seinen Mitarbeitern in **Not- und Eilfällen** und in Fällen, wo eine andersartige Kommunikation bzw. eine Verschiebung in die Freizeit nicht möglich ist, diese mit betrieblichen Mitteln zu gestatten. Hierauf hat der Mitarbeiter sogar einen Rechtsanspruch.[28] Dies sollte der Arbeitgeber auch im Hinblick auf mögliche arbeitsrechtliche Konsequenzen bereits in der Verbotsregelung klarstellen (Formulierungsbeispiel in Abschn. 1.3.4). Die Verbotsregelung sollte auch mobile Endgeräte wie Blackberry, Speichermedien, Notebooks und PDAs einbeziehen.

Im Streitfall liegt die **Beweislast** für ein unzulässiges Verhalten des Arbeitnehmers, das zu einer Kündigung berechtigen soll, grundsätzlich beim Arbeitgeber. Dies bedeutet bei der Nutzung von E-Mail und Internet, dass nicht nur der Verstoß gegen arbeitsrechtliche Regelungen an sich, sondern

---

[27] Dies ergibt sich aus § 241 Abs. 2 BGB.

[28] *Hanau/Hoeren*, Private Nutzung durch Arbeitnehmer, S. 20.

regelmäßig auch deren Umfang bewiesen werden muss. Dies zeichnet sich in der aktuellen Rechtsprechung ab.[29]
Der Betriebsrat darf gem. § 87 Abs. 1 Nr. 6 BetrVG bei der Einführung einer solchen Regelung mitbestimmen, wenn die Medien überwacht werden sollen. Die Einführung solcher Medien und die Untersagung der privaten Nutzung hingegen unterliegen nicht der Mitbestimmung durch den Betriebsrat.[30] Der Betriebsrat hat lediglich ein Recht darauf, über die Einführung von E-Mail- und Internetzugang gemäß §§ 80 Abs. 2, 90 Abs. 1 BetrVG informiert zu werden.[31] Gleiches gilt für die Arbeitnehmer gemäß § 81 Abs. 4 Satz 1 BetrVG.[32]

Betriebliche Übung

Trotz eines Verbots kann es zu einer rechtmäßigen, privaten Nutzung des Internets durch den Arbeitnehmer kommen, wenn ein Fall einer betrieblichen Übung vorliegt. Dazu kommt es, wenn es (entgegen einer anderslautenden Anweisung) für den Arbeitgeber erkennbar ist, dass der Internetzugang regelmäßig auch privat genutzt wird. Duldet er diesen Umstand, so darf der Mitarbeiter grundsätzlich auf den Fortbestand der Praxis vertrauen. Dauert dieser Zustand **6 Monate oder länger** an, so entsteht eine betriebliche Übung, die einen Anspruch des Mitarbeiters darauf begründet, dass die geduldete E-Mail- und Internetnutzung weiterhin gewährt wird.
Damit begeht der Mitarbeiter selbst bei extensiver, privater Nutzung von E-Mail und Internet keine arbeitsrechtliche Pflichtverletzung mehr. Allerdings kann ein rein passives Verhalten des Arbeitgebers den Vertrauensschutz einer betrieblichen Übung nicht rechtfertigen.[33] Es ist vielmehr erforderlich, dass der Arbeitgeber die sich eingebürgerte, private Nutzung der Beschäftigten offensichtlich kennt und über mindestens 6 Monate hinweg hinnimmt.
Ein Vertrauen darauf, dass sich Anweisungen und Praktiken bezüglich der Internetnutzung schon irgendwie im Betrieb herumsprechen würden, ist nicht ausreichend. Vielmehr muss der Arbeitgeber mittels geeigneter arbeitsvertraglicher Regelungen oder durch den Abschluss entsprechender Betriebs- und Dienstvereinbarungen gewährleisten, dass jeder Mitarbeiter ein entsprechendes Nutzungsverbot kennt.[34] Um sicherzugehen, dass eine solche betriebliche Übung nicht entsteht, ist dem Arbeitgeber außerdem zu einer stichprobenartigen Kontrolle und der Ahndung von Verstößen zu raten.[35]
Eine Rückgängigmachung einer bisher erlaubten, privaten Nutzung ist unproblematisch, wenn die Erlaubnis von vornherein als «freiwillig» durch den Arbeitgeber gekennzeichnet war. Dann kann er die Regelung einfach zurücknehmen. Hat der Arbeitnehmer jedoch einen Anspruch aus betrieblicher Übung erworben, so setzt das nunmehrige Verbot eine Änderungskündigung voraus.

Umgang mit der Privatnutzung von Internet und E-Mail

In den zurückliegenden Jahren gab es 2 Urteile von Landesarbeitsgerichten, die die Arbeitgeber bei der Kontrolle auch privater, elektronischer Kommunikation nicht mehr als Diensteanbieter im Sinne des Telekommunikationsgesetzes angesehen haben.[36] Die Urteile sind im Ergebnis sicherlich begrüßenswert, lassen jedoch in der juristischen Begründung Schwächen erkennen:
Vertretbar ist die Ansicht, dass Beschäftigte nicht «Dritte» sind, für die der Arbeitgeber TK-Dienste erbringt. Die Beschäftigten sind auch bei der privaten Nutzung der betrieblichen Kommunikationsmittel in die Unternehmensorganisation eingebunden und stehen nicht außerhalb des Unternehmens. Vor allem aber «erbringt» ein Arbeitgeber gegenüber den Beschäftigten keine TK-Dienste. Vielmehr ist er ausschließlich Bezieher der TK-Dienste und lässt lediglich in einem gewissen Rahmen zu, dass Beschäftigte die zu Unternehmenszwecken bezogenen TK-Dienste nutzen. Die Möglichkeit der privaten Nutzung macht den Arbeitgeber nicht vom Bezieher von TK-Diensten zum Erbringer und Anbieter von TK-Diensten, da der Zweck des Bezugs von Diensteanbietern nach wie vor

---

[29] LAG Hamm, Urteile v. 3.5.2007, 15 Sa 1880/06 und v. 18.1.2007, 15 Sa 558/06.
[30] LAG Hamm, Beschluss v. 7. 4. 2006, 10 TaBV 1/06, NJW 2007, S. 716
[31] Zur Ausstattungspflicht des Betriebsrats mit diesen Medien vgl. Abschn. 7.3.
[32] Vgl. *Ernst*, NZA 2002, S. 585, 586.
[33] Vgl. *Mengel*, BB 2004, S. 2014.
[34] So auch LAG Rheinland-Pfalz, Urteil v. 12.7.2004, 7 Sa 1243/03, MMR 2005, S. 176 ff.
[35] Ob dies tatsächlich notwendig ist, ist umstritten, a. A. *Beckschulze*, DB 2007, S. 1526.
[36] LAG Niedersachsen, Urteil v. 31.5.2010, 12 Sa 875/09 und LAG Berlin-Brandenburg, Urteil v. 16.2.2011, 4 Sa 2132/10.

ausschließlich die Nutzung zu Unternehmenszwecken bleibt.[37] Mit dieser Lösung wäre dem Arbeitgeber somit die Kontrolle auch privater Kommunikation von Beschäftigten zumindest im Hinblick auf das Fernmeldegeheimnis erlaubt.

Datenschutzrechtliche Einwilligung

Datenschutzrechtlich ist die Frage mit den meisten Aufsichtsbehörden im Hinblick auf die Kontrolle des Datenverkehrs und im Hinblick auf die Archivierung von E-Mails durch eine kombinierte Lösung einer Einwilligung und – soweit möglich – einer Betriebsvereinbarung gelöst. Die Beschäftigten sollten jeder einzeln eine Einwilligung unterzeichnen, in der sie bestätigen, dass sie im Falle einer privaten Nutzung von E-Mail und Internet mit der vollumfänglichen Kontrolle durch den Arbeitgeber einverstanden sind und dass ihnen bei einer Verweigerung dieses Einverständnisses die Privatnutzung dieser betrieblichen Arbeitsinstrumente untersagt ist. Ein Beispielstext hierzu könnte wie folgt aussehen:

Einwilligung in die Einschränkung des Fernmeldegeheimnisses

Mir ist bewusst, dass die private Nutzung des Internets und des E-Mail-Services im Unternehmen nur unter den folgenden Bedingungen erlaubt ist:

1. Die Privatnutzung erfolgt nur in geringem Umfang und beeinträchtigt nicht die Arbeitsleistung.
2. Der Arbeitgeber darf sowohl den E-Mail-Verkehr als auch den Internet-Datenverkehr vollumfänglich und ohne Einschränkung auch hinsichtlich der Inhalte kontrollieren.

Mit ist weiter bekannt, dass mir bei Ablehnung dieser Kontrollrechte durch den Arbeitgeber eine private Nutzung dieser Dienste vollständig untersagt ist. Ich bin darüber aufgeklärt worden, dass ein rückwirkender Widerruf dieser Einwilligung für Daten aus der Vergangenheit aufgrund der gesetzlichen Archivierungspflichten nicht möglich ist und dass ein Widerruf deshalb die Kontrollrechte des Arbeitgebers für diese Daten nicht umfasst. Ich bin damit einverstanden, dass der Arbeitgeber diese Erlaubnis zur Privatnutzung jederzeit widerrufen kann. <Soweit eine Betriebsvereinbarung existiert:> Die Betriebsvereinbarung zur Nutzung von Internet- und E-Mail-Diensten wurde mir zugänglich gemacht und ihre Inhalte sind mir bekannt.
Hinsichtlich der gesetzlichen Archivierungspflichten kann eine Betriebsvereinbarung ein hilfreiches Instrument zur Regelung sein. Soweit Betriebsvereinbarungen auch für eine Regelung der Privatnutzung herangezogen werden, ist mit Blick auf die Datenschutz-Aufsichtsbehörden hier zur Vorsicht zu raten, da nicht alle diese Lösung akzeptieren.

Inhalte einer Betriebsvereinbarung zu E-Mail und Internet

Im Hinblick auf die Inhalte einer solchen Betriebsvereinbarung (BV) sollen hier kurz die wichtigsten Regelungspunkte aufgezeigt werden:

- Reichweite der BV bezogen auf die Unternehmens- bzw. Konzernstruktur
- Anwendbarkeit nur für Arbeiter und Angestellte, §§ 77, 5 BetrVG
- Umfassende Einbeziehung aller Geräte und Dienste in den sachlichen Anwendungsbereich, die der elektronischen Kommunikation in irgendeiner Form dienen, als Besonderheiten sind hier nur exemplarisch zu nennen VoIP-Dienste, elektronische Kalender (insbesondere mit Gruppenfunktionen), mobile Endgeräte wie Telefone oder Tablets, Desktop-PCs, Laptops, USB-Sticks und Multifunktionsgeräte wie z. B. FollowMe-Printer oder Cloud-Anwendungen
- Klare Benennung der Ziele, hier insbesondere die Archivierungspflichten. Eine Erwähnung der Kontrollpflichten des Arbeitgebers kann ebenfalls nicht schaden
- Regelung des allgemeinen Verhaltens im Kontext mit diesen Systemen, insbesondere zu E-Mail-Diensten:
  - Ausschluss widerrechtlicher Handlungen
  - Netzwerk und Unternehmensinteressen darf nicht geschadet werden
  - Geheimhaltung von Zugangsdaten zu betrieblichen Systemen und Untersagung der Nutzung derselben Zugangsdaten im privaten Bereich
  - Anlegen eines E-Mail-Ordners «privat», in den private E-Mails verschoben werden
  - Keine Bearbeitung betrieblicher E-Mails von privaten Accounts aus

[37] So Deiters: Betriebsvereinbarung Kommunikation - Beschäftigteninteressen und Compliance bei privater Nutzung von Kommunikationsmitteln im Unternehmen, ZD 2012, S. 109.

- Aufnahme eines Hinweises, dass Spam-E-Mails automatisch ausgefiltert werden
- Aufnahme der Zweckbindung der Protokollierung des Datenverkehrs zur Analyse und Korrektur technischer Fehler, zur Gewährleistung der Systemsicherheit, zur Optimierung und Steuerung der Kommunikationssysteme, zur statistischen Feststellung des Gesamtnutzungsvolumens und zur Missbrauchskontrolle
- Beschreibung des Archivierungsverfahrens für E-Mails

Beweisverwertungsverbote im Kündigungsfall

Geraten die Interessen des Arbeitgebers mit denen des Arbeitnehmers im Falle einer beabsichtigten Kündigung aufgrund eines Fehlverhaltens in Konflikt miteinander, muss der Arbeitgeber beim konkreten Vorgehen das Persönlichkeitsrecht des Mitarbeiters achten, weil sonst gerichtliche Verwertungsverbote der erlangten Beweise entstehen können. Das BAG hat hierzu im Sommer 2013 ein vielbeachtetes Urteil gesprochen, das den Schutz des Persönlichkeitsrechtes beim Sammeln von Beweisen für einen Kündigungsgrund gegen Arbeitnehmer in ein zentrales Licht rückt.[38] Das Urteil zwingt den Arbeitgeber zu einem datenschutzrechtlich korrekten Vorgehen, wenn er die Unwirksamkeit der ausgesprochenen Kündigung verhindern will.
Das BAG hatte darüber zu entscheiden, ob der Arbeitgeber mit der heimlich durchgeführten Spindkontrolle gegen das Persönlichkeitsrecht des Klägers verstoßen hatte und ob die in dem Spind aufgefundenen Beweismittel zur Begründung der verhaltensbedingten Kündigung im Rahmen des Kündigungsschutzprozesses verwertbar waren. Das Gericht ging im Ergebnis von einem unverhältnismäßigen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers aus und rechtfertigte dies über § 32 BDSG. § 32 BDSG erfasst nicht nur elektronische («automatisiert verarbeitete») Daten, sondern Datenerhebungen über Beschäftigte in jeder Form. Das Gericht hätte vom Arbeitgeber erwartet, dass dieser bei der Prüfung, ob der Eingriff in das Persönlichkeitsrecht durch das Öffnen des Schrankes erforderlich war, die Grundsätze der Verhältnismäßigkeit beachtet hätte. Er hätte also prüfen müssen, ob er das gleiche Ergebnis nicht mit milderen Mitteln hätte erreichen können. Im vorliegenden Fall hätte der Arbeitgeber z. B. den Beschäftigten zur Öffnung des Spinds hinzuziehen können. Dies hätte den Eingriff gegenüber einer heimlichen Öffnung gemindert.
Zwar werden auch weiterhin nicht alle rechtswidrig erlangten Beweise einem Verwertungsverbot unterliegen. Das BAG führt dementsprechend zutreffend aus, dass die ZPO kein ausdrückliches prozessuales Verwendungs- bzw. Verwertungsverbot für rechtswidrig erlangte Informationen oder Beweismittel kenne. Aus § 286 ZPO i. V. m. Art. 103 Abs. 1 GG folge vielmehr die Verpflichtung der Gerichte, den von den Parteien eines Zivilprozesses vorgetragenen Sachverhalt und die von ihnen angebotenen Beweise zu berücksichtigen. Zu einem Verwertungsverbot komme man deshalb nur, wenn es sich entweder direkt aus § 32 BDSG ergebe oder wenn durch das Vorbringen der Beweise vor Gericht ein erneuter bzw. fortgesetzter Eingriff in das allgemeine Persönlichkeitsrecht des Beschäftigten vorläge und dieser Eingriff nicht durch Interessen des Arbeitgebers gerechtfertigt sei.
Dieses Urteil ist für Unternehmen vor allem deshalb wegweisend, weil die Gerichte nun künftig Beweise, die unter Verstößen gegen das Persönlichkeitsrecht erlangt wurden, deutlich kritischer prüfen werden als bisher. Damit Kündigungen vor Gericht nicht für unwirksam erklärt werden, sollten Arbeitgeber beim Sammeln von Beweisen ihre Maßnahmen genau abwägen, ob sie in diesem Umfang erforderlich sind. Eine schriftliche Niederlegung dieses Vorgehens ist zu empfehlen, um es später transparent machen zu können. Im Zweifelsfall und beim Verdacht von strafbaren Handlungen eines Arbeitnehmers sollte der Arbeitgeber künftig schon früh an das Einschalten staatlicher Ermittlungsbehörden denken, um solche Beweisverwertungsverbote zu umgehen. Liegt keine strafbare Handlung vor, sollte der Arbeitgeber im Zweifel die Ermittlungen vor dem Ausspruch einer Kündigung fortführen. Hierbei ist allerdings auf die 2-Wochen-Frist des § 626 Abs. 2 BGB zu achten.
Aus dem Urteil folgen damit erhöhte Anforderungen für Arbeitgeber und der Datenschutz erlangt eine Stärkung, die der zunehmenden Bedeutung von Daten heutzutage gerecht wird.

Kontrolle von Telekommunikationsanlagen

Wie auch bei den anderen Medien muss bei der Überwachung der Telekommunikation im Unternehmen ein Ausgleich zwischen dem berechtigten Kontrollinteresse des Arbeitgebers und dem Persönlichkeitsrecht des Arbeitnehmers gefunden werden. Ähnlich wie bei einer Überwachung des

[38] BAG, Urteil v. 20.6.2013, 2 AZR 546/12.

Internets sollte bei der Telekommunikation unterschieden werden zwischen den statistischen Daten und den Inhalten. Neben den Rechten von Beschäftigten und Arbeitnehmern müssen auch die Rechte der Angerufenen berücksichtigt werden.

Rechtliche Grundlagen

Für die vollständige Speicherung von Anrufzeit, -dauer und Rufnummern der Beteiligten dient § 28 Abs. 1 Satz 1 Nr. 2 BDSG als Rechtsgrundlage. Im Rahmen dieser Abwägung ist festzustellen, ob das Interesse des Arbeitgebers an der Speicherung dieser statistischen Daten das Interesse seiner Beschäftigten und der Angerufenen hieran überwiegt.
Das hauptsächliche Interesse des Arbeitgebers liegt neben der technischen Anlagenkontrolle maßgeblich daran, das **Ausmaß privater Telefonate zu kontrollieren**. Argument gegen private Telefonate sind die unmittelbar entstehenden Kosten, aber insbesondere auch der Verlust von Arbeitszeit, die eigentlich dem Arbeitgeber zu widmen wäre. Trotz verschiedener Ansichten in der Literatur darüber, ob die vollständigen Nummern oder nur ein Teil hiervon gespeichert werden darf, ist obergerichtlich anerkannt, dass die vollständige Speicherung zulässig ist.[39] Hinzu kommt, dass der Arbeitgeber die gesetzlich eingeräumte Möglichkeit hat, den vollständigen Einzelverbindungsnachweis vom Telekommunikationsunternehmen einzufordern, wenn die Voraussetzungen des § 99 Abs. 1 TKG vorliegen. Dafür muss beispielsweise angegeben werden, dass die Mitarbeiter und Personalvertretungen hierüber informiert sind. Die vollständige Rufnummernspeicherung und deren Verwendung ist mitbestimmungspflichtig gem. § 87 Abs. 1 Nr. 6 BetrVG.
Hinsichtlich des **Mithörens von Telefonaten** ist Rechtsgrundlage das «Recht am gesprochenen Wort», das aus dem Persönlichkeitsschutz der Art. 1 Abs. 1 und 2 Abs. 1 GG abgeleitet wird. Ein Eingriff in dieses Grundrecht bedarf in jedem Fall einer **besonderen Rechtfertigung**.
Zusammengefasst kann gesagt werden, dass ein Mithören oder Aufzeichnen ohne Einwilligung oder gar Wissen der Betroffenen niemals zulässig sein kann. Geschieht das Mithören offen und unter einer ggf. wirksamen Einwilligung der Beteiligten, bedarf es im Beschäftigtenverhältnis dennoch einer Rechtfertigung. Näheres zu den Möglichkeiten im Einzelnen in Abschn. 3.2.1.

Kontrollmöglichkeiten

Die Kontrollmöglichkeiten des Arbeitgebers werden begrenzt durch die Zweckbindung der Daten und den damit einhergehenden, eingeschränkten Nutzungsmöglichkeiten. Eine Auswertung der Daten richtet sich künftig nach dem Kriterium der «ordnungsgemäßen Durchführung» des Arbeitsverhältnisses, wie es die Zweckbindung des § 32 BDSG fordert. Eine Auswertung darf deshalb insbesondere zur Missbrauchs- sowie zur Kostenkontrolle durchgeführt werden. Die Daten zur Beurteilung des Leistungsverhaltens heranzuziehen (z. B. zur Überprüfung der Einhaltung von Pausenzeiten), stellt einen zu tiefen Eingriff in das Persönlichkeitsrecht des Mitarbeiters dar und nähert sich bereits einer Totalüberwachung. Dies ist mit der freien Entfaltung der Persönlichkeit nicht vereinbar, § 75 Abs. 2 BetrVG.

Mithören und Aufzeichnen

Das **heimliche Mithören und Aufzeichnen** von Telefongesprächen Beschäftigter ist **unzulässig**, unabhängig davon, ob es sich um private oder dienstliche Telefonate handelt.[40] Die heimliche Aufzeichnung von Gesprächen als die im Vergleich zum bloßen Mithören schwerer wiegende Variante kann sogar den Straftatbestand des § 201 Abs. 1 Nr. 1 StGB verwirklichen. Jeder der am Gespräch Beteiligten darf grundsätzlich davon ausgehen, dass niemand dieses mithört oder gar aufzeichnet.[41]
Das heimliche Mithören bleibt auch für den Fall untersagt, dass damit zivilrechtliche Beweismittel gewonnen werden sollen. Das Interesse, Beweise für ein zivilrechtliches Verfahren zu sichern, reiche nicht aus, um in das Recht am gesprochenen Wort einzugreifen, dafür müsse vielmehr eine über das «schlichte» Beweisinteresse hinausgehende Beweisführungsnot bestehen, so das Bundesverfassungsgericht.[42] Diese Not wird beispielsweise für den Fall einer Notwehrsituation oder notwehrähnlichen Lage bejaht.

---

[39] BAG, Beschluss v. 27.5.1986, 1 ABR 48/84.
[40] BVerfG, Beschluss v. 9.10.2002, 1 BvR 1611/96, 1 BvR 805/98.
[41] BVerfG, Beschluss v. 9.10.2002, 1 BvR 1611/96, 1 BvR 805/98.
[42] BVerfG, Beschluss v. 9.10.2002, 1 BvR 1611/96, 1 BvR 805/98.

Das **offene Mithören bzw. Aufzeichnen** bedarf im Beschäftigtenverhältnis grundsätzlich der **Einwilligung des Angerufenen**. Ob dies explizit (also durch ein opt-in) oder auch implizit (durch ein opt-out) geschehen kann ist differenziert zu bewerten. Dabei ist zu berücksichtigen, dass eine bleibende und reproduzierbare Aufzeichnung eines Gespräches grundsätzlich ein schwererer Eingriff in das Persönlichkeitsrecht des Betroffenen ist als das bloße Mithören. Dies zeigt sich auch daran, das ersteres im Strafgesetzbuch mit Strafe bedroht ist und zweites nicht (vgl. § 201 StGB). Das Bundesverfassungsgericht stellt hierzu folgenden Leitsatz auf: "Eine Einwilligung in eine Persönlichkeitsbeeinträchtigung kann nicht nur ausdrücklich, sondern auch stillschweigend erklärt werden. Eine konkludente Einwilligung darf [...] angenommen werden, wenn ein bestimmtes Verhalten in einem solchen Maße üblich und geradezu selbstverständlich ist, dass entsprechend dem Grundgedanken des § 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Zustimmung des Betroffenen ausgegangen werden kann, sofern er dem Verhalten nicht widerspricht."[43] - Wird der Betroffene also zuvor explizit darauf hingewiesen, dass ein Gespräch von einem Dritten (bloß) mitgehört wird, kann die Möglichkeit zu widersprechen (opt-out) wohl als zulässig angenommen werden. Dafür spricht auch, dass die Situation, in der dies heutzutage am häufigsten der Fall ist – z.B. bei einem Anruf als Verbraucher bei einem Dienstleister in einer geschäftlichen Situation – mittlerweile von einer gewissen Üblichkeit ausgegangen werden kann. Die Ansage, dass Gespräche möglicherweise zu Trainingszwecken mitgehört werden können, dürfte den meisten Anrufern bereits vertraut sein.
Anders ist dies im Hinblick auf eine Aufzeichnung eines Gespräches zu bewerten: Wird hier die Möglichkeit derselben zu wiedersprechen zu spät wahrgenommen, kann es bereits zu einer bleibenden Aufnahme gekommen sein. Die Folgen wären damit ungleich größer als beim bloßen Mithören. Deswegen ist eine unterschiedliche Behandlung der beiden Sachverhalte gerechtfertigt. Ist also die Aufzeichnung eines Gesprächs geplant, sollte der Angerufene zuvor über diesen Plan informiert werden und wenn er dem zustimmt, sollte nach Beginn der Aufnahme die Einwilligung des Angerufenen wiederholt werden, damit selbige auch aufgezeichnet ist. Dies dient vor allem Beweiszwecken im Hinblick auf § 201 Abs. 1 Nr. 1 StGB. Von einer konkludenten Zustimmung mit der Möglichkeit eines opt-outs kann bei einer Aufzeichnung deshalb grundsätzlich nicht ausgegangen werden.

Hinsichtlich des Beschäftigten kann aufgrund des Abhängigkeitsverhältnisses in dieser Situation von keiner freiwilligen Einwilligung ausgegangen werden. Deshalb muss sich die Zulässigkeit grundsätzlich aus den Kontrollpflichten des Arbeitgebers hinsichtlich des Gesprächsinhalts ergeben. In engen Grenzen ist deshalb die offene Erhebung von Kommunikationsinhalten zulässig zu Zwecken der Einarbeitung und Überprüfung in der Probezeit, aber auch während der Laufzeit des Vertrags zur Qualitätskontrolle stichprobenweise. Die Grenzen sollten sich in etwa an dem im Urteil des Bundesarbeitsgerichtes von 1996 orientieren (BAG, Beschluss vom 30.08.1995 - 1 ABR 4/95) das für eine entsprechende Betriebsvereinbarung, die dies erlaubt, entschieden hat. Dies kann auch heutzutage im Lichte des § 32 BDSG so gesehen werden. Eine lückenlose Erhebung von Kommunikationsdaten und –inhalten ist aber auch hier unzulässig.[44]
Ein regelmäßiges Aufzeichnen ist bei bestimmten Geschäften am Telefon jedoch unerlässlich. Dies gilt beispielsweise für Telefonate im Rahmen von Bank- und dort insbesondere Wertpapiergeschäften: hier ist eine Aufzeichnung der Gesprächsinhalte für den Arbeitgeber zwingend notwendig, um im Nachhinein die durch den Anrufer gegebenen Anordnungen beweisen zu können, und sich so vor schadensersatzrechtlichen Ansprüchen zu schützen. Das Recht des Beschäftigten am gesprochenen Wort tritt hier ausnahmsweise im Rahmen einer Interessenabwägung zurück. Sollten die Beteiligten mit der Aufzeichnung der Inhalte nicht einverstanden sein, muss das Gespräch beendet und die Transaktion z.B. schriftlich fortgeführt werden.
Die Ausrichtung und Absicherung des am Telefon durchgeführten Geschäfts kann somit eine Rechtfertigung für den Arbeitgeber zum Aufzeichnen des Gesprächs darstellen. Dennoch sind auch in diesem Fall alle Beteiligten hierüber zu informieren.Liegt eine Einwilligung in das Aufzeichnen nicht vor, kann sich der Arbeitgeber auch hier **strafbar gem.** § 201 Abs. 1 Nr. 1 StGB machen.

[43] BVerfG, Beschluss v. 9.10.2002, 1 BvR 1611/96, 1 BvR 805/98, Zeile 46
[44] WHW/Byers B.VIII. Rn. 12; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 758 ff. § 32 Abs. 1 S. 1 BDSG.

Mitarbeiter mit Sonderstatus

Besondere Beachtung finden sollte die Kontrolle der Telekommunikationsdaten bei Mitarbeitern, die einem Sonderstatus dahingehend unterliegen, dass sie anderen Gruppen gegenüber zu Verschwiegenheit bzw. Vertraulichkeit verpflichtet sind. In dem Fall muss ggf. das Kontrollinteresse des Arbeitgebers dahinter zurückstehen. Explizit vor Kontrollen geschützt sind die **Träger eines Berufsgeheimnisses** gem. § 1 Abs. 3 Satz 2 BDSG. Die Berufsgruppen hierzu ergeben sich aus § 203 Abs. 1 StGB. Hier darf eine Speicherung der Telekommunikationsdaten, die zur Identifizierung von Gesprächspartnern führen könnte, nicht stattfinden.
Umstritten, aber wohl zu bejahen ist das Verbot der Speicherung von Rufnummern sowohl angewählter wie auch eingehender Gespräche bei **Journalisten**. Unabhängig davon, ob man auf das Zeugnisverweigerungsrecht[45] oder das Grundrecht der Pressefreiheit verweist, erfordert eine funktionierende, freie Presse einen wirksamen Schutz von deren Quellen.
Ebenfalls untersagt ist die Kontrolle der Telefonate des **betrieblichen Datenschutzbeauftragten**, der den Betroffenen gegenüber zu Verschwiegenheit über deren Identität verpflichtet ist, § 4f Abs. 4 BDSG.
Anders ist die bei Telefonaten des **Betriebs- bzw. Personalrats**. Unter dem Aspekt der Kostenkontrolle können die Gesprächsdaten der ausgehenden (nicht aber eingehender) Gespräche gespeichert werden. Eine Auswertung über diesen Zweck hinaus jedoch darf nicht stattfinden.

Inhalte einer Dienstanweisung zu elektronischen Kommunikationssystemen

Alternativ zu einer **Betriebsvereinbarung**, die die Überwachungs- und Protokollmöglichkeiten mit dem Betriebsrat abstimmt, kann jedes Unternehmen eine **Dienstanweisung** «Elektronische Kommunikationssysteme und informationstechnische Infrastruktur» an seine Mitarbeiter herausgeben, die die Nutzung des Unternehmensnetzwerks, von Internet und E-Mail-Diensten transparent macht und regelt.
Diese Inhalte sollten abgedeckt werden:

- Gegenstand und Geltungsbereich der Dienstanweisung
- Zielsetzung (informations- und kommunikationstechnische Infrastruktur mit dem Schutz der Persönlichkeitsrechte zu verbinden)
- Dokumentation: Speicherfristen und Umfang mit Daten
- Nutzung der Kommunikationstechniken
  - E-Mail-System
  - Internetzugang
  - Maßstab der Nutzung ist Ansehen des Unternehmens
- Fürsorgepflicht des Arbeitgebers (Privatnutzung dieser Medien beschränken auf Notfälle und unaufschiebbare Fälle, bei denen eine andere Erreichbarkeit nicht möglich ist)
- Besondere Regelungen zur elektronischen Post
- Besondere Regelungen für die Internetnutzung (Überwachungsumfang)
- Umgang mit dem konzerninternen Netz
  - Aufzeichnungen und Auswertungen benennen
  - Zwecke der Auswertung (neben Datensicherheit auch Missbrauchskontrolle)
  - Fremde Soft- und Hardware
  - Untersagung von webbasierten Programmen (sog. Cloud-Computing z. B. durch Office-Produkte von «Google»)
- USB-Policy zum Umgang mit mobilen Speichermedien (sämtliche Speichermedien, PDAs, Blackberrys[46], Handys)
- Benennung der Dienstanweisung als verbindlich, der bei Zuwiderhandlung arbeitsrechtliche Maßnahmen folgen können

[45] Vgl. §§ 53 Abs. 1 StPO, 383 Abs. 1 Nr. 5 ZPO.
[46] Der Einsatz von BlackBerrys im Unternehmen ist beteiligungspflichtig, ArbG Darmstadt, Beschluss v. 11.4.2007, 5 BV 7/07.

Digitale Personalakten

Das papierlose Büro ist noch immer ein Wunsch vieler Unternehmer, dessen Erfüllung in der Zukunft liegt. Dennoch rücken mit den heute verfügbaren Technologien solche Träume bereits in greifbare Nähe. Mit digitalen Personalakten ist die Ersetzung der Papierakte gemeint, die heute schon vielfach zumindest ergänzend zum Einsatz kommt. Mit dem Scannen von Dokumenten, einem Dokumentenmanagement oder einer komplexen HR-Software dienen noch existierende Papierakten lediglich zur Archivierung.
Neben der Ersparnis von Papierbergen steht dabei vor allem im Vordergrund, dass nun jedem Zugriffsberechtigten jederzeit überall eine vollständig bearbeitbare Akte zur Verfügung steht und dass notwendige Statistiken leichter zu erstellen und zu pflegen sind. Die digitalen Akten bieten viele neue Gestaltungs- und Auswertungsmöglichkeiten.

Grundsätze der Personalaktenführung

Eine Personalakte beinhaltet regelmäßig den gesamten dienstlich relevanten Lebensablauf eines Mitarbeiters, belegt und ergänzt durch weitere Dokumente. So sammeln sich in der Akte regelmäßig höchst sensible Daten über den jeweiligen Beschäftigten, die einen entsprechenden Schutz verdienen. Das Führen einer Personalakte und die Aufzeichnung dieser Daten ist für den Arbeitgeber aber keineswegs verpflichtend. Der Arbeitgeber ist gesetzlich nicht verpflichtet, eine Personalakte zu führen und der Beschäftigte hat kein generelles Recht darauf, dass der Arbeitgeber bestimmte Daten oder Dokumente für ihn aufbewahrt.
Allerdings muss der Arbeitgeber das Persönlichkeitsrecht und die freie Entfaltung der Persönlichkeit seiner Beschäftigten schützen und fördern.[47] Hieraus lassen sich Pflichten ableiten, die für den Fall einzuhalten sind, dass der Arbeitgeber eine Personalakte über seine Beschäftigten anlegt. Daraus haben sich die klassischen Grundsätze des Personalaktenrechts herausgebildet.[48] Diese sind der

- Grundsatz der Vertraulichkeit
- Grundsatz der Richtigkeit
- Grundsatz der Zulässigkeit und
- Grundsatz der Transparenz

Diese Grundsätze müssen eingehalten werden, unabhängig davon, in welcher Form – ob digital oder in Papier – die Akte geführt wird.

Vertraulichkeit der Personalakte

Die Vertraulichkeit einer Akte ist gewährleistet, wenn die Zugriffsmöglichkeiten so gering wie möglich gehalten werden und der Nutzerkreis nach genauen Regeln definiert ist. Außerhalb des Nutzerkreises ist jedem der Zugang zu verweigern. Die berechtigten Nutzer haben die erhaltenen Informationen nur in gesetzlich legitimierten Fällen oder Fällen der wirksamen Einwilligung durch den Beschäftigten an Dritte weiterzugeben. Bei der Entwicklung eines Berechtigungskonzepts für den Zugriff auf digitalisierte Akten sollte man sich deshalb von der Frage leiten lassen: Muss ein Mitarbeiter der Abteilung A, B, C im Rahmen seiner Aufgaben Zugriff auf bzw. Einblick in die enthaltenen Informationen X, Y, Z haben?
Unzulässig ist es beispielsweise, wenn ein ehemaliger Arbeitgeber dem neuen Arbeitgeber z. B. telefonische Auskunft über einen Beschäftigten erteilen soll. Eine legale Auskunft lässt die Zweckbindung der Daten auf diesem Weg nicht zu.[49]
Die Verarbeitung von Beschäftigtendaten in einem (internationalen) Konzern (shared services) sollte grundsätzlich bereits über Informationen und Regelungen im Arbeitsvertrag «angekündigt» werden. So sollte eine Personaldatenverarbeitung durch die Konzernmutter oder eine Einsatzmöglichkeit bei anderen Konzerntöchtern bereits im Arbeitsvertrag erwähnt werden. Sinnvoll ist es hier, den Zweck z. B. der idealen Personalverteilung im Unternehmen und einer möglichen Karriereförderung mit anzugeben.
Eine Konzernbetriebsvereinbarung ersetzt nicht die persönliche Einwilligung des Beschäftigten. Deshalb sollte man den Beschäftigten im Arbeitsvertrag in die konzernweite Verarbeitung seiner Daten konkret einwilligen lassen. Eine transparente Aufklärung des Beschäftigten im Arbeitsvertrag

---

47 § 75 Abs. 2 BetrVG und die allgemeinen Normen des BDSG.
48 Vgl. *Zilkens/Klett* Datenschutz im Personalwesen, DuD 2008, S. 41 ff.
49 Vgl. *Gola/Wronka* Handbuch zum Arbeitnehmerdatenschutz, 4.A., Rn. 1086 ff.

darüber, was mit seinen Daten warum passiert und die Einbeziehung einer möglichen expliziten Einwilligung hierein, wird sich auf die Zulässigkeit der Verwendbarkeit von Daten aus der Personalakte positiv auswirken.
Wie sich die Anwendung des § 32 BDSG, der lediglich § 28 Abs. 1 Nr. 1 BDSG a. F. ersetzen soll, entwickelt, ob diesem künftig auch eine Abwägung innewohnen wird oder ob man die zentralisierte Personaldatenverarbeitung unter die «ordnungsgemäße Durchführung des Arbeitsverhältnisses» wird fassen müssen, bleibt abzuwarten.

Richtigkeit und Vollständigkeit der Personalakte

Da der Arbeitgeber über seine Angestellten Leistungsdaten wie beispielsweise Leistungsbeurteilungen oder Urteile zur sachlichen Befähigung verfassen und speichern darf, ist der Grundsatz der Richtigkeit der Akte nicht ganz einfach umzusetzen. Der Grundsatz der Richtigkeit bezieht sich sowohl auf Tatsachenbehauptungen wie auf wertende Aussagen. Deswegen muss bei der Speicherung von Leistungsdaten darauf geachtet werden, dass der durch die Akte vermittelte Gesamteindruck des Beschäftigten zutreffend ist. Eine massiv unzutreffende Darstellung wäre ein unzulässiger Eingriff in das Persönlichkeitsrecht des Beschäftigten.
Aus dieser Feststellung erwächst das Recht des Beschäftigten, selbst Erklärungen in die Personalakte aufnehmen zu lassen[50] und der Anspruch auf Korrektur oder Entfernung unzutreffender Sachverhalte, § 34 BDSG.[51]
Als weiterer Teilaspekt tritt zur Richtigkeit die Vollständigkeit hinzu. Nur ein vollständiges Gesamtbild ist auch ein richtiges. Beide Parteien haben ein Anrecht auf eine lückenlose Darstellung der dienstlichen Laufbahn.[52]

Zulässigkeit und Transparenz der Personalakte

Die Unzulässigkeit von Personalakteninhalten ist an den soeben beschriebenen Grundsätzen zu messen. So können Daten unzulässig gespeichert sein, wenn deren Verwendung trotz inhaltlicher Richtigkeit gegen das **Persönlichkeitsrecht des Beschäftigten** verstoßen würde. Dies ist beispielsweise bei Daten der Fall, die bei einem **betrieblichen Eingliederungsmanagement** erhoben wurden: Diese dürfen nicht Bestandteil der Personalakte werden und auch nicht im Rahmen von Kündigungsverfahren gegen den Beschäftigten verwendet werden (Verwertungsverbot).[53] Unzulässig sind ebenso Inhalte, die nicht den wahren Tatsachen entsprechen oder ein verzerrtes Persönlichkeitsbild des Beschäftigten zeichnen.
Um dies kontrollieren zu können, gewährt der **Grundsatz der Transparenz** dem Beschäftigten ein Einsichtsrecht in seine eigene Personalakte, vgl. § 83 Abs. 1 BetrVG und § 34 BDSG. In den Tarifverträgen erhält der Transparenzgrundsatz teilweise eine besonders intensive Ausprägung: So regelt § 3 Abs. 6 TV-L[54], dass die Beschäftigten vor Eintragung von für sie ungünstigen Tatsachen in die Akte gehört werden müssen.

Gewährleistung der Datenschutzanforderungen bei der digitalen Akte

Eine rechtliche Grundlage für die automatisierte Verarbeitung von Beschäftigtendaten war in der Vergangenheit § 28 Abs. 1 Nr. 1 BDSG a. F. im Rahmen des Arbeitsvertrags. Dieser wurde zum 1.9.2009 durch § 32 BDSG ersetzt, der die Zweckbindung für Beschäftigtendaten auf Anbahnung, Durchführung und Beendigung des Beschäftigtenverhältnisses[55] beschränkt. Gleichwohl ändert sich an dieser Stelle für den Arbeitgeber wenig, da die grundsätzliche Führung von Personalakten zur Durchführung des Beschäftigtenverhältnisses datenschutzrechtlich zulässig bleiben wird, unabhängig davon, ob die Akten schon bisher strukturiert in einem systematischen Archivsystem oder in digitalisierter Form geführt wurden.

---

[50] § 83 Abs. 1 BetrVG.
[51] Oder außerhalb des Geltungsbereichs des BDSG gemäß §§ 242, 1004 BGB.
[52] BAG, Urteil v. 12.9.2006, 9 AZR 271/06.
[53] Vgl. dazu unten Checkliste im Abschnitt 7.6.2 zu den Anforderungen des Datenschutzes beim Eingliederungsmanagement.
[54] Tarifvertrag für den öffentlichen Dienst der Länder (TV-L) v. 12.10.2006 in der Fassung des Änderungstarifvertrags Nr. 2 v. 1.3.2009.
[55] § 3 Abs. 11 BDSG.

Verlust des Beweiswerts

Grundsätzlich ist das Digitalisieren von Dokumenten mit rechtlichen Risiken verbunden, da sich der Beweiswert im Rechtsstreit verringert oder zumindest ungeklärt ist. Vor Gericht gilt eine Urkunde dann als vollständig und richtig, wenn sie im Original unterzeichnet ist, § 420 ZPO. Das Gericht kann allerdings durch Inaugenscheinnahme eines ausgedruckten Dokuments dessen Inhalt im Rahmen einer freien Beweiswürdigung werten, § 286 Abs. 1 Satz 1 ZPO. Dies ist dem Gericht allerdings nicht in allen Verfahren(-steilen) möglich und hat nicht denselben Beweiswert wie eine Originalurkunde. Wenn das Dokument mit einer qualifizierten elektronischen Signatur (§ 2 Nr. 3 SigG[56]) versehen ist, ist nach dem Gesetzeswortlaut des § 371a Abs. 1 ZPO im Grunde eine Gleichstellung zur Originalurkunde gewollt. Dennoch ist dies umstritten, da teilweise die Gerichte trotz des eindeutigen Wortlauts gegen den Beweiswert einer solchen Signatur entscheiden.[57]
Dokumente, bei denen der Verdacht einer Fälschung aufkommen könnte, die dem Beschäftigten nach Beendigung des Arbeitsverhältnisses auszuhändigen oder die grundsätzlich wichtig für ein Beschäftigtenverhältnis sind, sollten deshalb auch künftig sicherheitshalber in Papierform vorgehalten werden.

Notwendigkeit einer Vorabkontrolle, § 4d Abs. 5 BDSG

Vor der Inbetriebnahme eines digitalisierten Personalaktensystems sollte der Datenschutzbeauftragte die Risiken einer solchen Verarbeitung durch eine Vorabkontrolle gem. § 4d Abs. 5 BDSG überprüfen und dokumentieren. Eine solche **Risikoanalyse** hilft, Schwachstellen und potenzielle Risiken zu identifizieren und diesen von Beginn an wirksam zu begegnen. Außerdem sollten im Rahmen der Vorabkontrolle auch Szenarien für die technische Verfügbarkeit über die gesamte Speicherdauer entworfen werden.

Ordnungsgemäße Archivierung

Da auch die Inhalte einer Personalakte in die Jahre kommen, sollte bei der Übernahme der alten Akten in das neue System geprüft werden, welche Dokumente übernommen werden müssen.
Mit einer solchen Überprüfung können gleich mehrere Ziele erreicht werden: Zum einen kann für mehr Datenschutz gesorgt werden, weil die Löschpflicht nach § 35 BDSG erfüllt wird. Zum anderen entstehen weniger Kosten für Speicherplatz und eventuell auch externe Dienstleister, die die Akteninhalte einscannen müssen.
Für die Archivierung digitalisierter Personalakten gelten dieselben Anforderungen wie für alle anderen personenbezogenen Daten. Dies sind insbesondere die Grundsätze ordnungsgemäßer datenverarbeitungsgestützter Buchführungssysteme (GOBS), vgl. hierzu oben Abschn. 2.1. zur E-Mailarchivierung. Unabhängig davon gelten die allgemeinen Anforderungen der Anlage zu § 9 BDSG, die die technischen Sicherheitsparameter für die Datenspeicherung vorgibt.

Auswertungsmöglichkeiten und Skilldatenbanken

Die gesteigerten Auswertungsmöglichkeiten, die sich aus vollständig digitalisierten Akten ergeben, bieten für Arbeitgeber und Arbeitnehmer Möglichkeiten zur **optimalen Nutzung eigener (betrieblicher und privater) Potenziale**. Grundsätzlich ist es dem Arbeitgeber deshalb erlaubt, sog. Skilldatenbanken über seine Beschäftigten oder Bewerber zu erstellen. Für die Zulässigkeit solcher Systeme muss streng darauf geachtet werden, dass die erstellten Profile ausschließlich Merkmale umfassen, die **für die Durchführung des Beschäftigtenverhältnisses notwendig** sind und dass der **Zugang zu den Datenbanken äußerst restriktiv gehandhabt** werden muss.
Des Weiteren muss darauf geachtet werden, dass bei Personalentscheidungen immer **ein Mensch das** «**letzte Wort**» hat und nicht die Maschine: Das Ergebnis einer Datenbankauswertung darf nicht als alleinige, automatische Grundlage für eine Personalentscheidung herangezogen werden. Aus diesem sog. Verbot der automatisierten Einzelentscheidung gem. § 6a BDSG heraus hat der Beschäftigte ein Anrecht auf die Offenlegung der Entscheidung, um noch einmal die Möglichkeit zu erhalten, Aspekte vorzubringen, die bei der Entscheidung möglicherweise außer Acht gelassen

---

[56] Signaturgesetz v. 16.5.2001, BGBl. I S. 876.

[57] So z. B. in BGH, Beschluss v. 25.10.2007, I ZB 19/07, in dem eine Titelausfertigung mit qualifizierter elektronischer Signatur trotz des eindeutigen Wortlauts des § 317 Abs. 5 ZPO als für die Vollstreckung ungeeignet beurteilt wird; zur Thematik: *Roßnagel/Wilke* NJW 2006, S. 2145.

wurden. Um das bewerten zu können, gibt § 6a Abs. 3 BDSG dem Betroffenen ein Recht auf Auskunft über den logischen Aufbau über das Auswertungsverfahren.

Checkliste digitale Personalakte

Folgende Eckpunkte sollten beim Anlegen von digitalisierten Personalakten beachtet werden. Diese können so auch Bestandteil einer Betriebsvereinbarung werden:

- Festlegung des Inhalts und Dauer der Aufbewahrung
- Regelungen über besonderen Schutz für Aktenteile mit sensiblen Daten wie z. B. Gesundheitsdaten.
- Prüfung, ob nicht ein berechtigter Widerspruch des Betroffenen für sensible Daten vorliegt, §§ 35 Abs. 5, 20 Abs. 5 BDSG i. V. m. Art. 14 Satz 1 Buchst. a EG-RL 95/46.
- Zugriffs-Berechtigungskonzept für Personalsachbearbeiter, Geschäftsführung und IT-Mitarbeiter.
- IT-Mitarbeiter sollten zum Akteninhalt nur durch ein geteiltes Passwort[58] Zugang erhalten.
- Regeln zur Auswertung der Akteninhalte (z. B. bei Data-Mining-Verfahren)
- Protokollierung, wer was wann an den Daten verändert.
- Transparenz für Beschäftigte: Auskunftsmöglichkeit über die Personen, die Zugriff zur eigenen Akte haben.

Anforderungen an Online-Bewerbungen

Der Bewerbungsprozess hat sich in den vergangenen zehn Jahren für Unternehmen stark gewandelt. Mussten früher alle Bewerbungen in Papierform erfasst und ausgewertet werden, so existieren heute bereits vollständige Online-Workflow-Prozesse, die von Beginn an die Daten der Bewerber in entsprechende Datenbanken einspeisen und dort auswertbar zur Verfügung halten. Dem ist datenschutzrechtlich grundsätzlich nichts entgegenzuhalten, solange die Daten sicher übermittelt werden und der Bewerber zuvor erfährt, was genau mit seinen Daten passiert. Hierfür bedarf es bei Online-Systemen einiger technischer Vorgaben und konkreter Einwilligungen der Betroffenen.
Dies ist bei Online-Bewerbungen zu beachten:

- Alle Dateneingaben sollten auf gesicherten Seiten erfolgen (https-Protokoll)
- Aufklärung über den Zweck und die genaue Verwendung der Daten (Zugriff durch Konzerngesellschaften, Verwendung für andere Positionen)
- Konkrete Einwilligung in die Datennutzung für den o. a. Zweck; ggf. Einwilligung in die Weitergabe an beauftragte Subunternehmer[59]
- Aufklärung über die Speicherdauer (grundsätzlich 6 Monate, bei begründeten Einzelfällen[60] nach vorheriger Einwilligung bis zu 3 Jahre)
- Explizite Einwilligung, wenn mehrere Unternehmen eines Konzerns Zugriff erhalten sollen.
- Aufklärung über zugreifenden Personenkreis (z. B. Betriebspsychologen, Recruiter, Subunternehmer).
- Für den Fall, dass Bewerbungen anhand bestimmter, vordefinierter Kriterien automatisiert abgelehnt werden, ist der Bewerber hierauf explizit hinzuweisen. Dem Bewerber ist im Falle der Ablehnung deshalb die Möglichkeit zur Stellungnahme zur Ablehnung einzuräumen.

Die oben unter Abschn. 6.2.4 beschriebenen **Skilldatenbanken** kommen insbesondere bei Bewerberverfahren zum Einsatz, um die oft hohe Anzahl an Bewerbungen schneller bewerten und beurteilen zu können. Das bedeutet, dass über jede Ablehnung einer Bewerbung letztlich immer ein Mensch das letzte Wort sprechen muss. Eine rein automatisierte Entscheidung ist datenschutzrechtlich unzulässig. Die Bewerber haben dieselben Auskunftsrechte wie schon oben beschrieben, insbesondere über den logischen Aufbau der automatisierten Entscheidung.
Daraus ergibt sich auf den ersten Blick ein Konflikt mit den für einen Arbeitgeber notwendigen Schutzmaßnahmen, die er aufgrund der **Vorgaben des Allgemeinen Gleichbehandlungsgesetzes (AGG)** ergreifen sollte: Aufgrund der möglichen schadensersatzrechtlichen Ahndung bei der Diskriminierung von Bewerbern im Sinne des AGG, kann keinem Arbeitgeber mehr geraten werden, Bewerbern Auskunft über die Ablehnungsgründe zu geben.

---

[58] Ein geteiltes Passwort ist ein Passwort, dessen zwei Hälften jeweils einer anderen Person bekannt sind: Um Zugang zu den Daten zu erhalten, müssen also beide Personen anwesend sein (Vier-Augen-Prinzip).

[59] Treffen diese eine Entscheidung im Bewerberverfahren, liegt regelmäßig keine Auftragsdatenverarbeitung gem. § 11 BDSG vor, sondern eine Funktionsübertragung, in die eingewilligt werden muss.

[60] Eine von vornherein pauschale Einwilligung aller Bewerber in diese Speicherdauer ist unwirksam.

Dennoch muss der Arbeitgeber gem. § 6a Abs. 3 BDSG Auskunft über den logischen Aufbau der automatisierten Verarbeitung geben. Beantragt der Bewerber also eine Auskunft hierüber gem. § 34 BDSG, so ist es jedoch ausreichend, wenn die Funktionsprinzipien der Anwendungssoftware bzw. die Grundzüge des Scoringverfahrens dargestellt werden.[61] Das Gesetz erwartet die Erläuterung, was mit den Daten geschieht, nicht jedoch die Preisgabe von Geschäftsgeheimnissen wie z. B. Auskunft über die eingesetzte Software.[62]

Rechte des Betriebsrats

Umfang der Mitbestimmung

Wie weit die Mitbestimmungsrechte der Betriebsräte bei digitalisierten Personalakten gehen, ist umstritten. Die Meinungen unterscheiden nach den Auswertungsmöglichkeiten, die sich aus dem jeweiligen System ergeben.[63] Da der Grund für die Einführung der digitalisierten Akten letztlich immer auch die besseren Kontroll- und Auswertungsmöglichkeiten sein werden, ist die zumindest theoretische Möglichkeit der technischen Überwachung der Beschäftigten einzuräumen. Damit greift das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG zumindest dann ein, wenn durch die Digitalisierung Leistungsdaten gesucht und differenziert zusammengestellt werden können.
Gemäß § 92 Abs. 1 BetrVG hat der Arbeitgeber den Betriebsrat über die Personalplanung, insbesondere über den gegenwärtigen und künftigen Personalbedarf, sowie über die sich daraus ergebenden personellen Maßnahmen und Maßnahmen der Berufsbildung anhand von Unterlagen rechtzeitig und umfassend zu unterrichten sowie Art und Umfang der erforderlichen Maßnahmen mit dem Betriebsrat zu beraten. Soweit die digitale Personalakte als Mittel der Personalplanung eingesetzt wird und Entscheidungshilfe dazu ist, welche Mitarbeiter an welchen Weiterbildungsmaßnahmen teilnehmen sollen, ist der Betriebsrat nach § 92 Abs. 1 BetrVG zu beteiligen.
Bei der Mitbestimmung durch den Betriebsrat sollte dieser darauf achten, dass die Auswertungen keine technische Totalüberwachung der Mitarbeiter ermöglichen und dass die erstellbaren Profile und Leistungsdaten ausschließlich Teilaspekte der beruflichen Tätigkeit beleuchten. Eine Berücksichtigung privater, familiärer oder gar konkreter gesundheitlicher Gründe muss hierbei ausgeschlossen sein. Eine Beschränkung der Digitalisierung auf die bloße Verwaltungserleichterung mit Auswertungen, die nicht darüber hinausgehen, als was durch Blättern in der Akte ebenfalls möglich wäre[64], ist abzulehnen. Beschränkte die Mitbestimmung des Betriebsrats eine Digitalisierung der Personalakten auf dieses Maß, würde das den Arbeitgeber in seiner unternehmerischen Entscheidungsfreiheit und der Wirtschaftlichkeit des Unternehmens über Gebühr einschränken.
Als Entscheidungsgrundlage kann dem Betriebsrat das Ergebnis der Vorabkontrolle des Datenschutzbeauftragten dienen.

Überwachungsmöglichkeiten

Ein uneingeschränkter Zugriff des Betriebsrats auf die Personalakten ist abzulehnen. Einem aus § 80 Abs. 2 BetrVG resultierenden Informationsanspruch steht das Persönlichkeitsrecht des Beschäftigten entgegen, dessen Ausprägung sich in § 83 Abs. 1 Satz 2 BetrVG widerspiegelt. Das Einsichtsrecht neben den Personalsachbearbeitern und der Geschäftsführung ist auf den Beschäftigten ggf. in Begleitung eines Betriebsrats beschränkt. Die uneingeschränkte Einsichtnahme unterliegt darüber hinaus der jeweiligen Einwilligung des Beschäftigten.
Aus § 80 Abs. 1 Nr. 1 BetrVG ergibt sich jedoch das Recht des Betriebsrats zu kontrollieren, ob die Normen zugunsten der Arbeitnehmer durch den Arbeitgeber eingehalten wurden. Deshalb sollte dem Betriebsrat ein Zugriff auf die aktuellen Stammdaten aller Beschäftigten eingeräumt werden, wenn dies verlangt wird.
Die Überwachung hinsichtlich der digitalisierten Personalakten durch den Betriebsrat sollte sich auf die Einhaltung der in der Betriebsvereinbarung festgelegten Verfahren und das vereinbarte Berechtigungskonzept beschränken.

---

61 *Bergmann, Möhrle, Herb* (Hrsg.), Kommentar zum BDSG, § 6a Rn. 14.
62 So auch der Erwägungsgrund 41 der EG-RL 95/46/EG.
63 Vgl. zum Meinungsstand *Gola,* Die Digitalisierung der Personalakte und der Datenschutz, RDV 2008, S. 135, 142.
64 So *Gola* a. a. O.

Elektronischer Versand von Gehaltsabrechnungen

Der Versand der Gehaltsabrechnungen an den Arbeitnehmer in elektronischer Form erscheint zeitgemäß und praktisch, kann doch so das Führen von umfangreichen Papierakten und der Aufwand der postalischen Versendung vermieden werden. Allerdings sollten Arbeitgeber nicht aus den Augen verlieren, dass bei der elektronischen Gehaltsabrechnung einige datenschutzrechtliche sowie technische Aspekte zu beachten sind. Auch die Rechte des Betriebsrates spielen bei der Einführung und Nutzung der elektronischen Gehaltsabrechnung eine Rolle. Schlussendlich sollte bedacht werden, dass gerade in der neuen Rechtsprechung das BAG dem Beschäftigtendatenschutz eine große Rolle eingeräumt hat.[65]
Beim elektronischen Versand von Gehaltsabrechnungen sind 2 Vorgänge zu beachten. Zum einen muss betrachtet werden, in welchem Format die Gehaltsabrechnung elektronisch gespeichert wird und versendet werden soll. Zum anderen ist die Sicherheit des Sendungsweges zu beurteilen.

Rechtliche Anforderungen

In der Regel dürfte eine elektronische Gehaltsabrechnung im pdf-Format abgespeichert und versandt werden. Das liegt zum einen daran, dass die Erstellung relativ problemlos zu bewerkstelligen ist. Zum anderen kann sich der Arbeitnehmer so seine Gehaltsabrechnung bei Bedarf ausdrucken. Zudem schreibt § 108 der Gewerbeordnung (GewO) vor, dass dem Arbeitnehmer die Gehaltsabrechnung in Textform auszuhändigen ist, sie muss demnach druckbar sein. Das Mindestmaß an das Format der elektronischen Gehaltsabrechnung muss sein, dass sie nachträglich nicht veränderbar ist. Das pdf-Format erfüllt diese Anforderung nur bedingt, da es durchaus Instrumente zur Bearbeitung gibt. Ideal wäre hierzu ein revisionssicheres Archiv-Format, das tatsächlich unveränderbar ist. Idealerweise sollte das Dokument zusätzlich mit einem Passwort versehen werden, das das Öffnen nur einem definierten Personenkreis erlaubt. So könnte z. B. jedem Arbeitnehmer bei seiner Einstellung bzw. bei der Einführung des elektronischen Verfahrens ein Passwort zugewiesen werden, dass nur er und die zuständige Stelle kennt.

Technische Anforderungen

Des Weiteren muss der Sendungsweg technisch aus Datenschutzsicht bewertet werden. Die Anforderungen hierfür legt § 9 BDGS und Anlage hierzu fest. Da die Gehaltsabrechnung auch sensible Daten, wie die Religionszugehörigkeit für den Kirchensteuerabzug und die Sozialversicherungsnummer des Arbeitnehmers enthalten, muss hier besonders sichergestellt werden, dass nicht unbefugte Dritte Einsicht in diese Daten nehmen können. Schon hieraus folgt, dass die E-Mail verschlüsselt versandt werden muss. Dabei sollte eine end-to-end-Verschlüsselung vom Rechner des Versenders bis zum Rechner des Empfängers zum Einsatz kommen, um eine größtmögliche Integrität gewährleisten zu können. Eine Alternative zur Verschlüsselung gibt es auch aufgrund der sonst entstehenden Haftungsrisiken für den Arbeitgeber hier nicht.
Sollten keine automatischen Verteiler beim E-Mail-Versand zum Einsatz kommen, muss darauf geachtet werden, dass bei einer manuellen Eingabe keine Fehler unterlaufen und die E-Mail eventuell bei einem anderen Empfänger ankommt. Dies lässt sich u. a. mit dem oben vorgeschlagenen Passwort-System vermeiden.

Gesundheitsdaten im Unternehmen

Die aktuellen Entwicklungen auf dem Gebiet des Personalmanagements, der Arbeitsorganisation und der Informationstechnologie am Arbeitsplatz haben die Erfassung personenbezogener Daten der Mitarbeiter verstärkt und ausgeweitet. Dieses Interesse richtet sich immer öfter auf die sog. «besonderen Arten personenbezogener Daten» im Sinne des § 3 Abs. 9 BDSG, bei denen es sich im Arbeitsverhältnis regelmäßig um Daten handelt, die die Gesundheit eines Menschen betreffen. Das Interesse eines Arbeitgebers an Gesundheitsdaten seiner Mitarbeiter ist häufig berechtigt. Es steht teilweise im Einklang mit dem der Mitarbeiter, ist diesem in einigen Fällen aber auch genau entgegengesetzt.
Die Gesundheit eines Mitarbeiters wird immer dann für den Arbeitgeber interessant, wenn beispielsweise die Ursache dafür im Bereich des Arbeitsplatzes liegt oder wenn die mangelnde

[65] BAG, Urteil v. 20.6.2013, 2 AZR 546/12 (LAG Hessen, ArbG Offenbach).

Gesundheit die Arbeitsleistung dauerhaft gefährdet. Dem steht wiederum das Interesse des Mitarbeiters an der Geheimhaltung seiner Privatsphäre entgegen, welches ein Ausdruck seines Persönlichkeitsrechts ist.
Um dieser teilweise komplexen Interessenlage gerecht zu werden, gibt es verschiedene Informations- und Geheimhaltungspflichten und -rechte.

Rechtsgrundlagen

Ein eigenes Gesetz zum Umgang mit Gesundheitsdaten oder zum Umgang mit Arbeitnehmer-Gesundheitsdaten existiert nicht. Die bestehenden Gesetze zum Umgang mit Gesundheitsdaten von Arbeitnehmern zeigen aber, dass dies auch nicht notwendig ist.
Die wichtigsten Normen für die Behandlung von Gesundheitsdaten im Beschäftigtenverhältnis sind:

1. **Ärztliche Schweigepflicht**: z. B. Patientengeheimnis gem. § 9 Musterberufsordnung der Ärztekammern[66] und § 203 StGB; ergänzt durch Datenverarbeitungsregeln im medizinischen Standesrecht.
2. **Datenverarbeitung durch private Arbeitgeber:** geregelt durch das Bundesdatenschutzgesetz. § 1 Abs. 2 Nr. 3 BDSG und § 27 BDSG legen die Anwendbarkeit fest. Spezielle Regelungen zum Umgang mit Arbeitnehmerdaten finden sich in den §§ 3 Abs. 11, 32 BDSG.[67] Diese legen fest, wer «Beschäftigter» ist und welche Zweckbindung für diese Daten im Allgemeinen gilt. Die bisher zentrale Regelung des § 28 Abs. 1 Satz 1, Nr. 1 BDSG wurde durch § 32 BDSG ersetzt. Zum speziellen Umgang mit Gesundheitsdaten enthält § 28 Abs. 6-9 BDSG Regelungen.
3. **Einwilligung des Betroffenen**: Eine Entbindung von der Schweigepflicht, wie auch die Verarbeitung von Gesundheitsdaten zu bestimmten Zwecken kann grundsätzlich auch auf einer Einwilligung basieren. Diese muss sich aber, neben den allgemeinen Anforderungen des § 4a BDSG, ausdrücklich auf die Verarbeitung der «sensitiven Daten» gem. § 3 Abs. 9 BDSG beziehen, § 4a Abs. 3 BDSG.
   Diese Einwilligung muss freiwillig erfolgen, d. h. ohne dass dies Konsequenzen für den Arbeitnehmer bei einer Verweigerung hat. Dies ist im Rahmen eines Beschäftigungsverhältnisses nicht unproblematisch, da hier häufig keine echte «Freiwilligkeit» vorliegen wird. Deshalb wurde für wirksame Einwilligungen im Beschäftigtenverhältnis ein Rahmen abgesteckt: Entweder dient die vorgesehene Nutzung der Daten (zumindest indirekt) maßgeblich den Interessen des Arbeitnehmers oder das Gesetz sieht diese Nutzung (zumindest mittelbar) vor.[68] Überschreitet die Einwilligung diese Anforderungen, so kann von einer Freiwilligkeit nicht mehr ausgegangen werden. Die Konsequenz ist eine Unzulässigkeit der Datennutzung.
4. **Der Betriebsrat** hat ein Mitbestimmungsrecht, soweit es sich um allgemeinverbindliche Regelungen zur Nutzung von Gesundheitsdaten handelt, § 87 Abs. 1 Nr. 1, 7 BetrVG. So z. B. für Datenerhebungen im Bewerbungsverfahren, bei der Gesundheitsvorsorge, bei der Erkundung von Gesundheitsproblemen im Betrieb oder für das Verfahren des betrieblichen Eingliederungsmanagements (BEM).[69] Das Mitbestimmungsrecht ist aber auf kollektivrechtliche Regelungen begrenzt: Bereits mehrfach haben Arbeitsgerichte in vergangenen Jahren Urteile gegen Personalvertretungen gefällt, die daran scheiterten, dass der Arbeitgeber bei der angegriffenen Maßnahme lediglich Einzelfälle klären und keine allgemeinverbindliche Regelung treffen wollte.
   Folgende Aspekte sollten dabei in einer **Betriebsvereinbarung** im Rahmen des § 87 Abs. 1 Nr. 7 BetrVG berücksichtigt werden:
   - Anlass der Datenerhebung bzw. Verarbeitung
   - Beteiligte mit Rechten und Pflichten
   - Art und die Verwendung der Daten
   - Umfang der Übermittlungen (Zweckbindung)
   - Datensicherheit und Aufbewahrung (Dauer und Löschung)
   - Kontrolle durch Betriebsrat und Datenschutzbeauftragten (zwingend)

---

66 MBO ÄK.
67 Sind am 1.9.2009 in Kraft getreten.
68 *Däubler*, Gläserne Belegschaften, Rn. 23.
69 Nicht aber zwingend bei der Beurteilung individueller Fälle im Rahmen des BEM; dies ist abzulehnen, wenn der Arbeitnehmer die Beteiligung des Betriebsrats nicht wünscht, vgl. LAG Hamburg, Urteil v. 21.5.2008, H 3 TaBV 1/08. Vgl. hierzu auch Abschn. 7.6.

Bewerbungsverfahren

Im Rahmen von Bewerbungsverfahren möchten Arbeitgeber häufig Auskünfte zu bestehenden Vorerkrankungen, Schwerbehinderungen oder zur Schwangerschaft haben. Diese Auskünfte sind dann zu gewähren, wenn sie für die ordnungsgemäße und sichere Durchführung des Beschäftigtenverhältnisses notwendig sind.
Für die Gesundheit sensible Arbeitsbereiche sehen häufig eine Eingangsuntersuchung vor, bevor die Tätigkeit überhaupt begonnen werden kann:

- Gem. § 43 Abs. 1 Infektionsschutzgesetz (IfSG) müssen Personen in der Lebensmittelproduktion oder in Küchen über eine Bescheinigung des Gesundheitsamts nachweisen, dass bestimmte Infektionskrankheiten nicht vorliegen.
- Ebenfalls eine verpflichtende Eingangsuntersuchung findet beim Umgang mit strahlenexponierten Tätigkeiten gem. §§ 60, 64 Strahlenschutzverordnung (StrlSchVO) statt.
- Weitere Regelungen gibt es für den Umgang mit biologischen Arbeitsstoffen[70], Röntgenstrahlung[71] oder für Seemänner.[72] Hier hat der Arbeitgeber die Pflicht, seinen Mitarbeitern diese Untersuchungen anzubieten. Für diese ist die Teilnahme freiwillig.

Sollen darüber hinaus Gesundheitsdaten von Bewerbern erhoben werden, so ist die Festlegung der Auswahlkriterien mitbestimmungspflichtig gem. § 95 Abs. 1, 2 BetrVG.
Neben der systematischen Erhebung und Speicherung von Bewerberdaten möchte ein Arbeitgeber schon nach dem Bewerbungsgespräch einschätzen können, ob der Bewerber geeignet ist oder nicht. Allerdings kann er Informationen in Bezug auf den gesundheitlichen Zustand nur eingeschränkt erfragen, weil die Gesetze das Persönlichkeitsrecht des Bewerbers schützen.
Grundsätzlich gilt: Der Arbeitgeber muss ein berechtigtes und schutzwürdiges Interesse an der Frage nach Gesundheitsdaten haben.[73] Dieses ist vor allem dann gegeben, wenn die Antwort notwendig ist, um die körperliche, geistige und gesundheitliche Eignung (nur) für die vorgesehene Tätigkeit festzustellen.[74]

Gesundheitsdaten während des Arbeitsverhältnisses

Der Arbeitnehmer hat grundsätzlich die Pflicht, sich «**krank zu melden**», wenn er aus gesundheitlichen Gründen nicht zur Arbeit erscheinen kann. Hierbei hat der Arbeitgeber kein Recht zu erfahren, welche gesundheitlichen Gründe dies im Detail sind. Er kann lediglich eine den Krankenzustand bestätigende Bescheinigung eines Arztes verlangen. Die Arztbescheinigung ist regelmäßig ab dem dritten Tag der Erkrankung vorzulegen.[75] Will der Arbeitgeber diese bereits eingeführte Vorlagefrist verkürzen, so ist dies mitbestimmungspflichtig gem. § 87 Abs. 1 BetrVG.[76]
Der Arbeitgeber hat das Recht sog. «**Krankengespräche**» nach Beendigung der Krankheit mit dem Arbeitnehmer durchzuführen, wobei dieser keine Details der Erkrankung nennen muss. Ein Mitbestimmungsrecht des Betriebsrats hierbei hängt von dem Ziel des Gesprächs ab. Ist das Ziel lediglich, festzustellen, ob der Beschäftigte noch den Anforderungen des Arbeitsplatzes gewachsen ist, bzw. ob künftig mit weiteren Störungen des Austauschverhältnisses zu rechnen ist, stellt dies keine Maßnahme des Gesundheitsschutzes im Sinne des § 87 Abs. 1 Nr. 7 BetrVG dar[77], weil es sich dann um keine allgemeinverbindlichen Maßnahmen für den Betrieb handelt.
Möchte der Arbeitgeber herausfinden, ob eine eine verhaltensbedingte Kündigung rechtfertigende negative Zukunftsprognose gegeben ist, sollte der Arbeitnehmer im eigenen Interesse überlegen, ob er dem Arbeitgeber Gesundheitsdaten offenbart, um eine Kündigung abzuwenden.
Eine Reihe weiterer Rechtsgrundlagen regelt die **Übermittlung von Gesundheitsdaten** im Beschäftigtenverhältnis:

- Ergänzend zu § 32 BDSG regelt § 28 Abs. 6 Nr. 3 BDSG die Zulässigkeit der Erhebung und Weiterverarbeitung von Gesundheitsdaten, soweit dies «zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht,

---

70 § 15 Biostoffverordnung.
71 Röntgenverordnung.
72 § 81 Abs. 1 SeemannsG.
73 BAG, Urteil v. 20.2.1986, 2 AZR 244/85, NZA 1986, S. 739.
74 Vgl. dazu «Anbahnung des Arbeitsverhältnisses».
75 § 5 Abs. 1 EFZG.
76 Vgl. LAG Hamburg, Urteil v. 21.5.2008, H 3 TaBV 1/08.
77 LAG Hamburg, a. a. O.

dass das schutzwürdige Interesse des Betroffenen» diesen überwiegt. Die Norm erfasst aber nur den Zweck der «Durchsetzung» nicht schon die «Begründung» solcher Ansprüche.

- Gem. § 69 Abs. 4 SGB X kann die Krankenkasse dem Arbeitgeber mitteilen, ob die Fortdauer oder erneute Arbeitsunfähigkeit eines Arbeitnehmers auf derselben Krankheit beruht. Diese Information benötigt der Arbeitgeber für den Entgeltfortzahlungs-Anspruch nach § 3 Abs. 1 Satz 2 EFZG.[78]
- Drogen- und Alkoholtests können nur bei «ernsthafter Besorgnis»[79] über eine Abhängigkeit begründet werden. Eine pauschale Untersuchung ist grundsätzlich unzulässig.
- Ein eindeutiges Verbot zur Nutzung von Gesundheitsdaten für bestimmte Zwecke enthält § 291a Abs. 8 SGB V im Bezug auf die elektronische Gesundheitskarte (eGK).

Gesundheitsdaten beim Betriebsarzt

Sinn und Zweck des Betriebsarztes ist die Förderung von Gesundheit und Arbeitssicherheit im Unternehmen. Dabei schützt er die Gesundheit der Arbeitnehmer, dient aber gleichzeitig auch den Interessen des Arbeitgebers. Dennoch unterliegt er wie alle anderen Ärzte auch der ärztlichen Schweigepflicht aus § 9 MBO-ÄK[80] bzw. § 203 StGB. Dies gilt auch gegenüber dem Arbeitgeber, § 8 Abs. 1 Satz 3 ASiG.[81]
Bei einer Einstellungsuntersuchung wird allerdings stillschweigend vorausgesetzt, dass das Ergebnis der Untersuchung dem Arbeitgeber so weit zur Kenntnis gegeben wird, wie die Einschränkungen für die Ausübung der Tätigkeit notwendig sind. Dabei besteht kein Informationsrecht des Arbeitgebers über die Art der Erkrankung oder über prognostizierte Entwicklungen.
Die Einholung einer pauschalen Entbindung von der Schweigepflicht im Rahmen des Arbeitsvertrags ist aufgrund des enormen Verhandlungsungleichgewichts unwirksam.[82] Jegliche Einwilligung des Arbeitnehmers muss einzelfallbezogen sein und kann jederzeit widerrufen werden.
Gesundheitsdaten bzw. Diagnosedaten, die im Rahmen von verpflichtenden Einstellungs- bzw. Nachuntersuchungen[83] vorgenommen werden, dürfen dennoch ausdrücklich nicht an das Unternehmen übermittelt werden, § 15 Abs. 2 Nr. 9 SGB VII. Zu den beim betrieblichen Eingliederungsmanagement erhobenen Daten vgl. unten Abschn. 7.6.2. Eine Übermittlung der Diagnose an den Träger der Unfallversicherung oder den Gewerbearzt ist für den Betriebsarzt verpflichtend, wenn er einen begründeten Verdacht für das Vorliegen einer Berufskrankheit hat, § 202 SGB VII i. V. m. § 5 BKV.[84]
Die vom Betriebsarzt erhobenen Gesundheitsdaten sind grundsätzlich streng getrennt von Personalakten aufzubewahren bzw. zu speichern. Der Betriebsarzt hat Sorge dafür zu tragen, dass ausschließlich seine Hilfspersonen Zugriff hierauf erhalten. Die Speicherdauer für diese Daten beträgt 10 Jahre.

Anforderungen an Speicherung und Verarbeitung

Soweit der Arbeitgeber befugt zum Besitz von Gesundheitsdaten ist, darf er diese auch speichern und im Rahmen der Zweckbindung nutzen. Sie dürfen in der Personalabteilung gespeichert werden und unterliegen dann nicht mehr dem Patientengeheimnis. Die Zweckbindung und damit die Verwendung der Daten richtet sich entweder nach der Einwilligung des Beschäftigten oder dem Zweck der Erhebung, der regelmäßig durch den Arbeitsvertrag definiert wird. Sind bei den gespeicherten Gesundheitsdaten besonders sensible Daten wie beispielsweise Gutachten gespeichert, so muss eine Kenntnisnahme auch durch den Personalsachbearbeiter begrenzt werden, wenn sie nicht zwingend notwendig ist.[85]
Gesundheitsdaten unterliegen teilweise aufgrund ihrer Zweckbindung sogar gerichtlichen Verwertungsverboten: So dürfen beispielsweise die Daten aus der Durchführung eines betrieblichen

---

78 *Franzen,* RDV 2003, S. 5 f.
79 BAG, Urteil v. 12.8.1999, 2 AZR 55/99, DB 1999, S. 2369.
80 Musterberufsordnung-Ärztekammer.
81 Arbeitssicherheitsgesetz.
82 *Bergmann, Möhrle, Herb* (Hrsg.), Kommentar zum BDSG, § 28 Rn. 66.
83 § 15 SGB VII.
84 Berufskrankheitenverordnung.
85 So auch BAG, Urteil v. 12.9.2006, 9 AZR 271/06.

Eingliederungsmanagements nicht bei einer krankheits- (personen-)bedingten Kündigung verwendet werden (vgl. dazu Abschn. 7.6.2).[86]
Dem Datenschutzbeauftragten des Unternehmens ist auf Anforderung Einsicht sowohl in Personalakten wie auch in Gesundheitsakten zu gewähren, § 4g Abs. 1 BDSG. Für den Datenschutzbeauftragten gilt zum Schutz dieser Daten seine Verschwiegenheitspflicht aus § 4f Abs. 4 BDSG, ein entsprechendes gerichtliches Zeugnisverweigerungsrecht des Dateninhabers (z. B. eines Rechtsanwalts) wird gem. § 4f Abs. 4a BDSG auf den Datenschutzbeauftragten übertragen.
Eine **Löschpflicht von Gesundheitsdaten** ergibt sich für den Arbeitgeber, wenn Daten zu Unrecht erhoben wurden, ihre Richtigkeit nicht vom Arbeitgeber bewiesen werden kann oder ihre Kenntnis für die Erfüllung der Pflichten nicht mehr erforderlich ist. Folgende Löschfristen sollten eingehalten werden:

- Krankheitsdaten von Arbeitnehmern: 12 Monate nach Beginn der Erkrankung, wenn die Fehlzeiten in einem Jahr 6 Wochen nicht übersteigen.
- Übersteigen die Fehlzeiten 6 Wochen in einem Jahr, so darf auf diese Daten für ein Kündigungsverfahren 4 Jahre lang zurückgegriffen werden.
- Die Speicherfrist für Daten aus dem betrieblichen Eingliederungsmanagement ist umstritten: die Daten sollten frühestens nach 3 Jahren, sicherheitshalber erst nach 5 Jahren in Absprache mit dem Betroffenen gelöscht werden.
- Gesundheitsdaten unterliegen regelmäßig nicht der 10-jährigen Speicherfrist, die sich für steuerlich relevante Unterlagen aus § 257 HGB und § 147 AO ergeben.

Betriebliches Eingliederungsmanagement

§ 84 Abs. 2 SGB IX sieht im Interesse der Gesundheitsprävention ein betriebliches Eingliederungsmanagement (BEM) bei Arbeitnehmern vor, die im Jahr länger als 6 Wochen krankheitsbedingt arbeitsunfähig waren. Das BEM ist eine Aufgabe des Arbeitgebers, dem hiermit ein Teil der Verantwortung für die Gesundheit der Beschäftigten als Pflicht aus dem Arbeitsverhältnis übertragen wurde.
Es ist im Rahmen des BEM zu klären, wie die **Arbeitsbedingungen** gestaltet werden können, um dem Betroffenen einen Verbleib in seiner Tätigkeit zu ermöglichen bzw. wie die Arbeitsunfähigkeit insgesamt überwunden werden kann. Innerhalb des Unternehmens sind die Personalvertretung und, wenn es sich um Schwerbehinderte oder gleichgestellte Beschäftigte handelt, die Schwerbehindertenvertretung einzubeziehen. Soweit erforderlich, wird der Betriebsarzt hinzugezogen.
Ziele des BEM sind Gesundheit, Leistungsfähigkeit, Motivation und Belastbarkeit der Mitarbeiter im Hinblick auf den Bestand des Arbeitsverhältnisses zu erhalten. Das grundsätzlich individuell zu gestaltende Eingliederungsmanagement basiert auf dem Prinzip des Dialogs und des Konsens. Dies ergibt sich aus dem Prinzip der Zusammenarbeit.[87][88]
Der Arbeitgeber muss dem Beschäftigten diese Möglichkeit anbieten, wenn die Voraussetzungen für das BEM vorliegen. Dies ist der Fall, wenn Beschäftigte innerhalb eines Jahrs **länger als 6 Wochen ununterbrochen oder wiederholt arbeitsunfähig krank** waren.
Für alle folgenden Maßnahmen ist grundsätzlich die **Zustimmung des Beschäftigten** notwendig. Das Vorgehen im Rahmen des BEM sollte also gemeinsam miteinander entwickelt werden. Die Zustimmung des Betroffenen ist auch notwendig für die Einschaltung von Dritten (intern oder extern).

Rechte und Pflichten der Beteiligten

Alle am BEM Beteiligten haben Rechte und Pflichten, die im Folgenden kurz zusammengefasst werden.[89] Um die Maßnahmen zu koordinieren kann ein sogenanntes «**Integrationsteam**» mit Vertretern aller beteiligten Gremien eingesetzt werden. Der Arbeitgeber-Vertreter sollte hierbei Entscheidungsbefugnis besitzen und aufgrund der Zweckbindung der Daten und der getrennten Aufbewahrung der Daten von den Personalakten kein Mitarbeiter der Personalabteilung sein. Externe Dritte (Dienstleister, staatliche Ämter) sind nicht Bestandteil des Integrationsteams, sie stehen lediglich beratend zur Seite.

---

[86] *Gundermann/Oberberg*, Datenschutzkonforme Gestaltung des Eingliederungsmanagements, RDV 2007, S. 105, 108.
[87] § 84 Abs. 1 Satz 1 SGB IX.
[88] Beitrag «Betriebliches Eingliederungsmanagement».
[89] Angelehnt an die Liste des GDD-Arbeitskreises «Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen», veröffentlicht in den GDD-Mitteilungen 2/2007, S. 7 ff.

Rechte und Pflichten von

- Arbeitgeber
  1. Pflicht zur Durchführung und Verantwortung für den Ablauf des Verfahrens
  2. Prüfung, ob die Voraussetzung für die Einleitung eines BEM vorliegen.
  3. Erste Kontaktaufnahme mit dem Betroffenen für Aufklärung und Ziel des Betroffenen
  4. Einholung einer schriftlichen Zustimmung des Betroffenen für die Durchführung des BEM
  5. Mit Zustimmung des Betroffenen Einbeziehung externer oder interner Dritter (gilt auch für Betriebs-, Schwerbehinderten- oder Personalvertretungen)[90]
  6. Regelmäßige Unterrichtung des Betroffenen über Fortschritte
- Betroffenen
  1. Zustimmung zur Einleitung des Verfahrens
  2. Mögliche Ablehnung von der Hinzuziehung bestimmter Dritter
  3. Beteiligung am gesamten weiteren Prozess
  4. Auskünfte geben über Belastungen am Arbeitsplatz, Auswirkungen auf die Leistungsfähigkeit
  5. Mitwirkung an ggf. notwendigen ärztlichen Untersuchungen
- Personalvertretung / Betriebsrat
  1. Recht auf Anstoß zur Einleitung des BEM
  2. Mitarbeit im Integrationsteam möglich
  3. Mitbestimmungspflicht nur bei Einführung eines standardisierten Verfahrens für das gesamte Unternehmen, nicht jedoch bei Einzelfällen
  4. Recht zur Überwachung, dass Arbeitgeber die ihm obliegenden Pflichten erfüllt

  Im Hinblick auf die Benennung der Namen der Mitarbeiter, die länger als 6 Wochen erkrankt waren, an den Betriebsrat, hat das BAG entschieden, dass der Arbeitgeber verpflichtet ist, diese Namen weiterzugeben.[91] Die Mitteilung der Namen der für die Durchführung eines betrieblichen Eingliederungsmanagements in Betracht kommenden Arbeitnehmer an den Betriebsrat sei zur Durchführung der sich aus § 80 Abs. 1 Nr. 1 BetrVG, § 84 Abs. 2 Satz 7 SGB IX ergebenden Überwachungsaufgabe erforderlich. Der Arbeitgeber muss dabei dem Betriebsrat die Namen der Arbeitnehmer mit Arbeitsunfähigkeitszeiten von mehr als 6 Wochen im Jahreszeitraum auch dann mitteilen, wenn diese der Weitergabe nicht zugestimmt haben. Die Erhebung und Nutzung dieser Angaben sei zur Erfüllung der sich für den Arbeitgeber aus § 84 Abs. 2 SGB IX ergebenden Pflichten nach § 28 Abs. 6 Nr. 3 BDSG zulässig. Dies umfasse auch deren Übermittlung an den Betriebsrat.
- Externe Dritte: Mögliche Themen für externe Dritte sind die Erbringung von Leistungen zur
  1. Erhaltung der Erwerbsfähigkeit
  2. ergonomischen Arbeitsplatzgestaltung
  3. beruflichen Qualifizierung
  4. Gewährleistung der Arbeitssicherheit
  5. Eine Beteiligung externer Dritter sollte erst erfolgen, wenn die innerbetriebliche Klärung konkrete Maßnahmen nahelegt.

Anforderungen des Datenschutzes

Die Einhaltung der Datenschutzbestimmungen bei der Durchführung des BEM ist einer der wichtigsten Bestandteile, um eine vertrauensvolle Zusammenarbeit mit dem Betroffenen zu ermöglichen. Da im SGB IX und X keine datenschutzrechtlichen Bestimmungen enthalten sind, muss auf die allgemeinen Bestimmungen zurückgegriffen werden.
Im Lichte des § 32 BDSG betrachtet, ist die Erhebung der Daten notwendig, um das Beschäftigtenverhältnis ordnungsgemäß durchführen zu können. Damit ist die grundsätzliche Datenerhebung im BEM auch von der neuen Grundsatznorm des BDSG erfasst. Die Datenerhebung (!) bei einem BEM unterliegt allerdings nicht der Regelung des § 28 Abs. 6 Nr. 3 BDSG, der die Verarbeitung für eigene Geschäftszwecke erlaubt, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche notwendig ist. Dies gilt auch auf dem Hintergrund des obigen Beschlusses des BAG fort, da dort diese Norm als Rechtfertigung für die Datenweitergabe diente,

[90] Abweichende Ansicht zur GDD von 2007, aufgrund abweichender Rechtsprechung (vgl. hierzu auch Abschn. 7.6.4).
[91] BAG, Beschluss v. 7.2.2012, 1 ABR 46/10.

nicht jedoch zur Datenerhebung. Dieser teilweise in der Literatur vertretenen Ansicht[92] kann aber insbesondere auf dem Hintergrund des Urteils des BAG vom 12.7.2007[93] nicht gefolgt werden. Das BAG hat hier festgestellt, dass die Daten aus einem BEM nicht als Begründung für eine Kündigung herangezogen werden dürfen

Das BEM darf allerdings **nicht** zur **Erhebung medizinischer Daten beim Arbeitgeber** führen. Die Einwilligung des Beschäftigten ist Voraussetzung für Einleitung und Fortführung des BEM. Das Verfahren ist einzustellen, sobald der Betroffene seine Mitarbeit hieran einstellt. Aufgrund der zu erhebenden Gesundheitsdaten gelten die Anforderungen an eine qualifizierte, datenschutzrechtliche Einwilligung gem. § 4a Abs. 3 BDSG, die über die Speicherung von Gesundheitsdaten aufklärt. Da das BEM meist gestaffelt in verschiedene Phasen abläuft, ist vor Beginn jeder Phase sicherzustellen, dass die vorgesehenen Maßnahmen und das Hinzuziehen von Dritten von der Einwilligung des Betroffenen abgedeckt sind.[94]

Um sicherzustellen, dass die Daten ausschließlich im Rahmen ihrer vorgesehenen Zweckbindung verwendet werden, müssen konkrete **Gesundheitsdaten des Betroffenen**[95] **getrennt** von den übrigen Daten **aufbewahrt** werden. Diese Daten sollten ausschließlich demjenigen zur Kenntnis gegeben werden, der diese für die Durchführung seiner Aufgabe unbedingt benötigt.

Der Betriebsarzt, der der ärztlichen Schweigepflicht unterliegt und Mitglied im Integrationsteam ist, kann anhand der medizinischen Diagnosen beurteilen, ob Maßnahmen des Eingliederungsmanagements geeignet sind und die Genesung ausreichend unterstützen. Deshalb ist die Kenntnis der konkreten Gesundheitsdaten für die Planung der Einzelmaßnahmen nicht notwendig. Das Integrationsteam sollte also keine Kenntnis hiervon erhalten.

Der Betriebsarzt darf die Diagnosen nur mit Zustimmung des Betroffenen Dritten zugänglich machen.

Andere Daten, die bei Durchführung des BEM anfallen, sind dem Arbeitgeber zur Verfügung zu stellen. Dies können Daten zur Aufklärung von Krankheitsursachen im Betrieb sein, wenn z. B. bestimmte Arbeitsbedingungen mit erhöhten Krankheitsraten einhergehen. Zu diesen Daten gehören selbstverständlich auch Daten über grundsätzliche Einschränkungen der Einsatzmöglichkeiten des Betroffenen oder eventuell zu erwartende Veränderungen des Krankheitsverlaufs ggf. mit und ohne weitere Maßnahmen.

[Beginn Tipp]

Praxis-Tipp

So führen Sie Akten im BEM

Die im Wege des BEM erhobenen Daten dürfen aufgrund des verstärkten Schutzbedürfnisses bei sensiblen Daten **nicht zusammen mit der Personalakte** gespeichert werden.[96]

Die Speicherung muss technisch und organisatorisch getrennt von der Personalakte erfolgen.

In die Personalakte darf lediglich aufgenommen werden, dass

- ein BEM mit bestimmten Maßnahmen angeboten wurde und
- ob der Beschäftigte einverstanden mit der Durchführung war, und
- ob eine Umsetzung der Maßnahmen erfolgte.

Nicht in die Personalakte gehören

- medizinische Daten des Betroffenen
- Gutachten und
- Stellungnahmen von Rehabilitationsträgern.

Die BEM-Akte darf nicht elektronisch gespeichert werden.[97]

Aktendoppel sind nicht zulässig.

Die **Speicherdauer** der BEM-Akte ist nicht eindeutig. Zu empfehlen ist eine Speicherung über 5 Jahre nach Überwindung der Dauererkrankung des Mitarbeiters aus dem Betrieb.[98]

---

92 *Gaul*, Aktuelles Arbeitsrecht, 2006, S. 186 ff.

93 Vgl. hierzu Abschn. 7.6.4, Rechtsprechung zum BEM.

94 *Bergmann, Möhrle, Herb* (Hrsg.), Kommentar zum BDSG, § 28 Rn. 82g.

95 Sensible Daten im Sinne des § 3 Abs. 9 BDSG.

96 Vgl. BAG, Urteil v. 12.9.2006, 9 AZR 271/06.

97 *Bergmann, Möhrle, Herb* (Hrsg.), Kommentar zum BDSG, § 28 Rn 82i.

98 So *Bergmann, Möhrle, Herb* a. a. O.; Berliner Landesbeauftragte für Datenschutz in Tätigkeitsbericht 2006, Ziff. 2.4.

Eine Verwendung der erhobenen Daten im Rahmen eines **Kündigungsverfahrens** ist aufgrund der Zweckbindung der erhobenen Daten und der ausdrücklich erforderlichen Einwilligung des Betroffenen in die Speicherung nicht zulässig.[99]
Der Umgang mit den Daten des Beschäftigten sollte vor Beginn des Verfahrens in einer Vereinbarung schriftlich festgelegt werden. Eine generelle Regelung hierfür kann auch im Rahmen einer Dienst- oder Betriebsvereinbarung erfolgen, die dann mitbestimmungspflichtig gem. § 87 Abs. 1 Nr. 7 BetrVG ist.
Die am BEM Beteiligten unterliegen sämtlich der **Schweigepflicht**. Diese ergibt sich im Einzelnen für

- Mitarbeitervertreter aus § 22 MVG,
- Schwerbehindertenvertreter aus §§ 96 Abs. 7 und 97 Abs. 7 SGB IX,
- für Rehabilitationsträger und Integrationsamt aus § 35 SGB I i. V. m. §§ 67 ff. SGB X.

[Ende Tipp]

Betriebsvereinbarung BEM

Dem Betriebsrat kommt eine Mitbestimmungspflicht im Rahmen des BEM dann zu, wenn der Arbeitgeber eine generelle Regelung für den Ablauf des Eingliederungsmanagements festlegen möchte, § 87 Abs. 1 Nr. 7 BetrVG. Diese Vorgehensweise ist grundsätzlich zu begrüßen, da ein Rahmen-Regelwerk den Beteiligten des oft sehr individuell ablaufenden BEM eine gewisse Sicherheit im Ablauf und im Umgang mit den Daten gibt.
Eine Betriebsvereinbarung zur Durchführung des BEM sollte deshalb folgende Punkte regeln[100]:

- Wer ist Vertreter des Arbeitgebers und spricht mit dem Beschäftigten?
- Systematische Festlegung der Information des Beschäftigten über Art und Verwendung der anfallenden Daten (z. B. über Formular)
- Aufklärung über den besonderen Schutz der Gesundheitsdaten beim Betriebsarzt und dessen Schweigepflicht
- Untersuchungsmethode für Gefährdungspotenziale am Arbeitsplatz
- Berücksichtigung vorangegangener Gefährdungsbeurteilungen[101]
- Speicherdauer der erhobenen Daten
- Wie erfolgt eine Kontrolle des BEM?
- Zweckbindung der Daten mit dem alleinigen Ziel Erhaltung des Arbeitsplatzes

Konsequenzen unbefugter Nutzung

Sollte sich ein Verdacht einer missbräuchlichen Nutzung der technischen Einrichtungen durch einen Beschäftigten bestätigen, stellt sich die Frage nach den Konsequenzen. Neben den arbeitsrechtlichen Maßnahmen wie Abmahnung und Kündigung, kommen organisatorische Maßnahmen wie Sperrung von Zugängen in Betracht. Weiter stellt sich die Frage nach der Haftung sowohl vom Beschäftigten gegenüber dem Arbeitgeber, wie auch vom Arbeitgeber gegenüber Dritten.

Arbeitsrechtliche Maßnahmen

Der mittlerweile recht umfangreichen Rechtsprechung zu arbeitsrechtlichen Maßnahmen beim missbräuchlichen Umgang mit Internet, E-Mail und Telefon lässt sich nur eines mit Gewissheit entnehmen: Die Zulässigkeit arbeitsrechtlicher Maßnahmen ist fast immer abhängig von den Umständen des Einzelfalls. Dabei ist immer zu berücksichtigen, welche Ausgangssituation im Unternehmen gegeben war und wie schwer der Verstoß des Mitarbeiters wiegt. Im Folgenden sollen die abwägungserheblichen Punkte dargestellt werden, die in eine Entscheidung über arbeitsrechtliche Maßnahmen einfließen sollten.
Folgende **Ausgangssituationen** im Unternehmen sollten in eine arbeitsrechtliche Maßnahme wertend einbezogen werden:

- Die private Nutzung der Medien (Internet, E-Mail oder Telefon) ist nicht ausdrücklich verboten oder
- die private Nutzung der Medien ist ausdrücklich vollständig verboten oder
- die private Nutzung wurde in geringem Umfang erlaubt oder

---

[99] *Gundermann/Oberberg*, a.a.O. S. 108; *Namendorf/Natzel* DB 2005, S. 1794 (1795).
[100] Orientiert an der Liste von *Gundermann/Oberberg* a. a. O., S. 110.
[101] Dokumentation gem. § 6 ArbSchG.

- die private Nutzung war zwar verboten; das Verbot wurde jedoch ganz offensichtlich niemals kontrolliert, sodass der Beschäftigte eine Duldung privater Nutzung annehmen durfte.

Als zweiter Aspekt sollte die **Schwere des Verstoßes** abgewogen werden. Hierbei können u. a. folgende Teilaspekte relevant sein:

- Ist dem Unternehmen tatsächlich ein Schaden entstanden? Wie hoch ist dieser?
- Welcher Schaden hätte im Extremfall eintreten können? (finanziell, Ansehen in der Öffentlichkeit)
- Wurde gegen Strafgesetze, interne Regeln verstoßen? Unbewusst oder absichtlich? (z. B. Betrachten von pornografischen oder rassistischen Inhalten)
- Lag ein bewusst betrügerisches Verhalten mit Schädigungsabsicht vor?
- Lag eine besondere Einzelsituation bei dem Beschäftigten vor (z. B. zwingende private Hintergründe?)
- Wie gravierend war der Verstoß?

Anhand dieser Kriterien sollte eine **Abwägung** über die Schwere des Verstoßes getroffen werden. In der Rechtsprechung zeichnet sich eine Tendenz ab, die den Vertrauensverlust gegenüber dem Arbeitnehmer bzw. das Kostenargument in vielen Fällen stattgeben. Die fristlose Kündigung wird vor allem bei strafbarem Verhalten wie nicht gestatteten Inhalten (Rassismus, Kinderpornografie)[102] sowie zivilrechtlich schädigendem Verhalten (vertragswidrige Handlungen, Werkspionage, unmittelbare Kostenverursachung z. B. durch 0900er-Telefonnummern)[103] bejaht.

Die Nicht-Beachtung der Mitbestimmungsrechte bei der Einrichtung solcher Missbrauchskontrollen im Unternehmen kann unangenehme Folgen für den Arbeitgeber nach sich ziehen. Wurde der Kontrollprozess ohne Hinzuziehung des Betriebsrats eingerichtet, so kann daraus ein Verwertungsverbot für die gewonnenen Erkenntnisse im Kündigungsverfahren resultieren.[104] Zu den weiteren Anforderungen bei Vornahme von Kontrollen, um Verwertungsverbote zu vermeiden, vgl. oben Abschn. 2. Ebenfalls kann in Betriebsvereinbarungen aufgenommen werden, dass bei einer Erkenntnisgewinnung außerhalb der vereinbarten Kontrollen automatisch ein Verwertungsverbot entsteht. Es greift in diesem Fall § 35 Abs. 2 Satz 2 Nr. 1 BDSG ein, der eine Löschung von Daten vorsieht, wenn deren Speicherung rechtswidrig erfolgt ist.

Haftung von Arbeitnehmern

Ob ein Arbeitnehmer für einen durch ihn verursachten Schaden haftet, hängt vom Grad seines Verschuldens ab. Verursacht er einen Schaden aufgrund von leichter Fahrlässigkeit, so muss er dafür nicht einstehen. Vollständig einstehen muss er für den Schaden bei grober Fahrlässigkeit oder wenn er vorsätzlich handelt. Liegt der Verschuldensgrad dazwischen, so wird der Haftungsanteil meist gequotelt. Diese Aufteilung greift aber nur dann ein, wenn der Schaden im Rahmen einer betrieblichen Tätigkeit eingetreten ist. Ist der Schaden durch eine nicht erlaubte Privatnutzung eingetreten, so zählt das nicht mehr zum Betriebsrisiko des Arbeitgebers.[105]

Deshalb kann die Frage, wie deutlich die nicht erlaubte Privatnutzung tatsächlich im Unternehmen verboten war, auch für die Haftungsfrage äußerst relevant sein. Ggf. muss sich der Arbeitgeber ein Mitverschulden anrechnen lassen[106], wenn er keine ausreichenden Sicherheitsmaßnahmen (Firewall, Virenschutz etc.) ergriffen hat oder der Arbeitnehmer berechtigterweise von einer erlaubten Privatnutzung im streitigen Ausmaß ausgehen durfte.

Anspruchsgrundlagen des Arbeitgebers gegen den Arbeitnehmer sind

- bei Verlust von Arbeitszeit durch Privatnutzung der Medien § 325 Abs. 1 S. 1 und 2 BGB
- bei arbeitsvertragswidrigem Verhalten durch Verursachung von Virenbefall oder absichtlicher Schädigung von Sicherheitssystemen § 280 Abs. 1 BGB
- bei einem bloßen Vermögensschaden am Eigentum des Arbeitgebers als deliktische Anspruchsgrundlage § 823 Abs. 1, 2 BGB[107])

---

[102] BAG, Urteil v. 7.7.2005, 2 AZR 58/04.
[103] BAG, Urteil v. 6.11.2003, 2 AZR 631/02.
[104] LAG Hamm, Urteil v. 25.1.2008, 10 Sa 169/07.
[105] Vgl. «Arbeitnehmerhaftung im Arbeitsverhältnis».
[106] § 254 BGB.
[107] Ggf. i. V. m. § 263 StGB (Betrug.

Konsequenzen für den Arbeitgeber

Dem Arbeitgeber drohen bei Verstößen gegen datenschutzrechtliche Vorgaben an einigen Stellen Verwertungsverbote für die datenschutzrechtlich unrechtmäßig gewonnenen Erkenntnisse. Zwar kennen die deutschen Prozessordnungen kein generelles Verwertungsverbot für solche unrechtmäßig gewonnenen Erkenntnisse, aber insbesondere im Arbeitsrecht lassen die Gerichte eine Wertung dieser Beweise gegen den Arbeitnehmer regelmäßig nicht zu.[108]

Sind solche Verwertungsverbote unter Verletzung des Persönlichkeitsrechts oder von Mitbestimmungsrechten des Betriebsrats gewonnen worden, so greift regelmäßig § 35 Abs. 2 S. 2 Nr. 1 BDSG ein, der eine Löschung unrechtmäßig gespeicherter Daten vorsieht. Dies hat zur Folge, dass Ausdrucke oder Aufzeichnungen vor Gericht nicht vorgelegt werden dürfen und die Daten an sich gelöscht werden müssen.

Daneben drohen dem Arbeitgeber Geldbußen wegen datenschutzrechtlicher Ordnungswidrigkeiten von bis zu 300.000 EUR oder darüber hinaus, wenn diese Summe den aus dem Verstoß gewonnenen wirtschaftlichen Vorteil nicht überwiegt, § 43 Abs. 1 und 2 BDSG.[109] Für besonders schwere Verstöße drohen der verantwortlichen Person (nicht dem Unternehmen) Geldstrafe oder bis zu zwei Jahre Haft, § 44 BDSG.

Die geplante EU-Datenschutzgrundverordnung sieht eine deutliche Verschärfung der Geldstrafen für Unternehmen vor. Danach sollen künftig bei Datenschutzverstößen bis zu 5 % des Konzern(!)-Umsatzes als Strafzahlung fällig werden können.

[108] *Gola,* Datenschutz und Multimedia am Arbeitsplatz, Rn. 353 m. w. N.

[109] Inkrafttreten dieser geänderten Norm am 1.9.2009.