

Datenrechtliche Entgleisungen

Das Vertrauen in den betrieblichen Datenschutz ist derzeit schwer erschüttert. Für den missbräuchlichen Umgang mit Arbeitnehmerdaten scheint es drei Hauptursachen zu geben: Überzogener Wissensdrang der Unternehmen, die fehlende Umsetzung des Bundesdatenschutzgesetzes (BDSG) in den Überwachungssystemen und eine teilweise unklare Gesetzeslage.



„Der verantwortungsvolle Umgang mit persönlichen Daten im Rahmen des Arbeitsverhältnisses ist für die Arbeitgeber genauso wichtig, wie die Sicherung der Unternehmensdaten vor unerlaubten Zugriffen“, unterstreicht Roland Wolf von der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA). Gerne würde man dieser Aussage zustimmen, doch aufgrund zahlreicher Datenskandale in deutschen Unternehmen fällt das zunehmend schwer. Vielmehr entsteht der Verdacht, dass manche Unternehmen beliebig Mitarbeiterdaten sammeln, kontrollieren und verwenden. Überprüfungen von privaten Kontobewegungen sind dabei nicht die Spitze des Eisbergs. Das Ausschneffeln des Privatlebens, Abhören und Ausspähen von Mitarbeitern bis in die Vorstandsetage, Sammeln von Informationen über das Liebesleben von Familienangehörigen - dies alles sind keine wahnhaften Fantasien, sondern Praxis im Umgang mit persönlichen Daten von Mitarbeitern. Die Liste der Rechtsverstöße ist lang: Heimliches Sammeln und Erforschen externer Daten, betriebliche Mitbestimmung missachten und Datenschutzbeauftragte nicht informieren.

Wie kommt es zu den Fehlgriffen? Leisten die modernen Informationstechnologien dem „Forscher- und Wissensdrang“ von Unternehmen Vorschub? Liegt es daran, dass Beschäftigtendaten nicht mehr nur in Papier-Akten,

sondern auch in leistungsfähigen Personalinformationssystemen gesammelt werden, deren Zugriffsrechte oft nicht eindeutig geklärt sind? Oder fehlen klare rechtliche Vorgaben? Der Bundesdatenschutzbeauftragte Peter Schaar gegenüber der Personalwirtschaft: „Das rasante Anwachsen von Datenbeständen, deren fortschreitende Vernetzung und der hohe ökonomische Wert von personenbezogenen Daten multiplizieren das Gefahren- und Missbrauchspotenzial.“

Präventive Kontrollen

Der Hauptgrund für die Auswertung der sensiblen Daten der Arbeitnehmer liegt im Interesse der Arbeitgeber, Rechtsverstöße möglichst früh zu erkennen und schon im Keim zu ersticken. Fraglos ein berechtigtes, zentrales Eigenanliegen: Schließlich ist in Deutschland fast jeder zweite Arbeitgeber bereits Opfer von Wirtschaftskriminalität geworden. Die finanziellen Schäden sind enorm. „Die Verantwortlichen befinden sich in einer Zwickmühle: Zum einen müssen sie Korruption oder andere Delikte möglichst effizient bekämpfen, zum anderen kann ein falsch verstandener Tatendrang bei der internen Verbrechensbekämpfung schnell zur Verletzung von Mitarbeiter- oder Mitbestimmungsrechten des Betriebsrats führen“, so Bernhard Steinkühler, Fachanwalt für Arbeitsrecht und Dozent an der School Governan-

ce, Risk & Compliance, Berlin. Bislang können sich Unternehmen auf das Bundesdatenschutzgesetz (BDSG) und diverse Einzelgesetze stützen. Und hier entzündet sich der Streit: Viele Datenschützer und Experten erklären, diese Vorgaben würden nicht ausreichen, um das spezielle datenrechtliche Verhältnis von Arbeitgebern und Arbeitnehmern zu regeln. Die gesetzlichen Unklarheiten können ungewollt zu Verstößen führen. Doch es beginnt schon einen Schritt vorher: In vielen Unternehmen sind selbst die unstrittigen Vorgaben des BDSG nicht hinreichend in den Systemen hinterlegt.

Integration des BDSG

Diese sollten so angelegt sein, dass die Anforderungen des Datenschutzrechts und der Mitbestimmung umgesetzt sind. Die Skandale der vorigen zwei Jahre haben in Unternehmen dazu geführt, Personalstammdaten- und CRM-Systeme mit Blick auf die technische und organisatorische Einhaltung des BDSG zu analysieren. Dr. Andreas Knäbchen, Partner Enterprise Risk Services bei Deloitte: „Es setzt sich die Erkenntnis durch, dass das Augenmerk insbesondere auf die Berechtigungen für Datenzugriffe gelegt werden muss. Bewährte Verfahren bestehen in der Vergabe minimaler Berechtigungen, entsprechend dem tatsächlich gegebenen geschäftlichen Bedarf oder dem Vier-

Augen-Prinzip. Letzteres hat sich bereits für die Kontrolle von finanziellen Transaktionen bewährt.“

Die Dokumentation der entsprechenden Prozesse und Regelungen sollte dabei so professionell wie ansonsten auch üblich erfolgen. Richtschnur können etablierte Industriestandards sein, beispielsweise der ISO-Standard für Managementsysteme der Informationssicherheit (ISO 27001). Kontrollen der getroffenen Regelungen können manuell erfolgen oder automatisiert in den IT-Systemen ablaufen.

Schwachstellen im System

Regelprozesse zur Steuerung der Datenschutz-Risiken sehen idealerweise folgendermaßen aus: Nach Klärung der rechtlichen Vorgaben sollte festgelegt werden, wie die Kontrolle für die Einhaltung der gesetzlichen Vorschriften aussieht. Dazu müssen aus den gesetzlichen Regelungen spezifische Vorgaben für die eigene Organisation, die Prozesse und die IT-Systeme abgeleitet werden. Dann erfolgt die Umsetzung dieser Vorgaben und die regelmäßige Überprüfung der Kontrollziele durch unabhängige Stellen. Damit werden häufig die Innenrevision oder Wirtschaftsprüfer betraut.

„Das Ziel muss sein, die Regelprozesse des BDSG zu implementieren und im internen

Kontrollsystem abzubilden. Dies geschieht auch über Ergänzungen zu Personal- oder CRM-Systemen“, erläutert Dr. Knäbchen, Deloitte. Beispielsweise können Applikationen so zugeschnitten sein, dass Personalstammdatensysteme Daten nur für diejenigen offen legen, die nach Gesetz oder innerbetrieblichem Ablauf Zugriff haben dürfen. Die Regelungen, die intern getroffen sind, gelten natürlich auch, wenn HR- oder CRM-Dienstleistungen über einen Partner abgewickelt werden. Hier bestehen oft Lücken. So würden beispielsweise Kontrollbefugnisse in den Auslagerungsverträgen fehlen. Zudem fänden regelmäßige Kontrollen durch die unternehmenseigene Revision oder andere Stellen nicht statt oder der Dienstleister sei über den Schutzbedarf der ihm anvertrauten Datenbestände nicht genügend aufgeklärt.

Im Dschungel der rechtlichen Grundlagen

In der Praxis sind die Regelungen für den Arbeitnehmerdatenschutz alles andere als leicht zu interpretieren. Bestehende Rechtsgrundlagen finden sich unter anderem im BDSG, im Grundgesetz, Telekommunikationsgesetz, Betriebsverfassungsgesetz, im Arbeitssicherheitsgesetz und der EU-Richtlinie zum Arbeitnehmerschutz. Selbst für

Juristen ist es schwierig, den Durchblick zu behalten; für Geschäftsführer und Datenschutzbeauftragte kleiner und mittlerer Unternehmen ist es fast unmöglich. Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit den 80er Jahren bereichsspezifische Regelungen und damit einen eigenen Arbeitnehmerdatenschutz.

Der Bundestag hat dem Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften zugestimmt, der im September in Kraft tritt. Doch die Datenlage in den Betrieben ist nicht explizit geregelt worden. Einzig die Stellung der betrieblichen Datenschutzbeauftragten wurde gestärkt; zudem können die Aufsichtsbehörden künftig bei Verstößen höhere Bußgelder verhängen. Die kontroverse Diskussion zwischen Gesetzgeber, Arbeitgebern, Gewerkschaften und Datenschützern geht also weiter und wird bei jedem öffentlich bekannt gewordenem Verstoß neue Brisanz gewinnen.

Grauzonen beseitigen

Eindeutig ist die Haltung des Bundesdatenschutzbeauftragten Schaar, der für ein Arbeitnehmerdatenschutzgesetz plädiert: „Das Bundesdatenschutzgesetz gilt für viele Bereiche. Es enthält vor allem allgemeine Abwägungsinteressen, die nicht speziell auf das

Arbeitsverhältnis zugeschnitten sind. Dies führt oft zu ganz erheblichen Auslegungsschwierigkeiten.“

Arbeitgeber und Arbeitnehmer sind daher im Wesentlichen darauf angewiesen, sich an der lückenhaften und im Einzelfall nur schwer zu erschließenden Rechtsprechung zu orientieren. Weiterhin können Betriebsvereinbarungen und Absprachen mit dem betrieblichen Datenschutzbeauftragten helfen, aber sie können natürlich kein Arbeitnehmerdatenschutzgesetz ersetzen. Von einer Regelung für Mitarbeiter würden nicht nur die Arbeitnehmer, sondern auch die Arbeitgeber profitieren. Für Schaar hätte ein Arbeitnehmerdatenschutzgesetz entscheidende Vorteile: „Wenn Rechtssicherheit geschaffen ist, wissen Unternehmen, dass sie sich auf dem richtigen Weg befinden. Grauzonen fallen weg, weil die rechtlichen Grundlagen dann für jedes Unternehmen definiert sind.“ Er fordert beispielsweise, dass die Datenerhebung grundsätzlich beim Arbeitnehmer selbst erfolgt, und dass Arbeitnehmer umfassend darüber zu informieren sind, welche Daten auf welche Weise und zu welchem Zweck über sie erhoben und in welcher Art und Weise ausgewertet werden. Auch schlägt er vor, die Rolle des betrieblichen Datenschutzbeauftragten zu stärken und seine umfassende Beteiligung vor der Umsetzung betrieblicher Maßnahmen sicherzustellen.

BDA gegen Arbeitnehmerdatenschutzgesetz

Die BDA hält ein eigenständiges Arbeitnehmerdatenschutzgesetz für überflüssig. Rechtsexperte Roland Wolf: „Wir haben das BDSG, das die wesentlichen Fragen auch im Arbeitsverhältnis klärt. Das schließt nicht aus, in einzelnen Bereichen Klarstellungen vorzunehmen, zum Beispiel beim Datenaustausch im Konzern - hier können klarere Vorgaben die Handhabbarkeit des Gesetzes verbessern, doch ein eigenständiges Arbeitnehmerdatenschutzgesetz ist dafür auf keinen Fall notwendig.“

Doch die Praxis zeigt: Das BDSG ist auslegbar und führt dazu, dass Arbeitgeber in großem Stil daneben greifen, wenn sie wirt-

schaftskriminelles Verhalten verhindern wollen. Brauchen Unternehmen Nachhilfe in Gesetzeskunde? Nein, argumentiert die BDA: „Dort, wo Verfehlungen und Probleme aufgetreten sind, ist schon nach geltendem Recht eine Klärung erfolgt. Das zeigt, dass das geltende Recht hinreichende Handlungsmöglichkeiten bietet. Aus Einzelverstößen kann man keinesfalls schließen, dass Arbeitgeber in ihrer Gesamtheit das Datenschutzrecht nicht anwenden. Solche Einzelfälle sind kein Indiz dafür, dass ein eigenständiges Arbeitnehmerschutzgesetz geschaffen werden muss“, so Roland Wolf.

Bleibt jedoch die Frage, ob es wirklich im Sinne von Arbeitgebern ist, erst zu reagieren, wenn das Kind in den Brunnen gefallen ist und Mitarbeiter an die Presse gegangen sind. Der Reputationsschaden ist enorm: Nicht nur die eigenen Beschäftigten fühlen sich als „gläserne Mitarbeiter“ und das Vertrauensverhältnis leidet. Auch Geschäftspartner, Zulieferer und Kunden werden skeptisch, ob ihre sensiblen Geschäftsdaten wirklich vor Spionage-Attacken sicher sind.

Screenings in Verdachtsfällen

Die bisherigen Entscheidungen der Arbeitsgerichte zeigen, dass Kontrollmaßnahmen gegenüber den Mitarbeitern datenschutzrechtlich zulässig sein können, wenn konkrete Anhaltspunkte für eine Straftat oder schwere Verfehlungen bestehen. In diesen Fällen ist es dem Arbeitgeber auch gestattet, den verdächtigen Arbeitnehmer durch einen Privatdetektiv überwachen zu lassen. Rechtsanwalt Bernhard Steinkühler betont: „Bloßes Misstrauen reicht nicht aus. Wird der Arbeitnehmer tatsächlich einer vertrags- oder gesetzeswidrigen Handlung überführt, haftet er gegenüber dem Arbeitgeber auf Ersatz der Detektivkosten, wenn der Privatermittler gerade wegen des konkreten Tatverdachts beauftragt wurde.“

In der Diskussion stehen derzeit die Daten-Screenings. Es existieren zwar keine gesetzlichen Regelungen oder Urteile, die ein „Screening“ der Mitarbeiter generell verbieten, aber einem präventiven Abgleich

nahezu aller Arbeitnehmerdaten stehen datenschutzrechtliche Erwägungen entgegen. Eine allgemeine und massive Kontrolle der Belegschaft führt nicht nur zu einem „Generalverdacht“, sondern verletzt auch die Persönlichkeitsrechte der Arbeitnehmer. Eine unternehmensweite pauschale Kontrolle ohne Verdachtsmoment ist nach Einschätzung von Arbeitsrechtlern und Datenschutzexperten nicht zulässig. Umfassende Daten-Screenings, wie sie bei großen Unternehmen zur Korruptionsbekämpfung durchgeführt wurden, sieht der Bundesdatenschutzbeauftragte Peter Schaar sehr skeptisch: „Allenfalls bei einem konkreten Anlass und der Begrenzung auf die Mitarbeiter, die beispielsweise in einem korruptionsgefährdeten Arbeitsbereich tätig sind, können Screening-Verfahren in Frage kommen. Der betriebliche Datenschutzbeauftragte und der Betriebsrat sind in jedem Fall rechtzeitig vor der Durchführung derartiger Maßnahmen zu beteiligen.“

Sensibilität wächst

Eine positive Konsequenz der Datenskandale: Heute schenken Betriebe Datenschutzbeauftragten mehr Gehör in Situationen, in denen ihre Forderungen sonst als lästiges Übel betrachtet wurden. Aus gutem Grund: Arbeitnehmer, die sich nicht ernst genommen fühlen, leiten drastische Schritte ein: Sie gehen an die Staatsanwaltschaft oder an die Öffentlichkeit. Unternehmen dagegen scheuen schon allein beim Thema „Arbeitnehmerdaten und ihr Schutz“ die Öffentlichkeit. Offiziell möchte kein Datenschutzbeauftragter und Personalvorstand zu dem Thema Stellung beziehen. Das ist wenig nachvollziehbar; aber wenn bei betriebsinternen Vorgängen Unternehmen mit Arbeitnehmerdaten genauso zugeknöpft umgehen wie mit der bloßen Anfrage nach ihrer betrieblichen Schutzpraxis, dann kann man sicher sein, dass zukünftig mehr Sensibilität im Umgang mit den Daten der Arbeitnehmer herrscht.

Christiane Siemann,
freie Wirtschaftsjournalistin, Düsseldorf