MEYER-KÖRING

Anwaltstradition seit 1906

Beschäftigtendatenschutz in Krankenhäusern

Sebastian Witt

Beschäftigtendatenschutz in Krankenhäusern

Der Datenschutz fristet im Alltag von Arbeitsverhältnissen eher ein Schattendasein. Gelegentlich dringt er jedoch in das Bewusstsein, meist aufgrund medienwirksamer Datenschutzskandale, wie bspw. bei der Deutschen Bahn, Lidl oder Aldi. Allerdings werden diese Erkenntnisse nur selten umgesetzt. In den vergangenen Jahren wurden Personalabteilungen kaum im Datenschutz geschult, Betriebs- oder Dienstvereinbarungen hierzu geschlossen oder die gesetzlichen Vorgaben aktiv berücksichtigt. Denn all dies wird in der Praxis häufig als sperrig und entscheidungshemmend empfunden. Die Deutsche Bahn hat dieser Eindruck 1.123.503,50 Euro gekostet.

Denn auch wenn die subjektive Einschätzung zutreffen mag, täuscht dies nicht darüber hinweg, dass der Datenschutz im betrieblichen Alltag eine ständige Rolle spielt. Rechtsprechung und Behörden messen ihm immer größere Bedeutung zu. Dieser Trend wird mit der Verabschiedung des neuen Beschäftigtendatenschutzgesetzes fortschreiten. Aktuell hat die Bundesregierung einen Entwurf vorgestellt (BDSG-E), der nach Anhörung der Sachverständigen überarbeitet und endverhandelt wurde. Damit dürfte es nur noch eine Frage der Zeit sein, bis die neuen Regelungen in das Bundesdatenschutzgesetz (BDSG) aufgenommen werden.

Aus diesem Grunde sollten Krankenhäuser die Vorgaben des BDSG aktiv aufgreifen, ihr Handeln in dem gesetzlich vorgegebenen Rahmen optimieren und vor allem die Folgen (auch unbeabsichtigter) Verstöße gegen das BDSG bedenken. Wie bereits erwähnt: Im Falle der Deutschen Bahn betrug das Bußgeld wegen Verstößen gegen das BDSG über 1,1 Mio Euro. Angesichts dessen kann es sich kein Krankenhaus in Deutschland leisten, den Datenschutz zu unterschätzen oder gar zu missachten.

Der vorliegende Beitrag will deshalb Verständnis für eine unbekannte Materie wecken.

I. Ausgangspunkt

Spätestens seit dem so genannten „Volkszählungsurteil" des Bundesverfassungsgerichtes[1] wird dem Recht auf informationelle Selbstbestimmung Verfassungsrang zugemessen. Das BDSG und andere spezialgesetzliche Vorschriften wollen die damit verbundenen Vorgaben näher konkretisieren. Das BDSG zielt deshalb auf einen umfassenden Schutz persönlicher Daten in allen Lebenslagen ab. Seine Vorschriften enthalten Vorgaben für Vertragsbeziehungen im Allgemeinen (§ 28 BDSG) und Arbeitsverhältnisse im Besonderen (§ 32 BDSG).

[1] BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83

II. Datenschutzrechtliche Grundlagen

Alle Krankenhäuser haben unabhängig von ihrer Rechtsform und Trägerschaft den Schutz personeller Daten zu gewährleisten. Für Kliniken in kirchlicher Trägerschaft, auf die Kirchenrecht Anwendung findet, ergibt sich diese Pflicht aus kirchenrechtlichen Datenschutzordnungen, die mit dem BDSG nahezu inhaltsgleich sind. Für alle übrigen Krankenhäuser gilt das BDSG. Hierdurch wird für alle Beschäftigten in Kliniken ein nahezu gleichförmiger Schutz gewährleistet. Die nachstehenden Ausführungen betreffen somit im Grundsatz alle Krankenhausträger. Übrigens wird die Differenzierung zwischen kirchlichem und weltlichem Recht mit Inkrafttreten des BDSGE voraussichtlich enden, da der Entwurf keine Bereichsausnahme für die Kirche und ihre Einrichtungen mehr vorsieht.

Das BDSG schützt personenbezogene Daten. Hierunter zählen nahezu alle Informationen über eine Person. Betrifft eine Angabe eine Personengruppe, kann es sich gleichwohl um personenbezogene Daten handeln. Voraussetzung ist indes, dass die Gruppe klein und individualisierbar genug ist, um Rückschlüsse zuzulassen. Die Informationen müssen nicht immer konkretisiert sein. Circa- und Wahrscheinlichkeitsangaben stehen ihnen gleich und sind am Maßstab des BDSG zu beurteilen, sofern die Informationen Rückschlüsse auf eine Person zulassen oder geeignet sind, das Verhalten des Empfängers zu beeinflussen.

Findet das BDSG Anwendung, muss der Verantwortliche seine Pflichten stets sowohl bei der Datenerhebung als auch -verarbeitung und -nutzung beachten.

- Als „Datenerhebung" gilt jede Maßnahme, durch die zielgerichtet Daten über den Betroffenen beschafft werden. Als Kontrolle ist regelmäßig zu fragen, ob der Empfänger anschließend mehr über den Betroffenen weiß als vorher. Deshalb kann auch die Kombination mehrerer bekannter Informationen zu einer neuen Erkenntnis eine Datenerhebung sein.
- Zur „Datenverarbeitung" zählen das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Die Vorschrift betrifft nicht nur EDV-gestützte Vorgänge (bspw. das Speichern von Daten auf einem USB-Stick, DVD), sondern auch andere Handlungen, bei denen Informationen verkörperlicht werden (bspw. Notizen auf Zetteln). Der Begriff der Datenverarbeitung ist damit sehr weit gefasst.
- Als „Datennutzung" gilt schließlich jede Verwendung personenbezogener Daten, die nicht bereits Datenverarbeitung ist. Es handelt sich um einen Auffangtatbestand, damit letztlich alle Vorgänge mit Daten erfasst werden.

Jede Erhebung, Verarbeitung und Nutzung von Daten bedarf nach § 4 BDSG einer Erlaubnis durch Gesetz, andere Rechtsvorschriften oder den Betroffenen selbst.

- Die gesetzliche Erlaubnis zum Umgang mit Daten kann durch das BDSG selbst oder andere Normen erfolgen.
- Als „andere Rechtsvorschrift" sieht das Bundesarbeitsgericht vor allem Regelungswerke an, die gesetzesgleich wirken, ohne selbst Gesetz zu sein. Deshalb kann sich aus einem Tarifvertrag ebenso wie aus einer Betriebs- oder Dienstvereinbarung mit der jeweiligen Interessenvertretung eine Rechtfertigung zur Erhebung, Verarbeitung oder Nutzung von Daten ergeben.
- Zuletzt kann der Betroffene selbst in die Erhebung, Verarbeitung oder Nutzung seiner Daten einwilligen. Eine solche Einwilligung bedarf zwingend der Schriftform. Sie muss daher von dem Betroffenen im Original unterzeichnet sein. Darüber hinaus muss sie dem „FIS-Grundsatz" genügen. Eine rechtswirksame Einwilligung setzt damit Freiwilligkeit voraus und erfordert, dass der Betroffene

über die Reichweite seiner Einwilligung informiert ist und diese nur spezifisch erteilt. In der juristischen Literatur wird darüber gestritten, ob Arbeitnehmer auf eine Bitte ihres Arbeitgebers tatsächlich „freiwillig" entscheiden können. Nicht wenige Autoren lehnen dies ab. Aber auch diejenigen, die bei Beschäftigten noch eine autonome Entscheidung für möglich halten, erwarten mindestens, dass die Datenschutzerklärung separat erteilt wird und deshalb nicht bereits Bestandteil eines Arbeitsvertrages ist. Daher ist eine inhaltlich und räumlich abgrenzbare und separat zu unterzeichnende Vereinbarung empfehlenswert.

III. Typische Situationen im Arbeitsverhältnis und ihre datenschutzrechtliche Bewertung

1. Bewerbungsverfahren

a) *Erstellung eines Bewerberprofils*

Schon vor Begründung eines Arbeitsverhältnisses gewährt das BDSG dem Arbeitnehmer einen weitgehenden Schutz. Denn im Bewerbungsverfahren gelangt der potentielle Arbeitgeber in den Besitz einer Vielzahl personenbezogener Daten über den Betroffenen. Typischerweise enthält eine Bewerbung den Namen, die Anschrift und Telefonnummer sowie einen E-Mail-Account des Bewerbers, Angaben über seine fachlichen und persönlichen Fähigkeiten, zu seinem bisherigen beruflichen Werdegang und letztlich seinem Alter. All dies sind personenbezogene Daten. Das BDSG will sie schützen. Jede Erhebung, Verarbeitung und Nutzung erfordert deshalb – aufgrund der fehlenden gesetzlichen und in der Regel auch gesetzesähnlichen Rechtfertigung – die Einwilligung des Betroffenen.

Heutzutage nutzen viele Personalleiter mehr Quellen als die Bewerbungsunterlagen, um sich über die Bewerber zu informieren. Rund 30 % der Personalabteilungen greifen hierfür auf das Internet, vor allem soziale Netzwerke (bspw. XING, Facebook, studiVZ u.ä.) zurück[2]. Das BDSG erlaubt dies in § 32 BSDG nicht; auch der Bewerber willigt nach allgemeiner Ansicht nicht schon mit seiner Bewerbung ein, alle denkbaren Medien zu verwerten. Mithin kommt nur § 28 Abs. 1 Nr. 2, 3 BDSG als Rechtfertigung in Betracht. Diese Bestimmung behandelt u.a. die Datenerhebung aus öffentlich zugänglichen Quellen vor der Anbahnung rechtsgeschäftlicher Schuldverhältnisse, also auch Arbeitsverhältnisse. Allerdings ist diese Form der Datenerhebung nur gestattet, wenn sie zur Wahrung berechtigter Arbeitgeberinteressen erforderlich ist und schutzwürdige Belange des Betroffenen nicht überwiegen.

- Mit anderen Worten bedarf es zunächst eines inhaltlichen Zusammenhanges zwischen der Datenerhebung und der auszuübenden Tätigkeit.
- Überdies muss die Recherche erforderlich sein, um Erkenntnisse über die Eignung des Bewerbers zu erhalten. Bei Kinderkrankenpflegern kann daher die Frage nach Ermittlungsverfahren wegen sexuellen Missbrauchs durchaus berechtigt sein. Allerdings gilt auch hier der Grundsatz der Datensparsamkeit. Werden bei der Recherche auch Erkenntnisse gewonnen, die nicht mit dem zu besetzenden Arbeitsplatz in Verbindung stehen (bspw., dass der Bewerber noch bei seinen Eltern wohnt), hat der Arbeitgeber sie zu ignorieren. Diese Daten dürfen weder erhoben noch verarbeitet oder genutzt werden.

[2] Studie des Bundesverbandes Deutscher Unternehmer

- Zuletzt sind die berechtigten Interessen des Arbeitnehmers zu ermitteln und zu prüfen, ob sie überwiegen. Es genügt daher nicht, dass ein Arbeitgeber nachvollziehbare Motive für seine Recherche vorweisen kann. Sie müssen auch angesichts der schutzwürdigen Interessen des Betroffenen legitim sein. Hierbei spielt es eine Rolle, wenn der Bewerber seine Informationen im privaten Umfeld verbreitet hat. Soziale Netzwerke, die vor allem privaten Charakter haben (bspw. Facebook, studiVZ usw.) sind deshalb aus jeglicher Recherche ausgenommen. Auf berufsbezogenen Internetplattformen (bspw. XING) ist demgegenüber die Datenerhebung, -verarbeitung und -nutzung meist erlaubt.

Sind diese Voraussetzungen nicht kumulativ erfüllt, führt die Datenerhebung, -verarbeitung und -nutzung zu einer Ordnungswidrigkeit, die – wie oben erwähnt – Bußgelder auslösen kann.

In der Praxis wird gegen derartige Bedenken häufig eingewandt, der Bewerber werde dies nicht herausfinden; Verstöße blieben daher letztlich sanktionslos. Deshalb seien datenschutzrechtliche Bedenken nur Theorie. Die Argumentation ist jedoch nicht rechtlicher, sondern rein tatsächlicher Natur und basiert auf dem „Prinzip Hoffnung". Sie schützt – wie der Fall der Deutschen Bahn zeigt – nicht vor Rekordbußgeldern. Zudem ist häufig festzustellen, dass die Schwierigkeiten im Detail liegen, wenn bspw. im Rahmen einer Betriebsratsanhörung erläutert wird, warum der nach den Bewerbungsunterlagen besser qualifizierte Bewerber nicht zum Vorstellungsgespräch eingeladen wurde.

b) *Bewerbungsgespräch*

Auch im Bewerbungsgespräch setzt das Datenschutzrecht Grenzen. Sie ergänzen die ohnehin strengen Vorgaben des Allgemeinen Gleichbehandlungsgesetzes (AGG) oder Schwerbehindertenrechts (§ 81 SGB IX).

- Nach der Rasse, ethnischen Herkunft, dem Geschlecht, der Religion oder Weltanschauung, einer Behinderung, dem Alter oder der sexuellen Identität darf der Arbeitgeber demnach nur dann fragen, wenn das betreffende Merkmal wegen der Art der auszuübenden Tätigkeit oder der Bedingung der Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt und die Frage auch im Übrigen angemessen ist (§ 8 AGG).
- Darüber hinausgehende Fragen (bspw. zum bisherigen Verdienst, Hobbies, dem beruflichen Werdegang u.ä.) darf der Arbeitgeber nur stellen, sofern die gewünschten Informationen erforderlich sind.

Fehlt es an der Erforderlichkeit, begeht der Arbeitgeber mit der Datenerhebung, -verarbeitung oder -nutzung eine Ordnungswidrigkeit; der Bewerber hat überdies das so genannte „Recht zur Lüge". Er darf unrichtige Angaben machen, ohne dass ihm hieraus ein Nachteil erwächst.

c) *Ärztliche (Einstellungs-) Untersuchungen und sonstige Tests*

Viele Arbeitgeber setzen heutzutage im Rahmen des Bewerbungsverfahrens auf Verhaltensanalysen, Persönlichkeitstests oder ärztliche Untersuchungen. Auch deren Zulässigkeit bestimmt sich vor allem danach, ob die Informationen für die Begründung des Arbeitsverhältnisses erforderlich sind (§ 32 Abs.1 S. 1 BDSG).

In diesem Zusammenhang ist immer wieder festzustellen, dass der Einstellungsuntersuchung keine weiteren (eventuell sogar regelmäßigen) Untersuchungen im Arbeitsverhältnis folgen. Der Häufigkeit vergleichbarer Untersuchungen wird aber Bedeutung zugemessen. Denn sie wirft die Frage auf, welche Eigenschaften für eine Einstellung wichtiger sind als während des laufenden Arbeitsverhältnisses. Der Umstand, dass während der Beschäftigung keine Untersuchungen üblich sind, indiziert die fehlende Erforderlichkeit. Der Arbeitgeber muss in diesem Fall schon konkrete Gründe für die Untersuchung anführen können.

d) *Nicht berücksichtigte Bewerber*

Weist der Arbeitgeber einen Bewerber ab, ist die Speicherung der von ihm zur Verfügung gestellten Daten in aller Regel nicht mehr erforderlich. Das allgemeine Persönlichkeitsrecht schließt das Recht ein, darüber zu bestimmen, ob der Arbeitgeber die im Bewerbungsverfahren erfragten persönlichen Daten aufbewahren darf oder ob deren Vernichtung verlangt werden kann.

Dies gilt umso mehr für Informationen, die der Bewerber möglicherweise ungefragt und ohne erkennbaren Zusammenhang mit der auszuübenden Tätigkeit erteilt hat (bspw. Hobbies, sportliche Aktivitäten, Vereinszugehörigkeiten u.ä.). Hier ist ein besonderer Schutz geboten, der eine schnelle Datenvernichtung erforderlich macht.

Es sind zwar Fälle denkbar, in denen der ablehnende Arbeitgeber ein berechtigtes Interesse zur Aufbewahrung solcher Daten vorweisen kann. Sie sind jedoch selten. Nachvollziehbar ist dies zur Abwehr von Ansprüchen nach dem AGG. Die Speicherung von Bewerberdaten wenigstens bis zum Ablauf der gesetzlichen Ausschlussfristen für diese Ansprüche (§ 15 Abs. 4 AGG) scheint deshalb legitim.

2. Internet, E-Mail und Telefonnutzung am Arbeitsplatz

Nahezu jeder Arbeitsplatz ist heute „multimedial" und ist damit nicht nur über ein Telefon und Fax mit der Welt verbunden, sondern auch über E-Mail, Intranet und Internet. Dies gilt für die Verwaltung von Krankenhäusern ebenso wie für Arbeitsplätze in der Pflege. In der Praxis hat kaum ein Arbeitgeber Regeln zur Verwendung dieser Medien erlassen. Deshalb gibt es selten klare Vorgaben, ob der Beschäftigte sie (auch) zu privaten Zwecken nutzen darf.

Der Arbeitgeber kann jedoch frei entscheiden. Er ist befugt, die private Nutzung vollständig zu verbieten oder sie zuzulassen. Auch kann er sie zunächst erlauben, die Erlaubnis aber mit einem Widerrufsvorbehalt verbinden. Wird dieser sauber formuliert, hält sich der Arbeitgeber sämtliche Handlungsoptionen offen.

Fehlt es hingegen an eindeutigen Regeln oder ist die Privatnutzung eventuell sogar gestattet, ist der Arbeitgeber arbeits- und datenschutzrechtlich in seinen Möglichkeiten begrenzt:

- Wird die private Nutzung von Internet und E-Mail am Arbeitsplatz untersagt, ergeben sich für den Arbeitgeber organisatorische und disziplinarische Vorteile: Organisatorisch ist er berechtigt, das Nutzungsverhalten seiner Mitarbeiter stichprobenartig zu kontrollieren und gerade im Falle ihrer Abwesenheit Einsicht in die übersandten elektronischen (und damit im Zweifel dienstlichen) Unterlagen zu nehmen. Nur eine lückenlose und jederzeitige Kontrolle soll ausgeschlossen sein, um den „gläsernen Arbeitnehmer" zu verhindern. Dies wird aus § 28 Abs. 1 Nr. 1 BDSG gefolgert. In aller Regel genügen die damit verbundenen Kompetenzen dem Arbeitgeber jedoch, um seine berechtigten Interessen zu verfolgen. Disziplinarisch wird durch das vollständige Verbot der Privatnutzung gewährleistet, dass jeder Verstoß als arbeitsvertragswidriges Verhalten geahndet werden kann und – ggf. nach Abmahnung – zur Kündigung berechtigt.
- Sind die Befugnisse des Arbeitnehmers zur Privatnutzung des Internet- und E-Mail-Verkehrs nicht eingeschränkt oder gibt es keine Regelung, muss der Arbeitgeber in seinem Verhalten vor allem das Telekommunikationsgesetz (TKG) beachten. Daraus folgen noch höhere Hürden als beim BDSG. Denn die herrschende Meinung stellt einen Arbeitgeber, der die Privatnutzung gestattet, Telekommunikationsanbietern gleich. Er unterliegt damit den gleichen Anforderungen wie bspw. die Telekom gegenüber ihren Kunden. Der Arbeitgeber hat deshalb das Fernmeldegeheimnis nach § 88 TKG zu beachten und ist nur selten zur Kontrolle der Verkehrsdaten oder -inhalte berechtigt. Daten aus der Internet- und E-Mail-Nutzung darf er nur dann erheben, wenn tatsächliche Anhaltspunkte für einen Missbrauch vorliegen oder dies zum Aufdecken sowie Unterbinden von Leistungserschleichung und sonstigen rechtswidrigen Inanspruchnahmen notwendig ist. Die Hürden der Prüfung

sind damit sehr hoch. Damit nicht genug, stellen sich Schwierigkeiten bei der Abwesenheit der geschützten Arbeitnehmer. Da der Arbeitgeber selbst auf den auch privat genutzten E-Mail-Account nur mit konkreter Einwilligung des Nutzers zugreifen darf, kann es im Falle seiner Abwesenheit zu Ablaufstörungen kommen, wenn betriebliche E-Mails nicht zur Kenntnis genommen und damit auch nicht bearbeitet werden. Ist ein Mitarbeiter ausgeschieden, stellen sich im Ergebnis die gleichen Probleme. Denn auch dann ist davon auszugehen, dass der (auch) zur Privatnutzung eingerichtete E-Mail-Account private Informationen enthält, auf die der Arbeitgeber keinen Zugriff hat. Auch nach Beendigung eines Beschäftigungsverhältnisses ist der Arbeitgeber an das Fernmeldegeheimnis gebunden.

Die damit verbundenen Einschränkungen sind ernst zu nehmen. Denn neben allgemeinen Aufsicht- und Ordnungswidrigkeiten sind strafrechtliche Folgen im Falle der Verletzung des Fernmeldegeheimnisses möglich. Die Folgen eines Verstoßes sind damit noch schwerer als im Falle „einfacher" datenschutzrechtlicher Verstöße.

3. Videoüberwachung am Arbeitsplatz

Die multimediale Vernetzung von Arbeitsplätzen macht nicht bei E-Mail und Internet halt; auch der Einsatz von Videotechnik und Webcams ist auf dem Vormarsch. Hierbei stehen jedoch in aller Regel weniger die Überwachung einzelner Arbeitnehmer als vielmehr die Prozesssteuerung oder Verhinderung von Straftaten, sei es an Kunden oder Eigentum, im Vordergrund. Kameras finden sich auf Parkplätzen, dem Gelände oder speziellen Gebäudeteilen (bspw. Säuglingsstationen).

Auch wenn die Videotechnik nicht vorrangig dazu dient, Arbeitnehmer zu überwachen, können deren Interessen tangiert sein. Dies hängt jedoch im Wesentlichen von Art und Umfang der verwendeten Videotechnik sowie dem konkreten Beobachtungsraum ab.

- In öffentlich zugänglichen Räumen erlaubt § 6b BDSG den offenen Einsatz von Videoüberwachung, soweit dies zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Betroffenen überwiegen.
  - Der Begriff des öffentlich zugänglichen Raums ist eng zu verstehen. Er erfasst nur solche Bereiche, die ohne Überwindung einer geschlossenen Begrenzung von einer unbestimmten Vielzahl von Personen betreten werden können und nach ihrer Zweckbestimmung der Allgemeinheit zugänglich sind. Bei Flughäfen und Bahnhöfen ist dies sicher der Fall; bei dem Gelände eines Krankenhauses und seinen Parkplätzen mag dies ebenfalls noch zu vertreten sein; bei Büro- und Arbeitsräumen sowie Stationen lässt sich jedoch nur schwerlich vertreten, dass es sich um öffentlich zugängliche Räume handelt.
  - Aber selbst wenn es sich um einen öffentlich zugänglichen Raum handelt, schränkt das Merkmal der Erforderlichkeit die Handlungsoptionen ein. Sie fehlt, wenn Alternativen zur Wahrung der eigenen Interessen zur Verfügung stehen und dadurch die Videoüberwachung entbehrlich wird.

  Diese Grenzen sind bei der verdeckten Überwachung öffentlicher Räume noch enger. Denn allein die Ausübung des Hausrechts oder die Zweckmäßigkeit in der Aufgabenerfüllung genügen in diesem Fall nicht mehr. Vielmehr muss der konkrete Verdacht einer strafbaren Handlung oder einer schwerwiegenden Verfehlung zu Lasten des Arbeitgebers vorliegen; weniger einschneidende Mittel zur Aufklärung des Verdachtes dürfen nicht zur Verfügung stehen.

– Für nicht öffentlich zugängliche Räume gilt dies umso mehr. Denn hier fehlt bereits ein Erlaubnistatbestand wie für öffentliche Räume (§ 6b BDSG). Die Rechtsprechung hat deshalb sowohl für die heimliche wie auch offene Videoüberwachung am Arbeitsplatz auf § 32 BDSG zurückgegriffen und sie allenfalls zur Aufdeckung von Straftaten erlaubt. Auch dann muss der Kameraeinsatz aber erforderlich und im Verhältnis zu den Interessen der Betroffenen angemessen sein. So dürfen keine anderen Aufklärungsmöglichkeiten vorhanden sein; zudem ist der überwachte Bereich auf das notwendige Mindestmaß zu beschränken. Das Bundesarbeitsgericht hat diese Voraussetzungen zwar schon in verschiedenen Fällen bejaht; die Hürden sind jedoch nicht gering.

Sowohl bei öffentlich zugänglichen wie nicht öffentlichen Räumen sind der Betriebsrat oder eine Mitarbeitervertretung bei der Einführung und Veränderung der Videoüberwachung zu beteiligen. Die vorherige Einbindung der Interessenvertretungen steht jedoch dem Erfolg der Überwachung letztlich häufig entgegen.

Erkenntnisse aus einer Videoüberwachung, die unter Verletzung datenschutzrechtlicher Bestimmungen gewonnen wurden, dürfen vor Gericht nicht zu Lasten des Beschäftigten verwertet werden. Umgekehrt stehen ihm Entschädigungs- und Unterlassungsansprüche zu. Auch der Betriebsrat kann eine beteiligungswidrige Unterlassung ggf. gerichtlich durchsetzen.

IV. Ausblick auf das BDSG-E

Im Koalitionsvertrag haben sich CDU und FDP vor dem Hintergrund der Datenschutzskandale bei der Deutschen Bahn und Lidl auf eine Reform des BDSG geeinigt. Ziel sind praxisgerechte Regelungen für Bewerber und Arbeitnehmer sowie eine für Arbeitgeber verlässliche Regelung im Kampf gegen Korruption. Die Vorschläge der Regierung liegen seit Oktober 2010 vor. Sie sind in der Literatur und verschiedenen Expertenanhörungen stark kritisiert worden. Besonders handwerkliche Fehler wurden beanstandet. Der Regierungsentwurf wurde deshalb noch einmal stark überarbeitet. Die Regierungsfraktionen haben sich jetzt auf eine abschließende Fassung verständigt. Sie liegt derzeit beim Bundesministerium des Innern und soll gemeinsam mit Vorschriften zur Vorratsdatenspeicherung in den Gesetzgebungsgang eingebracht werden. Leider ist sie nicht öffentlich und nur in Ausschnitten bekannt.

Im Vergleich zu dem BDSG ergeben sich für die erwähnten typischen Situationen im Arbeitsverhältnis folgende Änderungen:

1. Bewerbungsverfahren

Der Datenschutz vor Begründung eines Arbeitsverhältnisses wird in §§ 32 bis 32b BDSG-E behandelt. Der Schutzmaßstab geht über den bisherigen Rahmen in weiten Teilen hinaus.

a) *Erstellung eines Bewerberprofils*

Zwar wird zunächst klargestellt, dass der Arbeitgeber den Namen, die Anschrift, die Telefonnummer und einen E-Mail-Account vor Begründung eines Beschäftigungsverhältnisses erheben darf. Während jedoch bislang weitergehende Informationen eingeholt werden konnten, soweit sie *„zur Begründung des Arbeitsverhältnisses"* erforderlich sind, wird nunmehr auf die Erforderlichkeit ***„für die vorgesehenen Tätigkeiten"*** abgestellt. Bei enger Auslegung sind Fragen zu den Gehaltsvorstellungen des Bewerbers deshalb künftig unzulässig.

§ 32 Abs. 6 BDSG-E stellt klar, das sämtliche Beschäftigtendaten unmittelbar bei dem Bewerber zu erheben sind. Fragen beim Vorarbeitgeber sind damit grundsätzlich unzulässig. Etwas anderes gilt nur dann, sofern der Arbeitnehmer ausdrücklich und schriftlich in die Fragen eingewilligt hat. Den Beschäftigten ist auf Verlangen darüber Auskunft zu geben, welche Informationen vom Vorarbeitgeber erteilt wurden. Gleiches gilt für den Zugriff auf soziale Netzwerke, die der Arbeitgeber nur dann einsehen darf, wenn er hierauf hingewiesen hat. Die Einsicht in private Netzwerke (Facebook, StudiVZ u.ä.) ist grundsätzlich verboten.

b) *Bewerbungsgespräch*

Hinsichtlich des Fragerechtes im Bewerbungsgespräch bleibt es zunächst bei den gesetzlichen Vorgaben des AGG. Nach § 32 Abs. 2 BDSG-E sollen künftig jedoch auch Fragen zu Vorstrafen, der Gesundheit, den Vermögensverhältnissen oder laufenden Ermittlungsverfahren nur dann zulässig sein, wenn die Information eine wesentliche Anforderung zur Ausübung der beruflichen Tätigkeit sind. Hiervon ist fast nie auszugehen. Die vermittelnde Fassung des BDSG-E sieht nach unseren Informationen vor, dass ein berechtigtes Interesse für diese Fragen ausreichen soll.

c) *Einstellungsuntersuchungen und sonstige Tests*

Ärztliche Einstellungsuntersuchungen und Eignungstests sind künftig nach § 32a Abs. 1 BDSG-E nur dann zulässig, wenn und soweit die zu ermittelnden gesundheitlichen Voraussetzungen wegen der Art der auszuübenden Tätigkeit eine wesentliche und entscheidende berufliche Anforderung darstellt. Der Beschäftigte muss über den Zweck der Untersuchung sowie Art und Umfang informiert werden und hierin sowie in die Weitergabe des Ergebnisses an den Arbeitgeber eingewilligt haben.

Sonstige Untersuchungen und Prüfungen sind nach aktueller Fassung von § 32a Abs. 2 BDSG-E nur dann zulässig, wenn sie nach wissenschaftlich anerkannten Methoden durchgeführt werden. Dies kann bei Assessment-Centern oder anderen Eignungstests zu Verwerfungen führen. Denn Schreibtests, die bei der Suche nach einer Sekretariatskraft durchaus üblich sind, werden regelhaft nicht nach wissenschaftlichen Methoden durchgeführt und dürften deshalb künftig unzulässig sein.

c) *Abgelehnte Bewerber*

Wie schon in der Vergangenheit sind Beschäftigtendaten zu löschen, sofern der Bewerber abgelehnt wurde (§ 32b Abs. 3 BDSG-E). Das Gesetz lässt auf die Pflicht zur „unverzüglichen" Löschung nach der Ablehnungsentscheidung schließen. Dies kann mit den Vorgaben des AGG kollidieren.

2. Internet-, E-Mail- und Telefonnutzung am Arbeitsplatz

In diesem Bereich bleibt es nach § 32i BDSG-E im Wesentlichen bei den derzeit geltenden Rahmenbedingungen. Die Bestimmung befasst sich mit der beruflichen Nutzung von Telefon, Internet und E-Mail. Es verbleibt hierbei bei dem bisherigen Grundsatz: Was nicht erlaubt ist, ist verboten.

Ist allein die berufliche Nutzung erlaubt, darf der Arbeitgeber hinsichtlich des E-Mail-Verkehrs und Internetverhaltens aus Gründen des ordnungsgemäßen Betriebes und der Datensicherheit, zu Abrechnungszwecken oder zu stichprobenartigen und anlassbezogenen Leistungs- und Verhaltenskontrolle einschließlich der Verhinderung oder Aufdeckung von Vertragsverletzungen Daten erheben, verarbeiten und nutzen.

Das BDSG-E misst dem gesprochenen Wort ein besonderes Schutzbedürfnis zu. Heimliches Mithören wird deshalb untersagt. Bei den Inhaltsdaten der nur zu beruflichen Zwecken erlaubten Telefonnutzung muss die Erhebung, Verarbeitung und Nutzung von Daten nicht nur erforderlich sein; der Beschäftigte und seine Kommunikationspartner müssen auch zuvor eingewilligt haben. Sie sollen nach der Gesetzesbegründung anzunehmen sein, sofern beide Gesprächspartner das Telefonat nach der Unterrichtung fortsetzen.

Ist die private Nutzung erlaubt oder wird sie geduldet, verbleibt es im Übrigen bei den bisherigen Rahmenbedingungen.

3. Videoüberwachung am Arbeitsplatz

Das BDSG-E enthält eine grundlegende Änderung hinsichtlich der heimlichen Videoüberwachung. Sie ist generell unzulässig. Erlaubt wird allein die heimliche Überwachung mittels Fotoapparat oder Fernglas.

Eine offene Überwachung wird in nicht öffentlich zugänglichen Betriebsgeländen, Gebäuden oder Räumen zur Zutrittskontrolle, zur Wahrnehmung des Hausrechts, zum Schutze des Eigentums, zur Sicherheit des Beschäftigten, zur Sicherung von Anlagen, zur Abwehr von Gefahren für die Sicherheit des Betriebes oder zur Qualitätskontrolle gestattet, sofern die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Eine Überwachung von Teilen der Betriebsstätten, die überwiegend der privaten Lebensgestaltung dienen, ist unzulässig. Die gewonnenen Erkenntnisse sind unverzüglich zu löschen, sofern sie zur Erreichung des Speicherzwecks nicht mehr erforderlich sind. In öffentlich zugänglichen Räumen verbleibt es im Übrigen bei den Vorgaben aus § 6b BDSG.

Das BDSG-E ordnet für den Fall eines unterlassenen Hinweises auf die Videoüberwachung ein Bußgeld von bis zu 50.000,00 Euro an.

4. Rechtfertigungstatbestände

Es bleibt zunächst auch im Anwendungsbereich des BDSG-E bei der gesetzlichen Grundkonzeption, dass die Datenerhebung, -verarbeitung und -nutzung durch Gesetz, gesetzesähnliche Regelungen oder Einwilligung des Betroffenen gestattet werden kann. Dies ist vor allem auf eine Intervention in der letzten Sekunde zurückzuführen.

Denn § 32l Abs. 1 BDSG-E erklärte im Regierungsentwurf die Einwilligung in die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten über die im Gesetz vorgesehenen Möglichkeiten hinaus generell für unzulässig. Der vermittelnde Regierungsentwurf hat diese aufgeweicht. Danach ist die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten auf der Grundlage einer Einwilligung möglich, sofern der Betroffene über ihren Zweck und die Möglichkeit des Widerrufs schriftlich informiert wurde und er von dieser Widerrufsoption nicht binnen zwei Tagen nach der Erklärung Gebrauch gemacht hat.

Auch die deutlich eingeschränkten Möglichkeiten zum Abschluss von Dienst- oder Betriebsvereinbarungen auf dem Feld des Beschäftigtendatenschutzes wurden wieder weitestgehend der bestehenden Rechtslage angepasst. Nur in eng umgrenzten Fällen sollen die gesetzlichen Schutzmaßstäbe auch für die Betriebspartner verbindlich sein. Dies gilt bspw. für § 32d Abs. 3 BDSG-E, der den Fall der Deutschen Bahn abhandelt. Hier wurden automatisiert Beschäftigtendaten mit Daten von Auftragnehmern (Rechnungserstellern) abgeglichen und geprüft, ob es Überschneidungen gab. Dies soll künftig nur in anonymisierter oder pseudonymisierter Form erfolgen dürfen. Es steht den Betriebspartnern nicht frei, diese letzte Einschränkung aufzuheben.

V. Fazit

Das Schattendasein des Beschäftigtendatenschutzes wird seinen inhaltlichen Vorgaben und den Konsequenzen von Verstößen nicht gerecht. Arbeitgeber müssen ihr Verhalten darauf einstellen, um den mitunter drastischen Sanktionen des BDSG und TKG zu entgehen.

Dies ist umso wichtiger, da in der Praxis immer wieder (unbeabsichtigt) gegen die gesetzlichen Schutzmaßstäbe verstoßen wird. Dabei bestünde sogar die Möglichkeit, Dienst- oder Betriebsvereinbarungen abzuschließen, durch die weite Teile der bisherigen Praxis legalisiert werden.

Vor diesem Hintergrund kann nur dringend geraten werden, diese Abläufe zu überprüfen und entsprechende Regularien zu schaffen.

Zum Autor

Sebastian Witt wurde 1975 geboren, ist verheiratet und Vater von zwei Söhnen.

Herr Witt ist seit annähernd 10 Jahren ausschließlich im Bereich des Arbeitsrechts anwaltlich tätig. Er ist Fachanwalt und geschäftsführender Partner der Sozietät MEYER-KÖRING Rechtsanwälte Steuerberater in Bonn. Dort berät und vertritt er überwiegend Krankenhäuser, vor allem in katholischer Trägerschaft. Den Schwerpunkt seiner Tätigkeit bildet die Betreuung von Umstrukturierungen, insbesondere Personalabbaumaßnahmen, Outsourcings und Schließungen von Abteilungen oder Einrichtungen.

Daneben ist Herr Witt Referent und Autor in verschiedenen arbeitsrechtlichen Handbüchern. Bspw. hat er im Handbuch Krankenhaus-Arbeitsrecht neben anderen Beiträgen auch das Kapitel „Outsourcing und Betriebsübergang" verfasst. U.a. hierzu hält er regelmäßig Vorträge vor Fachpublikum.

Kontakt: Tel. +49 (0) 228 72636-48 | witt@meyer-koering.de

MEYER-KÖRING

Anwaltstradition seit 1906

Meyer-Köring | Rechtsanwälte und Steuerberater Partnerschaftsgesellschaft

Büro Bonn
Oxfordstraße 21
53111 Bonn

Telefon +49 (0) 228 72636-0
Telefax +49 (0) 228 72636-77

bonn@meyer-koering.de
www.meyer-koering.de

Büro Berlin
Schumannstraße 18
10117 Berlin

Telefon +49 (0) 30 206298-6
Telefax +49 (0) 30 206298-89

berlin@meyer-koering.de
www.meyer-koering.de