

Arbeitsrecht

Arbeitnehmerdatenschutz

Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

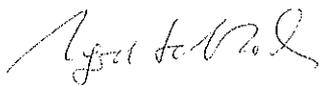
am 31. März 2010 hat das Bundesministerium des Innern Eckpunkte zur Neuregelung des Beschäftigtendatenschutzes vorgelegt. Damit soll die Vereinbarung im Koalitionsvertrag umgesetzt werden, Mitarbeiterinnen und Mitarbeiter vor Ausforschung an ihrem Arbeitsplatz wirksam zu schützen. Tatsächlich wird aber, wenn diese Eckpunkte tatsächlich umgesetzt werden sollten, nicht der Schutz verstärkt, sondern Ausforschung legitimiert.

Mit der Begründung, Korruption bekämpfen zu wollen oder die Einhaltung von Compliance-Anforderungen durchzusetzen, will das Bundesministerium des Innern, dass Daten von Beschäftigten, soweit sie sowieso vorhanden sind, erhoben, gespeichert und verwendet werden dürfen. Eine Eingrenzung dieser ausufernden Überwachung soll lediglich nach dem Maßstab der Erforderlichkeit und Verhältnismäßigkeit erfolgen, Begriffe, die sehr dehnbar sind. Mit diesen sog. unbestimmten Rechtsbegriffen wird aber jedem Arbeitnehmer und jeder Arbeitnehmerin zugemutet, mit seinem Arbeitgeber einen Streit darüber zu führen, was im Einzelfall erforderlich und verhältnismäßig ist.

Der DGB und seine Mitgliedsgewerkschaften fordern seit langem ein transparentes Arbeitnehmerdatenschutzgesetz, das das Persönlichkeitsrecht jedes Einzelnen in den Mittelpunkt stellt. Was nun geplant wird, stellt jedoch das Interesse der Unternehmen an der Überwachung ihrer Beschäftigten in den Mittelpunkt.

Hiergegen wenden wir uns nachdrücklich. Mit dem beigefügten Newsletter wollen wir informieren – zugleich auf grundlegende Änderungen hinweisen. Dafür werden wir politisch eintreten und würden uns freuen, wenn wir entsprechende Unterstützung erhielten.

Mit freundlichen Grüßen



Ingrid Sehrbrock
Stellv. DGB-Vorsitzende

Inhaltsverzeichnis

| | Seite |
|---|-----------|
| I. Überblick über die Eckpunkte des Beschäftigtendatenschutzgesetzes | 4 |
| 1. Einstellungsverfahren | 4 |
| 2. Korruptionsbekämpfung | 4 |
| 3. Überwachung | 4 |
| 4. Verschlechterungen durch Vereinbarungen/ Einwilligung | 5 |
| II. Bewertung der Eckpunkte des BMI | 5 |
| 1. Datenerhebung im Einstellungsverfahren | 5 |
| 2. Gesundheitliche Untersuchungen | 7 |
| 3. Korruptionsbekämpfung und Durchsetzung von Compliance-Anforderungen | 8 |
| 4. Videoüberwachung | 10 |
| 5. Ortungssysteme | 11 |
| 6. Verwendung biometrischer Daten | 12 |
| 7. Nutzung von Telefon, E-Mail und Internet | 12 |
| 8. Kollektivrechtliche Vereinbarungen | 13 |
| 9. Einwilligung | 13 |
| III. Forderungen des DGB | 14 |
| (Auszüge aus dem Beschluss des Bundesvorstandes vom 02.12.2008) | |

1. Überblick über die Eckpunkte des Beschäftigtendatenschutzgesetzes

Das BMI formuliert in seinen Eckpunkten, dass durch umfassende allgemeingültige Regelungen für den Datenschutz am Arbeitsplatz die Rechtslage deutlich gemach und insgesamt mehr Rechtssicherheit erreicht werden soll.

1. Einstellungsverfahren

Im Einstellungsverfahren soll der Arbeitgeber Beschäftigendaten erfragen dürfen, die er für nötig hält, um die Eignung des Bewerbers festzustellen. Gesundheitliche Untersuchungen und weitere nicht näher spezifizierte Prüfungen sollen zulässig sein, wenn der Arbeitgeber sie für „erforderlich“ hält, um die – wie auch immer definierte – Eignung für die vorgesehenen Tätigkeiten festzustellen.

2. Korruptionsbekämpfung

Im Mittelpunkt der Eckpunkte stehen die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen. Sie sollen es dem Arbeitgeber gestatten, grundsätzlich vorhandene Beschäftigendaten zu verwenden, soweit dies „erforderlich“ und „verhältnismäßig“ ist. Ein konkreten Verdacht gegenüber einem Beschäftigten, – wobei nicht erkennbar ist, welche Anforderungen an einen solchen Verdacht gestellt sind –, sollen dem Arbeitgeber das Recht geben, zusätzliche Daten unter strengeren Voraussetzungen erheben zu dürfen.

3. Überwachung

Ebenso sollen Videoüberwachungen von nicht öffentlich zugänglichen Betriebsstätten möglich sein, wenn wichtige betriebliche Interessen dies erfordern. Eine Definition der wichtigen betrieblichen Interessen fehlt in den Eckpunkten. Nur bei Betriebsräumen, die überwiegend zur privaten Lebensgestaltung des Beschäftigten dienen, also beispielsweise bei Bereitschaftsdienst (Zimmer eines Arztes) sollen ausgeschlossen sein.

Die Nutzung von Ortungssystemen und biometrische Verfahren sollen ebenfalls, – wenn auch eingeschränkt –, zulässig sein. Die Nutzung von Telefon, Internet und E-Mail sollen ebenfalls zum Zweck der Korruptionsbekämpfung und Compliance-Anforderungen im „erforderlichen Maß“ kontrollierbar sein. Interessen der Beschäftigten sollen dabei lediglich berücksichtigt werden müssen.

Keine Regung bleibt unbemerkt – Ständige Arbeitsplatzüberwachung in einer Spielhalle

Lange Zeit war Sabine F. (Name geändert) mit ihrem Arbeitsplatz zufrieden: An den Schichtdienst in der Spielhalle hatte sie sich gewöhnt, die Kollegen waren nett, der Chef annehmbar, und die Arbeit selbst konnte sie gut bewältigen. Doch die Bedingungen haben sich seit einiger Zeit dramatisch verschlechtert, seit es eine neue Vorgesetzte gibt. „Sie ist misstrauisch und unterstellt allen Angestellten kriminelle Absichten.“ Anders lässt sich aus Sabine F.'s Sicht jedenfalls nicht die permanente Videoüberwachung ihres Arbeitsplatzes erklären. „Natürlich habe ich nichts dagegen, dass Kameras an der Kasse und bei den Spielautomaten angebracht sind. Schließlich gibt es Überfälle auf Spielhallen. Ich selbst habe das zweimal in meiner Zeit hier erlebt. Aber ich möchte nicht durchgehend an meinem Arbeitsplatz hinter dem Counter gefilmt werden – zumal es dort nichts gibt, was ich oder meine Kollegen ‚mitgehen‘ lassen würden.“ Da sie während ihrer achtstündigen Schichten immer am Arbeitsplatz bleiben muss und es keinen Pausenraum gibt, kann Sabine F. nicht einmal unbemerkt ihre Mahlzeiten zu sich nehmen. „Alles wird aufgezeichnet, jedes Naseschnauben, jeder Blick.“

4. Verschlechterungen durch Vereinbarungen/ Einwilligung

Schließlich ist vorgesehen, dass Betriebs- und Dienstvereinbarungen oder durch Tarifverträge von den gesetzlichen (Verbots) Vorschriften abgewichen werden kann. Ebenso soll die Zulässigkeit der individuellen Einwilligung des Beschäftigten nicht ausgeschlossen, sondern auf ausdrücklich geregelte Fälle beschränkt werden. Bei Ausscheiden aus dem Beschäftigungsverhältnis ist vorgesehen, dass die Daten des Beschäftigten solange aufbewahrt werden dürfen, wie sie zur Abwicklung des Arbeitsverhältnisses benötigt werden.

II. Bewertung der Eckpunkte des IIM

1. Datenerhebung im Einstellungsverfahren

Der Arbeitgeber soll nur die Beschäftigtendaten erfragen dürfen, die er benötigt, um die **Eignung** des Bewerbers für eine in Betracht kommende Tätigkeit festzustellen.

Den Eckpunkten ist nicht zu entnehmen, ob damit nur die fachliche Eignung gemeint ist, also nur objektive Feststellungen getroffen werden dürfen oder ob der Arbeitgeber zum Beispiel unter dem Begriff „persönliche Eignung“ auch deutlich über die fachlichen Anforderungen hinaus Beschäftigtendaten erfragen und ermitteln darf. Unklar ist, welche Kriterien für die Eignung des Bewerbers angelegt werden, d.h., inwieweit hier der Arbeitgeber von vornherein eine weitgehende Freiheit zur Festlegung der Kriterien hat. Wenn nämlich nicht nur **rein objektive, fachliche Kriterien** angelegt werden müssen, sind dem Aushorchen, Ausforschen und Ausfragen Tür und Tor geöffnet.

Denn, wenn zum Beispiel der Arbeitgeber der Meinung ist, zur persönlichen Eignung gehöre auch die Bereitschaft, abends und am Wochenende zu arbeiten, wären damit Fragen nach der persönlichen Lebensgestaltung, der Familienplanung, nach bestehenden Betreuungspflichten, nach Hobbys, nach ehrenamtlichem Engagement oder parteipolitischer Betätigung zulässig.

Und niemand von uns weiß, wie lange die Bänder aufbewahrt werden.“ Seit über 15 Jahren arbeitet die Frau in der Spielhalle in einer norddeutschen Stadt, aber noch nie zuvor hat sie sich so viele Sorgen um ihren Arbeitsplatz gemacht wie in letzter Zeit. Denn sie vermutet, dass die neue Vorgesetzte nach Abmahnungs- und Kündigungsgründen sucht. „Ständig führt sie neue Vorgaben ein, etwa die, dass wir jedes Mal aufstehen sollen, wenn ein neuer Kunde die Spielhalle betritt. Das mache ich nicht, weil ich keinen Sinn darin erkennen kann. Doch wird auch dies genauestens von der Kamera eingefangen.“ Selbstverständlich ist Sabine F. klar, dass es nicht unbedingt ums Aufstehen oder Sitzenbleiben geht. „Ich gehöre zu den älteren, erfahrenen Beschäftigten mit Vollzeitstelle und verhältnismäßig guter Bezahlung. Solche Leute möchte die Chefin loswerden.“

Telefonüberwachung bei der Deutschen Telekom

Unter Bezeichnungen wie „Clipper“ und „Rheingold“ ließ die Deutsche Telekom in den Jahren 2005 und 2006 die Telefonverbindungen von Aufsichtsräten und Managern sowie „der wichtigsten über die Telekom berichtenden deutschen Journalisten“ und auch etlicher Gewerkschafter auswerten. Es sei darum gegangen, „undichte Stellen im Vorstand und Aufsichtsrat aufzuspüren“. Da es Unstimmigkeiten über die Honorierung dieser illegalen Dienstleistung kam, lieferten die

Datenerhebung bei wem?

Aus den Eckpunkten geht nicht hervor, inwieweit die Daten beim Beschäftigten selbst erhoben werden müssen. Dies entspricht zwar dem Grundsatz des Bundesdatenschutzgesetzes, allerdings gibt es immer wieder Tendenzen, so genannte frei zugängliche Daten, grundsätzlich für nutzbar zu halten. Dies würde bedeuten, dass Vorgehensweisen, wie zum Beispiel so genannte Scornings (Detektierten werden beauftragt, im privaten Umfeld des Bewerbers nach Auffälligkeiten zu suchen, z. B. wird kontrolliert, ob auffällig viele Alkoholflaschen im Abfall sind, welche Zeitungen gelesen werden, wie das Freizeitverhalten ist usw.) und Internetrecherchen weiterhin möglich sein könnten. Bloße Mutmaßungen und nicht Fakten werden so zum Maßstab von personellen Entscheidungen. Berücksichtigt man dabei ferner, dass es weder eine Kontrolle des Wahrheitsgehalts von Interneteinträgen noch der Zustimmung desjenigen, über den Informationen im Netz vorhanden sind, gibt, können, ohne dass der Betroffene überhaupt etwas davon weiß, Informationen erhoben und verarbeitet werden, die die Einstellungschancen von Anfang an vernichten.

Einwilligung

Ganz allgemein legen die Eckpunkte fest, dass die Einwilligung der Beschäftigten in die Erhebung, Verarbeitung und Nutzung ihrer Daten auf ausdrücklich geregelte Fälle beschränkt werden soll. Was das für Fälle sind, wird nicht ausgeführt. Sollte allerdings geplant sein, eine Einwilligung schon im Einstellungsverfahren als Abweichung von grundsätzlichen Einschränkungen (sofern sie überhaupt vorhanden sind) zuzulassen, dann wären damit eventuelle Schranken wertlos.

Denn gerade im Einstellungsverfahren wird jeder Bewerber auf Aufforderung des potentiellen Arbeitgebers in jede Datenermittlung oder -verwendung einwilligen, damit er überhaupt eine Chance auf den Arbeitsplatz hat. Generell gilt, dass aber auch im bestehenden Beschäftigungsverhältnis die Einwilligung als Mittel einer Abweichung von gesetzlichen Verboten niemals ein geeignetes Mittel sein kann. Denn Beschäftigte sind faktische nicht frei in ihrer Entscheidung eine Einwilligung zu geben. Sie werden in aller Regel den Wünschen des Arbeitgebers Folge leisten, um ihre Arbeitsbedingungen und ggf. ihr Beschäftigungsverhältnis nicht zu gefährden.

geprellten Detektive dem „Spiegel“ das brisante Material.

Videüberwachung in Fleischfabrik

Bei Tönnies, einem fleischverarbeitenden Betrieb in Rheda-Wiedenbrück, wurden die Beschäftigten an ihren Arbeitsplätzen sowie in den Sozial- und Umkleieräumen mit Videokameras überwacht, um Diebstählen vorzubeugen und die Einhaltung von Hygienevorschriften zu kontrollieren. Die Geschäftsleitung behauptete zunächst, dass die Mitarbeiter/innen über die Überwachung informiert gewesen seien, doch gab es bei Tönnies keine Arbeitnehmervertretung, die einzig autorisiert gewesen wäre, dem Videoeinsatz zuzustimmen.

Drogeriekette Müller sammelte Krankendaten

Kranke Beschäftigte sehen sich häufig dem Argwohn ihres Arbeitgebers ausgesetzt, ob die Krankschreibung gerechtfertigt war. So sammelt auch die Drogeriekette Müller akribisch die Krankendaten ihrer rund 18.000 Beschäftigten. Nach einem krankheitsbedingtem Ausfall wurden Beschäftigte zum Gespräch mit ihrem Vorgesetzten bestellt. Dabei wurde gemeinsam ein Formular „Krankenrückkehrgespräch“ ausgefüllt, das unter anderem erfrage, ob der Beschäftigte bereits wegen derselben Ursache zuvor erkrankt gewesen und ob die Genesung vollständig sei. Die wenigsten Be-

Information über Datenerhebung, -speicherung und -verwendung

Aus den Eckpunkten geht ebenfalls nicht hervor, inwieweit der Arbeitgeber über die Ermittlung von Daten informieren muss. Gerade wenn geplant sein sollte, allgemein zugängliche Daten ohne Information des Beschäftigten verwenden zu dürfen, muss verpflichtend der Beschäftigte darüber informiert werden. Denn nur dann hat er die Möglichkeit, sich gegen falsche oder verleumderische Informationen zur Wehr zu setzen. Hier zum Beispiel vorzusehen, dass nur dann über Daten informiert werden muss, wenn der Arbeitnehmer dazu auffordert, ist praxisfern. Denn weder im laufenden Beschäftigungsverhältnis und schon gar nicht vor einer Einstellung im Bewerbungsverfahren wird es ein Arbeitnehmer wagen, Informationen über die ihn betreffenden Daten zu verlangen, weil er mit Nachteilen rechnen muss.

Darüber hinaus muss geregelt werden, dass die Daten, die rechtmäßig erhoben wurden, nicht an Dritte weitergegeben werden dürfen und nach Erfüllung des Zwecks, für den sie erhoben wurden (unverzüglich), zu löschen sind. Unrechtmäßig erhobene Daten dürfen unter keinen Umständen verwendet werden.

2. Gesundheitliche Untersuchungen

Nach den Eckpunkten sollen **gesundheitliche Untersuchungen oder Prüfungen** dem Erforderlichkeitsgrundsatz unterliegen. Unklar ist, was unter Prüfungen zu verstehen ist. Dieser allgemeine Begriff legt die Befürchtung nahe, dass damit weitestgehend alle Tests, wie Stresssimulationen, Psychospiele, Befragungen usw. umfasst sind. Damit können Persönlichkeitsprofile erstellt werden, die in den Schutzbereich des Privaten erheblich eingreifen. Und dies, obwohl erhebliche Zweifel an der Aussagekraft solcher Tests bestehen und keine Notwendigkeit dafür besteht.

Ähnlich wie bei den Einstellungsfragen und der Erhebung von Daten für das Einstellungsverfahren stellt sich auch hier die Frage, wie die **Eignung für eine konkret vorgesehene Tätigkeit** festgelegt wird. Völlig unklar ist, welche Kriterien dafür angelegt werden, und ob zum Beispiel subjektive Wünsche des Arbeitgebers ebenfalls zur Datenerhebung zulässig sind. Die aufgeführten Beispiele in den Eckpunkten bestärken die Befürchtung, dass es weitgehend der Dispositionsfreiheit des Arbeitgebers überlassen bleibt, welche Untersuchungen

schäftigten hatten den Mut, die Beantwortung des Fragebogens zu verweigern, obwohl sie wussten, dass diese Art der Ausforschung zu Erkrankungen und Genesung gesetzlich nicht zulässig sei.

Siemens ließ Betriebsräte bespitzeln

Beiläufig wurde während des Prozesses um Schmiergeldzahlungen bei Siemens im Juni 2008 auch bekannt, dass in einer Unternehmenssparte zwei Betriebsräte bespitzelt worden sind. Ein Ex-Manager sagte im Prozess aus, dass diese „besonders renitenten“ Betriebsräte im früheren Siemens-Festnetzbereich ICN durch Detektive beschattet wurden.

Heimliche Videos von Verkaufsgesprächen

Vier Außendienstmitarbeiter einer Thyssen-Krupp-Tochterfirma für Treppenlifte sind 2004/2005 per Videoaufnahmen bei Verkaufsgesprächen bespitzelt worden. Bekannt wurde der Fall erst erheblich später.

Videouberwachung bei Müller-Milch

In offensichtliche Widersprüche verwickelte sich die Geschäftsleitung der Großmolkerei Müller-Milch in Aretsried vor Gericht. Unternehmensvertreter hatten dargelegt, dass die auf dem Gelände installierten Videokameras allein der Gebäudesicherung dienten und nicht der Verhaltens- und Leistungskontrolle. Doch genau dazu das Überwachungssystem nachweislich

und „Prüfungen“ er für notwendig hält. So wird zum Beispiel bei der Frage, ob bei Kontakt mit allergenen Stoffen eine solche Untersuchung auf Allergien angeordnet werden darf, nichts dazu gesagt, dass sichergestellt sein muss, dass alle technischen Möglichkeiten vorher ausgeschöpft sind, um auch bei einer bestehenden allergischen Disposition trotzdem eine entsprechende Tätigkeit ausüben zu können. Dann wäre nämlich eine solche Untersuchung ggf. zur Feststellung von Drogen und Alkohol überflüssig.

Ebenso ist unklar, wie die Aussage zu interpretieren ist, dass Blutuntersuchungen nicht routinemäßig zulässig sind. Ob damit sichergestellt ist, dass solche Untersuchungen nur im absoluten Ausnahmefall überhaupt verlangt werden können, scheint zumindest sehr fraglich.

Aus den Eckpunkten geht nicht hervor, ob der Arbeitgeber unverlangt vom Beschäftigten zur Verfügung gestellte Daten verwenden darf. Dazu müssten jedenfalls klare Regelungen geschaffen werden, die dies ausdrücklich verbieten – und zwar ausnahmslos. Geschieht dies nicht, braucht der Arbeitgeber nur ein Signal zu geben, dass er Interesse an bestimmten Daten hat, ohne sie ausdrücklich zu fordern, und ihm werden die Daten „unverlangt“ zur Verfügung gestellt. Der Datenschutz bleibt dabei vollkommen auf der Strecke.

Löschung von Daten

Ebenso wenig ist den Eckpunkten zu entnehmen, wann Daten, die berechtigterweise ermittelt worden sind, gelöscht werden müssen oder wann Bewerbungsunterlagen zurückzugeben sind. Notwendig wäre die Regelung, dass die Daten unverzüglich zurückzugeben bzw. zu löschen sind. Damit ist sichergestellt, dass die Daten nur solange gespeichert bzw. aufbewahrt werden, wie es zwingend erforderlich ist.

Die sog. Erforderlichkeit muss im Gesetz durch Konkretisierungen praxistauglich gemacht werden, ansonsten entscheidet in der Realität der Arbeitgeber über die Reichweite des Datenschutzes allein.

in mindestens einem Fall eingesetzt worden: Eine Beschäftigte hatte drei Abmahnungen erhalten, weil sie innerhalb von neun Tagen einige Mal zwischen ein und vier Minuten verspätet zu arbeiten begonnen hatte. Als Beweis wurden die Videoaufnahmen geltend gemacht, die angeblich gar nicht zur Verhaltens- und Leistungskontrolle genutzt wurden.

Betriebsratsgründung gefilmt

In einer Münchener Filiale der Fast-Food-Kette Burger King wurde im April 2008 die Wahlversammlung für die Gründung eines Betriebsrates auf Video aufgezeichnet.

Bespitzelung bei der Deutschen Bank

Gegen Vorstände, Manager, einen Gewerkschaftsvertreter im Aufsichtsrat sowie einen kritischen Aktionär richteten sich Ausforschungen, die die Deutsche Bank in Auftrag gegeben hatte. So wurde auf den für ver.di damals im Aufsichtsrat sitzenden Vertreter eine Detektei angesetzt, weil er verdächtigt wurde, Quartalszahlen aus dem Jahr 2001 an die Nachrichtenagentur Reuters geleitet zu haben. Ebenso wurden Vorstände bespitzelt, denen man unterstellte, Kontakte zum einstigen Medienunternehmen Kirch zu haben. Einen auf Ibiza lebenden kritischen Aktionär beobachteten die Detektive intensiv. Zudem suchten sie nach Schwächen des Mannes und setzten weibliche Lockvögel auf ihn an, heißt es in dem Bericht.

3. Korruptionsbekämpfung und Durchsetzung von Compliance-Anforderungen

Das BMI plant, dass im Zusammenhang mit dem Arbeitnehmerdatenschutz klare gesetzliche Regelungen geschaffen werden, die dem Arbeitgeber Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen ermöglichen. Dazu sollen **grundsätzlich** vorhandene Beschäftigtendaten verwendet werden dürfen, soweit dies erforderlich und verhältnismäßig ist, um die Begehung von Vertragsverletzungen usw. aufzudecken oder zu verhindern. Beim konkreten Verdacht soll außerdem die Ermittlung zusätzlicher Daten möglich sein. Die Nutzung von Telekommunikations- und Telemedien sowie Videoüberwachung kann ebenfalls möglich sein.

Damit stellt das BMI nicht den Schutz persönlicher Daten der Beschäftigten im Arbeitsverhältnis in den Mittelpunkt der gesetzlichen Neuregelung, sondern das Ziel ist es, für die Unternehmen einen Rahmen zu schaffen, in dem möglichst viele Beschäftigtendaten genutzt werden können, um vermeintlich oder möglicherweise auch tatsächlich vorhandene Korruption oder Vertragsverstöße aufzudecken. Damit werden grundsätzlich alle Beschäftigten unter den **Generalverdacht** gestellt, korrupt zu sein bzw. gegen andere Gesetze oder Vorschriften zu verstoßen. Mit diesem Ansatz erfolgt eine völlige Wertverschiebung, wobei vollkommen ausgeblendet wird, dass Compliance Anforderungen vor allem auf das rechtmäßige Verhalten von Vorständen und Führungskräften abzielt. Gleichwohl soll es als Begründung dienen, Beschäftigte zu überwachen.

Die Tatsache, dass **allgemein zugängliche Arbeitnehmerdaten** genutzt werden können, um Vertragsverletzungen zu Lasten des Arbeitgebers aufzudecken, soweit dies erforderlich und verhältnismäßig ist, macht die **Datenverwendung grenzenlos**. Weder erfolgt eine Einschränkung im Hinblick auf die Vertragsverletzung noch geht aus den Eckpunkten hervor, welche Kriterien für die Erforderlichkeit und Verhältnismäßigkeit angelegt werden. Insbesondere ist kein Vorrang des Persönlichkeitsrechts des Beschäftigten intendiert.

Ebenso wenig geht aus den Eckpunkten hervor, in welchem Verhältnis staatliche Ermittlungen zu den eigenen Ermittlungen des Arbeitgebers stehen. Um den Persönlichkeitsrechten der Beschäftigten gerecht zu werden, darf es nur absolute Ausnahme sein, dass der Arbeitgeber selbst gegen seine Beschäftigten ermit-

Heimliche Videoüberwachung in Kleinbetrieb

Ende Dezember 2009 ließ der stellvertretende Werksleiter eines Kleinbetriebes im thüringischen Eichsfeld heimlich eine Videoüberwachungsanlage installieren. Mitarbeiter/innen fanden kurz darauf in einem Schrank ein Aufzeichnungsgerät und entdeckten über die Rückverfolgung der Kabel die versteckt angebrachte Kamera. Der Werksleiter erklärte daraufhin, es gehe ihm um die Aufdeckung möglicher Diebstahle. Doch war die Anlage auf Arbeitsplätze mit Kleinteilpressen gerichtet, in deren Nähe sich überhaupt keine lukrativen Wertgegenstände befinden. Insofern lag der Verdacht nahe, dass es der Firmenleitung bei der Überwachung allein um die Kontrolle der Arbeit und Leistung ging. Inzwischen wurde die Anlage entfernt.

Rasterfahndung bei der Deutschen Bahn

Die Deutsche Bahn AG stellte 2002 und 2003 den Großteil seiner Beschäftigten unter Korruptionsverdacht und ließ 173.000 von ihnen per Datenabgleich überprüfen. Am Ende fanden sich bei 100 der Überprüften konkrete Hinweise auf Korruption. Schon vorher war bekannt geworden, dass die Bahn AG über leitende Beschäftigte durch eine Detektei heimlich umfangreiche Datensammlungen auswerten ließ. Tätig wurde dieselbe Detektei, die auch für die Deutsche Telekom umfangreiche Listen über Verbindungsdaten zusammengestellt hatte.

telt. Richtigerweise müsste eine solche gesetzliche Regelung vorsehen, dass grundsätzlich Datenerhebung, -speicherung und -verwendung im Arbeitsverhältnis zum Zwecke der Aufdeckung von Straftaten bzw. Vertragsverstößen nur zulässig ist, wenn ein begründeter dringender Verdacht vorliegt und eine Aufklärung auf andere Art und Weise, insbesondere durch Einschaltung der Polizei bei Straftaten, nicht möglich ist. Dazu müsste außerdem vorgesehen werden, dass die Gründe und Maßnahmen dokumentiert werden und der erzwingbaren Mitbestimmung der betrieblichen Interessenvertretung unterliegen. Soweit keine betriebliche Interessenvertretung vorhanden ist, müsste eine andere neutrale Stelle über das Vorgehen informiert werden, die auch Rechte haben muss, das Anliegen abzuwehren. Nur so kann sichergestellt werden, dass dem Persönlichkeitsschutz der Beschäftigten Rechnung getragen wird. Die Eckpunkte lassen dagegen eher vermuten, dass der Arbeitgeber die Befugnisse einer „**Ersatz-Polizei**“ erhalten soll.

Soweit es die Eckpunkte vermuten lassen, geht der Vorschlag des BMI in eine völlig andere Richtung. Offenbar geht man davon aus, dass das Interesse des Betriebes an der Aufdeckung von Vertragsverstößen soweit geht, dass geradezu zwangsläufig auch ohne jeden konkreten Anlass grundsätzlich Persönlichkeitsrechte der Beschäftigten außer Kraft gesetzt werden müssen. Berücksichtigt man die Rechtsprechung des Bundesverfassungsgerichts zur automatisierten Erfassung von Autokennzeichen und die dort aufgestellten Grenzen, wird deutlich, dass eine anlasslose, nur zum Zwecke der Prävention durchgeführte Verletzung des Schutzbereichs des Grundrechts auf informationelle Selbstbestimmung in keinem Fall zulässig sein kann. Diese Grundsätze müssen für alle technischen Einrichtungen, die zur Überwachung der Beschäftigten geeignet sind, eingehalten werden. Dass dies mit dem vom BMI vorgelegten Entwurf erreicht wird, scheint nach den Eckpunkten gänzlich ausgeschlossen.

4. Videoüberwachung

Nach den Eckpunkten soll die Videoüberwachung von nicht öffentlich zugänglichen Betriebsstätten zulässig sein, soweit dies zur Wahrung wichtiger betrieblicher Interessen erforderlich und verhältnismäßig ist. Wie diese wichtigen betrieblichen Interessen definiert werden, und wie viel Spielraum dabei der Arbeitgeber hat, ist offen. Je weiter und allgemeiner aber solche betrieblichen Interes-

Unter die Lupe genommen wurden insgesamt 774 Führungskräfte und 500 Ehepartner/innen. Die Detektei sammelte dabei insbesondere Daten über wirtschaftliche Aktivitäten außerhalb der Bahn AG. Dazu gehörten Angaben u.a. zur Position, zum Firmensitz, Stammkapital und zur Bonität. In einem anderen Fall ließ die Bahn AG die Festplatten und im Netz gespeicherte Daten von vier Beschäftigten speichern, die der Vorteilsnahme verdächtigt wurden. Die Detektei erhielt diese Daten und überprüfte anschließend den Lebensstil eines der Observierten, inklusive Reisevorlieben und Familienverhältnisse.

Krankendatensammlung bei Daimler in Bremen

Mindestens 40 Beschäftigte im Daimler-Werk Bremen gerieten 2008 ins Blickfeld der Werkssicherheit. Die hatte illegal Krankendaten dieser Mitarbeiter/innen gespeichert. Ein Jahr später gelangten die Daten durch einen anonymen Absender zu „Radio Bremen“, das diesen Fall von Datenmissbrauch öffentlich machte. Die zugesandte CD enthielt Daten über die Krankheitsdauer und auch über Krankheitsgründe, die so detailliert waren, dass man sie – nach Angaben des Zusenders – betroffenen Mitarbeiter/innen hätte zuordnen können.

sen gefasst werden, umso mehr werden die Persönlichkeitsrechte der Beschäftigten eingeschränkt.

Heimliche Videoüberwachung soll nicht etwa gänzlich ausgeschlossen sein, sondern für konkrete Verdachtsfälle zugelassen werden. Welche weiteren Voraussetzungen dafür gelten sollen, geht aus den Eckpunkten nicht hervor und sind wohl auch nicht vorgesehen. Auch hier soll wohl die Polizei keine Funktion haben – allein der Arbeitgeber ermittelt.

Vorgesehen ist, dass die Videoüberwachung von Betriebsräumen, die **überwiegend** zur privaten Lebensgestaltung der Beschäftigten dienen, untersagt werden soll. Insbesondere ist unklar, wie das „überwiegend für private Lebensgestaltung“ definiert werden soll. Es könnte so zu verstehen sein, dass beispielsweise Umkleieräume, die ja nicht überwiegend zur privaten Lebensgestaltung der Beschäftigten dienen, sondern eben nur zum Umziehen, durch Video überwacht werden dürfen. Auch Pausen- und Raucherräume dürften wohl kaum unter diese Einschränkung „überwiegend zur privaten Lebensgestaltung“ fallen. Denn immer dort, wo Räume gemeinsam mit anderen Beschäftigten genutzt werden, entfällt das Kriterium der überwiegend privaten Lebensgestaltung.

Aus den Beispielfällen ergibt sich zudem, dass Videoüberwachung sehr weitgehend zulässig sein soll. Die Tatsache, dass generell Eingänge eines Betriebsgeländes oder Verteilzentren für Wertbriefe beobachtet werden dürfen, bedeutet, dass damit Daten erhoben werden können, die zur Leistungs- und Verhaltenskontrolle der Beschäftigten geeignet sind. Im Zusammenhang damit, dass grundsätzlich vorhandene Beschäftigtendaten, die auf diese Art und Weise erworben werden, immer genutzt werden können zur Durchsetzung von Compliance-Anforderungen und damit zur Durchsetzung aller vom Arbeitgeber gesetzten Regelungen, eröffnet dies die Möglichkeit zur Totalüberwachung.

Wird dies dann noch ergänzt durch die Möglichkeit der heimlichen Videoüberwachung, wird der bessere Persönlichkeitsschutz von Beschäftigten im Arbeitsverhältnis, der eigentlich mit einem Arbeitnehmerdatenschutzgesetz erreicht und der die Konsequenz aus den Datenverstößen im Einzelhandel, bei der Bahn oder der Telekom war, ins Gegenteil verkehrt. **Nicht mehr Datenschutz wird er-**

Systematische Mitarbeiterbespitzelung beim Discounter Lidl

Der Discounter Lidl hatte einen Teil seiner Beschäftigten in den Filialen mittels Videokameras und Detektivüberwachung systematisch ausspioniert. Die Detektive fertigten Protokolle an, aus denen detailliert hervorging, zu welchen Zeiten Mitarbeiter/innen die Toilette aufsuchten. Außerdem stellten sie Mutmaßungen über Privatbeziehungen der Beschäftigten an und gaben persönliche Wertungen ab, etwa dass Observede mit ihrer Arbeit überfordert seien oder eventuell dem kriminellen Milieu nicht fern stünden, weil sie Tattoos oder Piercings trugen.

reicht, sondern Überwachungen wie von Lidl und Co werden legitimiert.

5. Ortungssysteme

Mit der Regelung zu den Ortungssystemen soll ein Ausgleich der schutzwürdigen Interessen der Beschäftigten mit dem Interesse der Arbeitgeber in Einklang gebracht werden. Allein die Tatsache, dass die Verwendung von Ortungssystemen für die Koordinierung der Betriebstätigkeit zulässig sein soll, erschwert die Kontrolle des Missbrauchs erheblich. Denn sowohl im Außendienst als auch bei Kraftfahrern oder bei Arbeitnehmern auf wechselnden Baustellen kann mit der Begründung, eine Koordinierung könne notwendig werden, eine Ortung und Aufzeichnung des Aufenthalts der Beschäftigten möglich sein. Zu verhindern, dass diese Daten dann zur Leistung von Verhaltenskontrollen missbraucht werden, dass dadurch Druck auf Beschäftigte ausgeübt wird, dass sie einer permanenten Bespitzelung ausgesetzt werden, ist unmöglich.

Wie darüber hinaus sichergestellt werden soll, dass eine personenbezogene Ortung bei der Verwendung von Ortungssystemen an beweglichen Sachen ausgeschlossen wird, ist äußerst fraglich. Nur ein grundsätzliches Verbot kann sicherstellen, dass dem Grundrechtsschutz im Arbeitsverhältnis Rechnung getragen wird. Zumindest muss ein Verwertungsverbot vorgesehen werden.

6. Verwendung biometrischer Daten

Die grundsätzliche Verwendung biometrischer Daten im Arbeitsverhältnis wird in keiner Weise problematisiert, sondern lediglich an betriebliche Gründe zur Autorisierung und Identifizierung geknüpft. Es reicht also aus, dass der Arbeitgeber entscheidet, dass zukünftig der Zugang über einen Fingerabdruck kontrolliert werden soll, um die Erhebung dieses biometrischen Datums zu rechtfertigen. Dies greift in unerträglichem Maße in das informationelle Selbstbestimmungsrecht – ohne dass es dafür die geringste Notwendigkeit gibt. Nicht einmal der Staat verlangt von seinen Bürgern eine solche Form der Identifizierung, sondern lässt den einfachen Personalausweis genügen.

7. Nutzung von Telefon-, E-Mail und Internet

Auch bei diesen Vorschlägen, die sich aus den Eckpunkten ergeben, wird deutlich, dass nicht der Schutz der Beschäftigten Ziel der Neuregelung ist, sondern die Rechtfertigung und Legitimierung von Bespitzelung und Ausforschung. Berechtigte schutzwürdige Interessen des Beschäftigten sind lediglich zu beachten, im Vordergrund steht aber, dass dem Arbeitgeber grundsätzlich gestattet wird, zum Zwecke der Korruptionsbekämpfung und zur Durchsetzung von Compliance-Anforderungen, lediglich begrenzt durch das erforderliche Maß, den Kommunikationsfluss kontrollieren dürfen. Das erforderliche Maß wird dann allerdings, so ist zu vermuten, vom Arbeitgeber selbst festgelegt.

Ebenso soll nach dem Beispiel zulässig sein, dass der Arbeitgeber kontrollieren darf, ob bei der Beschränkung auf ausschließlich berufliche Nutzung verbotene Inhalte aufgerufen werden. Will er dies feststellen, muss er aber zunächst die Inhalte generell kontrollieren. Er greift damit in die Persönlichkeitsrechte der Beschäftigten in unerträglichem Maße ein. Wenn außerdem ausgeführt wird, dass die Inhalte von Telefonaten einem besonderen Schutz unterliegen, dann wird verkannt, dass die Kommunikation heute ebenso über E-Mail-Verkehr wie über Telefon erfolgt. Mit welcher Berechtigung ein anderer Maßstab für Telefonate angelegt wird, als für den E-Mail-Verkehr, ist nicht erklärbar.

8. Kollektivrechtliche Vereinbarungen

Soweit vorgesehen wird, dass durch Betriebs- und Dienstvereinbarungen oder Tarifverträge eigenständige Grundlagen für eine zulässige Datenerhebung und -verwendung vorgesehen werden können, kann dies nur zulässig sein, wenn die Vereinbarung zu einer Verbesserung des im Wege einer Vergrößerung des Arbeitnehmerdatenschutzes, nicht zu Abweichungen nach unten von dem durch das Gesetz zu garantierende Schutzniveau führt. Insbesondere können Betriebsvereinbarungen zur Durchsetzung von Compliance-Anforderungen, die sowieso schon durch die Vorschläge des BMI vorgenommenen Aushöhlungen des Persönlichkeitsschutzes noch weiter ausdehnen. Dies wäre mit dem grundgesetzlichen Schutz des allgemeinen Persönlichkeitsrechts in keiner Weise zu vereinbaren.

9. Einwilligung

Wie bereits unter Punkt 1 aufgeführt, ist die Einwilligung im Arbeitsverhältnis zu Datenerhebung-, -speicherung und -verwendung kein geeignetes Mittel, um den Schutz der Beschäftigten in irgendeiner Form zu gewährleisten. Arbeitnehmer im Beschäftigungsverhältnis sind nicht frei in ihren Entscheidungen. Sie sind immer dem Druck ausgesetzt, sich entsprechend den Wünschen des Arbeitgebers verhalten zu müssen, wollen sie nicht riskieren, unter Druck gesetzt zu werden oder gar ihren Arbeitsplatz zu verlieren. Im Zweifel wird kein Arbeitnehmer aus Gründen des Datenschutzes seinen Arbeitsplatz riskieren. Richtig wäre deshalb, grundsätzlich die Einwilligung der Beschäftigten in Datenerhebung-, -speicherung und -verwendung als Mittel der Legitimation auszuschließen.

Fazit:

Die Eckpunkte lassen befürchten, dass die Vorstellungen des BMI in eine vollkommen falsche Richtung gehen. Nicht der Persönlichkeitsschutz der Beschäftigten ist Anliegen des Gesetzgebungsvorhabens, sondern eine Legitimation von ausufernder Datenermittlung-, -speicherung und -verwendung zur Kontrolle und Überwachung der Beschäftigten. Arbeitnehmerinnen und Arbeitnehmer werden unter den Generalverdacht gestellt, grundsätzlich gegen arbeitsvertragliche und gesetzliche Pflichten zu verstoßen, und nur durch Mittel des Ausspionierens und Überwachens soll dem Rechnung getragen werden können. Dies entspricht genau der Argumentation, die beim flächendeckenden Scannen von Kontodaten oder der Videoüberwachung im Einzelhandel angewendet wurde.

III. Forderungen des DGB

(Auszüge aus dem Beschluss des Bundesvorstandes vom 02.12.2008)

1. Die gezielte Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz, aber auch im privaten Umfeld muss ausdrücklich verboten werden. Es muss klargestellt werden, dass weder eine direkte Überwachung durch Beauftragte, Externe noch durch Mitarbeiter oder eine indirekte Überwachung durch Video- oder Tonaufnahmen gerechtfertigt ist. Soweit der Schutz von Anlagen eine Überwachung notwendig macht, ist dies durch Betriebsvereinbarung zu regeln. Ebenso wenig kann die Kontrolle der Beschäftigten durch

Auswertung oder mit Hilfe computergesteuerter oder biometrischer Systeme erlaubt sein. Nur für den Fall, dass der begründete Verdacht einer strafbaren Handlung, eines Missbrauchs oder einer schwerwiegenden Schädigung des Arbeitgebers besteht, kann auf gesetzlicher Grundlage eine Überwachung im Einzelfall zulässig sein. Die Anordnung einer solchen Überwachung bedarf jedoch immer der Zustimmung der betrieblichen Interessenvertretung. Ebenso kann ausnahmsweise die Überwachung aufgrund höherrangiger Interessen wie der Sicherheit und der Gesundheit der Bevölkerung (z. B. bei der Überwachung von Atomkraftwerken) gerechtfertigt sein. Dann muss der Eingriff in das Persönlichkeitsrecht der Beschäftigten so gering wie möglich gehalten werden.

2. Bei elektronischer Datenverarbeitung ist eine besondere Schutzbedürftigkeit in Bezug auf das allgemeine Persönlichkeitsrecht gegeben, da im Hinblick auf die Vielzahl und die Qualität der verwendeten Daten, die Kombinations- und Auswertungsmöglichkeiten, den Kontextverlust und die zeitlich unbegrenzte Verfügbarkeit besondere Risiken bestehen. Um der strukturellen Unterlegenheit von Beschäftigten Rechnung zu tragen, kann deshalb das grundsätzliche Verbot des Zugriffs auf personenbezogene oder beziehbare Nutzerdaten bei der Verwendung moderner Kommunikationsmittel durch den Arbeitgeber auch nicht durch eine generelle Einwilligung des Arbeitnehmers ausgeschlossen werden. Durch gesetzliche Regelungen kann die Datenerfassung durch Arbeitgeber aus dringenden betrieblichen Gründen für bestimmte Fälle vorgesehen werden.
3. Das Fragerecht des Arbeitgebers bei der Einstellung und die Möglichkeit der Anordnung von ärztlichen Untersuchungen muss gesetzlich auf die Fälle beschränkt werden, die die Rechtsprechung bislang vorsieht. Das bedeutet, dass nur die Fragen bei der Einstellung zulässig sind, die für die konkrete Tätigkeit von entscheidender Bedeutung sind. Ebenso darf nur dann eine ärztliche Untersuchung angeordnet werden, wenn dies ausdrücklich gesetzlich geregelt ist (z. B. im Jugendarbeitsschutzgesetz). Verboten werden muss, dass der Arbeitgeber die Ergebnisse ärztlicher Untersuchungen entgegennimmt oder verwendet, insbesondere im Zusammenhang mit Pflichtverletzungen aus dem Arbeitsvertrag. Dies muss im besonderen Maße für Ge-

nomanalysen gelten. Für Drogen- und Alkoholtests muss gelten, dass ihre Durchführung weder angeordnet, noch die Ergebnisse entgegengenommen werden dürfen, es sei denn, es liegt ein begründeter Verdacht des Drogen- und Alkoholmissbrauchs vor und der Beschäftigte hat in den Test eingewilligt. Außerdem muss vor Anordnung aller Untersuchungen die Zustimmung des Betriebsrates vorliegen.

4. Sofern Beschäftigte gleichzeitig auch Kunden ihres Arbeitgebers sind, wie dies z.B. bei Banken, Versicherungen oder auch in Krankenhäusern häufig der Fall ist, muss sicher gestellt werden, dass die den Kundenbereich betreffenden Daten gesondert geführt und geschützt werden. Insbesondere muss gewährleistet sein, dass die personalverantwortliche Stelle auf die Daten nicht zugreifen kann.
5. Sofern Arbeitnehmer interne Daten über schwerwiegende Rechtsverstöße des Arbeitgebers, die geeignet sind, Gesundheit oder Leben der Beschäftigten oder der Allgemeinheit zu gefährden, wie zum Beispiel bei den Fleisch- oder Schwarzgeldskandalen der jüngsten Vergangenheit an staatliche Stellen weiterleiten müssen sie vor Repressalien durch den Arbeitgeber geschützt werden. Dies kann dadurch erfolgen, dass das Recht zur Weitergabe ausdrücklich geregelt wird, mit der Folge, dass dieses Recht dann dem Maßregelungsverbot unterliegt.
6. Erlaubte Datenerhebung muss diskriminierungsfrei erfolgen, unrechtmäßig erworbene Daten müssen einem Beweisverwertungsverbot unterliegen.
7. Die Einhaltung der gesetzlichen Bestimmungen kann nur dann gewährleistet werden, wenn die alleinige Last der Durchsetzung ihrer Rechte durch Klage von den betroffenen Beschäftigten genommen wird. Die Erfahrung zeigt, dass Arbeitnehmer im bestehenden Beschäftigungsverhältnis in der Regel nicht gegen den Arbeitgeber klagen können. Zu groß ist die Gefahr von Repressalien bis hin zur Kündigung. Deshalb reicht es nicht aus, dass gesetzlich ein so genanntes Maßregelungsverbot vorgesehen wird, d. h., dass dem Arbeitgeber verboten wird, Beschäftigte wegen der Wahrnehmung ihrer An-

sprüche aus einem Arbeitnehmerdatenschutzgesetz zu benachteiligen. Vielmehr muss ein Verbandsklagerecht vorgesehen werden.

8. Um den gesetzlichen Regelungen auch tatsächlich Wirkung zu verleihen, sind angemessene und abschreckende Sanktionen vorzusehen. Zum einem muss demjenigen, dessen Persönlichkeitsrecht verletzt worden ist, ausdrücklich ein konkreter Anspruch auf Schmerzensgeld in Form einer Entschädigung, entsprechend der Entschädigungsregelung in § 15 AGG bei Verstoß gegen das Diskriminierungsverbot, zugbilligt werden. Dieser Entschädigungsanspruch kann entweder direkt für bestimmte Verstöße die Höhe der Entschädigung regeln oder die gesetzliche Regelung muss den abschreckenden Charakter einer solchen Entschädigungszahlung ausdrücklich hervorheben. Darüber hinaus muss die Verletzung des allgemeinen Persönlichkeitsrechts strafbewehrt werden. Die bloße Ordnungswidrigkeit reicht angesichts der rechtsverneinenden Praxis der Arbeitgeberseite nicht aus.