Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 A

Deutscher Gewerkschaftsbund
Bundesvorstand
Abteilung Recht

Stellungnahme

zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230)

Vorbemerkung:

Die Bundesregierung hat am 25.8. 2010 den Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes beschlossen. Damit sollen entsprechend dem Koalitionsvertrag mit umfassenden allgemeingültigen Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit erreicht werden.
Dieser Ansatz ist durchaus zu begrüßen. Der Entwurf bleibt aber deutlich hinter dem zurück, was im Koalitionsvertrag vereinbart war. Dort heißt es: „*Wir setzen uns für eine Verbesserung des Arbeitnehmerdatenschutzes ein und wollen Mitarbeiterinnen und Mitarbeiter vor Bespitzelungen an ihrem Arbeitsplatz wirksam schützen.“*

Diesen Anforderungen wird der Entwurf nicht gerecht. Erforderlich wären klare Begrenzungen durch gesetzliche Verbote der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Außerdem fehlen in dem Entwurf Regelungen zu Schadensersatz- und Entschädigungsansprüchen und ausdrückliche Verwertungsverbote. Richtigerweise hätte dieser Bereich in einem eigenständigen Gesetz geregelt werden müssen. Durch den vorliegenden Entwurf wird kein effektiver Datenschutz im Beschäftigtenverhältnis gewährleistet werden können. Es fehlt jegliche Transparenz, denn das BDSG gehört nicht einmal zu den aushangpflichtigen Gesetzen.

Der DGB hat bereits im Dezember 2008 Eckpunkte zu den notwendigen gesetzlichen Regelungen zum Arbeitnehmerdatenschutz beschlossen. Danach muss Zweck des Datenschutzes sein, den Einzelnen davor zu schützen, dass durch Missbrauch seiner Daten eine Beeinträchtigung seines grundrechtlich geschützten Persönlichkeitsrechts erfolgt. Insbesondere muss die gezielte Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz, aber auch im privaten Umfeld ausdrücklich verboten werden. Dazu gehört z.B. auch der Einsatz von Detektiven und sog. Testkäufern. Der Begriff der Überwachung ist dabei weit zu verstehen, d. h., sowohl Video- und Tonaufnahmen, direktes Ausspähen, Abgleichen von Daten (insbesondere dem persönlichen Bereich zurechenbaren wie Kontonummer, Postverkehr u. ä.), Kontrolle von Telefongesprächen und bei der Verwendung moderner Kommunikationsmittel wie E-Mail und Internet, Scannen und das Erstellen von Bewegungsprofilen mit Hilfe vor Ortungssystemen müssen erfasst werden. Ausnahmen von diesem grundsätzlichen Verbot dürfen nur für gesetzlich ausdrücklich geregelte Fälle, wenn eine andere Möglichkeit der Aufklärung, insbesondere die Einschaltung von Polizei und Staatsanwaltschaft nicht möglich ist, z.B. bei begründetem Verdacht einer strafbaren Handlung oder schwerwiegender Schädigung des Arbeitgebers oder Gefährdung zugelassen werden. Ebenso muss für diese Fälle ein Verfahren gesetzlich geregelt werden, das das Zustimmungserfordernis der betrieblichen Interessenvertretung und, falls diese nicht vorhanden ist, die Einbeziehung einer neutralen Stelle, z. B. den Landesdatenschutzbeauftragten, sowie Dokumentationspflichten und die Pflicht zum geringstmöglichen Eingriff festlegt.

Der Grundansatz der Bundesregierung geht in eine völlig andere Richtung. Vorgesehen ist, den Datenschutz vor allem dem Interesse der Unternehmen an Korruptionsbekämpfung und zur Einhaltung von Compliance-Anforderungen unterzuordnen. Dies führt nicht zu mehr, sondern zu weniger Datenschutz. Dieser Ansatz eröffnet die Möglichkeit, weitgehend den Datenschutz auszuhebeln mit der Begründung, pflichtwidriges Verhalten aufdecken zu wollen. Damit wird das bestehende Schutzniveau erheblich unterschritten. Dies entspricht exakt den Forderungen, die die Arbeitgeberverbände seit Jahren in der Diskussion um den Datenschutz immer wieder erheben. Hinzu kommt, dass der Begriff Compliance nicht gesetzlich definiert ist und sehr weitgehende Möglichkeiten des Arbeitgebers beinhaltet, „Wohlverhalten“ der Beschäftigten zu fordern – und mit den geplanten

Neuregelungen auch zu überwachen. Zusammen mit den unbestimmten Rechtsbegriffen „Erforderlichkeit“ und „Verhältnismäßigkeit“ sind damit der Willkür Tor und Tür geöffnet. Denn mit der Begründung, die Einhaltung von Compliance-Anforderungen kontrollieren zu müssen, setzt der Arbeitgeber selbst den Maßstab der Erforderlichkeit und die Bedingungen der Verhältnismäßigkeit. Das entspricht weder dem Prinzip der Rechtssicherheit, noch ist es transparent.

Sinnvollerweise kann „Compliance“ nur die Einhaltung des geltenden Rechts bedeuten. Dazu gehören aber gerade auch das informationelle Selbstbestimmungsrecht der Arbeitnehmer und der Beschäftigtendatenschutz. Es gibt keine Rechtfertigung dafür, unter den Aspekten von Compliance und Korruptionsbekämpfung neue Einschränkungen des Datenschutzes vorzunehmen und damit einen „Freibrief“ für Ausforschung auszustellen. Die fehlende Rechtfertigung für Eingriffe in Beschäftigtengrundrechte kann durch schwammige Begriffe höchstens überdeckt, aber nicht ersetzt werden.

Der Entwurf enthält keine klaren, eindeutigen Vorschriften zur wirksamen Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten und zum Schutz des Persönlichkeitsrechts. Die vorgeschlagenen Regelungen enthalten dagegen wachsweiche, dehnbare Formulierungen, die den Arbeitgebern viele Möglichkeiten eröffnen können, die gesetzlich zur Verfügung gestellten Instrumente zum „Ausspionieren“ zu nutzen. Es wird infolge des Gesetzes zu Auseinandersetzungen in den Betrieben und Unternehmen über die Zulässigkeit von z.B. der Nutzung und Verwendung biometrischer Merkmale von Beschäftigten kommen, mit denen sich dann die Gerichte befassen müssen, weil die vorgeschlagenen Regelungen Spielräume in Auslegung und Anwendung offen lassen. Die unbestimmten Begriffe „betriebliche Gründe“ und „schutzwürdige Belange/Interessen des Beschäftigten“ ziehen sich wie ein roter Faden durch den Gesetzentwurf und gelten sowohl vor als auch während des Beschäftigungsverhältnisses Im Übrigen fehlt es an Regelungen zum Gebot der Datensparsamkeit. Dies müsste ausdrücklich als Grundsatz festgehalten werden.

Problematisch ist vor allem auch der versteckte und verschachtelt gestaltete Einwilligungsvorbehalt „zu Gunsten“ der Beschäftigten, den das Gesetz an verschiedenen Stellen vorsieht. Das Beschäftigungsverhältnis ist keine gleichrangige Beziehung. Es besteht eine Abhängigkeit der ArbeitnehmerInnen, die es dem Arbeitgeber im Zweifel möglich macht, eine Generaleinwilligung zur Datenerhebung schon bei Aufnahme des Arbeitsverhältnisses zu erhalten. Die Freiwilligkeit der Einwilligung ist deshalb sehr zweifelhaft

Selbst die „Verbesserungen“ gegenüber dem Vorentwurf des BMI ändern an dieser Bewertung nichts. Denn als einzige wesentliche Änderung in diese Richtung ist die Beschränkung der heimlichen Videoüberwachung zu werten. Die hätte aber einer verfassungsrechtlichen Überprüfung sowieso nicht standgehalten. Da gleichzeitig die Möglichkeiten zur Anordnung von Gesundheitsuntersuchungen erheblich ausgeweitet werden, erscheint der Entwurf in der Gesamtbewertung eher noch negativer als der Vorentwurf. Das auch von Arbeitgeberseite Kritik geübt wird, liegt in der Natur der Sache, da sie immer ein Interesse daran hat, Schutzrechte so weit wie möglich einzuschränken. Ein Indiz für die Ausgewogenheit der Regelung ist das nicht.

Ein Gesetz, das keinen politischen Mehrwert im Sinne von mehr Arbeitnehmerschutz darstellt und sogar noch hinter dem Status Quo, den die Rechtsprechung gesetzt hat, zurückbleibt, wird von den Gewerkschaften ausdrücklich abgelehnt. Das Gesetz schafft Rechtsgrundlagen, die das Ausspionieren von Beschäftigten ausdrücklich ermöglichen.

Das System des elektronischen Entgeltnachweises ELENA hat viel Widerstand ausgelöst. Wenn aber schon die Sammlung von Daten zur Gewährung von Leistungen der Sozialversicherungsträger im Hinblick auf die Rechtsprechung des BVerfG zur Vorratsdatenspeicherung verfassungsrechtlich bedenklich ist, um wie viel problematischer ist die Eröffnung von fast unbeschränkten Möglichkeiten für den Arbeitgeber, Daten zu sammeln und aufzubewahren und sie zur Überwachung seiner Beschäftigten zu nutzen?

Zu den Regelungen im Einzelnen

Zu Art. 1 Nr. 3:
Die Regelung bedarf der Klarstellung. Es ist sicherlich nicht Sinn der Neuregelung, den Datenschutz unter den Vorbehalt einer Betriebsvereinbarung zu stellen. Dies ist auch nach der bisherigen Rechtsprechung nicht möglich. Diese stellt vielmehr inhaltliche Anforderungen an eine Betriebsvereinbarung. Diese sind gesetzlich zu definieren. Darüber hinaus ist gesetzlich klarzustellen, für welche konkret bezeichneten Regelungen eine Betriebsvereinbarung in Frage kommt. Insbesondere die Übermittlung personenbezogener Daten an Dritte kann nicht allein auf eine Betriebsvereinbarung gestützt werden, wenn die persönliche Einwilligung des Betroffenen nicht vorliegt.

Zu Art. 1 Nr. 5: § 27 Abs. 3 Anwendungsbereich:
Der Anwendungsbereich ist weit gefasst. Sowohl der sachliche als auch der personelle Anwendungsbereich soll umfassend sein. Dies wird grundsätzlich begrüßt.

Zu Art. 1 Nr. 7: § 32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses:
Zu Abs. 1:
Vorgesehen ist, dass der Arbeitgeber Beschäftigtendaten erfragen darf, die er benötigt, um die Eignung des Bewerbers für eine in Betracht kommende Tätigkeit festzustellen. Dabei wird nicht nur auf die fachliche Eignung abgestellt, sondern es wird ganz allgemein von Eignung gesprochen und dann ausdrücklich auf die persönlichen Fähigkeiten, Kenntnisse und Erfahrungen zurückgegriffen. Damit wird dem Arbeitgeber ein erheblicher Spielraum eingeräumt, da er selbst definieren kann, welche persönlichen Voraussetzungen er für notwendig hält und welche nicht. Eine objektive Feststellung der Erforderlichkeit ist damit von vorneherein erheblich eingeschränkt, da der Arbeitgeber einerseits die Kriterien für die Eignung aufstellt und dann selbst darüber entscheidet, was zur Feststellung dieser Kriterien erforderlich ist. Um diese Voraussetzungen feststellen zu können, wird die Erhebung aller nur denkbaren Daten möglich sein. Das Persönlichkeitsrecht kann nur dann wirksam geschützt werden, wenn nur rein objektive, auf die fachliche Eignung bezogene Kriterien zugelassen werden. Nur auf diese fachlich bezogenen Kriterien dürfen sich Fragen oder andere Datenermittlungen beziehen. Denn nur so kann festgestellt werden, welche Daten tatsächlich erforderlich sind.

Zu Abs. 2:
Darüber hinaus soll die Datenerhebung nach Abs. 2 in Bezug auf rassische und ethnische Herkunft, Behinderung, Gesundheit, sexuelle Identität, Vermögensverhältnisse, Vorstrafen oder laufende Ermittlungsverfahren dann erfolgen können, wenn die Voraussetzungen von § 8 Abs. 1 AGG vorliegen. Das ist dann der Fall, wenn diese Angaben wegen der Art der auszuübenden Tätigkeit oder den Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen darstellt sind. Teilweise entspricht diese Regelung der ebenfalls unzureichenden Regelung im AGG.
Bereits in der Stellungnahme des Deutschen Gewerkschaftsbundes zum AGG-Gesetzentwurf ist darauf hingewiesen worden, dass hier nicht die Art der auszuübenden Tätigkeit **oder** die Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen sein können, sondern es muss sich um eine Sowohl-als-auch-Regelung handeln, d. h., sowohl die Art der auszuübenden Tätigkeit als auch die Bedingungen ihrer Ausübung müssen bestimmte Fragen rechtfertigen, ansonsten wird in das Persönlichkeitsrecht zu weit eingegriffen. „Oder“ müsste also durch „und“ ersetzt werden.
Völlig inakzeptabel ist es, die Frage nach der Gesundheit zuzulassen. Einerseits regelt Abs. 3, dass von Beschäftigten keine Auskunft darüber verlangt werden kann, ob eine Schwerbehinderung oder Gleichstellung mit einem Schwerbehinderten vorliegt, andererseits sollen Fragen nach der Gesundheit aber zulässig sein. Dies ist vollkommen widersprüchlich. Darüber hinaus ist die Frage insbesondere dann äußerst problematisch, wenn man es bei der bisherigen Formulierung belässt und die Bedingungen der Ausübung als alleiniges Kriterium zulässt. Die Bedingungen der Ausübung können nämlich einseitig vom Arbeitgeber bestimmt werden, und unterliegen keinem objektiven Prüfungsmaßstab.
Die Frage nach den Vermögensverhältnissen ist ebenfalls durch nichts zu rechtfertigen, da keine Konstellation denkbar ist, in der die privaten Vermögensverhältnisse in irgendeinem Zusammenhang eine wesentliche oder entscheidende berufliche Anforderung sein könnten. Gerade die Vermögensverhältnisse sind ebenso wie z.B. die Familienplanung eine ausschließlich private Angelegenheit – sie gehen den Arbeitgeber schlicht nichts an.

Wir schlagen – im Sinne von Transparenz und Rechtsklarheit- vor, einen Katalog mit unerlaubten Fragebereichen – wie etwa Schwangerschaft, Familienplanung oder Gewerkschaftszugehörigkeit – ausdrücklich in das Gesetz aufzunehmen. Sowohl vom BAG als auch vom EuGH gibt es dazu eine differenzierte Rechtsprechung.

Zu Abs. 3:
Diese Regelung dient der Klarstellung und ist daher zu begrüßen.

Zu Abs. 4:
Die Regelung entspricht § 9 Abs. 1 AGG, die ihrerseits aber wegen der Verletzung des Art. 4 Abs. 2 der Richtlinie 2000/78/EG europarechtswidrig ist. Danach ist die Frage nach der Zugehörigkeit zu einer Religionsgemeinschaft oder Weltanschauungsgemeinschaft nur dann zulässig, wenn unter Beachtung des Selbstverständnisses der jeweiligen Religionsgemeinschaft im Hinblick auf ihr Selbstbestimmungsrecht **und** (und eben nicht „oder“) nach der Art der Tätigkeit diese Zugehörigkeit eine gerechtfertigte berufliche Anforderung darstellt. Dies muss klargestellt werden. Denn sonst wäre auch die Frage nach der Religionszugehörigkeit bei Tätigkeiten zulässig, die mit dem Verkündungsbereich nichts zu tun haben, z. B. bei einer Reinigungskraft. Die wäre aber mit der Richtlinie nicht zu vereinbaren und ginge auch deutlich über die berechtigten Interessen von Religionsgemeinschaften hinaus.

Zu Abs. 5:
Die Regelung stellt eine Verbesserung gegenüber dem ursprünglichen Entwurf dar, ist aber immer noch nicht klar. In der vorliegenden Form könnte sie so gelesen werden, dass ein Arbeitgeber, der Zwecke der Berichterstattung oder Meinungsäußerung verfolgt, also z. B. ein Verlag, pauschal Daten über die politische Meinung und Gewerkschaftszugehörigkeit der Beschäftigten erheben dürfte. Das ist sicherlich nicht gemeint, muss aber ausdrücklich ausgeschlossen werden.

Zu Abs. 6:
Mit der Regelung, dass Beschäftigtendaten, die allgemein zugänglich sind, auch erhoben und genutzt werden dürfen, und lediglich ein vorheriger Hinweis notwendig ist, werden Vorgehensweisen wie z. B. sog. Scorrings (Detekteien 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. Informationen, deren Wahrheitsgehalt nicht überprüft wird und auch nicht überprüft werden kann, werden damit personelle Entscheidungen beeinflussen können. Berücksichtigt man dabei, dass es jede Menge Informationen auf frei zugänglichen Plattformen gibt, die ohne Wissen und erst recht ohne Zustimmung derjenigen, über die Informationen eingestellt werden, wird deutlich, dass hier Informationen erhoben werden können, die auch im Interesse der Arbeitgeber keinesfalls zur Eignungsfeststellung genutzt werden sollten. .Denn ohne dass damit sinnvoll eine Entscheidung getroffen werden kann, verletzt eine solche Ermittlung das Persönlichkeitsrecht der Betroffenen.

Ebenso ist es falsch, eine Datenerhebung bei Dritten zuzulassen, wenn der Bewerber einwilligt. Denn diese Einwilligung wird im Zweifel erteilt werden müssen, soll die Bewerbung erfolgreich sein. Ebenso ist es unzureichend, den Bewerber nur auf Verlangen über den Inhalt der erhobenen Daten zu unterrichten. Denn im Zweifel wird dieses Verlangen nicht geäußert, um die weiteren Chancen nicht zu verbauen. Deshalb muss der Bewerber über alle über ihn erhobenen Daten informiert werden, und zwar ohne konkrete Aufforderung.

Nach der Begründung des Entwurfs (Bes. Teil, S. 13) stellt diese Bestimmung keine den § 4 BDSG ausschließende, sondern eine diesen „ergänzende“ Regelung dar. Das schafft eine intransparente, unklare und konturlose Ermächtigung für den Arbeitgeber, die in der Praxis zu Ausweitung und Missbrauch geradezu einlädt.

Zu Abs. 7:
In Abs. 7 wird festgelegt, dass die Datenerhebung an den Maßstab der Verhältnismäßigkeit geknüpft ist.
Das sollte zur Klarstellung der Beweislast in positiver Fassung geschehen und indem klargestellt wird, dass es sich um eine zusätzliche Hürde für Datenerhebungen handelt. Diese dürfen also unter Beachtung aller übrigen Rechtmäßigkeitsvoraussetzungen nur dann durchgeführt werden, wenn sie verhältnismäßig sind. Aus Gründen der Transparenz sollte die Methode der Verhältnismäßigkeitsprüfung im Text selbst beschrieben werden.

Zu § 32a: Ärztliche Untersuchungen und Eignungstests vor Begründung eines Beschäftigungsverhältnisses

Zu Abs. 1:
Satz 1 erster Teil wird akzeptiert. Nicht akzeptiert wird die Alternative, dass die Bedingungen der Arbeitsausübung ausreichen, um Daten durch Untersuchungen zu erheben. Hier gilt das zur Frage nach der Gesundheit in § 32 Abs. 2 Gesagte entsprechend. Nur dann, wenn der Arbeitgeber alles ihm Mögliche getan hat, um eine Gesundheitsgefährdung am konkreten Arbeitsplatz auszuschließen, kann überhaupt eine gesundheitliche Untersuchung zulässig sein. Die Fälle müssen ausdrücklich gesetzlich geregelt werden und dürfen nicht der Entscheidungsbefugnis des einzelnen Arbeitgebers überlassen bleiben.
Die ärztliche Untersuchung und Weitergabe des Ergebnisses durch den Vorbehalt der Einwilligung des Arbeitnehmers rechtfertigen zu wollen, ist praxisfern. Eine datenschutzrechtlich relevante Einwilligung setzt die Freiwilligkeit der Entscheidung voraus. Insbesondere im Bewerbungsverfahren wird aber im Zweifel kein Bewerber eine Einwilligung zu einer gesundheitlichen Untersuchung verweigern, wenn der Arbeitgeber sie einfordert, weil er ansonsten nicht weiter für die Einstellung in Betracht kommt.
Die Einwilligung sollte im Übrigen wegen der im Interesse des Bewerbers gebotenen Warnfunktion an die Schriftform gebunden sein.

Zu Abs. 2:
Durch die Regelung in Abs. 2 wird dem Arbeitgeber jede Möglichkeit gegeben, durch weitere Untersuchungen und Prüfungen, die nicht weiter spezifiziert sind, den Bewerber umfassend auszuforschen. Weder ist näher beschrieben, was unter Untersuchungen zu verstehen ist, noch sind Prüfungen (außer durch die Umschreibung „Eignungstest“) in irgendeiner Art eingegrenzt. Darüber hinaus gilt auch hier das zu § 32 Abs. 2 gesagte: die Notwendigkeit der Prüfung an die Art der Tätigkeit oder die Bedingungen ihrer Ausübung zu knüpfen überlässt es dem Arbeitgeber, die Bedingungen der Ausübung festzulegen und damit die Rechtfertigung für bestimmt Untersuchungen und Prüfungen anzuordnen. Objektive Notwendigkeit wird nicht gefordert – subjektive Wünsche des Arbeitgebers genügen. Völlig ad absurdum geführt wird die Regelung dadurch, dass der Eignungstest nach wissenschaftlich anerkannten Methoden durchzuführen ist, **sofern solche bestehen**. Dies bedeutet im Umkehrschluss, dass dann, wenn keine Fachkunde besteht, die Tests trotzdem durchgeführt werden dürfen. Damit ist jeder noch so obskure Test zulässig.

Letzter Satz klärt die Schweigepflicht nur für Personen, die ohnehin einer Schweigepflicht unterliegen. Nach unserer Ansicht ist die Schweigepflicht ausnahmslos auf alle mit der Untersuchung befassten Personen auszuweiten.

Der Absatz muss ersatzlos gestrichen werden, wenn im Einstellungsverfahren keine umfassende Durchleuchtung der Bewerber gewollt ist.

Zu § 32b: Datenverarbeitung und -nutzung vor Begründung des Beschäftigungsverhältnisses

Zu Abs. 1:
Wir verweisen auf die Kritik zu § 32a Abs. 1. Durch das Abstellen ausschließlich auf die allgemeine Eignung des Bewerbers ist dem Arbeitgeber ein ausufernder Spielraum überlassen, welche Daten er zur Feststellung dieser Eignung für notwendig hält, da er selbst die Kriterien der Eignung festlegen kann.
Außerdem fehlt bei der letzten Alternative („oder für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich") jeder eingrenzende Maßstab. Klar ist nur, dass es noch sonstige Parameter außer der Eignung geben soll. Welche anderen Umstände gemeint sind, von denen die Einstellungsentscheidung abhängig gemacht werden soll, wird nicht einmal in der Entwurfsbegründung angedeutet.

Zu Abs. 2:
Es ist inakzeptabel, dass der Arbeitgeber, Daten, die er, auf welchem Weg auch immer, erhalten hat, mit der Begründung, sie seien für seine Entscheidung zur Begründung des Beschäftigungsverhältnisses notwendig, verarbeiten und nutzen kann. Noch gesteigert wird dies, wenn der Beschäftigte ihm „unverlangt" Daten übermittelt. Die Kräfteverhältnisse im Arbeitsverhältnis und insbesondere im Bewerbungsverhältnis ermöglichen so dem Arbeitgeber immer den Zugang. Er kann immer mehr oder weniger deutlich machen, dass er erwartet, dass ihm bestimmte Informationen „unverlangt" zur Verfügung gestellt werden. Mit einer tatsächlichen Freiwilligkeit hat dies in dieser Abhängigkeitssituation überhaupt nichts zu tun.
Darüber hinaus fördert die Regelung innerbetriebliches „Denunziantentum"; bezeichnend die Begründung, S. 14: „ihm auf andere Weise *zugetragen*". Der gesamte Abs. 2 sollte deshalb gestrichen werden.

Zu § 32c: Datenerhebung im Beschäftigungsverhältnis

Zu Abs. 1:
Es ist unklar, welche Beschäftigtendaten überhaupt erforderlich sind zur Beendigung des Arbeitsverhältnisses. Klar ist, dass bestimmte Daten zur Durchführung und zur Abwicklung des Beschäftigungsverhältnisses und natürlich auch zur Begründung des Beschäftigungsverhältnisses notwendig sind. Welche Daten aber zur Beendigung des Beschäftigungsverhältnisses notwendig sein könnten, ergibt sich weder aus dem Gesetz noch aus der Begründung. Hier ist eine Klarstellung erforderlich. Abzulehnen und klar auszuschließen ist jedenfalls eine allgemeine Erlaubnis von Datenerhebungen zur Vorbereitung von Kündigungen und einer „Munitionssammlung" für künftige Kündigungsschutzprozesse.

Zu Abs. 2:
Hier wird auf die Ausführung zu § 32a verwiesen.

Zu Abs. 3:
Grundsätzlich sollten nur die gesetzlich ausdrücklich vorgeschriebenen Untersuchungen zulässig sein, wie z.B. nach Arbeitsmedizinverordnung. Mit der Berechtigung, Untersuchungen oder Tests über die gesetzlich vorgeschriebenen Untersuchungen hinaus anordnen zu können, wenn der Arbeitgeber sie für erforderlich hält, erhält der Arbeitgeber einen Freibrief, krankheitsbedingte Kündi-

gungen oder Kündigungen wegen Leistungsmängeln sowie Versetzungen und Änderungskündigungen vorzubereiten. Damit verschlechtert der Gesetzentwurf Arbeitnehmerrechte eklatant. Der Arbeitnehmer kann sich kaum gegen die Anordnung einer solchen Untersuchung wehren, auch wenn er sie für noch so unberechtigt hält. Denn eine Weigerung im Beschäftigtenverhältnis ist in der Regel mit Konsequenzen verbunden, und diese können häufig nicht als Benachteiligung nachgewiesen werden.
Werden die Ergebnisse der arbeitsmedizinischen Untersuchungen missbräuchlich genutzt, können unliebsame oder leistungsschwächere Beschäftigte zukünftig stark unter Druck gesetzt werden. Außerdem besteht bei obligatorischen Gesundheitstests die Gefahr der Diskriminierung. Deshalb wird beispielsweise die obligatorische Testung auf HIV durch die IAO-Empfehlung 200 (Recommendation concerning HIV and AIDS and the World of Work) abgelehnt, die auch von der Bundesregierung mit Unterstützung der Arbeitgeberverbände und der Gewerkschaften beschlossen worden ist. Auch wenn argumentiert werden könnte, dass solche Daten für das Gesundheitsmanagement benötigt werden, um bessere Prävention leisten zu können bestehen bei der Datenerhebung Zielkonflikte zwischen besserer Prävention und dem Schutz individueller Daten (zum Bsp. auch bei der Gefährdungsbeurteilung oder im Rahmen des Betrieblichen Eingliederungsmanagements). Generell werden deshalb Eignungsuntersuchungen von den meisten Experten sehr kritisch gesehen. Der DGB und seine Mitgliedsgewerkschaften lehnen die Regelung nachdrücklich ab. Die Bedingungen der Ausübung können nämlich einseitig vom Arbeitgeber bestimmt werden, und unterliegen keinem objektiven Prüfungsmaßstab. Darüber hinaus müssen dann, wenn die Bedingungen der Ausübung eine konkrete gesundheitliche Gefährdung darstellen können, zunächst alle Maßnahmen unternommen werden, um die gesundheitliche Gefährdung auszuschließen (vgl. z. B. § 4 ArbSchG: Gefahren sind an ihrer Quelle zu bekämpfen und individuelle Maßnahmen nachrangig).

Zu § 32d: Datenverarbeitung und -nutzung im Beschäftigungsverhältnis

Zu Abs. 1 und 2:
Hier wird auf das bereits Gesagte zur Erforderlichkeit und Verhältnismäßigkeit verwiesen. Es bleibt allein in der Hand des Arbeitgebers, nach welchen Kriterien er seine Entscheidungen treffen will. Ein Arbeitnehmer wird während des Arbeitsverhältnisses dagegen nicht klagen – will er nicht seinen Arbeitsplatz verlieren.

Zu Abs. 1 Nr. 2:
Der damit frei erlaubte Austausch von Zwecken ist abzulehnen. Damit ist eine unkontrollierbare Lockerung der Zweckbindung der erhobenen Daten verbunden („Gelegenheitsfunde“).

Zu Abs. 2:
Vgl. Anm. zu § 32b Abs. 2 und zu § 32 c Abs. 1.

Zu Abs. 3:
Diese Regelung stellt das Kernstück der Neuregelung dar. Sie ist geeignet, sogar den Schutz der, wie dargestellt unzureichend durch die übrigen Neuregelungen geschaffen wird, ins Gegenteil umzukehren. Nach dieser Regelung darf der Arbeitgeber Beschäftigtendaten, die er rechtmäßig erworben hat, immer verwenden, wenn er die Begehung von Pflichtverletzungen zu seinen Lasten oder Straftaten durch den Beschäftigen aufdecken will. Es gibt keinerlei Vorschriften darüber, welche Voraussetzungen dafür vorliegen müssen, ob z. B. ein konkreter Verdacht oder irgendwie geartete Anhaltspunkte für tatsächliche Vertragsverletzungen vorliegen müssen, oder ob eine abstrakte Gefahr im Sinne des Polizeirechts oder darüber hinaus ausreichen soll. Immerhin ist gegen-

über dem Referentenentwurf des BMI der Datenabgleichung zur Verhinderung von Straftaten oder Pflichtverletzungen nicht mehr vorgesehen und es muss sich außerdem um schwerwiegende Pflichtverletzungen handeln. Durch die fehlende Definition, wann die Voraussetzungen vorliegen, Daten zur Aufdeckung verwenden zu dürfen, wird diese Verbesserung jedoch sehr relativiert. Denn die Regelung, dass im Verdachtsfall die Daten personalisiert werden dürfen, legt den Schluss nahe, dass der automatisierte Abgleich auch ohne konkreten Verdacht erfolgen darf. Dann würde aber der Begriff „aufdecken" zwangläufig auch die Prävention einschließen – es bleibt also in der Wirkung bei der früheren Fassung. Positiv ist, dass durch die beispielhafte Inbezugnahme der §§ 266, 299,331 und 334 StGB der Begriff der schwerwiegenden Vertragsverletzung näher definieret wird. Allerdings berücksichtigt auch die Neufassung in keiner Weise das Strafverfolgungsmonopol des Staates, sondern der Arbeitgeber wird durch diese Regelung zu einer Art Betriebspolizei, die selbst ermittelt und zu einer Betriebsstaatsanwaltschaft, die selbst Anklagen erhebt. Dies alles aber, ohne dass die Einschränkungen staatlicher Ermittlungen bei Straftaten oder Ordnungswidrigkeiten vorliegen müssen. Damit und weil insbesondere ungeklärt ist, ab wann der Arbeitgeber „aufdecken" darf, sind die Ausforschungsmöglichkeiten nach diesem Teil des Entwurfs eher noch weitergehender. Hier werden die Vorgänge bei der Deutschen Bahn im Nachhinein legalisiert und gerechtfertigt. Schließlich ist noch darauf hinzuweisen, dass es keinerlei Verfahrensvorschriften gibt, wie anonymisiert und pseudonymisiert werden soll. Denn tatsächlich könnte das wirksam nur erfolgen, wenn ein unabhängiger Dritter mit dem Abgleich beauftragt würde. Im Betrieb selber ist es dagegen kaum möglich die Anonymität zu gewährleisten.
Die Regelung wird insgesamt strikt abgelehnt und muss ersatzlos gestrichen werden.

Zu Abs. 4:
Es ist ungenügend, dass der Arbeitgeber lediglich den Dritten, den er ja selber mit der Datenverarbeitung beauftragt hat bzw. durch den er die Nutzung zulässt, nur darauf hinweisen muss, dass er Daten nur für den Zweck verarbeiten und nutzen darf, zu dessen Erfüllung sie ihm übermittelt wurden. Es muss vielmehr vorgesehen werden, dass dann, wenn der Dritte, dessen Dienste sich der Arbeitgeber bedient, gegen diese Verpflichtung verstößt, der Arbeitgeber dafür in Anspruch genommen werden kann. Außerdem muss festgelegt werden, dass nach Auftragende die Daten unverzüglich zu löschen sind.

Zu Abs. 5:
Die Regelung ist geeignet, die Persönlichkeitsrechte zu stärken und wird deshalb begrüßt – durch die weitgehenden Befugnisse, die der Arbeitgeber aber ansonsten erhält, wird sie entwertet.

Zu § 32e: Datenerhebung, -verarbeitung und -nutzung ohne Kenntnis des Beschäftigten zur Verhinderung und Aufdeckung von Straftaten und anderen schwerwiegenden Pflichtverletzungen im Beschäftigungsverhältnis

In diesem Paragraphen setzt sich die in § 32d Abs. 3 vorgenommene Verschiebung des Schwerpunkts der Neuregelung vom Schutz von Beschäftigtendaten und der grundgesetzlich garantierten Persönlichkeitsrechte von Beschäftigten hin zur Berechtigung des Arbeitgebers zur weitgehenden weiteren Datenerhebung und -nutzung mit der Begründung, z.B. Korruption bekämpfen zu wollen, weiter fort.

Zu Abs. 2:
Es ist kritisch zu sehen, dass überhaupt Beschäftigtendaten ohne Wissen der Betroffenen erhoben werden dürfen. Voraussetzung ist zwar, dass Tatsachen den Verdacht begründen müssen, dass

eine schwerwiegende Vertragsverletzung zu Lasten des Arbeitgebers, die den Arbeitgeber zu einer fristlosen Kündigung berechtigen würde, oder eine Straftat vorliegt. Welche Anforderungen an Tatsachen und Verdacht gestellt werden ist jedoch offen. Richtigerweise müssten Tatsachen einen hinreichenden Tatverdacht begründen um Rechtssicherheit herzustellen. Auch fehlt es an jeder Abgrenzung zum Ermittlungsmonopol des Staates bei Straftaten. Die Tatsache, dass nach Nr. 2 auch die Verhinderung von Pflichtverletzungen und Straftaten ausreicht, um die Datenerhebung zu legitimieren wirft außerdem die Frage auf, welche Anforderungen für diesen Fall vorgesehen sind. Denn die Anforderung, dass Tatsachen den Verdacht begründen müssen ist ausdrücklich nur für Nr. 1 vorgesehen. Nr. 2 knüpft nur an die Erforderlichkeit an, die vom Arbeitgeber zunächst ohne weitere Überprüfung, etwa durch den Datenschutzbeauftragten, festgesetzt wird. Der Beschäftigte kann diese Erforderlichkeit nicht einmal überprüfen lassen, weil er ja gerade keine Kenntnis von der Datenerhebung hat.
Zwar wird in diesem Absatz die Verwendung von Daten nicht ausdrücklich geregelt – sie scheint aber immanent erlaubt zu sein. Denn ohne Verwendung kann die Erhebung allein nicht zur Aufdeckung oder Verhinderung von Straftaten oder Pflichtwidrigkeiten führen. Außerdem müsste klargestellt werden, auf welche konkrete Gruppe oder Person sich die Datenerhebung beziehen soll. Dabei ist die entsprechende Regelung nicht auf Korruptionsbekämpfung beschränkt, sondern gilt für Straftaten ganz allgemein. Auch der Diebstahl von Bagatellgegenständen ist eine Straftat. Selbst wenn nur ein diesbezüglicher Verdacht besteht, ist es nach dem Entwurf dem Arbeitgeber erlaubt, heimlich Daten zu erheben. Damit wird der Verdachtskündigung Vorschub geleistet.

Zu Abs. 3:
Das zur Frage der Erforderlichkeit in Abs. 2 ausgeführte gilt in gleicher Weise für die Verhältnismäßigkeitsprüfung: sie ist erst möglich, wenn die Verletzung des Persönlichkeitsrechts bereits erfolgt ist. . Damit wird aber keinerlei Transparenz hergestellt.

Zu Abs. 4:
Die Regelung geht in die richtige Richtung sollte aber unter Nr. 1 bezüglich des zeitlichen Umfangs einschränkender sein, da die vorgesehene Regelung missbrauchsanfällig ist.

Zu Abs. 5:
Es fehlen Regelungen, wie und bei wem die Dokumentation zu erfolgen hat sowie Sanktionsregelungen bei unterlassener Dokumentation.
Darüber hinaus ist keinerlei vorherige Information beispielsweise der betrieblichen Interessenvertretung oder des Datenschutzbeauftragten vorgesehen, ebenso wenig wie eine Kontrolle durch diese Gremien. Hier muss ein eigenständiges Mitbestimmungsrecht konstituiert werden.

Um einen angemessenen Ausgleich zwischen den Interessen des Arbeitgebers und denen der Beschäftigten zu erreichen, müsste zumindest vorgesehen werden, dass Ausmaß, Ziel und Methode der Datenerhebung, -verarbeitung und -nutzung vorab festgelegt und dokumentiert werden, dass vor Einleitung der Maßnahmen der betriebliche Datenschutzbeauftragte und die betriebliche Interessenvertretung und, soweit eine dieser Institutionen oder beide nicht vorhanden sind, eine unabhängige Stelle, z. B. beim Landesbeauftragten für den Datenschutz, beteiligt wird.

Zu Abs. 7:
Die Regelung wird begrüßt, wobei allerdings nicht klar ist, worin die Notwendigkeit der Inbezugnahme von Abs. 6 S. 2-4 liegt, da es sich um ein absolutes Verbot und eine uneingeschränkte

Löschungsvorschrift handelt – für eine Dokumentation des Grundes der Speicherung oder Löschung, oder die Löschung spätestens am Ende des Kalenderjahres ist also eigentlich kein Raum.

Zu § 32f: Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen

Es fehlen Regelungen gegen den Einsatz von Detektiven und Systemen zur Mitteilung von Korruptionsverdächtigungen von Beschäftigten („internes Whistleblowing“).

Zu Abs. 1:
Auch mit dieser Neuregelung werden die betrieblichen Interessen über das informationelle Selbstbestimmungsrecht der Beschäftigten gestellt. Mit dem Insbesonderenkatalog werden die Zutrittskontrolle, die Wahrnehmung des Hausrechts, der Schutz des Eigentums und Qualitätskontrollen auf eine Stufe mit besonderen Sicherheitsinteressen auch für die Beschäftigten oder der Gefahrenabwehr gestellt. Damit ist die Definition der wichtigen betrieblichen Interessen auf einer sehr niedrigen Schwelle angesiedelt und lässt es zu, dass beispielsweise eine Videoüberwachung, die bei Lidl erhebliche Empörung ausgelöst hat, zukünftig zulässig sein wird. Denn dort war es gerade der Schutz des Eigentums und die Verhinderung von Ladendiebstählen, die Lidl als Begründung dafür angeführt hat, dass die Überwachungen durchgeführt worden sind. Deshalb ist es notwendig, dass der Insbesonderenkatalog beschränkt wird auf die Fälle, in denen ein besonderes Sicherheitsinteresse aufgrund der Besonderheiten der jeweiligen Arbeitsstätte besteht.

Nicht akzeptabel ist aber, dass nach dem Entwurf demnächst in jedem Betrieb die offene Videoüberwachung zur Grundausstattung gehören wird. Diese wird dann zusätzlich noch zur Verhaltens- und Leistungskontrolle eingesetzt werden. Nach der Rechtsprechung des BAG sind der Videoüberwachung strenge Grenzen gezogen worden. Hiervon ist dem Gesetzentwurf nichts zu erkennen. Schließlich ist die notwendige Transparenz immer noch nicht hergestellt. Ziel ist der generelle Ausschluss der heimlichen Videoüberwachung. Ein allgemeiner Hinweis auf den bloßen „Umstand“ der Videoüberwachung reicht dazu nicht. Hier ist eine Konkretisierung erforderlich, damit deutlich wird, wie, an welcher Stelle und wann die Videoüberwachung erfolgt. Fehlen diese Voraussetzungen erhält der Arbeitgeber vom Gesetzgeber die Handhabe, jederzeit eine Videoüberwachung im Betrieb einzusetzen, nachdem sie dies vorher (wo auch immer) kenntlich gemacht haben.
.
Zu Abs. 2:
Die Regelung wird grundsätzlich begrüßt, müsste aber dahingehend geändert werden, dass Betriebsstätten, die **auch** zur privaten Lebensgestaltung des Beschäftigten dienen, nicht per Video überwacht werden dürfen. Nur so kann sichergestellt werden, dass die Privatsphäre von Beschäftigten auch am Arbeitsplatz ausreichend geschützt wird. Außerdem sollte klargestellt werden, dass dort generell ***jede*** Überwachung unzulässig ist. Auch ist der kollektive und kommunikative und nicht nur der individuelle Rückzugsraum entgegen der Begründung, S., schutzwürdig (Pausen- und Raucherräume).

Zu § 32g: Ortungssysteme

Zu Abs. 1:
Die Nutzung von Ortungssystemen zur Sicherheit der Beschäftigten ist grundsätzlich nicht zu beanstanden. Es müsste jedoch gesetzlich geregelt werden, in welchen konkreten Fällen Ortungssysteme überhaupt zur Sicherheit der Beschäftigten eingesetzt werden dürfen. Überdies ist für den jeweiligen Einsatz eine schriftliche Einverständniserklärung nach ausreichender Information erforderlich. Inwieweit zur Koordinierung des Einsatzes von Beschäftigten eine Nutzung von Ortungssystemen zulässig sein soll, ist nicht erkennbar. Insbesondere ist nicht erkennbar, welche Fallgruppen hier erfasst werden sollen. Wenn es beispielsweise darum geht, den Einsatz von Berufskraftfahrern bei einer Spedition oder einem Taxiunternehmen zu koordinieren, ist die Verwendung von Ortungssystemen überflüssig, da ein eventuell notwendig werdender neuer Einsatz dem jeweiligen Beschäftigten sowieso mündlich übermittelt werden muss. Vorher ihn dann auch noch zu orten, ist überflüssig. Die Zulässigkeit einer solchen Ortung beinhaltet vielmehr die Gefahr, dass durch eine solche Ortung die Fahrer unter ständiger Beobachtung gestellt werden. Insofern bietet zwar der letzte Satz von Abs. 1 eine gewisse Sicherheit, besser wäre es jedoch, grundsätzlich die Verwendung zur Koordinierung des Einsatzes auszuschließen.

Unklar ist, wie die Ortung auf die Arbeitszeit beschränkt werden kann. Nach der Begründung sind offenbar Pausenzeiten und Ähnliches der Arbeitszeit zugerechnet worden.

Zu Abs. 2 und 3:
Die Regelungen sind grundsätzlich nicht zu beanstanden.

Zu § 32h: Biometrische Verfahren

Zu Abs. 1:
Dass die Verwendung biometrischer Merkmale, außer die in Form von Lichtbildern ohne Einwilligung der Betroffenen zulässig sein soll, ist nicht einsichtig. Tatsächlich sollte auch hier eine schriftliche Einwilligung notwendig sein. Mit der Regelung, dass betriebliche Gründe zu Autorisierungs- und Authentifikationszwecken ausreichen, um die Verwendung biometrischer Merkmale erforderlich zu machen, wird dem Arbeitgeber ein Alleinentscheidungsrecht übertragen, biometrische Merkmale zu erheben und zu verwenden. Die Einschränkung zur Autorisierungs- und Authentifikationszwecken hilft dabei nicht. Es ist eine grundsätzliche Frage, ob zu diesen Zwecken biometrische Merkmale und damit ganz grundlegende Bereiche der Privatsphäre vom Arbeitgeber erhoben werden dürfen. Zwingend muss nach unserer Auffassung eine Einschränkung auf sicherheitsrelevante Bereiche erfolgen. Dass jeder Arbeitgeber zukünftig Fingerabdrücke oder Irisaufnahmen für den Zugang zu allen Betriebsstätten verwenden darf, ist viel zu weitgehend und daher abzulehnen.
S. 2 enthält zwar ein Einwilligungserfordernis, lässt dafür aber jede Eingrenzung der zulässigen Ziele vermissen. Das ist angesichts der begrenzten Aussagekraft von Einwilligungen des Beschäftigten im Arbeitsverhältnis abzulehnen.

Zu § 32i: Nutzung von Telekommunikationsdiensten

Zu Abs. 1:
Die Regelung in Abs. 1 ist abgesehen von Nr. 3 angemessen. Bezüglich der Regelung in Nr. 3 wird auf die Ausführungen zu § 32d Abs. 3 verwiesen.
Die Regelung dient nur dem Zwecke der Verhaltens- und Leistungskontrolle.

Zu Abs. 2:
Bei dieser Regelung wird der einschränkende Charakter der Nutzungserlaubnis von Telekommunikationsdaten in § 32i ausgehebelt. Wie bereits mehrfach gesagt, ist angesichts des Kräfteverhältnisses im Arbeitsverhältnis die Einwilligung des Beschäftigten kein angemessenes Regulativ bezüglich des Missbrauchs von Arbeitnehmerdaten. Ebenso wenig sind die berechtigten Interessen des Arbeitgebers eine Einschränkung, denn nach der gesamten Anlage der Neuregelung geht die Wertung des Gesetzgebers dahin, dass die berechtigten Interessen auf einer sehr niedrigen Schwelle vorliegen. Die Sonderregelungen für die Arbeit in Callcentern nach Satz 2 und 3 sind ebenfalls völlig unangemessen. Sie geben dem Arbeitgeber ein weitgehendes Recht, die berufliche Tätigkeit der Mitarbeiter dauerhaft aufzuzeichnen. Dies entspräche an anderen Arbeitsplätzen einer Dauerbeobachtung durch Video. Dass hier außerdem eine bloße Benachrichtigung, aber nicht einmal eine vorherige Einwilligung des Beschäftigten, so unzureichend sie auch sein mag, vorgesehen ist, setzt die Beschäftigten in Callcentern einem erheblichen Überwachungsdruck aus. Ebenso wenig ist die Einwilligung der Kommunikationspartner ein einschränkendes Kriterium, als sich an der bisherigen völlig unbefriedigenden Praxis nichts ändert.

Es sollte klargestellt werden, dass eine schriftliche Einwilligung des Arbeitnehmers (nicht vorab im Arbeitsvertrag) und eine ausdrückliche Erklärung des Kommunikationspartners erforderlich ist.

Zu Abs. 3:
Es wird auf die Ausführung zu Abs. 1 verwiesen.

Zu § 32j: Unterrichtungspflichten

Zu Abs. 1:
Die Regelung ist nicht weitgehend genug. Es ist nicht ausreichend, dass der Arbeitgeber bei unrechtmäßiger Übermittlung oder Kenntniserlangung bei Dritten dies dem Arbeitnehmer mitteilt. Er hat vielmehr alles ihm Zumutbare zu tun, um daraus entstehende Schäden auszuschließen und auf den Dritten einzuwirken, dass die Daten unverzüglich gelöscht werden.

Zu § 32 l: Einwilligung, Geltung für Dritte, Rechte der Interessenvertretung, Beschwerderecht, Unabdingbarkeit

Zu Abs. 4:
Es ist praxisfern, das Recht der Beschäftigten, Verstöße gegen die unbefugte Datenerhebung, -verwendung oder –nutzung bei der zuständigen Behörde erst zuzulassen, wenn Vorab einer Beschwerde im Betrieb nicht abgeholfen wurde. Gerade in schweren Fällen, in denen der Beschäftigte davon ausgehen muss, dass der Rechtsverstoß mit voller Absicht erfolgt ist, wird er durch die Notwendigkeit, zunächst eine interne Beschwerde vorzunehmen. einem erheblichen Druck ausgesetzt. Er wird in diesen Fällen immer mit Repressalien rechnen müssen – und im Zweifel die Be-

schwerde unterlassen. Im Übrigen konterkariert die Regelung die Rechtsprechung des BAG zu whistleblowing, die gerade dann, wenn der Arbeitgeber der „Täter“ ist, keine interne Beschwerde verlangt, weil sie unverhältnismäßig ist. Im Übrigen dürfte eine solche Beschränkung auch gegen die EU Datenschutzrichtlinie verstoßen. Denn nach Artikel 28 Absatz 4 der EU-Datenschutzrichtlinie 95/46 steht jedermann, das Recht zu, sich bei Verdacht auf Verstöße gegen Datenschutzbestimmungen direkt an unabhängige Kontrollbehörden zu wenden. Eine Einschränkung ist gerade nicht vorgesehen.

Zu Nr. 10 Ergänzung von § 43:
Die Vorschriften des § 43 lediglich und unvollständig zu ergänzen, wird den Bedürfnissen nach wirksamen und abschreckenden Sanktionen nicht gerecht. Zum einen werden nicht einmal alle Verstöße gegen die Pflichten des Arbeitgebers aus den Neuregelungen in den Bußgeldkatalog aufgenommen (z. B. fehlt die Erlangung von Daten von Dritten ohne Einwilligung nach § 32a Nr. 8), zum anderen müssten aber besonders schwere Verstöße auch strafbewehrt sein. Darüber hinaus fehlt die Regelung zu einem Entschädigungsanspruch des Beschäftigten bei Verletzung seines Persönlichkeitsrechts und ein Schadensersatzanspruch, wenn z. B. ein Bewerber aufgrund unrechtmäßig erlangter Daten im Bewerbungsverfahren die Stelle nicht erhält.

Zusammenfassung

Der Gesetzesentwurf verdient nicht den Namen, der ihm gegeben wurde. Es handelt sich nicht um den Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, sondern um einen Entwurf zur Regelung der Erlaubnis des Arbeitgebers zur Nutzung von Beschäftigtendaten. Die vorgesehenen Regelungen gehen viel zu weit und greifen in die Rechte der Beschäftigten, insbesondere in deren Recht auf informationelle Selbstbestimmung in nicht zu rechtfertigender Weise ein. Es ist fraglich, ob mit diesem Entwurf die Grenzen, die das Bundesverfassungsgericht für Eingriffe in das allgemeine Persönlichkeitsrecht in seinen datenschutzrechtlich relevanten Ausprägungen gesetzt hat, auch nur ansatzweise eingehalten werden. Es darf beim Datenschutz nicht darum gehen, Persönlichkeitsrechte auf denselben Rang wie das Recht der Unternehmer an ihrer wirtschaftlichen Betätigung zu stellen. Persönlichkeitsrechte müssen Vorrang haben und sind unverzichtbar.

GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERHEIT e.V.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 B

S t e l l u n g n a h m e

zum

a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes
(BT-Drucksache 17/4230)
unter Berücksichtigung des
Arbeitspapiers der Berichterstatter der Koalitionsfraktionen
(Ausschussdrucksache 17(4)255)

b) Gesetzentwurf der Fraktion der SPD
Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz)
(BT-Drucksache 17/69)

c) Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN
Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen
(BT-Drucksache 17/4853)

d) Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN
Persönlichkeitsrechte abhängig Beschäftigter sichern – Datenschutz am Arbeitsplatz stärken
(BT-Drucksache 17/121)

e) Antrag der Fraktion DIE LINKE
Datenschutz für Beschäftigte stärken
(BT-Drucksache 17/779)

erstellt von

Rechtsanwalt Andreas Jaspers,

Geschäftsführer der GDD e.V.

Gesellschaft für Datenschutz
und Datensicherheit e.V.
Pariser Str. 37 · 53117 Bonn
Tel.: 0228/69 43 13 · Fax: 0228/69 56 38
Internet: www.gdd.de · E-Mail: info@gdd.de

I. Vorbemerkung

Die Stellungnahme hat im Schwerpunkt den Gesetzentwurf der Bundesregierung zum Gegenstand (BT-Drucksache 17/4230). Zu den übrigen Gesetzentwürfen und Anträgen wird thematisch Bezug genommen.

Es ist zu begrüßen, dass die Bundesregierung ihrer Ankündigung gefolgt ist, in seinem Entwurf den Beschäftigtendatenschutz nicht in einem eigenständigen Gesetzeswerk, sondern als Abschnitt des Bundesdatenschutzgesetzes zu regeln. Positiv zu bewerten ist auch die Intention des Regierungsentwurfs, eine gesetzliche Konkretisierung des richterrechtlich geprägten Arbeitnehmerdatenschutzes herbeizuführen. Zugleich ist es für die Fortentwicklung des Beschäftigtendatenschutzes sinnvoll, den Einsatz der Informations- und Kommunikationstechnologien im Beschäftigungsverhältnis unter dem Gesichtspunkt des Persönlichkeitsrechtsschutzes zu konkretisieren.

Der Regierungsentwurf sieht keine Regelung der Datenschutzkontrolle beim Betriebsrat vor. Wie das Bundesarbeitsgericht in seiner Entscheidung vom 11.11.1997 angeregt hat, sollte in einem Arbeitnehmerdatenschutzgesetz die ungeklärte Rechtsfrage der Kontrolle des Betriebsrates durch den betrieblichen Datenschutzbeauftragten geregelt werden. Diese Rechtsfrage ist nach dem vorliegenden Entwurf weiterhin ungeklärt.

Der Referentenentwurf trägt auch nicht Datenverarbeitungen von Beschäftigten im Konzern und Unternehmensverbünden Rechnung. Zunehmend werden unternehmerische Ziele in nationalen und multinationalen Unternehmensverbünden verfolgt, wobei die Konzerne im wachsenden Maße darauf angewiesen sind, Mitarbeiterdaten im Rahmen ihrer Geschäftstätigkeit an konzernangehörige Unternehmen zu transferieren. Vielfach ist die Rechtsgrundlage für die notwendigen Datentransfers nicht ausreichend klar.

Generell ist im Hinblick auf die Gesetzestechnik anzumerken, dass entgegen der üblichen BDSG-Systematik getrennte Regelungen für die Datenerhebung bzw. die anschließende Datenverarbeitung und -nutzung geschaffen werden. Hier wäre es im Sinne der Verständlichkeit der gesetzlichen Regelungen ratsam, einheitliche Lebenssachverhalte jeweils in einer Vorschrift zusammenzuführen und z.B. eine Vorschrift über die Erhebung, Verarbeitung und Nutzung im Bewerbungsverfahren zu schaffen. Dadurch können auch gesetzliche Redundanzen und Verweisungen, die die Verständlichkeit und Lesbarkeit des Gesetzes erheblich erschweren, vermieden werden.

II. Zu den einzelnen Regelungen

Zu §§ 3 Nr. 12, 27 Abs. 3 BDSG-E (Definition Beschäftigtendaten)

Der Begriff der Beschäftigtendaten in § 3 Abs. 12 BDSG-E ist zu weit gefasst und entspricht daher nicht dem Anwendungsbereich der §§ 32 ff. BDSG-E. Hier bedarf es einer Trennung von Beschäftigten- und sonstigen personenbezogenen Mitarbeiterdaten. Auszunehmen aus den Beschäftigtendatenschutzregelungen der §§ 32 ff. BDSG-E sind Daten von Bewerbern und Mitarbeitern, deren Erhebung, Verarbeitung oder Nutzung nicht der Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses dienen sollen. Für diese personenbezogenen Daten gelten – je nach Art ihrer Verarbeitung – die allgemeinen Regelungen des BDSG bzw. das im Arbeitsrecht entwickelte Datenschutzrecht (vgl. Gola/Jaspers, RDV 2009, S. 212). Maßgebend für die Anwendung der §§ 32 ff. BDSG-E ist die beabsichtigte Zweckbestimmung der Daten (vgl. § 27 Abs. 3 BDSG-E).

Hier ist dem Vorschlag Nr. 1 der Berichterstatter der Koalitionsfraktionen zuzustimmen.

Zu §§ 4 Abs. 1, 32l Abs. 5 BDSG-E (Betriebsvereinbarungen)

Ein absolutes Verbot, durch Betriebsvereinbarungen zu Ungunsten der Beschäftigten vom Beschäftigtendatenschutzgesetz abzuweichen, hat nicht zu unterschätzende Konsequenzen in der Praxis. Der Vorteil von Betriebsvereinbarungen als Reglungsinstrument für den Umgang mit Beschäftigtendaten ist regelmäßig, verfahrens- oder anwendungsbezogen passgenaue betriebliche Regelung zu schaffen. Durch die geplante Neuregelung besteht die Gefahr, dass den Betriebspartnern die Motivation genommen werden wird, von dem flexiblen und bewährten Instrument der Betriebsvereinbarung Gebrauch zu machen. Die Betriebspartner hätten nach dem Gesetzentwurf jedenfalls nicht mehr wie bisher die Möglichkeit, die Unbestimmtheiten des BDSG zu beseitigen.

Bereits im Jahr 1986 hat das BAG (RDV 1986, S. 199 = DB 1986, S. 2080) entschieden, dass Betriebsvereinbarungen den Datenschutz der Arbeitnehmer auch abweichend vom Bundesdatenschutzgesetz regeln können. Nach der Entscheidung des BAG sind Betriebsvereinbarungen nicht darauf beschränkt, nur unbestimmte Rechtsbegriffe des BDSG unter Berücksichtigung der betrieblichen Besonderheiten näher zu konkretisieren oder den Arbeitnehmerdatenschutz zu verstärken. Danach stellt das BDSG keinen unabdingbaren Mindeststandard dar. Gleichzeitig hat das Gericht aber festgestellt, dass die Grundsätze über den Persönlichkeitsschutz im Arbeitsverhältnis zu beachten sind (vgl. zuletzt BAG, RDV 2008, S. 238, wonach der Grundsatz der Verhältnismäßigkeit als Prüfungsmaßstab heranzuziehen ist). Der Gestaltungsfreiraum der Parteien der Betriebs- oder Dienstvereinbarung ist nach dem BAG sofern begrenzt, als sie sich an „grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen“ auszurichten haben. Hierauf aufsetzend sieht der aktuelle Gesetzentwurf nunmehr unabdingbare Vorschriften zum Beschäftigtendatenschutz als zwingendes Gesetzesrecht vor. Ein Abweichen von den neuen Vorschriften zum Beschäftigtendatenschutz zu Ungunsten der Beschäftigten wäre mithin generell ausgeschlossen.

Bedenkt man den sich aus § 75 Abs. 2 BetrVG für Arbeitgeber und Betriebsrat gleichermaßen ergebenden Schutzauftrag, so sind Beispiele, in denen eine an sich nach BDSG unzulässige Personaldatenverarbeitung durch Betriebsvereinbarung gleichwohl gestattet sein könnte, bereits nach bisheriger Rechtslage ohnehin eher selten (vgl. Gola/Schomerus, BDSG, § 4 Rdnr. 10 m.w.N.). Vor diesem Hintergrund könnte man es bei der bisherigen Rechtslage belassen und ergänzend unmittelbar im Gesetzestext darauf hinweisen, dass Betriebs- oder Dienstvereinbarungen die gesetzlichen Regelungen durchaus konkretisieren

oder Alternativen gestalten können, um den jeweiligen betrieblichen Besonderheiten Rechnung zu tragen.

Zumindest sollten jedoch bei bestimmten Datenverarbeitungsverboten Öffnungsklauseln vorgesehen werden. Sinnvoll wäre es z.B. die am Verhältnismäßigkeitsgrundsatz orientierte Rechtsprechung des BAG zur heimlichen Videoüberwachung per Betriebsvereinbarung fortzuführen (vgl. zuletzt BAG, RDV 2008, S. 238). Schließlich gibt es in bestimmten Fällen kein anderes Mittel zur Aufklärung von Straftaten und auch für die betreffenden Mitarbeiter kann die allein vom Arbeitgeber – ohne eine gesetzlich befohlene Involvierung staatlicher Stellen – als ultima ratio veranlasste verdeckte Überwachung ein milderes Mittel sein. Dieses Beispiel verdeutlicht, dass gerade Betriebsvereinbarungen den vom Gesetzgeber angestrebten Interessenausgleich unternehmensspezifisch möglich machen können, ohne die gesetzgeberische Wertung eins zu eins zu übernehmen.

Zu berücksichtigen ist ferner, dass ein absolutes Verbot von zu Ungunsten der Beschäftigten abweichenden Betriebsvereinbarungen nach dem Gesetzentwurf mit dem weitgehenden Wegfall der Einwilligung als Rechtsgrundlage kumuliert, was nicht unbedingt im Sinne von informationeller Selbstbestimmung und unternehmerischer Selbstregulierung wäre. Insbesondere dort, wo dem Beschäftigten insgesamt eine Erweiterung seiner Rechtsposition zugebilligt werden soll (vgl. hierzu auch Art. 29-Gruppe, WP 114, S. 13), muss Raum für Individualeinwilligungen und Kollektivvereinbarungen verbleiben, selbst wenn letztere nicht exakt dem Datenschutzstandard des geplanten BDSG-Unterabschnitts zum Beschäftigtendatenschutz entsprechen. Einer expliziten Klarstellung im Gesetzestext – und nicht nur in der Gesetzesbegründung – bedarf insofern auch die nach Maßgabe einer Betriebsvereinbarung zulässige Kontrolle der privaten Internet- und E-Mail-Nutzung am Arbeitsplatz. Ansonsten bestünde die Gefahr, dass Arbeitgeber vorsichtshalber die Privatnutzung des Internet- und E-Mail-Systems gänzlich untersagen. Eine solche Lösung wäre aber weder praxistauglich noch interessengerecht. Die Notwendigkeit von Rechtsklarheit in diesem äußerst praxisrelevanten Punkt hat auch bereits der Bundesrat in seiner Stellungnahme zu dem Regierungsentwurf betont.

Für eine erweiterten Regelungsrahmen von Betriebsvereinbarungen spricht ferner, dass abweichende Betriebsvereinbarungen - in dem von der Rechtsprechung erlaubten Rahmen - weiterhin bei Verarbeitungen erlaubt sind, die nicht der Zweckbestimmung der §§ 32 ff. BDSG-E dienen, da hier das Verbot des § 32l Abs. 5 BDSG-E nicht gilt.

Schließlich ist darauf hinzuweisen, dass die bisherigen Bemühungen zahlreicher Betriebspartner, über Betriebsvereinbarungen einen sachverhaltsbezogenen Interessenausgleich herzustellen, nachträglich in Frage gestellt würden. Zu prüfen wäre in diesem Zusammenhang auch, inwieweit bereits abgeschlossene Betriebsvereinbarungen Bestandsschutz genießen müssen.

Zu § 32 BDSG-E (Fragerecht des Arbeitgebers)

§ 32 BDSG-E enthält Regelungen für die Datenerhebung vor Begründung des Beschäftigungsverhältnisses. Der Datenumgang im Zusammenhang mit internen Stellenausschreibungen stellt in der Praxis allerdings eine vergleichbare Problemstellung dar. Insofern ist eine Ergänzung der geplanten Regelung zu erwägen.

Die Regelung in § 32 Abs. 2 BDSG-E erweitert mit Blick auf Fragen zu Vermögensverhältnissen, Vorstrafen und laufenden Ermittlungsverfahren den Anwendungsbereich des Allgemeinen Gleichbehandlungsgesetzes (AGG). Bislang richtet sich der Berechtigung der Kenntnis von Vorstrafen oder Angaben über die Vermögensverhältnisse danach, ob sie für die Entscheidung über die Geeignetheit des Bewerbers für den zu besetzenden Arbeitsplatz erforderlich ist (§ 32 Abs. 1 S. 1 BDSG). In Betrachtung des § 32 Abs. 2 E-BDSG-E und des

§ 8 Abs. 1 AGG stellt sich die Frage, ob demnächst noch nach den gleichen Kriterien entschieden werden kann. Abzustellen ist nicht mehr auf die Erforderlichkeit der Information, sondern darauf, dass das Nichtvorliegen der Vorstrafe wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt. Die spezielle Regelung in § 32 Abs. 2 E-BDSG macht nur Sinn, wenn die Anforderungen für die Erhebung dieser Daten über die in der Generalklausel des § 32 Abs. 1 E-BDSG vorausgesetzte Erforderlichkeit hinausgehen. Abzustellen wäre darauf, welcher Maßstab an die Begriffe „ wesentlich und entscheidend“ zu stellen ist bzw. wann das Merkmal „unverzichtbare Voraussetzung“ für die zu erbringende Tätigkeit ist. Entscheidend im genannten Sinne ist eine Anforderung erst dann, wenn der Umstand aus objektiver Sicht in einem laufenden Arbeitsverhältnis kündigungsrelevant wäre.
Für die nicht diskriminierungsrelevanten Merkmale der Vermögensverhältnissen, Vorstrafen und laufenden Ermittlungsverfahren ist diese Anforderung im Bewerbungsverfahren zu hoch und in der Regel nicht eindeutig zu beurteilen. Hier sollte die bestehende Rechtlage, die an das Vorliegen eines berechtigten Interesses anknüpft, beibehalten werden. Dem Vorschlag Nr. 3 der Berichterstatter der Koalitionsfraktionen ist insoweit zuzustimmen.

Die Regelung des § 32 Abs. 3 BDSG-E gibt die bestehende Rechtslage wieder, wonach im Bewerbungsverfahren keine Auskunftspflicht im Hinblick auf das Vorliegen einer Schwerbehinderung besteht. Aus Gründen der Rechtsklarheit sollte jedoch ergänzend darauf hingewiesen werden, dass freiwillige Angaben des Bewerbers zur Inanspruchnahme seiner in SGB IX genannten Rechte verwendet werden dürfen.

Problematisch sind auch die gesetzlichen Vorschläge zur Internetrecherche des Arbeitgebers in § 32 Abs. 6 BDSG-E. Hier hat der Regelungsvorschlag zur Recherche in sozialen Netzwerken, der danach differenziert, ob die Darstellung der beruflichen Qualifikation oder lediglich der Kommunikation des Bewerbers dient, erhebliche Abgrenzungsschwierigkeiten zur Folge. Fraglich ist, wie angesichts der Dynamik der technischen Entwicklung diese Widmung nachvollzogen werden kann. Hier ist – entsprechend der Überlegung Nr. 4 der Berichterstatter der Koalitionsfraktionen - eine Differenzierung nach öffentlich zugänglichen Informationen und solchen, die nur einem eingeschränkten Benutzerkreis zur Verfügung gestellt werden, zielführender.

§ 32 Abs. 7 BDSG-E regelt den Grundsatz der Verhältnismäßigkeit bei der Datenerhebung vor Begründung eines Beschäftigungsverhältnisses. Mit Blick auf die Bedeutung des Verhältnismäßigkeitsprinzips empfiehlt sich, diesen Grundsatz in Zusammenhang mit der Regelung zur Erforderlichkeit in § 32a Abs. 1 BDSG-E zu verankern.

Zu § 32a BDSG-E (Ärztliche Untersuchungen / Eignungstests)

Nach § 32l Abs. 1 BDSG-E ist die Einwilligung als Erlaubnistatbestand nur noch in den im Gesetz genannten Fällen zulässig. Ein Beispiel ist die vor einer ärztliche Untersuchung notwendige abzugebende Erklärung (§ 32a Abs. 3 BDSG-E). Regelmäßig fehlt es jedoch an der zur Wirksamkeit der Einwilligung gebotenen Freiwilligkeit des Bewerbers, da er ohne Untersuchung nicht eingestellt würde.

Für ein gesetzliches Einwilligungserfordernis bei gesundheitlichen Untersuchungen bleibt in der Regel auch wenig Raum. Auf Grund von Vorschriften zur Arbeitssicherheit ist der Arbeitgeber zum Teil verpflichtet, vor Einstellung eine Untersuchung zu fordern. Die Teilnahme an der Untersuchung ist insofern notwendige Voraussetzung für die Einstellung. Daneben kann es weitere Fälle geben, in denen die gesundheitliche Tauglichkeit zwingende Voraussetzung für die Erfüllung der vorgesehenen arbeitsvertraglichen Verpflichtungen ist.

Sinn macht das Gebot der Einwilligung nur insofern, dass der Bewerber in dem in § 4a BDSG vorgeschrieben Umfang über Art und Weise und Ziel der Untersuchung aufzuklären ist. Statt der Einwilligung sollte daher diese Informationspflicht vorgesehen werden. Dass im übrigen eine Teilnahme von der Zustimmung des Betroffenen abhängt, ist sachbedingt.

Eine ähnliche Problematik stellt sich bei § 32a Abs. 2 BDSG-E, der die Durchführung von Eignungstests ebenfalls von der Einwilligung des Betroffenen abhängig macht. Auf welche Weise der Arbeitgeber die fachliche und persönliche Eignung eines Bewerbers ermittelt, ist zunächst seinem Ermessen überlassen. Insofern kann er die Entscheidung über die Einstellung auch von der Mitwirkung des Bewerbers an einem Assessment-Center abhängig machen. Auf eine förmliche Einwilligung kommt es insoweit nicht an, da es dem Bewerber freisteht, an dem Assessment-Center teilzunehmen oder nicht. Insoweit bedarf es hinsichtlich der Eignungstests nur einer gesetzlichen Klarstellung, dass diese nach den Regeln der Fachkunde durchzuführen sind.

Bestehen bleiben kann auch die Regelung in § 32a Abs. 2 Satz 5 BDSG-E, wonach bei Vorliegen beruflicher Schweigepflichten nur das Ergebnis des Eignungstests mitzuteilen ist. Jedoch sollte auch hier (vgl. § 32 Abs. 1 S. 5 BDSG-E) gegenüber dem Betroffenen die Pflicht bestehen, dieses Ergebnis zu begründen

Zu § 32b BDSG-E (Datenverarbeitung vor Begründung des Beschäftigungsverhältnisses)

§ 32b Abs. 2 BDSG-E regelt die Datenverarbeitung und -nutzung ohne vorherige Datenerhebung nach § 32a BDSG-E. Systematisch ist aber schwer abzugrenzen, wann eine solche Datenverarbeitung bzw. -nutzung ohne vorausgehende Erhebung vorliegt. Deshalb sollte der Gesetzgeber zum besseren Verständnis die Formulierung aus der Gesetzesbegründung aufgreifen, wo daran angeknüpft wird, dass der Arbeitgeber Beschäftigtendaten ohne Nachfrage vom Beschäftigten erhält bzw. ihm die Daten auf andere Weise zugetragen werden.

Die Regelung des § 32b Abs. 2 S. 2 BDSG-E erlaubt dem Arbeitgeber Initiativbewerbungen zu berücksichtigen. Aber auch freiwillige Mitteilungen in einem laufenden Bewerbungsverfahren werden vom Wortlaut erfasst. Zutreffend steht es einer Einwilligung gleich, wenn der Bewerber bestimmte Information im Rahmen eines Bewerbungsverfahrens ungefragt mitteilt und damit seinen Wunsch zu deren Berücksichtigung bei der Einstellungsentscheidung zum Ausdruck bringt. § 32b Abs. 2 S. 2 E-BDSG erlaubt jedoch dem Arbeitgeber diese Daten auch dann für die Feststellung der Eignung oder zur Entscheidung über die Begründung des Arbeitsverhältnisses heranzuziehen, auch wenn er sie nicht nach §32 oder §32a E-BDSG hätte erheben dürfen. Diese Regelung bedarf einer Einschränkung. Keine Verwendung finden dürfen Daten, durch die Mitbewerber diskriminiert oder indirekt – um gleichzuziehen – gezwungen werden, auf ihre Persönlichkeitsrechte zu verzichten. So wird ein nicht vorbestrafter Bewerber ggf. ein Führungszeugnis bereits von sich aus vorlegen. Eine Frau mag ggf. zu Recht denken, dass ein Arbeitgeber zu ihrer Einstellung motiviert wird, wenn sie ihm ein ärztliches Attest darüber vorliegt, dass sie nicht mehr schwanger werden kann. Würde der Arbeitgeber diese Information verwenden, würde das eine unzulässige Diskriminierung der Bewerber bedeuten, die von ihrem Schweigerecht Gebrauch machen. Zudem darf sich die Verarbeitungsermächtigung nur auf zur Zweck der Einstellung mitgeteilte Daten erstrecken. Daten die der Bewerber z.B. im Zusammenhang mit einer parallel bestehenden Kundenbeziehung, mitgeteilt hat, sind nicht verwertbar.

§ 32b Abs. 3 BDSG-E regelt, dass Bewerberdaten nicht gelöscht werden müssen, wenn der Beschäftigte in ihre weitere Speicherung eingewilligt hat. In der Praxis hat sich als interessengerecht herausgestellt, dass bei einem weiteren Interesse an einem Bewerber dieser

über die weitere Speicherung seiner Daten informiert und ihm ggf. ein Widerspruchsrecht eingeräumt wird.

Die beabsichtigte Neuregelung fordert hingegen eine förmliche Einwilligung nach § 4a BDSG. Dies ist für die Unternehmen mit erheblichem Aufwand verbunden und wird auch vom Bewerber als bürokratischer Formalismus empfunden.

Überdies könnte die beabsichtigte Regelung dahingehend interpretiert werden, dass ohne Einwilligung Bewerberdaten nach Abschluss des Bewerbungsverfahrens unmittelbar zu löschen sind. Eine weitere Speicherung kann jedoch auch auf Grund unternehmenseigener Interessen gerechtfertigt sein (z.B. Speicherung von Bewerberdaten, so lange ggf. noch Ansprüche wegen AGG-Verstößen geltend gemacht werden können). Insoweit empfiehlt sich, die vorgesehene Regelung ersatzlos zu streichen.

Hier sollte an die Rechtsprechung des BAG (NJW 1984 S. 2910) angeknüpft werden, die generell die fortdauernde Speicherung bei Bestehen berechtigter Interessen erlaubt, wodurch auch die Frage einer durch das AGG bedingten dreimonatigen Aufbewahrungsfrist abgedeckt wäre.

Offen ist, ob das Löschungsgebot auch für die in § 32 Abs. 1 S. 1 BDSG-E genannten Daten gilt, so dass, wie es der Praxis entspricht, die Tatsache der Bewerbung auch nach Abschluss des Verfahrens weiter gespeichert werden kann.

Zu § 32d Abs. 3 BDSG-E (Automatisierter Datenabgleich)

Vor dem Hintergrund in der Vergangenheit bekannt gewordener und schon seinerzeit als rechtswidrig einzustufender umfassender Datenabgleiche erscheint diese Regelung sinnvoll, weil sie Ausmaß und Folgen von Datenabgleichen mit Bezug auf Beschäftigtendaten begrenzt.

Auch für den Datenabgleich gilt der allgemeine datenschutzrechtliche Grundsatz, dass Überwachungsmaßnahmen zur Erreichung eines Zwecks erforderlich sein müssen. Nach dem Entwurfstext darf der Arbeitgeber nur zum Zweck der Aufdeckung von Straftaten oder anderer schwerwiegender Pflichtverletzungen einen Datenabgleich durchführen. Auch wenn sich nicht immer bei einem Unternehmen bereits ein konkreter Anlass dafür ergeben hat, wäre es unter dem Gesichtspunkt der Compliance rechtswidrig, erst auf diesen zu warten anstatt auf Grund von Eintrittswahrscheinlichkeiten (z.B. der gesamten Branche) mit diesbezüglichen Risiken zu rechnen. Anlässe für Überwachungsmaßnahmen müssen also nicht konkret eingetreten sein, sondern ergeben sich aus Gefährdungsanalysen. Die näheren Umstände dazu hat der Arbeitgeber nach dem Gesetzentwurf zu dokumentieren. Aus der Gefährdungsanalyse wird sich in der Regel ergeben, dass nicht alle Beschäftigten, sondern nur eine Gruppe von Beschäftigten für das zu untersuchende Risiko in Betracht kommt (z.B. Miles & More nur bei Vielfliegern).

Diese Konkretisierung des Erforderlichkeitsgrundsatzes sollte auch im Gesetzestext des § 32d Abs. 3 Satz 1 BDSG-E aufgenommen werden.

Wäre allerdings nur das Vorliegen eines Anfangsverdachtes der Anlass einer Überwachungsmaßnahme, setzt das voraus, dass mit Bestimmtheit zeitlich vorgelagert etwas Ordnungs- oder Gesetzwidriges, zumindest aber Unplausibles eingetreten ist. Letzteres lässt sich in der Regel nur durch vorher durchgeführte Datenabgleiche feststellen (z.B. Inventurdifferenz), die u.U. nicht erlaubt gewesen wären.

Der weite Begriff der Beschäftigtendaten kann dazu führen, dass jeder Datensatz einer Datei einen Personenbezug zu einem oder mehreren Beschäftigten aufweisen kann, die bei Pflichtverletzungen ggf. zur Verantwortung gezogen werden können. Das darf aber nicht bedeuten, dass eine verantwortliche Stelle als Unternehmen nicht mehr ihre geschäftlich anfallenden Daten prüfen darf, weil sie gleichzeitig als Arbeitgeber „Beschäftigtendaten" abgleicht.

Eine Beschränkung des automatisierten Datenabgleichs erfolgt zudem über die Forderung des Gesetzentwurfs nach datensparsamer Vorgehensweise. Nach dem Abziehen von Datenbeständen ohne Identifikationsmerkmale der Beschäftigten können anonyme Auswertungen produziert werden, und zwar dergestalt, dass einzelne nicht plausible Datenkonstellationen erkannt und gruppiert (z.B. in Fehlerklassen) dargestellt werden, aber keine Zuordnung zu einem Beschäftigten vorgenommen werden kann, weil die Auswertenden keinen Zugriff auf die dazugehörigen Identifikationsmerkmale haben. Erst in einem zweiten Schritt ist zu entscheiden, ob die Auswertung so viele gewichtige unplausible Konstellationen enthält, die eine weitere Aufklärung erforderlich macht. Abhängig von Risikolage kann auch eine pseudonyme Auswertung angezeigt sein, bei der zumindest ein Merkmal (z.B. Satznummer) mitgeliefert wird, welches im Nachhinein die Re-Identifizierung eines Beschäftigten ermöglicht.

Zu § 32e BDSG-E (Datenerhebung ohne Kenntnis des Betroffenen)

§ 32e Abs. 2 Nr. 1 BDSG-E stellt darauf ab, dass ein Verdacht gegen einen Beschäftigten vorliegt, im Beschäftigungsverhältnis eine schwerwiegende Vertragsverletzung begangen zu haben. In der Praxis wird es aber vielfach so sein, dass sich der Verdacht der schwerwiegenden Vertragsverletzung nicht gegen einen einzelnen Beschäftigten, sondern gegen eine Gruppe von Beschäftigten richtet, von denen einzelne oder mehrere die Tat begangen haben können. Insoweit bedarf es einer entsprechenden Anpassung des Gesetzestextes, wonach der Verdachtsmoment auf Beschäftigte (Plural) abstellt. Eine entsprechende Vorbildregelung für den Verdacht hinsichtlich einer Beschäftigtengruppe enthält § 32f Abs. 2 BDSG-E.

Abzustellen ist nach § 32e Nr. 1 BDSG-E auf eine schwerwiegende Vertragsverletzung zu Lasten des Arbeitgebers, die diesen zu einer fristlosen Kündigung aus wichtigem Grund berechtigen würde. Als Voraussetzung für konkrete Maßnahmen zur Durchsetzung der Compliance birgt dies erhebliche Risiken. Die Hürden für eine fristlose Kündigung gem. § 626 BGB sind sehr hoch und in der Regel auch unwägbar. Im Vorfeld ist kaum sicher prognostizierbar, ob sich bestehende Verdachtsmomente bestätigen werden und die aufzudeckende Vertragsverletzung eine außerordentliche Kündigung rechtfertigen wird. Daher sollte allein auf den konkreten Verdacht einer schwerwiegenden Vertragsverletzung abgestellt werden.

Zu § 32f BDSG-E (Offene Videoüberwachung)

§ 32f BDSG-E regelt die Beobachtung nicht öffentlich zugänglicher Betriebsstätten durch Videoüberwachung. Sinnvoll wäre, den Beschäftigtendatenschutz in Zusammenhang mit der Videoüberwachung in § 32f BDSG-E abschließend zu regeln, also auch Arbeitsplätze in öffentlich zugängliche Bereiche einzubeziehen.

Die zugelassenen Kontrollzwecke dienen sekundär auch einer Verhalts- und Leistungskontrolle. Gefahren für das Eigentum oder die Sicherheit am Arbeitsplatz können auch von Beschäftigten ausgehen und können nach ihrer Feststellung zu arbeitsrechtlichen Konsequenzen führen. In einem Satz 2 des Abs. 1 sollte jedoch klargemacht werden, dass die Heranziehung der Überwachungsergebnisse zwecks einer von der Zweckbestimmung losgelösten allgemeinen Leistungskontrolle unzulässig ist.

Zu § 32g BDSG-E (Ortungssysteme)

Die in § 32g Abs. BDSG-E geforderte unverzügliche Löschung ist zu restriktiv, da die Ortungsdaten ggf. auch für Dokumentationen und Rechtsstreitigkeiten relevant sein können. Ein Verweis auf die entsprechende Erforderlichkeit wäre besser.

Zu § 32h BDSG-E (Biometrische Verfahren)

Lichtbilder sind nicht regelmäßig biometrische Verfahren im Sinne der Vorschrift. Insoweit macht es Sinn, die Verwendung von Lichtbildern von Beschäftigten aus der Vorschrift des § 32h BDSG-E herauszulösen und allgemein zu regeln.

Zu § 32i BDSG-E (Nutzung von Telekommunikationsdiensten)

Die Regelungen über die Nutzung von Telekommunikationsdiensten differenzieren zwischen der Erhebung von Inhalten und Verkehrsdaten während der Kommunikation und der in Absatz 4 geregelten nachgelagerten Kontrolle. Die Regelungen beziehen sich dabei nur auf die dienstliche Kommunikation. Lediglich in § 32i Abs. 4 Satz 2 wird der Zugriff auf Daten der privaten Kommunikation zum Zwecke des ordnungsgemäßen Dienst- und Geschäftsbetriebs geregelt. Hier sollte aus Gründen der Rechtssicherheit auf „erkennbar“ private Daten abgestellt werden.

Da in der Praxis sehr häufig auch eine zumindest geduldete Privatnutzung der Telekommunikationsanlagen des Arbeitgebers anzutreffen ist, sollte eine Öffnung für eingeschränkte Kontrollmöglichkeiten durch den Arbeitgeber auf Grundlage einer Einwilligung ggf. nach den Vorgaben einer Betriebsvereinbarung vorgesehen werden. Hierzu bedarf es einer Öffnungsklausel für Betriebsvereinbarungen in § 32l Abs. 5 (siehe vorstehend) und einer Erweiterung der Tatbestände für eine erlaubte Einwilligung im beschäftiungsverhältnis.

Zu § 32j BDSG-E (Unterrichtungspflichten bei Datenpannen)

§ 32j BDSG-E fordert bei Datenverlusten immer die Unterrichtung des Beschäftigten und zwar unabhängig davon, ob der Datenverlust zu einer Beeinträchtigung der Rechte oder schutzwürdigen Interessen führt. Ein Bedürfnis für eine solche Regelung ist nicht ersichtlich. Dem Schutzbedürfnis der Betroffenen wird durch § 42a BDSG hinreichend Rechnung getragen. § 32j BDSG-E sollte daher ersatzlos gestrichen werden.

Zu § 32l BDSG-E (Einwilligung als Erlaubnistatbestand)

§ 32l BDSG-E verbietet die Einwilligung als Erlaubnistatbestand für den Umgang mit Beschäftigtendaten, sofern dies nicht ausdrücklich vorgesehen ist.

Hier ist zunächst vom Grundsatz her darauf hinzuweisen, dass die Einwilligung in Art. 7 a) der EG-Datenschutzrichtlinie (RL95/46/EG) einen eigenständigen Erlaubnistatbestand darstellt, der zwar unter dem Vorbehalt der Freiwilligkeit steht, nicht jedoch für das Beschäftigungsverhältnis eingeschränkt ist.

Die Regelungsentwurf verkennt, dass auch im Arbeitsverhältnis Einwilligungen vielfach notwendige Rechtsgrundlage sind. Die im Gesetz in Bezug genommenen Erlaubnistatbestände fehlen für solche Beschäftigungsverhältnisse, die nur mit einer Einwilligung des Bewerbers bzw. Arbeitnehmers durchführbar sind (z.B. Einwilligung in ein Prüfrecht vor Ort bei Telearbeit; Einwilligung in die Sicherheitsüberprüfung, Einwilligung in eine eingeschränkte Kontrolle der Privatnutzung von Telekommunikationsdiensten).

Zudem kommt es insbesondere in Konzernen unternehmensübergreifend zur Arbeit in Matrixstrukturen. Weiterhin ist Bestandteil der Personalarbeit der Aufbau von konzernweit zugänglichen Datenbanken mit Kenntnissen und Fähigkeiten (Skills) von Mitarbeitern. In Ermangelung einer anderen Rechtsgrundlage erfolgt die hierfür notwendige Datenverarbeitung auf Grundlage einer Einwilligung, deren Freiwilligkeit unproblematisch ist. Deshalb sollte von einem generellen Verzicht auf die Einwilligung als Erlaubnistatbestand für die Arbeit mit Beschäftigtendaten abgesehen werden. Die Einholung einer Einwilligung könnte jedoch klarstellend an die Voraussetzung geknüpft werden, dass der Arbeitgeber an ihrer Abgabe ein berechtigtes Interesse hat.

III. Evidente Regelungslücken

Weitergabe von Mitarbeiterdaten im Unternehmensverbund

Regelungsbedürftig ist die Weitergabe von Mitarbeiterdaten im Unternehmensverbund. Angesichts der Tatsache, dass weder die EU-Datenschutzrichtlinie noch das Bundesdatenschutzgesetz ein „Konzernprivileg“ kennen, ist vielfach ein notwendiger Austausch von Mitarbeiterdaten zwischen verbundenen Unternehmen datenschutzrechtlich nicht unproblematisch. Hier sollten für Tatbestände, die betriebswirtschaftlich sinnvoll und für den Datenschutz der Mitarbeiter regelmäßig unschädlich sind, wie der Betrieb von Shared-Service-Centern, die zentrale Führungskräftebetreuung oder die konzernweite Steuerung der IT-Infrastruktur, gesetzliche Zulässigkeitstatbestände geschaffen werden.

Ein Beispiel für eine Konzernklausel bietet der Gesetzentwurf von BÜNDNIS90/DIE GRÜNEN (BT-Drucksache 17/4853) in § 7 Abs. 2, der einen Zulässigkeitstatbestand für die Übermittlung von Beschäftigtendaten innerhalb von Konzernverbünden und eine Öffnungsklausel für entsprechende Betriebsvereinbarungen schafft. Die Regelung eines Konzernprivilegs kann unter den in diesem Gesetzentwurf genannten Vorrausetzungen als Ausgestaltung der Datenverarbeitung auf Grundlage einer Interessenabwägung erfolgen, die Art. 7 f) der EG-Datenschutzrichtlinie (RL95/46/EG) als generellen Erlaubnistatbestand vorsieht.

Unbeschadet von einer Konzernklausel bleibt das Erfordernis des angemessenen Schutzniveaus bei den konzernangehörigen Unternehmen gemäß § 4b Abs. 2 S. 2 BDSG.

Datenschutzkontrolle beim Betriebsrat

Die Kontrolle der personenbezogenen Datenverarbeitung beim Betriebsrat ist seit einer Entscheidung des Bundesarbeitsgerichtes aus dem Jahre 1997 gesetzlich ungeregelt. Das Bundesarbeitsgericht hatte seinerzeit entschieden, dass die Datenverarbeitung des Betriebsrates nicht durch den betrieblichen Datenschutzbeauftragten kontrolliert werden dürfe. Seitdem besteht im Unternehmen ein quasi kontrollfreier Raum. Die Gesetzeslücke führt dazu, dass zwar das Unternehmen gegenüber dem Betroffenen als verantwortliche Stelle zur Gewährleistung des Datenschutzes verpflichtet ist, diesen jedoch gegenüber dem Betriebsrat nicht durchsetzen kann.

Die vom BAG für seine Entscheidung angeführte mangelnde Unabhängigkeit des betrieblichen Datenschutzbeauftragten hat der Gesetzgeber durch den besonderen Kündigungsschutz in § 4f Abs. 3 Satz 4 BDSG teilweise korrigiert. Einer Erweiterung bedarf die Verschwiegenheitsverpflichtung des Datenschutzbeauftragten nach § 4f Abs. 4 BDSG, die sich bisher nur auf die Identität des Betroffen bezieht. Diese müsste um die Beratung und Kontrolle des Betriebsrates erweitert werden.

Bonn, den 17. Mai 2011

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 C

BDA
DIE ARBEITGEBER

Herrn
MR Dr. Heinz-Willi Heynckes
Leiter Sekretariat
Innenausschuss des
Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Arbeitsrecht

arbeitsrecht@arbeitgeber.de

T +49 30 2033-1200
F +49 30 2033-1205

18. Mai 2011
0200-1105-049/Wo/MH

Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes und anderen Entwürfen

Sehr geehrter Herr Dr. Heynckes,

anliegend finden Sie die gemeinsame Stellungnahme von BDI und BDA zu den Gesetzentwürfen zum Arbeitnehmerdatenschutz.

Die Ausarbeitungen beziehen sich auf:

- Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes der Regierung (Regierungskoalition),
- Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (SPD) und
- Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen (BÜNDNIS 90/DIE GRÜNEN).

Unsere Stellungnahme zum Arbeitspapier der Berichterstatter der Koalitionsfraktionen werde ich Ihnen am Freitag, 20. Mai 2011, übermitteln.

Mit freundlichen Grüßen

Roland Wolf

Katharina Ludewig

Anlage

BDA | Bundesvereinigung der Deutschen Arbeitgeberverbände

Mitglied von BUSINESSEUROPE

Hausadresse:
Haus der Deutschen Wirtschaft
Breite Straße 29, 10178 Berlin

Briefadresse:
11054 Berlin

www.arbeitgeber.de

Arbeitnehmerdatenschutz rechtssicher gestalten

Gesetzes- und Pflichtverstöße wirksam verhindern

Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes und anderen Entwürfen

18. Mai 2011

Aktenzeichen
02.02.02.04./Bal

Arbeitsrecht

arbeitsrecht@arbeitgeber.de

T +49 30 2033-1200
F +49 30 2033-1205

BDA Bundesvereinigung der
Deutschen Arbeitgeberverbände

EU-Register der Interessenvertreter
Nr. 7749519702-29

BDI Bundesverband der
Deutschen Industrie e.V.

EU-Register der Interessenvertreter
Nr. 1771817758-48

Mitglieder von
BUSINESSEUROPE

Haus der
Deutschen Wirtschaft
Breite Straße 29
10178 Berlin

Zusammenfassung

Die Einhaltung von Gesetzen, Verträgen und betrieblichen Regelungen ist für die Unternehmen ein wichtiges Anliegen. Hierzu gehört auch der Arbeitnehmerdatenschutz. Daher begrüßen BDA und BDI das Anliegen, die Rechtsfragen des Arbeitnehmerdatenschutzes im Rahmen des Bundesdatenschutzgesetzes klarzustellen. das Ziel muss sein, hierdurch rechtssichere Regelungen für Korruptions- und Kriminalitätsbekämpfung in den Unternehmen zu gewährleisten und gleichzeitig das in Deutschland hohe Niveau des Datenschutzes auch weiterhin im Betrieb sicherzustellen.

Ein eigenständiges Arbeitnehmerdatenschutzgesetz ist hierfür nicht notwendig. Die Gesetzentwürfe, die ein solch eigenständiges Gesetz vorsehen, kommen nicht umhin, auf das Bundesdatenschutzgesetz Bezug zu nehmen (vgl. § 4 der BT-Drs. 17/69 und § 4 Abs. 3 der BT-Drs. 17/4853). Auch soweit – zu Recht – der Arbeitnehmerdatenschutz weiterhin im Bundesdatenschutzgesetz verortet bleiben soll (Drs. 17/4230) bedarf der Gesetzentwurf erheblicher Änderungen, um die Compliance-Anforderungen der Unternehmen – zu denen auch der Datenschutz gehört – zu gewährleisten.

1. Gesetzentwurf der Bundesregierung (BT-Drs. 17/4230)

Der Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes erfüllt diese Zielsetzung noch nicht. In der vorliegenden Form ist er nicht geeignet, Rechtssicherheit für Arbeitgeber und Arbeitnehmer bei der Verwendung personenbezogener Daten im Arbeitsverhältnis und die Einhaltung der Compliance im Unternehmen zu gewährleisten.

Der Entwurf sieht achtzehn neue Informationspflichten vor und geht von einer zusätzlichen Kostenbelastung der Wirtschaft mit Informationspflichten von 9,49 Mio. Euro jährlich und einmaligen Umstellungskosten von 10,3 Mio. Euro aus. Insbesondere vor dem Hintergrund der begrüßenswerten Bemühungen der Bundesregierung, Bürokratie flächendeckend abzubauen, ist dieser Aufbau neuer Bürokratie bedenklich und besonders problematisch für kleine und mittlere Unternehmen.

Der Gesetzentwurf bedarf vielfältiger Korrekturen. In diesem Rahmen ist insbesondere erforderlich:

- Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine rechtssichere Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein. Betriebsnahe Lösungen sind wichtig, um die gesetzlichen Vorgaben in den Betrieben anzuwenden und mit Leben zu erfüllen. Dem Ziel eines praxisnahen Arbeitnehmerdatenschutzes genügen solche Regelungen vielfach besser und nachhaltiger als gesetzliche Regelungen.
- Nach dem Gesetzentwurf ist die Einwilligung des Arbeitnehmers in eine Datenerhebung, -verarbeitung und -nutzung grundsätzlich nicht mehr möglich. Dieser Ausschluss der Einwilligungsmöglichkeit wird den Interessen der Arbeitnehmer und der Arbeitgeber nicht gerecht. Die Möglichkeit der Einwilligung muss daher als Grundlage für eine Datenerhebung, -verarbeitung und -nutzung erhalten bleiben.
- Korruptions- und Kriminalitätsbekämpfung ist für Arbeitgeber und Arbeitnehmer ein wichtiges Anliegen. Arbeitnehmerdatenschutz muss die Bekämpfung von Korruption und Kriminalität unterstützen. Dazu sind präventive Kontrollen und Datenanalysen unabdingbar.

- Zur Unterstützung von Korruptions- und Kriminalitätsbekämpfung kann auch eine gezielte Videoüberwachung erforderlich sein. Deren absolutes Verbot ist nicht akzeptabel.
- Es muss klargestellt werden, dass die Regelungen des Gesetzesentwurfs ausschließlich auf Beschäftigtendaten und nicht auf Daten des Tagesgeschäfts (Geschäftsdaten aus Buchhaltungssystemen mit einer Verknüpfung zum Anwender oder Benutzer wie bspw. Personenkürzel o.ä.) bezogen sind. Hierzu ist eine Definition von Geschäftsdaten in Abgrenzung zu Beschäftigtendaten festzulegen.
- Die Nutzung elektronischer Kommunikation muss grundlegend geregelt werden. Hierzu ist insbesondere eine klare Regelung zum Verhältnis der datenschutzrechtlichen Vorschriften zum TMG und TKG zu treffen.
- Eine gesetzliche Regelung muss den Datenaustausch zwischen Konzernunternehmen sicherstellen. Bisher ist ein solcher auf die Konzernstruktur zugeschnittener Datenschutz nicht vorgesehen. Schon lange notwendig ist eine rechtssichere Möglichkeit, um zum Beispiel Beschäftigtendaten von Konzerntöchtern an die Konzernmütter weitergeben zu können.

2. Gesetzentwürfe von SPD (BT-Drs. 17/69)und BÜNDIS 90/DIE GRÜNEN (BT-Drs. 17/4853)

Die vorgelegten Gesetzentwürfe der Oppositionsfraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN weisen ebenfalls inhaltliche Mängel auf. Insbesondere ist es nicht akzeptabel, Beschäftigtendatenschutz zu einer Ausweitung von Mitbestimmungsrechten zu nutzen, z.B. indem die Berufung eines erstmals vorgesehenen Beschäftigtendatenschutzbeauftragten nur mit Zustimmung des Betriebsrats zulässig sein soll.

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230)

(Gesetzentwurf der Bundesregierung)

Im Einzelnen

1. § 3 – Definition von Beschäftigtendaten und Arbeitgeber

Regelungsgehalt: Beschäftigtendaten werden als personenbezogene Daten von Beschäftigten definiert. Arbeitgeber sind u. a. auch Dritte, denen Beschäftigte zur Arbeitsleistung überlassen werden.

Die Definition von „Beschäftigtendaten“ lässt die Auslegung zu, dass auch Daten den besonderen Bestimmungen zur Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten unterliegen sollen, die nicht unmittelbar mit einer Beschäftigung verbunden sind (wie zum Beispiel Kantinenabrechnungen, Arbeitgeberdarlehen). Die neuen Regelungen beschränken sich hingegen auf die „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“. Aus Gründen der Rechtsklarheit sollte sich der Zweckbezug zum Beschäftigungsverhältnis auch in der Definition der Beschäftigtendaten wie folgt wieder finden: „Beschäftigtendaten sind personenbezogene Daten von Beschäftigten, die im unmittelbaren Zusammenhang zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses stehen“.

Zur Abgrenzung des jeweiligen gesetzlichen Regelungsbereichs sollte klargestellt werden, dass Daten, die überwiegend dem Geschäftsbetrieb des Arbeitgebers zuzurechnen sind, nicht als Beschäftigtendaten gelten. Daten eines solchen Geschäftsbetriebs sind insbesondere Daten, die bei der Erfüllung der arbeitsvertraglichen Pflichten anfallen und keine Rückschlüsse auf besonders schützenswerte personenbezogene Daten des Arbeitnehmers im Sinne des § 3 Absatz 9 BDSG zulassen, wie beispielsweise der Benutzername in einem Buchhaltungssystem. Im Hinblick auf die Arbeitgeberdefinition sollte in der Gesetzesbegründung klargestellt werden, dass hiermit ausschließlich Fälle der Arbeitnehmerüberlassung im Sinne des AÜG gemeint sind.

2. § 4 Absatz 1 i.V.m. § 32l Absatz 5 – Betriebsvereinbarungen als andere Rechtsvorschriften

Regelungsgehalt: Der Gesetzentwurf sieht vor, dass andere Rechtsvorschriften im Sinne dieses Gesetzes auch Betriebs- und Dienstvereinbarungen sind. Diese Regelung wird durch § 32l Absatz 5 des Entwurfs eingeschränkt, der vorgibt, dass von den Vorschriften zum Arbeitnehmerdatenschutz nicht zu Ungunsten der Beschäftigten abgewichen werden kann.

Die Klarstellung, dass die Datenerhebung, -verarbeitung und -nutzung auch durch Betriebsvereinbarungen ausgestaltet werden kann, läuft durch die Einschränkung des § 32l Absatz 5 leer. Faktisch wird die Betriebsvereinbarung ausgeschlossen. der Gesetzgeber muss sich entscheiden, ob die Betriebsvereinbarung eine Abweichung ermöglichen soll. Um die Autonomie der Betriebsparteien zu erhalten, sollte § 35 Absatz 5 gestrichen werden.

Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein können. Betriebsnahe Lösungen sind wichtig, um die gesetzlichen Vorgaben in den Betrieben anzuwenden und mit Leben zu erfüllen. Dem Ziel eines praxisnahen Arbeitnehmerdatenschutzes genügen solche Regelungen vielfach besser und nachhaltiger als gesetzliche Regelungen.

Darüber hinaus ist eine Klarstellung dahingehend erforderlich, dass andere Rechtsvorschriften im Sinne von § 4 Absatz 1 auch Tarifverträge sein können. Tarifverträge werden nicht als sonstige Regelung erwähnt. Lediglich in der Gesetzesbegründung zu § 32l wird ausgeführt, dass nicht ausgeschlossen sei, dass Tarifverträge, Betriebs- oder Dienstvereinbarungen die gesetzlichen Regelungen konkretisieren oder Alternativen gestalten. Diese Wertung muss in den Gesetzestext einfließen. Es muss klar sein, dass die Datenerhebung, -verarbeitung und -nutzung wie bisher auch auf der Grundlage einer sonstigen Regelung wie in Tarifverträgen, Betriebs- und Dienstvereinbarungen erfolgen kann.

3. § 27 Absatz 3 – Anwendungsbereich der Vorschriften des BDSG für das Arbeitsverhältnis

Regelungsgehalt: § 27 Absatz 3 sieht vor, dass die Vorschriften des Beschäftigtendatenschutzes auch dann gelten, wenn Daten nicht automatisiert verarbeitet werden.

Es ist ein Systembruch, die nicht automatisierte Datenverarbeitung den Vorschriften des Beschäftigtendatenschutzes zu unterstellen. Dieser Systembruch muss beseitigt werden. Das Bundesdatenschutzgesetz dient dem Schutz vor den Gefahren, die sie sich aus der automatisierten Datenverarbeitung ergeben, beispielsweise aufgrund eines Kontextverlusts oder den Verknüpfungsmöglichkeiten.

Um diese Unklarheiten zu vermeiden, sollte deshalb zu der Rechtslage vor dem 1. September 2009 zurückgekehrt werden, nach der die entsprechenden datenschutzrechtlichen Regelungen nur bei automatisierter Verarbeitung von Dateien Anwendung finden. Es ist also ein einheitlicher Datenbegriff erforderlich.

4. § 32 - Datenerhebung vor Begründung eines Beschäftigungsverhältnisses

a) Absatz 1

Regelungsgehalt: Absatz 1 regelt die Zulässigkeit der Erhebung von Beschäftigtendaten vor Begründung eines Arbeitsverhältnisses. Abgesehen vom Namen, der Anschrift, Telefonnummer und E-Mail-Adresse darf alles erhoben werden, dessen Kenntnis erforderlich ist, um die Eignung des Beschäftigten für eine vorgesehene Tätigkeit festzustellen.

Der Arbeitgeber hat ein berechtigtes Interesse, im Rahmen der Bewerbung Erkenntnisse über sog. „soft skills“ wie Sozialkompetenz, Teamfähigkeit oder Zuverlässigkeit für jede in Betracht kommende Tätigkeit zu erlangen. Der Wortlaut des § 32 Abs. 1 des Entwurfs macht nicht deutlich, ob der Erwerb von Kenntnissen über solche „soft skills“ zulässig ist, weil der Arbeitgeber nur noch für die konkrete Tätigkeit erforderliche Kenntnisse und nicht auch allgemeine Fähigkeiten erfragen können soll, obwohl diese sogar als Ziel der Berufsausbildung ausdrücklich vom Gesetzgeber verlangt werden (Fähigkeiten iSd. BBiG).

Die Formulierung „Kenntnis (…) erforderlich (...), um die Eignung des Beschäftigten für die vorgesehenen Tätigkeiten festzustellen“ ist zu eng, falls z.B. noch nicht endgültig feststeht, auf welcher offenen Stelle der Arbeitnehmer eingesetzt werden soll. Besser wäre deshalb folgende Formulierung: „…für sämtliche in Betracht kommende Tätigkeiten festzustellen“. Gleichzeitig muss der Begriff der Erforderlichkeit ersetzt werden durch folgende Formulierung: „dem Zweck dient, die Eignung (…) festzustellen“.

b) Absatz 2

Regelungsgehalt: Absatz 2 des Entwurfs sieht vor, dass der Arbeitgeber außerhalb besonderer Erlaubnistatbestände gem. § 8 Absatz 1 AGG Auskunft über besondere Arten personenbezogener Daten nur verlangen kann, wenn und soweit sie „wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen darstellen“.

Die vorgesehene Beschränkung auf Daten, „soweit sie wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen darstellen“, schafft neue Rechtsunsicherheit aufgrund einer Vielzahl von Auslegungsmöglichkeiten. In der Praxis ist es schwierig zu entscheiden, ob die gewonnenen Erkenntnisse eine „wesentliche und entscheidende berufliche Anforderung“ für die auszuübende Tätigkeit darstellen. Da ein Verstoß gegen das Datenerhebungsrecht mit einem Bußgeld von bis zu 300.000 € bedroht ist, gilt es, solche Rechtsunsicherheiten unbedingt zu vermeiden.

Die strengen Anforderungen des § 8 Absatz 1 AGG sollen auch für die Frage nach Vorstrafen oder Ermittlungsverfahren gelten. Dies ist nicht gerechtfertigt. Nach der Rechtsprechung des BAG konnte nach Vorstrafen und nach den Vermögensverhältnissen gefragt werden, „wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert“ (BAG vom 25.4.1980 – 7 AZR 322/78). Dies muss ausreichend sein. Die Einführung des Begriffs „wesentliche und entscheidende berufliche Anforderungen“ ist eine Verschärfung, die vor dem Hintergrund der ausdifferenzierten Rechtsprechung nicht notwendig ist.

c) Absatz 3

Regelungsgehalt: Es ist ein generelles Verbot der Auskunftsbitte im Hinblick auf eine Schwerbehinderung vorgesehen.

Das ist überflüssig. Absatz 3 sollte gestrichen werden. Einzelfälle sollten im Gesetzentwurf nicht explizit aufgegriffen werden. Zudem unterliegen Gesundheitsdaten ohnehin dem besonderen Schutz des § 3 Abs. 9 BDSG und der Sondervorschriften des § 1 AGG und des § 81 Abs. 2 SGB IX.

d) Absatz 6

Regelungsgehalt: Dieser gibt vor, dass Beschäftigtendaten unmittelbar beim Beschäftigten zu erheben sind. Allgemein zugängliche Daten dürfen nur dann ohne Mitwirkung des Beschäftigten erhoben werden, wenn er hierauf vor der Erhebung hingewiesen wurde und sein schutzwürdiges Interesse nicht überwiegt. Eine Datenerhebung aus sozialen Netzwerken ist nicht möglich. Hiervon sind solche sozialen Netzwerke ausgenommen, die zur Darstellung der beruflichen Qualifikation bestimmt sind.

Diese Regelung wird der täglichen Praxis beim Umgang mit allgemein zugänglichen Daten nicht gerecht. Es ist nicht ersichtlich, warum im Bewerbungsverfahren nur unter erschwerten Voraussetzungen auf Zeitungsartikel, Interneteinträge etc. zurückgegriffen werden können soll. Insbesondere in Bezug auf das Internet ist zu berücksichtigen, dass jeder für das Einstellen von Beiträgen in der Regel selbst verantwortlich ist.

Nach diesen Vorgaben wäre ein Arbeitgeber quasi gezwungen, nach Eingang einer Bewerbung dem Bewerber individuell einen Hinweis zukommen zu lassen, sofern er allgemein zugängliche Informationen nutzen möchte. Andernfalls bliebe ihm nur, in der Stellenausschreibung einen entsprechenden Hinweis aufzunehmen, was in der Praxis für potentielle Bewerber aber eher abschreckend wirken könnte.

Durch die Vorschrift wird die Bereitschaft, Mitarbeiter einzustellen und Arbeitsplätze zu schaffen, neuen überflüssigen Belastungen ausgesetzt. Das Ziel des Arbeitsrechts, Beschäftigung zu fördern, wird hierdurch nicht unterstützt.

Weder der Gesetzestext noch die Begründung sehen eine klare Abgrenzung von sozialen Netzwerken und sozialen Netzwerken zur Darstellung der beruflichen Qualifikation vor. Es ist sehr wahrscheinlich, dass sich in Zukunft Netzwerke bilden, die sowohl die berufliche als auch die soziale Komponente gleich stark gewichten. Rechtsunsicherheit ist hier vorprogrammiert.

5. § 32a – ärztliche Untersuchungen und Eignungstests

a) Absatz 1

Regelungsgehalt: Absatz 1 regelt die Zulässigkeit von Gesundheitsuntersuchungen im Anbahnungsverhältnis. Die Erfüllung bestimmter gesundheitlicher Voraussetzungen muss wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung zum Zeitpunkt der Arbeitsaufnahme darstellen. Die Einwilligung des Beschäftigten ist erforderlich.

Die gesetzlichen Voraussetzungen, unter denen Gesundheitsuntersuchungen zulässig sein sollen, sind zu eng. So werden zum Beispiel in der chemischen Industrie vielfach bei Einstellungen Alkohol- und Drogenuntersuchungen unabhängig davon vorgenommen, wo der konkrete Einsatz später erfolgen soll. Dies ist notwendig, da der Konsum von Alkohol und Drogen nicht mehr dem privaten Bereich zugeordnet werden kann, wenn dadurch die sicherheitsempfindlichen Verfahrensabläufe in den Unternehmen gefährdet würden. Die Regelung sollte deshalb Gesundheitsuntersuchungen zulassen, um die Eignung des Bewerbers unabhängig von der auszuübenden Tätigkeit zu prüfen. Der Begriff der „Zweckdienlichkeit“ sollte in diesem Zusammenhang eingeführt werden. Unklar bleibt zudem, welche Tätigkeiten ihrer Art nach erfasst werden sollen. So kann ein gesunder Rücken für eine überwiegend sitzende Tätigkeit eine wesentliche und entscheidende berufliche Anforderung sein. Zudem muss ausreichend sein, den Beschäftigten über die Art der Untersuchung (Blut- und Urinuntersuchung) zu informieren, bevor eine Einwilligung erteilt wird.

Insgesamt muss das Verhältnis von Arbeitnehmerdatenschutz und Arbeitsschutz klargestellt werden. So muss sichergestellt werden, dass die Pflichtuntersuchungen, die die Verordnung zur arbeitsmedizinischen Vorsorge vorsieht, nicht den Voraussetzungen des § 32a Absatz 1 unterliegen.

b) Absatz 2

Regelungsgehalt: Absatz 2 regelt die Zulässigkeit von Eignungstests vor Begründung des Beschäftigungsverhältnisses. Die Untersuchung oder Prüfung muss wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung erforderlich sein, um die Eignung des Beschäftigten für die vorgesehene Tätigkeit festzustellen. Der Beschäftigte muss in den Eignungstest und in die Weitergabe der Ergebnisse des Tests an den Arbeitgeber einwilligen.

Die Restriktionen bei den grundsätzlich zulässigen Eignungstests sind zu weitgehend. Dies gilt insbesondere für die Erforderlichkeit der Untersuchung/Prüfung in Bezug auf die Art der auszuübenden Tätigkeit oder die Bedingungen ihrer Ausübung, aber auch für die notwendige Einwilligung. Die Teilnahme an Auswahl-/Testverfahren ist prinzipiell freiwillig. Eine explizite Einwilligung zu fordern, ist praxisfern.

Welches Ergebnis der Arbeitgeber erfahren darf, ist nicht hinreichend geklärt: Inhaltliche Untersuchungsergebnisse dürfen dem Arbeitgeber nicht zur Kenntnis gegeben werden, wenn die Tests durch Personen, die einer Schweigepflicht unterliegen, durchgeführt werden. Dann darf dem Arbeitgeber nur das „Ob“ zur Kenntnis gegeben werden. Dies ist praxisfern. So werden die meisten Assessment-Center unter der Beteiligung von Psychologen durchgeführt. Es wäre unpraktikabel, wenn der Arbeitgeber nur über das „Ob“ einer Eignung informiert wird. Nach der vorgeschlagenen Regelung wäre sogar eine Rangliste unter mehreren geeigneten Bewerbern unzulässig.

6. § 32b – Datenverarbeitung und -nutzung vor Begründung eines Beschäftigungsverhältnisses

Regelungsgehalt: Die weitere Nutzung von Bewerberdaten wird von der Erforderlichkeit für die Feststellung der Eignung des Beschäftigten für die vorgesehene Tätigkeit abhängig gemacht. Unverlangt eingesandte Daten dürfen nur soweit genutzt werden, wie dies für die vorgesehene Tätigkeit erforderlich ist. Beschäftigtendaten müssen entsprechend § 35 Absatz 2 Satz 2 gelöscht werden.

Auch hier ist die Voraussetzung der Erforderlichkeit wiederum zu eng, um bei der Entscheidung über die Nutzung von Daten eine rechtssichere Grundlage zu liefern. Das zeigt sich insbesondere dann, wenn der Arbeitgeber bei unverlangt durch den Bewerber überlassenen Daten zwischen erforderlichen und nicht erforderlichen Daten selektieren muss. So müsste der Arbeitgeber sich zum Beispiel fragen, ob er Bewerbungsunterlagen, in denen ein unter AGG-Aspekten kritisches und vom Arbeitgeber nicht verlangtes Bewerberfoto enthalten ist, weiter komplett einscannen kann oder hier – kaum praktikabel – eine Selektion in „erforderliche“ und „nicht erforderliche“ Daten vornehmen muss. Darüber hinaus muss berücksichtigt werden, dass der Bewerber mit der Zusendung seiner Daten diese freiwillig dem Arbeitgeber überlässt und sich hieraus für den Arbeitgeber zum Beispiel im Hinblick auf eine Angabe zur Schwerbehinderung gesetzliche Verpflichtungen ergeben.

Zur Vermeidung einer Überbürokratisierung des Bewerbungsverfahrens sollte daher auch hier der Begriff „erforderlich“ durch „dienlich“ ersetzt werden.

Zudem sollte die Formulierung „ohne dass der Arbeitgeber hierzu Veranlassung gegeben hat“ in „ohne dass der Arbeitgeber den Arbeitnehmer aufgefordert hat“ präzisiert werden. Andernfalls könnte man argumentieren, dass jede Überlassung von Informationen durch den Bewerber im Rahmen einer ausgeschriebenen Stelle letztlich durch den Arbeitgeber veranlasst ist.

Im Hinblick auf die Löschungsvorgaben sollte klargestellt werden, dass eine Speicherung nach § 35 Abs. 2 BDSG so lange zulässig ist, bis der Arbeitgeber mit Sicherheit davon ausgehen kann, dass keine Ansprüche zum Beispiel nach dem AGG gegen ihn geltend gemacht werden oder nach Ablauf der Probezeit feststeht, dass er auf keine anderweitigen Bewerber zurückgreifen muss. Im Hinblick auf die Einwilligung des Bewerbers in die weitere Speicherung sollte zudem sichergestellt bleiben, dass auch eine konkludente Einwilligung in die Aufbewahrung von Bewerberdaten möglich ist.

7. § 32c – Datenerhebung im Beschäftigungsverhältnis

Regelungsgehalt: § 32c regelt die Datenerhebung im Beschäftigungsverhältnis. Die Datenerhebung ist zulässig, wenn dies zu dessen Durchführung, Beendigung und Abwicklung erforderlich ist. Dazu gibt § 32c Regelbeispiele, in denen Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses erhoben werden dürfen. Hinsichtlich der Zulässigkeit von gesundheitlichen Untersuchungen und Eignungstests wird auf § 32a Absatz 1 und 2 verwiesen.

Gemäß § 32c Absatz 1 Satz 3 gilt § 32 Absatz 6 entsprechend. Damit wäre eine Erhebung allgemein zugänglicher Daten und von Daten aus sozialen Netzwerken im laufenden Beschäftigungsverhältnis eingeschränkt bzw. unzulässig. Dies widerspricht arbeitsrechtlichen Grundsätzen. Dem Arbeitnehmer obliegen Loyalitäts- und Rücksichtspflichten. Würde ein Arbeitnehmer zum Beispiel ehrverletzende Äußerungen über den Arbeitgeber in soziale Netzwerke einstellen, wäre die arbeitsrechtliche Sanktionierung de facto ausgeschlossen, da eine entsprechende Datenerhebung unzulässig wäre. Dies darf nicht sein. Der Arbeitgeber muss ein solches Verhalten sanktionieren können und zwar auch dann, wenn er zufällig hierauf stößt.

Klargestellt werden muss auch, dass die Erhebung, Nutzung und Verarbeitung von Gesundheitsdaten außerhalb von Gesundheitsuntersuchungen nach § 32c und d

zulässig ist. Dies gilt sowohl für Informationen zu Fehlzeiten als auch für eventuell bekannte Diagnosen, die für den Arbeitgeber für die Frage der Zulässigkeit einer personenbedingten Kündigung oder für andere Einsatzmöglichkeiten von erheblicher Bedeutung sein können. Zudem müssen die für die Praxis besonders wichtigen datenschutzrechtlichen Fragen bei der Durchführung des gesetzlich zwingenden Gesundheitsmanagements geklärt werden. Hier ist vor dem Hintergrund dieser Regelung sowie von § 32d Absatz 5 für die Betriebe nicht klar, welche Daten bei der Durchführung eines betrieblichen Eingliederungsmanagements erhoben und genutzt werden dürfen.

§ 32c Absatz 2 kann gestrichen werden, da die Veränderung der Tätigkeit unter die Durchführung des Beschäftigungsverhältnisses in Absatz 1 fällt. Die Regelung ist daher überflüssig.

Die in § 32c Absatz 3 vorgesehene Regelung, wonach ärztliche Untersuchungen gem. § 32a Absatz 1 und Eignungstests gem. § 32a Absatz 2 ohne konkreten Anlass unzulässig sein sollen, hat erhebliche Auswirkungen. In bestimmten Industriezweigen mit besonderem Gefahrenpotential, wie der chemischen Industrie, muss die Gewähr geboten werden, dass die erforderlichen Sicherheitsstandards eingehalten werden. Dies kann auch die Durchführung routinemäßiger Alkohol- und Drogenkontrollen erforderlich machen. Absatz 3 sollte deshalb ergänzt werden durch die Formulierung: „oder dies zur Arbeitssicherheit oder aus Gründen des Gesundheitsschutzes erforderlich ist“.

8. § 32d Datenverarbeitung und -nutzung im Beschäftigungsverhältnis

a) Absatz 3

Regelungsgehalt: Die Regelung sieht u. a. vor, dass zur Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen durch Beschäftigte im Beschäftigungsverhältnis ein automatisierter Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form durchgeführt werden kann.

Unternehmen sind kontinuierlich gestiegenen aktien- und gesellschaftsrechtlichen sowie aufsichtsbehördlichen Anforderungen in Bezug auf Organisations- und Sorgfaltspflichten ausgesetzt. Automatisierte Abgleiche von Beschäftigtendaten sind für die Erfüllung dieser Verpflichtungen wesentlich. Sie müssen sowohl präventiv als auch repressiv erfolgen können. Der Wortlaut des Gesetzentwurfs sowie die Gesetzesbegründung sprechen dafür, dass kein konkretisierter Verdacht vorliegen muss, bevor ein Abgleich durchgeführt werden kann. Um hier endgültige Klarheit zu schaffen, sollte der in vorherigen Referentenentwürfen genutzte Begriff „verhindern“ in Bezug auf Straftaten und Pflichtverletzungen wieder aufgenommen werden.

Darüber hinaus ist die Beschränkung der Überprüfungsmöglichkeiten insbesondere auf schwerwiegende Pflichtverletzungen zu eng. Der Arbeitgeber muss vielmehr in der Lage sein, Pflichtverletzungen, Ordnungswidrigkeiten oder Straftaten aufzudecken und zu verhindern, ohne zuvor zu einer rechtsunsicheren Prüfung gezwungen zu werden, ob der Sachverhalt tatsächlich eine „schwerwiegende Pflichtverletzung“ darstellt oder nicht.

Die Regelung, dass die Beschäftigten über Inhalt, Umfang und Zweck des automatisierten Abgleichs zu unterrichten sind, sollte klargestellt werden. Allenfalls kann gewollt sein, dass Personen, deren Daten personalisiert wurden, im Sinne des Transparenzgebots unterrichtet werden. Daher muss die Unterrichtungspflicht auf diesen Personenkreis beschränkt werden.

b) Absatz 5

Regelungsgehalt: Weiterhin wird geregelt, dass die automatisierte Zusammenführung einzelner Lebens- und Personaldaten kein Gesamtbild der wesentlichen geis-

tigen und charakterlichen Eigenschaften oder des Gesundheitszustandes des Beschäftigten ergeben darf.

Dieser Absatz sollte entfallen. Es ist völlig unklar, wann ein „Gesamtbild“ in diesem Sinne vorliegt. Zielt diese Regelung auf ein die gesamte Person im beruflichen wie persönlichen Umfeld umfassendes Bild oder genügt der Bezug zu bestimmten Lebensbereichen? Eine Eingrenzung auf den beruflichen Kontext könnte in der Konsequenz dazu führen, dass Arbeitnehmer nicht mehr von Unterstützungsleistungen des Arbeitgebers profitieren könnten. Dies gilt zum Beispiel im Hinblick auf Führungskräftepools. Gerade für Führungskräfte spielen neben den fachlichen auch die charakterlichen Eigenschaften eine wesentliche Rolle. Es ist deshalb für ein Unternehmen unvermeidbar, sich auch von den charakterlichen Eigenschaften eines Arbeitnehmers zu überzeugen, bevor diese Person in den Führungskräftepool aufgenommen wird. Würde sich hierdurch bereits ein Gesamtbild der wesentlichen geistigen und charakterlichen Eigenschaften ergeben, müssten entscheidende Kriterien bei der Auswahl von Führungskräften in Zukunft unberücksichtigt bleiben.

Unklarheit besteht auch in Bezug auf das „Gesamtbild des Gesundheitszustandes des Beschäftigten“. So muss es im Interesse beider Arbeitsvertragsparteien auch in Zukunft möglich sein, Fehlzeiten- und Krankengespräche zu führen. Das wird insbesondere im Hinblick auf das sog. betriebliche Eingliederungsmanagement deutlich. Um nach einer Erkrankung dem Arbeitnehmer eine sinnvolle und vernünftige Wiedereingliederung in den Betrieb zu ermöglichen, ist der Arbeitgeber darauf angewiesen, Informationen zum Gesundheitszustand des Betroffenen zu erhalten. Je weitergehender der Gesundheitszustand bekannt ist, desto besser kann der Arbeitnehmer bei der Rückkehr in den Betrieb unterstützt werden. Sollten in Zukunft aus datenschutzrechtlichen Gründen nur noch Teilbereiche des Gesundheitszustandes offengelegt werden dürfen, würde das betriebliche Eingliederungsmanagement sinnentleert.

9. § 32e – Datenerhebung zur Aufdeckung und Verhinderung von Straftaten und schwerwiegenden Pflichtverletzungen

Regelungsgehalt: Die Regelung sieht enge Voraussetzungen für die Erhebung von Arbeitnehmerdaten ohne Kenntnis des Arbeitnehmers vor. So soll dies u. a. nur möglich sein, wenn den Verdacht begründende Tatsachen auf eine Straftat bzw. schwerwiegende Pflichtverletzung vorliegen, die den Arbeitgeber zu einer Kündigung aus wichtigem Grund berechtigen würden. Zudem darf die Erhebung zur Verhinderung von Straftaten bzw. schwerwiegenden Pflichtverletzungen nur unter bestimmten Voraussetzungen erfolgen. Die Erforschung des Sachverhalts auf andere Weise müsste erschwert oder weniger erfolgversprechend sein. Die Datenerhebung wird sowohl zeitlich als auch im Hinblick auf die eingesetzten Mittel erheblich eingeschränkt. Der Kernbereich privater Lebensführung darf nicht angetastet werden.

Arbeitnehmerdatenschutz muss die Bekämpfung von Korruption und Kriminalität unterstützen. Die scharfen Voraussetzungen des § 32e sind vor dem Hintergrund der Haftungsrisiken der Unternehmensleitung im Hinblick auf die Einhaltung von Complianceregelungen bedenklich.

Der Anwendungsbereich des § 87 Abs. 1 Nr. 6 bei einer Datennutzung nach § 32e muss klargestellt werden. Es kann den Betriebsrat in eine kritische Lage bringen, wenn er vorab von bestimmten – heimlich vorzunehmenden – Datenerhebungen informiert ist. Soweit Maßnahmen nach § 32e als kollektive Maßnahmen mitbestimmungspflichtig sein sollten, sollte das Mitbestimmungsrecht für die konkrete Kontrolle/Ermittlung in eine nachträgliche Informationspflicht umgewandelt werden.

a) Absatz 2

Die Einschränkung in § 32e Absatz 2, dass eine Datenerhebung nur zulässig ist, wenn die Straftat bzw. Pflichtverletzung so schwerwiegend ist, dass sie den Arbeit-

geber zu einer Kündigung aus wichtigem Grund berechtigen würde, ist zu eng. Wann eine Kündigung aus wichtigem Grund heute – insbesondere nach der sogenannten Emmely-Entscheidung – noch möglich ist, lässt sich von niemandem sicher vorhersagen. Man kann dem Arbeitgeber schwerlich eine Verhältnismäßigkeitsprüfung auferlegen, die er nicht rechtssicher durchführen kann.

Darüber hinaus muss der Arbeitgeber berechtigt sein, Straftaten oder schwerwiegende Pflichtverletzungen von Anfang an zu unterbinden. Dies muss auch dann gelten, wenn er zufällig auf sie stößt. Sollte er erst einmal abwarten müssen, bis ein Verdacht durch Tatsachen begründet wird, würde dies dem Präventionsgedanken nicht gerecht.

Ist beispielsweise ein Mitarbeiter aus der Versicherungsbranche berechtigt, Ersatzleistungen bis zu einem bestimmten Betrag anzuweisen, so muss eine Überprüfung möglich sein, ob ein höherer Schadenbetrag zeitnah in mehrere Teilbeträge aufgeteilt wird, die auf demselben Konto gutgeschrieben werden. Nur so können rechtzeitig Hinweise auf einen Missbrauch der Befugnisse entdeckt werden. Gleiches gilt im Hinblick auf eine Überprüfung, ob Schadenzahlungen ständig knapp unter der Grenze der Regulierungsbefugnis liegen. Auch hier muss die Möglichkeit bestehen, Hinweise auf ein mögliches kollusives Zusammenwirken zwischen einem Mitarbeiter und einem Dritten aufdecken zu können. Derartige präventiv angelegte Prüfroutinen zur Verhinderung von Straftaten müssen auch im Rahmen von § 32e BDSG-E zulässig sein.

Es muss zudem ausreichend sein, dass ein Verdacht gegen eine konkrete Beschäftigtengruppe besteht, wie dies auch aus der Gesetzesbegründung hervorgeht. Dies sollte im Gesetzestext klargestellt werden.

Präventive Datenerhebung erhöht das Risiko entdeckt zu werden und reduziert damit die Wahrscheinlichkeit, dass kriminelle Handlungen begangen werden. Die Möglichkeiten, präventiv Daten zu erheben, sind im Gesetzentwurf jedoch zu eng gefasst. Eine Verknüpfung zwischen einer ursprünglichen Straftat bzw. schwerwiegenden Pflichtverletzung und im Zusammenhang damit stehenden weiteren Straftaten bzw. schwerwiegenden Pflichtverletzungen, um präventiv vorgehen zu können, wird den Erfordernissen der Praxis nicht gerecht. So muss z.B. eine Umfrage bei Lieferanten zur Abwicklung von Ausschreibungen bzw. zur Gewährung von Geschenken und Belohnungen weiterhin möglich sein.

b) Absatz 3

Wann die Erforschung des Sachverhalts auf andere Weise erschwert oder weniger erfolgversprechend wäre, ist völlig unklar und stellt die Arbeitgeber vor erhebliche Rechtsunsicherheiten. Diese der StPO entnommene Formulierung mag für staatliche Stellen angemessen sein. Ansonsten muss die Datenerhebung aber zulässig sein, wenn sie geeignet ist.

c) Absatz 4

Der Erhebungszeitraum sowie die für die Datenerhebung eingesetzten Mittel werden erheblich eingeschränkt. Auch hierdurch ergibt sich Rechtsunsicherheit. So stellt sich die Frage, was eine „planmäßig angelegte Beobachtung“ in diesem Sinne ist und unter welchen Voraussetzungen von getrennten Beobachtungen gesprochen werden kann.

Der Beobachtungszeitraum von 24 Stunden ohne Unterbrechung oder an mehr als vier Tagen ist zu kurz. Soll zum Beispiel durch einen Detektiv geklärt werden, welche Person von einem Telefon in einem ansonsten ungenutzten Gebäudeteil des Betriebs unerlaubter Weise Telefonate führt, kann hierfür eine Beobachtung erforderlich sein, die über den genannten Zeitraum hinausgeht.

d) Absatz 5

Entgegen dem Wortlaut des § 32e Absatz 5 soll nach der Gesetzesbegründung eine Pflicht zur schriftlichen Dokumentation bestehen. Eine schriftliche Dokumentation wäre jedoch unnötig bürokratisch. Es ist ausreichend, wenn der Arbeitgeber eine elektronische Dokumentation im Sinne von § 126b BGB vornimmt.

Die ebenfalls in Absatz 5 vorgesehene Unterrichtungspflicht kann in der Praxis zu Problemen führen, wenn zum Beispiel der Nachweis einer Pflichtverletzung (die aber tatsächlich begangen wurde) nicht erbracht werden kann. Es besteht die Gefahr, dass der Betroffene sogar zusätzlich motiviert wird, wenn zwar z. B. eine Straftat vorliegt, diese jedoch durch die Datenerhebung nicht nachgewiesen werden konnte.

Die Durchführung einer Vorabkontrolle vor Beginn der Datenerhebung steht der Notwendigkeit entgegen, kurzfristige Erhebungen durchzuführen und schafft hierdurch die Gefahr, dass der Zweck der Untersuchung nicht erreicht werden kann.

e) Absatz 7

Die Regelung zu Daten, die den Kernbereich privater Lebensgestaltung betreffen, wird in der Praxis zu Rechtsunsicherheit führen. Das gilt umso mehr, als auch in der Gesetzesbegründung offen gelassen wird, was unter dem Kernbereich privater Lebensgestaltung verstanden wird. So stellt sich z. B. die Frage, inwieweit ein Arbeitgeber bei einem Verdacht auf Vortäuschung einer Arbeitsunfähigkeit Nachforschungen anstellen kann, ohne hierdurch in den Kernbereich privater Lebensgestaltung einzugreifen. Um solche Rechtsunsicherheiten auszuräumen, sollte der Ausdruck entsprechend § 32f Absatz 2 Satz 2 des Gesetzentwurfs konkretisiert werden.

10. § 32f – Beobachtung nicht öffentlicher Betriebsstätten mit optisch-elektronischen Einrichtungen

Regelungsgehalt: § 32f regelt, dass eine offene Videoüberwachung in öffentlich nicht zugänglichen Betriebsstätten aus bestimmten Gründen zulässig ist. Schutzwürdige Interessen der Betroffenen am Ausschluss der Datenerhebung dürfen nicht überwiegen. Die in den Referentenentwürfen noch geregelte Möglichkeit der gezielten Videoüberwachung ist nun nicht mehr vorgesehen.

Es ist nicht nachvollziehbar, warum die nach der bisherigen Rechtslage als ultima ratio zulässige Videoüberwachung nun nicht mehr möglich sein soll. Der Gesetzentwurf bleibt hiermit weit hinter dem zurück, was sowohl vom Bundesarbeitsgericht als auch den Landesbeauftragten für den Datenschutz unter bestimmten Voraussetzungen als zulässig angesehen wird.

Das ist für die Praxis nicht hinnehmbar. So belaufen sich zum Beispiel im deutschen Einzelhandel die jährlichen Inventurverluste auf etwa 4 Milliarden Euro. Nach vorsichtigen Schätzungen ist davon auszugehen, dass gut ein Viertel hiervon, also etwa eine Milliarde Euro, auf Diebstähle durch eigene Mitarbeiter oder Lieferanten zurückzuführen ist. Vor diesem Hintergrund ist eine hohe Aufklärungsquote wesentlich. Die gezielte Videoüberwachung trägt erheblich dazu bei, die Aufklärung solcher Fälle voranzutreiben. Als konkretes Bespiel mag der Fall dienen, in dem aus einem Lager größere Mengen an Tabakwaren gestohlen worden waren. Nachdem weder der Einsatz von Detektiven während der Ladenöffnungszeiten noch sonstige Maßnahmen Aufklärung brachten, musste der Tabak außerhalb der Ladenöffnungszeiten entwendet worden sein. Nachdem der Einsatz eines Detektivs zu dieser Zeit zu auffällig gewesen wäre, wurde eine gezielte Videoüberwachung durchgeführt und eine Reinigungskraft als Täter überführt. Eine solche Überwachung würde bei der im Gesetzentwurf vorgesehenen Regelung entfallen, die Aufklärung wäre nicht mehr möglich.

Hinzu kommt, dass die gezielte Videoüberwachung bislang stets mit dem Einverständnis der Betriebsräte und der betrieblichen Datenschutzbeauftragten erfolgte. Vor diesem Hintergrund sollte die gezielte Videoüberwachung sowohl bei öffentlich zugänglichen als auch bei nicht öffentlich zugänglichen Betriebsstätten möglich sein.

Kritik ist auch an der jetzt vorgesehenen Ausgestaltung der offenen Videoüberwachung in § 32f zu üben.

So ist zwar die Regelung von konkreten Fällen, in denen generell die offene Videoüberwachung zulässig ist, sinnvoll. Diese Liste sollte jedoch Regelbeispiele enthalten und gleichzeitig noch ergänzt werden um den allgemeinen Punkt „Aufklärung von Straftaten".

Problematisch ist zudem der Verweis auf § 6b Abs. 3 BDSG. Danach dürfen die durch die Videoüberwachung gewonnen Daten nur für einen anderen Zweck verarbeitet werden, wenn dies zur Verfolgung von Straftaten erforderlich ist. Dies ist für das Arbeitsverhältnis nicht ausreichend. Die so gewonnenen Daten sollten auch dann für den Arbeitgeber verwertbar sein, wenn es sich um eine schwerwiegende Vertragsverletzung des Arbeitnehmers handelt. Bei der offenen Überwachung einer Maschine kann beispielsweise eine solche schwerwiegende Vertragsverletzung bemerkt werden. Wegen § 6b Abs. 3 BDSG kann der Arbeitgeber diese Zufallsfunde nicht als Beweismittel für die begangene arbeitsvertragliche Pflichtverletzung im Kündigungsschutzprozess verwerten. Dies ist mit dem Arbeitsverhältnis als Dauerschuldverhältnis nicht vereinbar, da das Arbeitsverhältnis ein Vertrauensverhältnis voraussetzt. Es ist deshalb klarzustellen, dass auch eine Verwertungsmöglichkeit für Zufallsfunde besteht, wenn eine schwerwiegende Vertragspflichtverletzung vorliegt.

Darüber hinaus muss weiterhin sichergestellt werden, dass bei Proben und Aufführungen von Theatern und Orchestern eine Übertragung des Geschehens auf der Bühne z.B. in die Räumlichkeiten des Leitungspersonals und die Aufenthaltsräume der Mitwirkenden möglich ist. Das ist notwendig, um die Leitung über den künstlerischen Proben- und Aufführungsverlauf zu informieren, bzw. die Mitwirkenden über den Stand der Probe/Aufführung, damit sie wissen, wann sie sich wieder zur Bühne begeben müssen. Um diese gängige Praxis auch in Zukunft beibehalten zu können, sollten Aufführungs- und Proberäume von Gebäuden, die der Durchführung öffentlicher Veranstaltungen dienen, von der Regelung des § 32f ausgenommen werden.

11. § 32g - Ortungssysteme

Regelungsgehalt: Ortungssysteme zur Bestimmung eines geographischen Standortes dürfen zur Sicherheit des Beschäftigten oder zur Koordinierung des Einsatzes des Beschäftigten eingesetzt werden. Sie dürfen unter bestimmten Voraussetzungen auch zum Schutz beweglicher Sachen eingesetzt werden.

Die Klarstellung der Zulässigkeit des Einsatzes von geographischen Ortungssystemen ist sinnvoll. Die in der Vorschrift vorgesehenen Einschränkungen sind allerdings zu restriktiv.

Die dort vorgesehene Verhältnismäßigkeitsprüfung ist zu eng, da verlangt wird, dass keine Anhaltspunkte bestehen dürfen, dass schutzwürdige Interessen des Beschäftigten am Ausschluss der Datenerhebung überwiegen. Der Einsatz von Ortungssystemen ist beispielsweise in Logistikunternehmen ein kaum mehr verzichtbares Werkzeug zum wirtschaftlichen Flotteneinsatz. Allein das Bestehen von Anhaltspunkten, dass schutzwürdige Interessen des Arbeitnehmers überwiegen, kann deshalb nicht ausreichend sein, um den Einsatz zu untersagen.

Die Beschränkung der Überwachungszeit auf die Arbeitszeit des Beschäftigten ist abzulehnen. Gerade bei Tätigkeiten, die außerhalb des Betriebs z.B. auf Baustellen ausgeführt werden, besteht oftmals auch außerhalb der regulären Arbeitszeit die

Gefahr, dass Dienstfahrzeuge durch Arbeitnehmer absprachewidrig für eigene Zwecke genutzt werden. Denkbar ist dies insbesondere in den Fällen, in denen dem Arbeitnehmer das Firmenfahrzeug zu dem Zweck überlassen wurde, Baustellen bzw. Kunden direkt von seiner Wohnung aus anzufahren. Hier muss es für den Arbeitgeber kontrollierbar sein, ob der Arbeitnehmer das Fahrzeug nach Feierabend oder vor Arbeitsbeginn nicht unrechtmäßig für private Zwecke einsetzt. Gleiches gilt z.B., wenn der Fahrer in der Fahrerkabine eines Nutzfahrzeugs übernachtet. Der Arbeitgeber könnte nach dem Gesetzestext nicht die Einhaltung der Ruhezeiten überwachen und das Fahrzeug durch das Ortungssystem sichern.

Unklar ist, für welche Zwecke Beschäftigtendaten, die beim Einsatz von Ortungssystemen erhoben werden, genutzt und verarbeitet werden dürfen. Wir gehen davon aus, dass die Koordinierung des Einsatzes von Beschäftigten auch die Kontrolle des Einsatzes erfasst. Dies sollte klargestellt werden. Ansonsten könnte aus der Beschränkung des § 32g Abs. 1 S. 4 geschlossen werden, dass die Nutzung der Daten zur Kontrolle der Vertragserfüllung unzulässig ist. Dies wäre wenig überzeugend. Ortungssysteme müssen auch zur Kontrolle der Vertragserfüllung durch den Arbeitnehmer (z.B. Außendienstmitarbeiter) zulässig sein – zumindest in den Fällen, in denen Ortungssysteme die einzige Kontrollmöglichkeit darstellen und dies ausdrücklich klargestellt wird.

Zudem entsteht durch Absatz 1 weitere Rechtsunsicherheit, da in Satz 4 im Hinblick auf die erlaubte Verarbeitung und Nutzung nur auf Absatz 1 Satz 1, nicht aber auf Absatz 2 verwiesen wird. Ortungssysteme dürfen nach Abs. 2 auch zum Schutz beweglicher Sachen eingesetzt werden, d.h. dass auch insofern die Verarbeitung und Nutzung von Daten zulässig sein müsste. Deshalb muss dies als zulässiger Zweck in Abs. 1 Satz 4 aufgenommen werden.

Unklar ist das Verhältnis zu § 32e. Durch die Pflicht zur Kenntlichmachung von Ortungssystemen gem. § 32g Absatz 1 S. 3 könnte eine Nutzung nach § 32e zur Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen ausgeschlossen sein. Dies wäre nicht akzeptabel. Es ist anerkannt, dass die Ortung weniger eingriffsintensiv ist als andere Grundrechtseingriffe, wie beispielsweise das heimliche Abhören eines Telefonates. Es ist deshalb durchaus berechtigt, die Ortung im Bereich der Arbeitnehmerüberwachung für die Aufklärung von Straftaten und schwerwiegenden Pflichtverletzungen zu verwenden. Im Hinblick auf § 32g Absatz 1 S. 3 ist deshalb klarzustellen, dass § 32e nicht eingeschränkt wird.

Nach Absatz 2 darf der Arbeitgeber Ortungssysteme auch zum Schutz beweglicher Sachen einsetzen, die vom Beschäftigten genutzt werden oder sich in seiner Obhut befinden. Die Ortung darf jedoch nicht erfolgen während der erlaubten Nutzung und der erlaubten Inobhutnahme der Sache. Dies ist mit dem Eigentumsrecht nicht vereinbar und bedarf daher einer Regelung dahingehend, dass es dem Arbeitgeber erlaubt sein muss, ein Ortungssystem einzusetzen, wenn der begründete Verdacht besteht, dass der Arbeitnehmer Eigentum des Arbeitgebers vertragswidrig oder gar zu Straftaten missbraucht.

Weiterhin scheint die geforderte unverzügliche Löschung nach Absatz 3 als zu eng, da die Ortungsdaten ggf. auch für Dokumentationen und Rechtsstreitigkeiten relevant sein können.

12. § 32h – Biometrische Verfahren

Regelungsgehalt: Biometrische Daten dürfen grundsätzlich nur zu Autorisierungs- und Authentifikationszwecken genutzt werden.

Es muss klargestellt werden, dass bei einer Nutzung der biometrischen Daten zu Autorisierungs- oder Authentifikationszwecken bei Zugangsberechtigungssystemen die üblicherweise mit Zugangserfassungssystemen verbundenen Daten erhoben und im Rahmen des § 32d genutzt werden können. So werden Zugangskontrollsys-

teme zu Räumen oder Daten und Diensten auch häufig als Zeiterfassung genutzt. Es muss sichergestellt sein, dass die so erhobenen Zeiterfassungsdaten nicht unter § 32h fallen, sondern entsprechend § 32d genutzt und verarbeitet werden können.

Auch hier muss der Begriff der „Erforderlichkeit“ überdacht werden. So könnte dieser Begriff hier dazu führen, dass eine biometrische Erhebung des Fingerabdrucks für das Einloggen auf einem Laptop nicht möglich ist, wenn gleichzeitig die Möglichkeit besteht, sich über ein Passwort einzuloggen. Das wäre vor dem Hintergrund des häufigen Missbrauchs von Passwörtern sehr bedenklich.

13. § 32i – Nutzung von Telekommunikationsdiensten

Die BDA begrüßt, dass der Gesetzgeber die Nutzung der betrieblichen Telekommunikationsdienste im Arbeitsverhältnis regelt. Derzeit sind bei Nutzung der betrieblichen Telekommunikationsdienste durch die Arbeitnehmer noch viele Fragen nicht abschließend geklärt, so dass eine gesetzliche Regelung, die in der Praxis zu mehr Rechtssicherheit führt, ein Gewinn für die Unternehmen wäre.

Die vorgeschlagene Regelung orientiert sich am Telekommunikationsrecht. Problematisch ist grundsätzlich, dass der Arbeitgeber bei zugelassener Privatnutzung nach wie vor als Diensteanbieter im Sinne des Telekommunikationsrechts angesehen werden kann, da dies im Gesetzestext nicht ausdrücklich ausgeschlossen ist. Hier muss die Chance genutzt werden, sich vom Telekommunikationsrecht – das auch in Terminologie und Systematik nicht auf die Rechtsbeziehung von Arbeitgeber und Arbeitnehmer passt – zu lösen und eine vollständig eigenständige Regelung zu finden.

So wurde bei der Vorratsdatenspeicherung, wie sie in den §§ 113 a TKG geregelt ist, in der Literatur die Frage erörtert, ob auch der Arbeitgeber zur Vorratsdatenspeicherung verpflichtet ist. Dies macht deutlich, dass die Anwendung der Telekommunikationsvorschriften auf das Verhältnis Arbeitgeber – Arbeitnehmer zu Rechtsunsicherheit führt. Auch fehlt es an einer überzeugenden Begründung, warum die Telekommunikationsvorschriften auf den Arbeitgeber Anwendung finden sollen. In der Gesetzesbegründung zum Telekommunikationsgesetz wurde klargestellt, dass beispielsweise Hotels, die eine entsprechende Nebenstellenanlage vorhalten, Diensteanbieter sind (BT-Drs. 13/3609). Dies ist nachvollziehbar, da diese ihren Gästen die Möglichkeit einräumen wollen, das Telefon oder den Zugang zum Internet ohne weitere Einschränkungen zu nutzen. Auch wenn der Arbeitgeber die private Nutzung zulässt, ist die Situation nicht mit dem des Hoteliers, der eine Nebenstellenanlage für seine Gäste vorhält, zu vergleichen.

Zu der Regelung im Einzelnen:

a) Absätze 1 und 3 - ausschließlich dienstliche Nutzung von Telekommunikationsdiensten

Regelungsgehalt: Ist die private Nutzung untersagt, so kann der Arbeitgeber die Verkehrsdaten erheben, verarbeiten und nutzen, wenn dies zur Gewährleistung des ordnungsgemäßen Betriebs des Telekommunikationsdienstes, zu Abrechnungszwecken oder zu stichproben- oder anlassbezogenen Leistungs- oder Verhaltenskontrollen erforderlich ist.

Auf die Inhaltsdaten von E-Mails kann der Arbeitgeber nur zugreifen, wenn dies zur Gewährleistung des ordnungsgemäßen Betriebes des Telekommunikationsdienstes oder zu einer stichprobenartigen oder anlassbezogenen Leistungs- und Verhaltenskontrolle erforderlich ist.

Dies ist zu eng. Für den Zugriff auf dienstliche E-Mails kann es keine Beschränkung geben. Dienstliche E-Mails sind Teil der Arbeitsleistung, als solche auch ggf. nach § 257 HGB zu archivieren. Rein dienstliche E-Mail-Korrespondenz ist auch immer

Korrespondenz des Arbeitgebers. Eine Einschränkung ist deshalb nicht akzeptabel und auch nicht wegen des Fernmeldegeheimnisses geboten. Ist die private Nutzung ausgeschlossen, so ist der Arbeitgeber kein Diensteanbieter i.S.d. Telekommunikationsrechts.

Ebenso ist im Hinblick auf die Erhebung von Verkehrsdaten eine nur auf bestimmte Fallgruppen beschränkte Gestattung nicht akzeptabel. Gerade im Bereich der rein dienstlichen Nutzung muss es dem Arbeitgeber unter anderem möglich sein, Leistungs- und Verhaltenskontrollen durchzuführen; dies schon im Hinblick auch auf die Einhaltung der rein dienstlichen Nutzung. Die anfallenden Daten sind hier alleine Teil der Arbeitsleistung.

Verkehrsdaten müssen auch erhoben werden können, um die wirtschaftliche Nutzung der telefonischen Kommunikationsmittel im Betrieb zu gewährleisten. Unternehmen müssen beispielsweise in der Lage sein, anhand der Verkehrsdaten die telefonische Auslastung von Arbeitnehmern ermitteln zu können, um die Abteilungen entsprechend zu besetzen und ein Kostencontrolling durchzuführen. Auch ist die dauerhafte Erhebung und Auswertung von Verkehrsdaten unverzichtbar, um einer Vereinbarung über variable Vergütung auf Basis von Erreichbarkeitsquoten oder der Anzahl der entgegengenommenen Anrufe durch Ermittlung des Anteils nachkommen zu können. Der Gesetzestext ist auch hier zu eng und muss entsprechend angepasst werden: Hier ist ergänzend klarzustellen, dass die bei der Nutzung von Telekommunikationsdiensten anfallende personenbezogene Daten vom Arbeitgeber erhoben, verarbeitet und genutzt werden dürfen, soweit dies zur Durchführung des ordnungsgemäßen Dienst- und Geschäftsbetriebs und für die Umsetzung von Vergütungsmodellen erforderlich ist

b) Absatz 2 - dienstliche Nutzung von Telefondiensten

Regelungsgehalt: Die Nutzung von Inhaltsdaten ist bei einer rein dienstlichen Nutzung nur zulässig, wenn dies zur Wahrung der berechtigten Interessen des Arbeitgebers erforderlich ist und beide Gesprächspartner im konkreten Einzelfall vorher informiert wurden und eingewilligt haben.

Die Regelung ist im Grundsatz gelungen und entspricht überwiegend der geltenden Rechtslage. Problematisch ist allerdings, dass – entgegen der Rechtsprechung – keinerlei Ausnahmen zulässig sind. Aus den Entscheidungen des BAG und des BVerfG lässt sich entnehmen, dass das heimliche Mithören von Telefonaten zwar grundsätzlich unzulässig ist. Das BAG erkennt jedoch im Grundsatz an, dass Rechtfertigungsgründe vorliegen könnten. In einer notstandsähnlichen Situation ist deshalb ein heimliches Mithören nach geltender Rechtslage zulässig (BAG, 29.06.2004 – 1 ABR 21/03). Bei Anwendung des § 32i nach dem Gesetzentwurf wäre dies nicht mehr zulässig. Entsprechend der geltenden Rechtsprechung muss in Ausnahmefällen auch ein heimliches Mithören von Telefonaten möglich sein.

Eine andere praktische Notwendigkeit ist eine Ausnahmeregelung für innerbetriebliche Notrufnummern, wie beispielsweise bei Werksfeuerwehren. In Notrufzentralen von Werksfeuerwehren werden alle eingehenden Notrufe aus Sicherheitsgründen aufgezeichnet ohne dass zuvor eine gesonderte Einwilligung eingeholt wird. Dies wäre für eine Notfallsituation völlig praxisfern und auch häufig kaum möglich. Insgesamt muss dies für alle sicherheitskritischen Leitstellen und Stellen zur Störungskoordination (z.B. Gasversorgung, Kraftwerke) gelten. Für diese Sonderfälle muss klargestellt werden, dass in diesen Fällen von den Voraussetzungen des § 32i Abs. 2 abgewichen werden kann.

c) Absatz 4 – erlaubte private Nutzung

Regelungsgehalt: Ist die private Nutzung von Telekommunikationsdiensten zugelassen, so kann der Arbeitgeber nach Abschluss der Telekommunikation sowohl die Verkehrsdaten als auch die Inhaltsdaten nur erheben, verarbeiten und nutzen,

wenn dies zur Gewährleistung des ordnungsgemäßen Dienst- und Geschäftsbetriebs unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat.

Diese so genannte Mischnutzung ist in der Praxis gängig. Sie ist wegen der zu engen Rechtsprechung z.B. bei Krankheitsfall, Ausscheiden des Mitarbeiters, Zugriffsrecht für andere Arbeitnehmer, aber auch bei der Kontrolle kaum zu handhaben. Vorangestellt werden muss, dass die Unternehmen ihren Mitarbeiter die private Nutzung – im sozialadäquaten Maß – durchaus einräumen wollen. Führt dies allerdings dazu, dass der Zugriff auf geschäftliche E-Mails wegen der verfehlten Anwendung der telekommunikationsrechtlichen Vorschriften gesperrt ist oder ansonsten bestehende Kontrollmöglichkeiten entfallen, muss der Arbeitgeber hier zum Schutz seiner berechtigten Interessen die private Nutzung untersagen. Eine Regelung der „Mischnutzung“ muss deshalb sicherstellen, dass der Zugriff auf geschäftliche Korrespondenz und die Kontrollmöglichkeiten nicht eingeschränkt wird. Zudem sollte klargestellt werden, dass der Arbeitgeber befugt ist, zu Abrechnungszwecken Daten zu erheben, zu nutzen und zu verarbeiten.

Darüber hinaus muss geklärt werden, ob und in welchem Ausmaß noch eine Missbrauchskontrolle bei übermäßiger privater Nutzung oder Versendung strafrechtlich relevanten Materials möglich ist. Dies ist vor dem Hintergrund, dass der Arbeitgeber bei erlaubter privater Nutzung als Diensteanbieter im Sinne des Telekommunikationsrechts angesehen werden muss, fraglich. Auch wenn man davon ausgeht, dass in den vorliegenden Fällen § 100 Abs. 3 TKG einschlägig ist, ist dies wenig überzeugend. Eine Missbrauchkontrolle nach § 100 Abs. 3 TKG muss der Bundesnetzagentur angezeigt werden. Dies ist völlig ungeeignet für die Situation im Arbeitsverhältnis, da es um Vertragsverletzungen in einem Vertrauensverhältnis geht. Zudem wäre dies in der Praxis insbesondere für kleinere und mittlere Unternehmen kaum handhabbar. Dies ist ein Bespiel dafür, dass die Diensteanbieterschaft des Arbeitgebers nicht praktikabel ist.

Nach § 32l ist eine Einwilligung nur noch in gesetzlich vorgesehenen Fällen möglich, wurde aber für die Mischnutzung nicht eingeräumt. Dies ist kontraproduktiv. Für den Fall der Mischnutzung muss eine Einwilligung des Arbeitnehmers in die Datenverarbeitung nach wie vor möglich sein. Die Einwilligung in die private Nutzung war bisher immer anerkannt, da keine Zwangssituation besteht, da der Arbeitnehmer auch auf die private Nutzung verzichten kann.

14. § 32j – Unterrichtungspflichten

Regelungsgehalt: Stellt ein Arbeitgeber Verletzungen der aufgeführten Regelungen fest, so muss er dies unverzüglich den Betroffenen mitteilen, bei schwerwiegenden Verstößen auch der Aufsichtsbehörde.

Die Vorschrift trifft eine schärfere Sonderregelung gegenüber dem im letzten Jahr eingefügten neuen § 42a BDSG und verweist zudem auf dessen Sätze 3 bis 4 und 6.

Die Verschärfung ist abzulehnen. Eine Unterrichtungspflicht sollte gegenüber dem Arbeitnehmer nur bestehen, wenn ihm Nachteile drohen. Da ein Verstoß gegen § 32j auch durch eine Ergänzung des § 43 als Ordnungswidrigkeit sanktioniert wird, kann in Fällen, in denen ein Verstoß gegen eine materielle Vorschrift vorliegt, die der Arbeitgeber nicht gemäß § 32j meldet, eine doppelte Sanktion greifen. Vor diesem Hintergrund und angesichts des § 42a, der diesen Bereich bereits regelt, sollte § 32j gestrichen werden.

15. § 32l – Einwilligung, Beschwerderecht, Unabdingbarkeit

a) Absatz 1

Regelungsgehalt: Nach § 32l Absatz 1 ist die Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten durch den Arbeitgeber auf Grund einer individuellen Einwil-

ligung des Arbeitnehmers abweichend von § 4 Absatz 1 BDSG nur zulässig, soweit dies in den Vorschriften des neuen Unterabschnitts ausdrücklich vorgesehen ist.

Die Einschränkung der Einwilligung ist nicht akzeptabel. Die Einwilligung ist wegen der Möglichkeit des Widerrufs bereits heute nicht die wichtigste Rechtsgrundlage für die im Beschäftigungsverhältnis erforderliche Datenverarbeitung. Sie ist aber unersetzlich für Datenverarbeitungen, die auf freiwilligen Leistungen im engen und weiteren Sinne des Arbeitgebers beruhen. Solche Leistungen für die Arbeitnehmer anzubieten, kann für Arbeitgeber gerade vor dem Hintergrund der demographischen Entwicklung zur Rekrutierung, Motivation und Bindung der Arbeitnehmer ein wesentlicher Aspekt sein. In einem Unternehmen beispielsweise, das vielfältige Möglichkeiten der Inanspruchnahme von Leistungen bietet (z.B. in Vereinen, Restaurantbetrieben, Sozialeinrichtungen wie Kindergärten, die jeweils eigene Rechtspersönlichkeiten darstellen können), kann es zudem im Interesse der jeweiligen Mitarbeiter liegen, durch Einwilligung die Verarbeitung und Nutzung ihrer personenbezogenen Daten freizugeben. Diese Interessen dürfen nicht unnötig beschränkt werden.

Darüber hinaus muss bedacht werden, dass bisher die Einwilligung des Arbeitnehmers die rechtssichere Möglichkeit war, mit Gesundheitsdaten im Rahmen des betrieblichen Eingliederungsmanagements nach § 84 Absatz 2 SGB IX umzugehen. Die Einwilligung des Arbeitnehmers muss auch in Zukunft möglich sein. Ein Wertungswiderspruch zwischen dem SGB IX und dem BDSG darf den Arbeitgeber nicht der Gefahr aussetzen, sich ordnungswidrig zu verhalten.

Die jetzt vorgesehene Regelung, dass die Einwilligungsmöglichkeit nur ausnahmsweise besteht, muss umgekehrt werden in ein Regel-Ausnahme-Verhältnis, nach dem die Einwilligung immer möglich ist, es sei denn, sie wird im Einzelfall ausdrücklich ausgeschlossen. Es muss zudem klargestellt werden, dass Einwilligungsmöglichkeiten aufgrund anderer Gesetze (z.B. zum betrieblichen Eingliederungsmanagement) bestehen bleiben.

In jedem Fall muss klargestellt werden, dass zumindest eine Betriebsvereinbarung die Einwilligung als Rechtsgrundlage festschreiben kann. Zumindest sollte zwischen „normalen“ Mitarbeitern und dem Management differenziert werden, wie dies auch im Arbeitsrecht geschieht und das Management, wie leitende Angestellte, vom Anwendungsbereich des § 4 Absatz 1 ausgenommen werden.

b) Absatz 4

Regelungsgehalt: Der Arbeitnehmer erhält ein Beschwerderecht bei der Aufsichtsbehörde.

Bereits heute kann der Betroffene sich jederzeit mit einer Eingabe an die Aufsichtsbehörde wenden. Deshalb ist die o.g. Regelung nicht erforderlich und sollte gestrichen werden.

c) Absatz 5

Regelungsgehalt: Die Möglichkeit zum Abschluss von Kollektivvereinbarungen wie u. a. Betriebs- und Dienstvereinbarungen wird durch § 32l Absatz 5 des Entwurfs faktisch ausgeschlossen, da von den Vorschriften zum Arbeitnehmerdatenschutz nicht zu Ungunsten der Arbeitnehmer abgewichen werden kann.

Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein können, auch wenn in einer solchen Betriebsvereinbarung teilweise von gesetzlichen Vorgaben abgewichen wird. Bislang wurden Betriebsvereinbarungen von Arbeitgebern und Arbeitnehmervertretern auch genutzt, um Rechtsunsicherheiten zu begegnen. Nachdem der Gesetzentwurf viele unbestimmte Rechtsbegriffe und andere Regelungen enthält, die zu Rechtsunsicherheit führen können, muss auch

weiterhin durch Betriebsvereinbarungen diese Unsicherheit unbeschränkt ausgeräumt werden können. Das gilt umso mehr, als auch der Begriff „zu Ungunsten“ ein unbestimmter Rechtsbegriff ist, der viele Fragen aufwirft. So müssten Arbeitgeber und Betriebsrat im konkreten Fall beurteilen, ob zum Beispiel eine zur gesetzlichen Regelung alternative Vorgabe eine Regelung zu Ungunsten des Arbeitnehmers ist. Das ist in der Praxis nicht zu leisten. Gleiches gilt für den Abschluss von Tarifverträgen. § 32l Abs. 5 sollte gestrichen werden.

16. Weiterer Klarstellungs- und Regelungsbedarf

a) Datenaustausch im Konzern

Der Gesetzentwurf sieht keine Regelung der Erleichterung des Datenverkehrs im Konzern vor.

Die nunmehr angestrebte bereichsspezifische Regelung zum Datenschutz bietet die Möglichkeit, eine auf Beschäftigtendaten beschränkte Regelung aufzunehmen. Diese sollte die Rechtsunsicherheit bei der Abgrenzung der Auftragsdatenverarbeitung von der Funktionsübertragung beseitigen und auch für Konzerne ohne Betriebsrat sowie für die leitenden Angestellten eine sinnvolle Möglichkeit schaffen, bei einer konzerninternen Bündelung von Aufgaben die Voraussetzung für eine Übermittlung zu schaffen. Dies muss auch für Konzernunternehmen mit Sitz der Konzernmutter im Ausland gelten. Bei der Überarbeitung der entsprechenden europarechtlichen Vorgaben sollte dieser Aspekt berücksichtigt werden.

Eine Regelung könnte wie folgt aussehen: Zumindest im Unterordnungskonzern muss eine Möglichkeit für die Weitergabe der Beschäftigtendaten der Tochter an die Mutter geschaffen werden. Dies entspricht der häufigen Praxiskonstellation, dass die Personalverwaltung einheitlich bei der Muttergesellschaft stattfindet. Verantwortlich für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes wäre die Konzernmutter. Der Arbeitnehmer wäre über die Weitergabe zu informieren. Zusätzlich müsste die Möglichkeit der Datenweitergabe zwischen Töchtern oder von der Muttergesellschaft an eine andere Tochtergesellschaft geregelt werden. Für Konzerne nach § 18 AktG muss die Möglichkeit eröffnet werden, die Daten von Tochter zu Tochter oder auch von der Muttergesellschaft an eine andere Tochter weiterzugeben. Der so entstehende weitergehende Datenfluss muss, um die datenschutzrechtlich notwendige Transparenz zu gewährleisten, verfahrensrechtlich anders abgesichert sein. Hier ist eine an § 11 BDSG angelehnte Gestaltung denkbar. Danach wäre der Vertragsarbeitgeber bei einer Verarbeitung von Daten durch ein anderes Konzernunternehmen für die Einhaltung der Vorschriften dieses Gesetzes verantwortlich – ähnlich wie bisher bei der Auftragsdatenverarbeitung. Hier kann, ähnlich wie in § 11 BDSG, verlangt werden, dass eine Vereinbarung zwischen den Unternehmen abgeschlossen wird, die sicherstellt, dass die entsprechenden Verfahrensanforderungen eingehalten werden, wobei jedoch nicht dieselben Kontrollpflichten ausgelöst werden dürfen.

b) Verhältnis zu Vorschriften aus anderen Gebieten des Arbeitsrechts

In den Unternehmen treten immer wieder Fälle auf, in denen arbeitsrechtliche und datenschutzrechtliche Pflichten kollidieren. Das daraus für die Unternehmen entstehende Dilemma ist nicht tragbar und bedarf vor dem Hintergrund der Einheit der Rechtsordnung einer dringenden Klärung. Eine solche Kollision ist zum Beispiel gegeben, wenn im Rahmen eines betrieblichen Eingliederungsmanagements der Betriebsrat vor der Einwilligung des Arbeitnehmers auf die Arbeitnehmerdaten zugreifen will und die Einigungsstelle dem Arbeitgeber eine entsprechende Verpflichtung auferlegt hat, während der Datenschutzbeauftragte die Weitergabe von Daten ohne Einwilligung als rechtswidrig ansieht. Problematisch ist zum Beispiel auch der Fall, in dem einem Arbeitnehmer wegen einer negativen Gesundheitsprognose gekündigt wurde und im anschließenden Kündigungsschutzprozess das Arbeitsgericht die Kündigung für rechtswidrig erklärt, weil der Arbeitgeber nicht nach evtl. geplan-

ten Rehamaßnahmen des Arbeitnehmers gefragt hat, obwohl dies datenschutzrechtlich nicht erlaubt ist.

c) Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung ist für viele kleine und mittlere Unternehmen eine rechtssichere Lösung, um den zahlreichen bürokratischen Pflichten, z.B. im Bereich der Entgeltabrechnung, nachzukommen. Die Anforderungen an die Auftragsdatenverarbeitung wurden mit der am 1. September 2009 in Kraft getretenen Änderung des § 11 BDSG bereits erheblich verschärft. Im Rahmen einer Neuregelung müssen deshalb mögliche Vereinfachungen geprüft werden. Bereits das Schriftformerfordernis stellt für die Praxis ein erhebliches Problem dar. Hier sollte als erster Entlastungsschritt zumindest die Möglichkeit der Textform nach § 126b BGB vorgesehen werden.

d) Sanktionslisten

Es fehlt bislang eine Aussage im Hinblick auf den Abgleich von Arbeitnehmerdaten mit den Sanktionslisten der so genannten Terrorismus-Verordnungen. Im Einführungserlass der Dienstanweisung „Zugelassener Wirtschaftsbeteiligter – AEO“ stellt das Bundesfinanzministerium klar, dass nach Auffassung der Bundesregierung ein Abgleich von Mitarbeiterdaten mit diesen Sanktionslisten datenschutzrechtlich zulässig ist. Diese Feststellung sollte klarstellend in die Regelungen zum Arbeitnehmerdatenschutz aufgenommen werden.

Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) (BT-Drs. 17/69)

(Fraktion der SPD)

Allgemein

Der Gesetzentwurf verfehlt die dringend notwendige Förderung der Rechtssicherheit und trägt zudem zu mehr Bürokratie im Arbeitsrecht bei. Nicht akzeptabel ist die Ausweitung der Mitbestimmungsrechte des Betriebsrats. Der Datenschutz soll das Persönlichkeitsrecht des Arbeitnehmers stützen. Er dient nicht dazu, Mitbestimmungsrechte auszuweiten.

Die wichtigsten Kritikpunkte

1. § 4 – Zulässigkeit der Datenerhebung und Datenverwendung

Regelungsgehalt: Der Gesetzentwurf soll als Spezialgesetz nur das Erheben und Verwenden von Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses regeln.

Selbst wenn man ein Arbeitnehmerdatenschutzgesetz befürworten würde, wäre dies nur sinnvoll, wenn sämtliche für das Arbeitsverhältnis geltenden datenschutzrechtlichen Vorschriften zusammengefasst würden. Mehr Rechtssicherheit und Rechtsklarheit würde nur dann erreicht, wenn das BDSG und andere datenschutzrechtlichen Vorschriften, z.B. im TKG, im Zusammenhang mit dem Arbeitsverhältnis durch das Beschäftigtendatenschutzgesetz vollständig ersetzt würden.

2. § 6 – Datenerhebung im Einstellungsverfahren

Regelungsgehalt: Festgelegt wird, dass Beschäftigtendaten unmittelbar beim Bewerber, bei Dritten nur mit Einwilligung des Bewerbers eingeholt werden dürfen und diese auch nur im Rahmen der Erforderlichkeit für die Eignung des Bewerbers erhoben werden dürfen, verbunden mit einer zusätzlichen Einschränkung des Fragerechts des (potentiellen) Arbeitgebers. Auch wird in Absatz 6 eine Kostenerstattungspflicht für den Arbeitgeber gegenüber dem Bewerber für das Vorstellungsgespräch begründet.

In erster Linie betreffen diese Regelungen arbeitsrechtliche und nicht originär datenschutzrechtliche Regelungen. Gerade das mit dem Gebot der unmittelbaren Datenerhebung einhergehende Verbot von Internetrecherchen, in denen der Arbeitnehmer seine Daten freiwillig und eigenverantwortlich preisgibt, wird die eigentliche Auswahl des Bewerbers immer mehr in die Probezeit verlagert. Es liegt nicht im Interesse gut qualifizierter Bewerber, wenn der Arbeitgeber weniger qualifizierte Bewerber einstellt, weil ihm gängige Erkenntnisquellen versperrt sind.

3. § 8 – Datenerhebung nach Begründung des Beschäftigungsverhältnisses

Regelungsgehalt: Festgelegt wird, dass die Datenerhebung durch den Arbeitgeber zulässig ist, wenn dies zu dessen Durchführung, Beendigung und Abwicklung erforderlich ist. Dazu werden Regelbeispiele gegeben, in denen Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses erhoben werden dürfen.

Diese Regelung führt zu Rechtsunsicherheiten, die über die Rechtsunsicherheiten auf Grund des bestehenden § 32 BDSG noch hinausgehen. Hierzu trägt beispielsweise die Vorschrift des Abs. 6 bei, wonach bei Datenerhebung die Zwecke, für die die Beschäftigtendaten erhoben werden, konkret festzulegen sind und die Datenerhebung einer Verhältnismäßigkeitskontrolle zu unterziehen ist. Aus der Begründung wird nicht deutlich, wie diese Zweckbestimmung vorgenommen werden muss und was daraus bei berechtigten Zweckänderungen folgt. Die Zulässigkeit der Datenerhebung setzt nach § 8 voraus, dass der Arbeitgeber eine gesetzliche oder sonstige Pflicht damit erfüllt. Es bleibt offen, ob auch die Erfüllung von Obliegenheiten durch den Arbeitgeber hiervon umfasst ist, beispielsweise bei der Durchführung eines betrieblichen Eingliederungsmanagements.

4. § 11 Opto-elektronische Einrichtungen (Videoüberwachung)

Regelungsgehalt: Die offene Videoüberwachung auf dem Betriebsgelände wird dergestalt eingeschränkt, dass sie nur zu ganz bestimmten Zwecken zulässig sein soll. Auch die zielgerichtete Videoüberwachung wird an sehr enge Voraussetzungen, wie das Vorliegen tatsächlicher Anhaltspunkte für den Verdacht einer Straftat geknüpft.

Die an § 6b BDSG angelehnte Regelung zur Videoüberwachung stellt ähnlich wie § 32 Abs. 1 Satz 2 BDSG zu hohe Anforderungen an deren Zulässigkeit. Die offene Videoüberwachung darf nicht an konkrete Vorgaben gekoppelt werden, sondern muss den betriebsspezifischen Gegebenheiten und Erfordernissen angepasst werden können. Auch vor dem Hintergrund, dass die Anforderungen an die Unternehmen Korruptionsbekämpfung sicherzustellen, ständig zunehmen und auf der anderen Seite die Anforderungen der Rechtsprechung an den Arbeitgeber bei verhaltensbedingter Kündigung und Verdachtskündigung gestiegen sind, muss eine Überwachung weiterhin möglich bleiben. Bei einer Verdachtskündigung muss der Arbeitgeber beispielsweise nachweisen, dass er alles ihm Mögliche unternommen hat, um die Angelegenheit aufzuklären. Diese hohen Anforderungen müssen ihre Entsprechung in den Möglichkeiten der Kontrolle finden.

5. § 12 Ortungssysteme

Regelungsgehalt: Die Möglichkeit des Einsatzes von Ortungssystemen (GPS) wird durch die Regelung des § 12 erheblich eingeschränkt, indem deren Einsatz auf die Erforderlichkeit für die Sicherheit der Beschäftigten und der Koordinierung der Einsätze beschränkt wird.

Die Möglichkeit des Einsatzes von Ortungssystemen, soweit dies erforderlich zur Sicherheit der Beschäftigten oder zur Koordinierung eines wechselnden Einsatzes der Beschäftigten ist, reicht nicht aus. In Tätigkeitsbereichen, in denen die Überwachung durch Ortungssysteme die einzige Möglichkeit ist, die Einhaltung von gesetzlichen und arbeitsvertraglichen Pflichten zu überprüfen, muss diese Überwachungsmöglichkeit genutzt werden können. Andernfalls würde auch hier die notwendige Gewährleistung von Compliance und Kriminalitätsbekämpfung behindert.

6. § 14 – Telekommunikationsdienste

Regelungsgehalt: Hiernach soll die Nutzung von Telefon, E-Mail, Internet oder anderen Telekommunikationsdiensten durch Vereinbarung mit dem Arbeitgeber geregelt werden können. Wird keine Vereinbarung getroffen, so soll die private Nutzung als erlaubt gelten. Daneben werden die Erhebungsrechte des Arbeitgebers von

Verkehrsdaten auch bei rein dienstlicher Nutzung nur für bestimmte Zwecke erlaubt, bei privater Nutzungserlaubnis noch weiter beschränkt.

Die Regelung des Abs. 1, wonach die Nutzung von Telefon, E-Mail, Internet oder anderen Telekommunikationsdiensten durch Vereinbarung mit dem Arbeitgeber geregelt werden kann und in dieser Vereinbarung festgelegt werden soll, ob und inwieweit die Nutzung der Telekommunikationsdienste auch zu privaten Zwecken erlaubt ist, beschreibt eine Selbstverständlichkeit, die sich aus allgemeinen Rechtsgrundsätzen ergibt. Der dritte Satz dieses ersten Absatzes bedeutet allerdings eine Abkehr von der bisherigen – von der Rechtsprechung geprägten – Rechtslage. Die Nutzung von Telefon, E-Mail, Internet und anderen Telekommunikationsdiensten zu privaten Zwecken soll als erlaubt gelten, wenn keine Vereinbarung getroffen wird und betriebliche Belange nicht beeinträchtigt werden. Es ist nicht nachvollziehbar, dass die private Nutzung von Betriebsmitteln des Arbeitgebers bei fehlender ausdrücklicher Regelung erlaubt sein soll. Den Eigentumsverhältnissen an diesen Arbeitsmitteln entsprechend müsste die Regelung umgekehrt lauten. Die Einschränkung, dass betriebliche Belange nicht beeinträchtigt werden dürfen, ist wiederum eine Selbstverständlichkeit, die sich aus den arbeitsvertraglichen Pflichten ergibt. Die Vorschrift greift in den grundgesetzlichen Eigentumsschutz des Arbeitgebers ein. Eine generelle Erlaubnis der privaten Nutzung von Informations- und Kommunikationseinrichtungen würde nicht nur das Eigentumsrecht des Arbeitgebers an diesen Einrichtungen empfindliche beeinträchtigen, sondern auch die im Synallagma stehenden arbeitsvertraglichen Pflichten des Arbeitnehmers in Frage stellen. Nutzt der Arbeitnehmer die Informations- und Kommunikationseinrichtungen für private Zwecke, so kann er währenddessen keine Arbeitsleistung erbringen und verstößt damit gegen seine arbeitsvertraglichen Pflichten. Wird eine gesetzliche Regelung zu dem Themenkomplex angestrebt, kann diese nur ein Verbot der privaten Nutzung von Informations- und Kommunikationseinrichtungen des Arbeitgebers mit Erlaubnisvorbehalt vorsehen.

7. § 20 – Einsichtsrecht

Regelungsgehalt: § 20 gibt dem Arbeitnehmer ein umfangreiches Recht zur Einsicht in seine Personalakte sowie zur Abgabe von hierin aufzunehmenden Erklärungen.

Hiermit wird wiederum eine rein arbeitsrechtliche, keine originär datenschutzrechtliche Regelung getroffen. Die Regelung überschneidet sich mit der Regelung des § 83 BetrVG und geht noch über diese hinaus. Ohne eine Klärung des Verhältnisses der Vorschrift des § 20 zu § 83 BetrVG sollte eine solche Doppelregelung nicht vorgenommen werden, weil sie zu zusätzlicher Rechtsunsicherheit und Unübersichtlichkeit führt. Stattdessen sollte allein der bisherige § 83 BetrVG beibehalten werden.

8. § 22 – Korrekturen

Regelungsgehalt: § 22 trifft Regelungen zu Ansprüchen des Arbeitnehmers auf Berichtigung, Entfernung und Sperrung seiner Daten.

Neben einer Anlehnung an § 20 BDSG wird hier auch eine arbeitsrechtliche Regelung zur Entfernung von „in Dateien gespeicherten Missbilligungen“ von Beschäftigten nach Ablauf von drei Jahren geregelt. Aus der Gesetzesbegründung ergibt sich, dass hiermit in erster Linie Abmahnungen gemeint sind. Bisher besteht nach der Rechtsprechung ein solches Recht auf Entfernung einer Abmahnung nur dann, wenn der abgemahnte Pflichtverstoß für das Arbeitsverhältnis bedeutungslos geworden ist. Deshalb ist die Einführung einer fixen Frist für den Entfernungsanspruch

problematisch. Zumindest muss die Frist mit der Bedingung verknüpft werden, dass das missbilligte Verhalten für das Arbeitsverhältnis nicht mehr von Bedeutung ist.

9. § 28 – Bestellung von Beauftragten für den Beschäftigtendatenschutz

Regelungsgehalt: § 28 legt fest, dass neben dem betrieblichen Datenschutzbeauftragten auch ein Beauftragter für den Beschäftigtendatenschutz zu bestellen sein soll.

Die Vorschrift des § 28 macht wiederum deutlich, dass eine Systematik, die ein Beschäftigtendatenschutzgesetz neben das Bundesdatenschutzgesetz stellt, für die Praxis untauglich ist. Sie hat zur Folge, dass zusätzlich zu dem Betrieblichen Datenschutzbeauftragten nach dem BDSG auch noch ein Beschäftigtendatenschutzbeauftragter vom Arbeitgeber zu bestellen ist, sofern er mindestens 5 Beschäftigte hat. Der Betriebliche Datenschutzbeauftragte nach dem Bundesdatenschutzgesetz hat selbstverständlich bereits heute die Aufgabe, über die Rechtmäßigkeit der Verwendung der Daten der Beschäftigten zu wachen. Eine zusätzliche Position ist aufgrund der Aufgaben des Betrieblichen Datenschutzbeauftragten nach dem BDSG überflüssig.

10. § 34 – Unabdingbarkeit, Verzicht, Verwirkung
Regelungsgehalt: Allgemein wird hier festgelegt, dass von den Vorschriften dieses Gesetzes nicht zu Ungunsten der Beschäftigten abgewichen werden kann.

Betriebsvereinbarung und Einwilligung sind zentrale Elemente des Datenschutzes, die durch die Norm ausgehebelt werden. Betriebs- und Privatautonomie werden eingeschränkt. Das ist kontraproduktiv und nicht nachvollziehbar.

Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen (BT-Drs. 17/4853)

(Fraktion BÜNDNIS 90/DIE GRÜNEN)

Allgemein

Der Gesetzentwurf vom 22.02.2011 gewährleistet insbesondere nicht die Rahmenbedingungen für eine gerade auch im Interesse der Belegschaft liegende effektive Kriminalitäts- und Korruptionsbekämpfung. In dem Regelwerk sind zwar teilweise auch praxisorientierte Ansätze enthalten, wie beispielsweise im Hinblick auf die gezielte Videoüberwachung. Der vorgelegte Gesetzentwurf erfüllt insgesamt die Anforderungen an eine sinnvolle und praxisnahe Regelung des Beschäftigtendatenschutzes aber nicht. Im Einzelnen sind nachstehend die wichtigsten Kritikpunkte des Entwurfs dargestellt.

Die wichtigsten Kritikpunkte

1. § 3 – Begriffsbestimmungen

Regelungsgehalt: In § 3 Absatz 4 definiert Beschäftigtendaten als personenbezogene oder personenbeziehbare Daten und Informationen über Angehörige der in § 1 Absatz 1 benannten Beschäftigtengruppen, die in Zusammenhang mit der Anbahnung, Begründung, Durchführung, Beendigung oder Abwicklung eines Beschäftigungsverhältnisses oder für die in diese Gesetz im Einzelnen aufgeführten zulässigen Zwecke verarbeitet werden.

Enthalten ist hier lediglich eine weite Definition des Begriffs des Beschäftigtendatums, nicht allerdings eine Abgrenzung zum Begriff des Geschäftsdatums. Eine Abgrenzung des jeweiligen gesetzlichen Regelungsbereichs ist notwendig, um Geschäftsdaten weiterhin sinnvoll bearbeiten zu können. Daten, die überwiegend dem Geschäftsbetrieb des Arbeitgebers zuzurechnen sind, müssen aus dem regelungsbereich ausgenommen werden.

2. § 4 – Zulässigkeit und Grundsätze der Datenverarbeitung

Regelungsgehalt: Nach Absatz 1 wird die Möglichkeit der Einwilligung auf ausdrücklich im Gesetz geregelte Fälle beschränkt.

Die Möglichkeit der Einwilligung des Beschäftigten in die Erhebung, Verarbeitung und Nutzung seiner Daten muss gewährleistet werden. Schon heute werden strenge Anforderungen an die Freiwilligkeit einer solchen Einwilligung gestellt. Unter diesen Voraussetzungen muss es auch weiterhin möglich sein, mit dem Beschäftigten als „Herr über seine Daten“ einzelfallbezogene und damit praxisgerechte Vereinbarungen zu treffen.

3. § 11 – „Raster-Abgleich“ von Beschäftigtendaten (Screening-Verfahren)

Regelungsgehalt: Die Vornahme eines Abgleichs von Beschäftigtendaten wird auf den Einzelfall beschränkt, soweit und solange konkrete Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis bestimmte Straftaten.

Unternehmen sind gesetzlichen und aufsichtsbehördlichen Anforderungen in Bezug auf Kriminalitäts- und Korruptionsbekämpfung ausgesetzt. Abgleiche von Beschäftigtendaten sind für die Erfüllung dieser Verpflichtungen unverzichtbar.

4. § 12 – Einsatz von Telekommunikationsdiensten

Regelungsgehalt: Im Fall einer privaten Nutzung von Telekommunikationsdiensten dürfen Verkehrsdaten nach § 12 nur unter engen Voraussetzungen und Inhaltdaten gar nicht verarbeitet bzw. ausgewertet werden. Zudem legt § 12 Absatz 1 Satz 3 fest, dass die angemessene private Nutzung von Telekommunikationsdiensten generell erlaubt sein soll, soweit keine anderweitige Vereinbarung vorliegt. Untersagt werden kann die private Nutzung hiernach nur im Rahmen einer individuellen oder Betriebsvereinbarung.

Den Eigentumsverhältnissen an diesen Arbeitsmitteln entsprechend müsste die Regelung genau umgekehrt lauten. Für den Fall, dass keine Regelung getroffen wurde, müsste sie automatisch verboten sein. Die Einschränkung, dass betriebliche Belange nicht beeinträchtigt werden dürfen, ist eine Selbstverständlichkeit, die sich aus den arbeitsvertraglichen Pflichten ergibt. Eine generelle Erlaubnis der privaten Nutzung von Informations- und Kommunikationseinrichtungen würde nicht nur das Eigentumsrecht des Arbeitgebers an diesen Einrichtungen beeinträchtigen, sondern auch die im Synallagma stehenden arbeitsvertraglichen Pflichten des Arbeitnehmers in Frage stellen. Nutzt der Arbeitnehmer die Informations- und Kommunikationseinrichtungen für private Zwecke, so kann er währenddessen keine Arbeitsleistung erbringen und verstößt damit gegen seine arbeitsvertraglichen Pflichten. Wird eine gesetzliche Regelung zu dem Themenkomplex angestrebt, kann diese nur ein Verbot der privaten Nutzung von Informations- und Kommunikationseinrichtungen des Arbeitgebers mit Erlaubnisvorbehalt vorsehen.

Eine Regelung der „Mischnutzung“ muss sicherstellen, dass der Zugriff auf geschäftliche Korrespondenz und die Kontrollmöglichkeiten nicht eingeschränkt wird. Darüber hinaus muss geklärt werden, ob und in welchem Ausmaß eine Missbrauchskontrolle bei übermäßiger privater Nutzung oder Versendung strafrechtlich relevanten Materials möglich ist.

5. § 15 – Einsatz von Ortungssystemen

Regelungsgehalt: Die Möglichkeit des Einsatzes von Ortungssystemen wird durch die Regelung erheblich eingeschränkt, indem deren Einsatz auf die Erforderlichkeit für die Sicherheit des Beschäftigten beschränkt wird.

Gerade im Außendienstbereich muss schon die Koordinierung von Einsätzen anhand der Übermittlung von Daten durch Ortungssysteme möglich sein. Zudem existieren Tätigkeitsbereiche, in denen die Überwachung durch Ortungssysteme die einzige Möglichkeit ist, die Einhaltung von gesetzlichen und arbeitsvertraglichen Pflichten zu überprüfen.

6. § 21 – Korrekturen

Regelungsgehalt: § 21 trifft Regelungen zu Ansprüchen des Arbeitnehmers auf Berichtigung und Löschung seiner Daten. Zudem sollen nach Ablauf von spätestens drei Jahren im nicht-öffentlichen Bereich die in Unterlagen oder Dateien aufgenommene Missbilligungen von Beschäftigten entfernt werden.

Gerade im Hinblick auf die Drei-Jahres-Frist wird hier eine arbeitsrechtliche Regelung getroffen. Aus der Gesetzesbegründung kann geschlossen werden, dass in erster Linie Abmahnungen gemeint sind. Bisher besteht nach der Rechtsprechung ein solches Recht auf Entfernung einer Abmahnung nur dann, wenn der abgemahnte Pflichtverstoß für das Arbeitsverhältnis bedeutungslos geworden ist. Deshalb ist die Einführung einer fixen Frist für den Entfernungsanspruch problematisch. Zumindest muss die Frist mit der Bedingung verknüpft werden, dass das missbilligte Verhalten für das Arbeitsverhältnis nicht mehr von Bedeutung ist.

7. § 28 – Betriebliche Datenschutzbeauftragte

Regelungsgehalt: § 28 beinhaltet eine Erweiterung der Befugnisse der betrieblichen Datenschutzbeauftragten und legt zudem fest, dass die Bestellung des betrieblichen Datenschutzbeauftragten nach § 4 f BDSG der Mitbestimmung des Betriebsrats unterliegen soll.

Diese Regelung bedeutet eine Ausdehnung der Mitbestimmung, die nicht Aufgabe des Datenschutzes ist.

8. § 34 – Unabdingbare Rechte der Beschäftigten

Regelungsgehalt: Der Abschluss von Betriebsvereinbarungen soll zur Regelung der Verarbeitung personenbezogener Daten ausdrücklich erlaubt sein., allerdings nur soweit sie den Schutz der personenbezogenen Daten durch dieses Gesetz nicht einschränken. Gleiches soll für Tarifverträge gelten.

Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein. Wann eine Abweichung „zu Ungunsten“ vorliegt, wirft darüber hinaus weitere Fragen und Rechtsunsicherheiten auf. Ausschlaggebend ist jedoch das Gesamtbild der Betriebsvereinbarung. Die Betriebsparteien müssen in der Lage sein, betriebsspezifische und damit praxisgerechte Vereinbarungen auch und gerade im Bereich des Beschäftigtendatenschutzes zu treffen, um betriebliche rechtssicherheit zu schaffen.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 C Anlage

Datenschutz im Betrieb übersichtlich und klar gestalten

Bewertung der Anregungen im Arbeitspapier der Berichterstatter der Koalitionsfraktionen zu der öffentlichen Anhörung am 23. Mai 2011 zu dem Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes - BT-Drs. 17/4320

20. Mai 2011

Zusammenfassung

Der Gesetzentwurf der Bundesregierung vom 25. August 2010 zum Beschäftigtendatenschutz weist mehrere Regelungsvorschläge auf, die einer klaren praxistauglichen Anwendung des Datenschutzes im Betrieb entgegenstehen. Die im Arbeitspapier der Berichterstatter aufgeworfenen Fragen und Hinweise machen dies deutlich. Die ebenfalls im Papier enthaltenen Anregungen bedeuten eine sinnvolle Weiterentwicklung des Regierungsentwurfs, beantworten aber nicht alle mit dem in Entwurf enthaltenen Vorschlägen.

Im Einzelnen

1. *§§ 3 Nr. 12, 27 Abs. 3 BDSG-E - Anwendungsbereich der Regelungen, begriff des Beschäftigtendatums*
Vorschlag: Aufnahme einer klarstellenden Eingrenzung des Beschäftigtendatums anhand der Zweckbestimmung der Erhebung, Verarbeitung und Nutzung von Daten.

Bewertung: Die Vorschläge zu §§ 3 Abs. 12 und 27 Abs. 3 machen zu Recht deutlich, dass zwischen Beschäftigtendaten auf der einen und zu Betriebszwecken benötigten Daten auf der anderen Seite unterschieden werden muss. Das gilt in besonderer Weise für ein Dauerschuldverhältnis Daher muss bereits im Gesetz geregelt werden, dass es für primär geschäftlichen Zwecken dienenden Daten bei der Anwendung insbesondere von § 28 BDSG bleibt

2. *§§ 4 Abs. 1, 32l Abs. 3, 5 BDSG-E – Zulässigkeit und Umfang von Betriebsvereinbarungen*
Vorschlag: Einführung einer Positivliste oder einer Negativliste zur Zulässigkeit einer Betriebsvereinbarung auch zu Ungunsten des Arbeitnehmers.

Bewertung: Es ist richtig, die Betriebsvereinbarung als Regelungsinstrument für den Datenschutz zu erhalten. Auf Grund der ohnehin starken Stellung des Betriebsrates, die z. B. durch das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG untermauert ist, und wegen der hohen Anforderungen, die die Rechtsprechung zur Berücksichtigung des Persönlichkeitsrechts der Arbeitnehmer durch die Betriebspartner entwickelt hat, bedarf es einer Einschränkung nicht. Selbst eine Negativliste ist daher überflüssig. Eine Positivliste erlaubter Regelungsmaterien für Betriebsvereinbarungen kann in keinem Fall alle denkbaren Fälle abdecken, die einer betrieblichen Ergänzung des Gesetzes bedürfen.

3. *§ 32 Abs. 2 BDSG-E – Zulässiger Umfang von Fragerechten*
Vorschlag: Anknüpfung der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung mit Blick auf das Fragerecht zu Vermögensverhältnisses, zu Ermittlungsverfahren und zu Vorstrafen (lediglich) an das Vorliegen eines berechtigten Interesses des Arbeitgebers, um so eine faktische Ausweitung des Allgemeinen Gleichbehandlungsgesetzes zu verhindern.

Bewertung: Die Erwägungen zum zulässigen Umfang des Fragerechts in § 32 Abs. 2 BDSG machen deutlich, dass die in Absatz 2 genannten Daten ohnehin durch das AGG in besonderer Weise geschützt sind.

4. *§ 32 Abs. 6 BDSG-E – Bewerberrechte in webbasierten sozialen Netzwerken*
Vorschlag: Differenzierung zwischen öffentlich zugänglichen Informationen und solchen Informationen, die der betroffene Bewerber nur einem eingeschränkten Adressatenkreis zur Verfügung gestellt hat. Eine Erhebung, Verarbeitung und Nutzung der öffentlich zugänglichen Informationen soll zulässig sein.

Bewertung: Es ist angemessen, den Zugriff auf Informationen in sozialen Netzwerken grundsätzlich zu erlauben und nur dort einzuschränken, wo der Bewerber sich geschützt im Netz bewegt. Das ist insbesondere dort der Fall, wo er den Zugriff auf seine Daten nur für „registrierte Freunde“ zulässt. Bei Daten, die ein Bewerber öffentlich zugänglich im Netz präsentiert, muss man davon ausgehen können, dass er die Kenntnisnahme freiwillig und eigenverantwortlich in Kauf nimmt. Darüber hinaus präsentieren einige Bewerber, gerade im Zuge der fort-

schreitenden Technisierung, bewusst Informationen frei zugänglich im Internet (so u.a. selbst gestaltetet homepages zur Präsentation technischer Fähigkeiten oder Listen wissenschaftlicher Veröffentlichungen). Es liegt nicht im Interesse gut qualifizierter Bewerber, wenn der Arbeitgeber weniger qualifizierte Bewerber einstellt, weil ihm gängige Erkenntnisquellen versperrt sind.

5. *§ 32c Abs. 3 BDSG-E – Zweifel an der fortdauernden Eignung*

Vorschlag: Aufnahme einer Einschränkung auf „ernsthafte“ Zweifel.

Bewertung: Der Begriff „ernsthafte Zweifel“ ist nicht justitiabel und für die Unternehmen auch kaum anwendbar. Wann beginnt ein Zweifel ernsthaft zu sein? Wenn es bei der Regelung im § 32c Abs.3 bleiben sollte, darf diese nicht noch durch den Begriff „ernsthaft“ weiter verunklart werden.

Ärztliche Untersuchungen zur Überprüfung der Eignung sind auch aus Gründen der Fürsorge und des Arbeitsschutzes geboten. So können z. B. bei Fahr-, Steuer- und Überwachungstätigkeit arbeitsmedizinische Untersuchungen aufgrund der Gefährdungsbeurteilung angezeigt sein, weil eine erhöhte Gefährdung besteht, der Arbeitgeber aber die körperliche und gesundheitliche Eignung des Arbeitnehmers für die Tätigkeit nicht selbst beurteilen kann.

Sollte § 32c Abs. 3 wie im Regierungsentwurf vorgesehen umgesetzt werden, handelt es bei dieser gesetzlichen Regelung um die einzige Grundlage, die den Arbeitnehmer verpflichtet, sich einer solchen Untersuchung zu unterziehen. Eine weitere Einschränkung des § 32c Abs. 3 darf daher nicht stattfinden.

6. *§ 32e Abs. 2 Nr. 1 BDSG-E – Erhebung von Daten ohne Kenntnis des Beschäftigten*

Vorschlag: Abkehr vom Tatbestandsmerkmal „zu einer Kündigung aus wichtigem Grund berechtigen würde“. Ersetzen dieser vorab einzelfallorientierten Interessenabwägung durch das an objektiven Kriterien orientierte Vorliegen eines wichtigen Kündigungsgrundes im Sinne von § 626 Abs. 1 BGB.

Bewertung: Es ist ein Schritt in die richtige Richtung, erhebliche Pflichtverletzung an objektiven Kriterien und nicht an die subjektive Auslegung des einzelnen Arbeitsgerichts zu knüpfen, wann das Fehlverhalten eines Arbeitnehmers einen wichtigen Grund im Sinne von § 626 Abs. 1 BGB für eine verhaltensbedingte Kündigung darstellt.

Die Vorschrift sollte generell weiter entwickelt werden. Die Erhebung von Daten nach § 32e des Entwurfes sollte möglich sein, wenn der Arbeitgeber Hinweise darauf erhält, dass ein für arbeitsrechtliche Reaktionen relevantes Verhalten des Arbeitnehmers vorliegt. So ist z.B. nach der neueren Rechtsprechung des Bundesarbeitsgerichts selbst im klaren Fall einer Unterschlagung und einer Untreuehandlung des Arbeitnehmers nicht immer der Weg für eine außerordentliche verhaltensbedingte Kündigung eröffnet. Liegen aber Tatsachen vor, die einen entsprechenden Verdacht auslösen, muss der Arbeitgeber hierauf auch durch die Erhebung weiterer Daten reagieren können.

7. *§ 32h Abs. 1 BDSG-E – Zulässigkeit der Verwendung biometrischer Daten*

Vorschlag: Nachfrage, ob die Regelung in ihrer jetzigen Form angemessen und eine Einschränkung der Erhebung, Verarbeitung und Nutzung von biometrischen Daten auf sicherheitsrelevante Bereiche praktikabel umsetzbar ist.

Bewertung: Vor dem Hintergrund der rasanten elektronischen Entwicklung ist bereits zweifelhaft, biometrische Daten – wie vom Gesetzentwurf vorgesehen – auf Authentifizierungs- und Autorisierungsprozesse zu beschränken. Eine weitere Beschränkung auf „sicherheitsrelevante“ Bereiche sollte daher unterbleiben und führt ebenso wie zum Beispiel der Begriff „ernsthafte Zweifel“ (siehe Nr. 5) zu erheblicher neuer Rechtsunsicherheit.

8. *§ 32i Abs. 2 BDSG-E – Vorab-Informationspflicht des Arbeitgebers*

Vorschlag: Die stichprobenartige Kontrollmöglichkeit bei telefonisch erbrachten Dienstleistungen als wesentlicher Inhalt der geschuldeten Arbeitsleistung, wird grund-

sätzlich befürwortet, ebenso wie die Informationspflicht. Anerkennung eines Klarstellungsbedürfnisses, dass der Arbeitgeber nicht zur konkreten Information über den Zeitpunkt der Kontrollen verpflichtet werden soll.

Bewertung: Die Erwägungen zur Vorabinformationspflicht bei § 32i Abs. 2 BDSG sind richtig. Die Festlegung einer Vorab-Informationspflicht widerspricht an sich schon dem Sinn- und Zweck einer stichprobenartigen Leistungs- und Verhaltenskontrolle. Eine stichprobenartige Leistungs- und Verhaltenskontrolle soll ausschnittsweise das natürliche Verhalten und die gewöhnliche Leistung zeigen. Erfolgt vorab eine Ankündigung einer solchen Kontrolle, zudem unter Angabe eines konkreten Zeitpunktes, so kann davon ausgegangen werden, dass das durchschnittliche Verhalten oder die gewöhnliche Leistung des Arbeitnehmers nicht widergespiegelt wird. Gerade hierauf ist ein Arbeitgeber jedoch angewiesen, insbesondere da es außerhalb solcher Maßnahmen nahezu unmöglich ist, die Qualität einer telefonisch erbrachten Dienstleistung zu ermitteln.

9. *§ 32i Abs. 4 BDSG-E – Private Nutzung dienstlicher Telekommunikationsanlagen*

Vorschlag: Die Eigenschaft des Arbeitgebers als Diensteanbieter im Sinne des TKG, wenn er den Arbeitnehmern die private Nutzung dienstlicher Telekommunikationsanlagen gestattet, wird vielfach als nicht praxisgerecht erachtet. Es wird daher erwogen, ob der jetzige Regierungsentwurf nicht auch für diese Fälle eine Regelung zu treffen hat und wie eine solche praxisgerecht und mit Berücksichtigung der Arbeitnehmerinteressen ausgestaltet sein sollte.

Bewertung: Eine Klarstellung, dass der Arbeitgeber nicht Dienstanbieter im Sinne des TKG wird, wenn er die Nutzung dienstlich gestellter Kommunikationsmittel auch für private Zwecke zulässt, ist sinnvoll, geboten und überfällig. Die Einordnung des Arbeitgebers als Diensteanbieter im Sinne des TKG führt im Ergebnis zu unerfüllbaren Aufgaben: So ist z. B. jeder Kaufmann nach § 257 Abs. 1 Nr. 2 und 3 HGB verpflichtet, abgesandte und empfangene Handelsbriefe sechs Jahre lang geordnet aufzubewahren. Nach ganz h.M. gilt diese Dokumentationspflicht auch für E-Mails. Um dieser Aufbewahrungspflicht nachkommen zu können, muss der Kaufmann als Arbeitgeber Zugriff auf den Inhalt der E-Mails nehmen können, um überhaupt beurteilen zu können, ob die Schriftstücke als Handelsbriefe aufbewahrungspflichtig sind. Der Zugriff darauf ist ihm jedoch bei privater Nutzung nach § 88 TKG versagt. Was soll der Arbeitgeber tun – seine Pflichten nach dem HGB oder dem TKG erfüllen? Darüber hinaus muss das Gesetz aber auch so gefasst werden, dass der Arbeitgeber Missbrauch durch Kontrollen verhindern kann. Die derzeitig geplante Regelung in § 32i Abs. 4 reicht hierfür nicht aus. Denn die Erhebung, Verarbeitung und Nutzung privater Daten und Inhalte ist danach nur zulässig, soweit sie zur Durchführung des ordnungsgemäßen Geschäftsbetriebs unerlässlich ist. Ob dies Missbrauchskontrollen rechtfertigt, ist zumindest fraglich.

10. § 32l Abs. 1 BDSG-E – Einwilligung als Rechtfertigung für Datenerhebung und -verarbeitung

Vorschlag: Die vorgesehene Regelung könnte auch dazu führen, dass die Einwilligung eines Arbeitnehmers auch in für ihn vorteilhaften Angelegenheiten keine zulässige Grundlage für eine Datenerhebung, -verarbeitung und -nutzung darstellt. Hier sollte eine praktikablere Lösung gefunden werden, ohne das Schutzniveau des Gesetzes zu unterschreiten. Denkbar erscheint hier eine Positiv- oder Negativliste.

Bewertung: Eine Einwilligung ist bereits nach der geltenden Systematik des BDSG nur wirksam, wenn sie freiwillig ist. Ebenso wie bei der Betriebsvereinbarung reicht dies als „Sicherung“ gegen eine missbräuchliche Nutzung dieses Erlaubnistatbestands aus. Wollte man etwas an der Freiwilligkeit ergänzen, könnte man erwägen, diese an einen Vermutungstatbestand zu knüpfen. Freiwilligkeit wäre danach dann zum Beispiel zu vermuten, wenn der Arbeitnehmer ein Überlegungsrecht eingeräumt bekommt. Dieses darf in keinem Fall mehr als drei Tage betragen. Darüber hinaus gilt auch hier: Eine Positivliste erlaubter Regelungsmaterien für Einwilligungen kann in keinem Fall

alle denkbaren Fälle abdecken, die eine betriebliche oder vertragliche Flexibilität erfordert.

11. *§ 32l Abs. 4 BDSG-E – „Whistleblower"-Regelung*

Vorschlag: In Erwartung einer möglichen Kollision mit Art. 28 Abs. 4 der Richtlinie 95/46/EG könnte eine Änderung von § 32l Abs. 4 BDSG-E erwogen werden.

Bewertung: Eine Regelung zum sogenannten Whistleblowing ist überflüssig. Sie ist auch nicht von Art. 28 der Richtlinie 95/46/EG gefordert. Schon heute kann jeder Arbeitnehmer sich an die zuständigen öffentlichen Stellen wenden. Er muss alleine zuvor einen innerdienstlichen Beschwerdeweg einhalten. Dies ist mit europäischem Recht kompatibel. Art. 28 der einschlägigen Richtlinie gebietet nicht, dass dies unmittelbar zu geschehen hat. Ein internes Klärungsverfahren wird nicht ausgeschlossen.

12. *Privilegierung der Datenweitergabe und -nutzung in verbundenen Unternehmen*

Vorschlag: Die Notwendigkeit wird anerkannt, einen Privilegierungstatbestand für Fälle der Datenweitergabe und -nutzung im Konzernverbund zu schaffen. Insbesondere im Hinblick auf die Datenschutzrichtlinie wird die Schaffung einer Norm zur gemeinsamen Verantwortlichkeit („joint controllership") der beteiligten datenverarbeiteten Stellen, d.h. Konzernmutter und jeweilige Konzerntochter vorgeschlagen.

Bewertung: Eine Regelung des Konzerndatenschutzes ist überfällig. Ein Instrument hierzu kann die Konzernbetriebsvereinbarung darstellen. Eine andere Option ist es, den Datenfluss innerhalb eines Konzerns an eine an § 28 Abs. 1 Nr. 2 BDAG orientierte Interessenabwägung zu knüpfen. Darüber hinaus ist auch die Einführung einer Regelung zu data sharing möglich, um die Nutzung von Daten im Verbund mehrerer Unternehmen zu erleichtern. Eine solche Regelung stellt aber nicht die einzige Möglichkeit dar, die mit europäischem Recht vereinbar wäre.

Ansprechpartner:

BDA | DIE ARBEITGEBER
Bundesvereinigung der Deutschen Arbeitgeber-verbände

Arbeitsrecht
T +49 30 2033-1200
arbeitsrecht@arbeitgeber.de

Prof. Dr. Gerrit Hornung

Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 D

Telefon Prof. Dr. Gerrit Hornung
0851 509-2380

Telefax 0851 509-2382

e-mail gerrit.hornung
@uni-passau.de

Datum 18. Mai 2011

Stellungnahme

zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung (Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230), zu weiteren Entwürfen der Fraktionen der SPD (Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis, BT-DRs. 17/69) und von BÜNDNIS 90/DIE GRÜNEN (Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen, BT-Drs. 17/4852) sowie zweier Anträge zum Beschäftigtendatenschutz (BT-Drs. 17/121 und 17/779)

1 Vorbemerkung

Das grundsätzliche Anliegen des vorliegenden Gesetzesentwurfs der Bundesregierung und der alternativ vorgelegten Entwürfe der Fraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN ist zu begrüßen. Die gegenwärtige Rechtslage wird maßgeblich durch die arbeitsgerichtliche Rechtsprechung bestimmt, die diese Aufgabe zwar insgesamt sachgerecht bewältigt hat, naturgemäß aber immer nur punktuellen und nachlaufenden Einfluss auf die Rechtsentwicklung nehmen konnte. Der Gesetzgeber sollte deshalb die Gelegenheit nicht verstreichen lassen, Leitlinien für die betriebliche Praxis vorzugeben, die zumindest einige grundlegende Rechtsfragen der Datenverarbeitung in diesem wichtigen Lebensbereich entscheiden.

Die vorgelegten Gesetzentwürfe sind komplex und umfangreich. Im Rahmen dieser Stellungnahme ist es daher nicht möglich, zu allen durch die Entwürfe aufgeworfenen rechtlichen und rechtspolitischen Fragen Stellung zu beziehen. Die folgenden Ausführungen

beschränken sich deshalb auf übergreifende Gesichtspunkte und Anmerkungen zu besonders wichtigen und kontroversen Fragen.

2 Grundsätzliche Gesichtspunkte

Aus grundsätzlicher Sicht sind drei Gesichtspunkte anzumerken.

Erstens fällt das Reformvorhaben in eine Zeit, in der auf europäischer Ebene eine Reform der Datenschutzrichtlinie[1] angestrebt wird (die Kommission hat am 4. November 2010 eine Mitteilung über ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vorgelegt,[2] die anschließende Konsultation befindet sich derzeit in der Auswertung). Das relativiert zum einen die Frage der Richtlinienkonformität des nationalen Vorhabens, die im Folgenden bei einigen Punkten relevant wird. Zum anderen verbleibt insgesamt das Risiko, für den Fall weitgehender Neuerungen auf europäischer Ebene das vorliegende Reformvorhaben – und andere, die in den Bereich des Datenschutzrechts fallen – zeitnah überarbeiten zu müssen.

Zweitens weisen die Entwürfe (der Regierungsentwurf noch mehr als die alternativ vorgelegten Entwürfe) eine erhebliche Komplexität auf, die durch Wiederholungen allgemeiner Prinzipien und eine unübersichtliche Verweisungstechnik bedingt ist. Allgemeine Grundsätze des Datenschutzrechts wie das Erforderlichkeitsprinzip werden in einer Vielzahl der Vorschriften explizit normiert, anstatt generalklauselartig vor die Klammer gezogen zu werden.

Drittens enthält der Entwurf an vielen Stellen offene Rechtsbegriffe und Verhältnismäßigkeitsklauseln, was sich angesichts der Unterschiede in der betrieblichen Praxis nicht vermeiden lässt. Gleichzeitig gilt es jedoch zu bedenken, dass die Entscheidung über die Zulässigkeit konkreter Datenverwendungen damit auch weiterhin maßgeblich bei den Gerichten liegen wird.

3 Einzelfragen

Aus dem Regelungsbereich der Entwürfe werden im Anschluss die folgenden besonders wichtigen Problemkomplexe behandelt:

- Abweichende Regelungen durch Betriebsvereinbarungen
- Ausschluss und Möglichkeit der Einwilligung

---

[1] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. EG Nr. L 281 vom 23. November 1995 S. 31.

[2] KOM(2010) 609 endgültig.

- Rechtsschutz (Beschwerderecht, Whistleblower, Verbandsklagerecht)
- Konzerndatenschutz
- Bewerberauswahl und soziale Netzwerke
- Organisatorische und technische Aspekte des Datenschutzes
- Regelungen zu Überwachung und Kontrolle im Betrieb (Compliance, Videoüberwachung, Biometrie, Telekommunikationsüberwachung)

3.1 Abweichende Regelungen in Betriebsvereinbarungen

Das Bundesarbeitsgericht geht in einer Entscheidung aus dem Jahre 1986 davon aus, dass durch Betriebsvereinbarungen zuungunsten der Beschäftigten von Regelungen des Datenschutzrechts abgewichen werden darf.[3] Diese Ansicht ist in Teilen der Literatur auf heftige Kritik gestoßen.[4] Dort hat sich weithin die Auffassung durchgesetzt, dass Betriebsvereinbarungen zwar die – notwendige und verdienstvolle – Aufgabe der Präzisierung und Konkretisierung allgemeiner datenschutzrechtlicher Anforderungen auf die jeweilige betriebliche Praxis leisten können, Arbeitgeber und Betriebsrat aber kein Mandat haben, gesetzlich vorgegebene Datenschutzrechte einzuschränken, die weithin grundrechtlich abgesicherten Persönlichkeitsschutz beinhalten. Diese Richtung schlägt § 32l Abs. 4 BDSG-E ein, der es generell untersagt, von den geplanten Neuregelungen zulasten der Beschäftigen abzuweichen. Entgegen der teilweise vorgetragenen Kritik in der Literatur sollte an dieser Vorschrift festgehalten werden. Dass die Abgrenzung des Anwendungsbereichs (Konkretisierung versus „Abweichung zuungunsten der Beschäftigten“) im Einzelfall problematisch sein kann,[5] ist kein Gegenargument, da sich hieran auch durch eine andere Formulierung des Anwendungsbereichs nichts ändern würde.

Allerdings kann nicht übersehen werden, dass Betriebsvereinbarungen bei dieser – auch nach dem Entwurf gewollten – Konkretisierungsleistung in Grenzbereichen operieren, weil sich jedes betriebliche Umfeld und jede Datenverarbeitung anders darstellen kann und deshalb die Konkretisierung datenschutzrechtlicher Prinzipien betriebsbezogen unterschiedlich ausfallen wird. Es ist in jedem Fall zu vermeiden, dass mit der Regelung „in Einzelfällen betriebsnahe, sachgerechte Lösungen ausgeschlossen werden“.[6]

---

3 BAG NJW 1987, 674, 677.

4 *Walz*, in: Simitis, BDSG, 6. Auflage 2006, § 4 Rn. 17; *Gola/Wronka*, Handbuch Arbeitnehmerdatenschutz, 5. Auflage 2009, Rn. 246; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Auflage 2010, § 4 Rn. 2; a.A. *Wank*, in: Erfurter Kommentar zum Arbeitsrecht, 9. Auflage 2009, § 4 Rn. 3; *Thüsing*, Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 105.

5 Darauf weist *Kort*, MMR 2011, 294, 298 f. hin; kritisch auch *Beckschulze/Natzel*, BB 2010, 2368 f.; *Thüsing*, NZA 2011, 16, 18.

6 So *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729, die den Vorschlag im Grundsatz befürworten.

Gesetzeswortlaut oder Begründung sollten deshalb klarstellen, dass die Präzisierung ausfüllungs- und wertungsbedürftiger Begriffe wie „private Lebensgestaltung“, „schutzwürdige Interessen der Beschäftigten“ oder „betriebliche Gründe“ zulässig ist. Auch auf Basis der aktuellen Fassung des Regierungsentwurfs wäre es beispielsweise zulässig, die näheren Umstände des Einsatzes biometrischer Verfahren im Betrieb durch eine Betriebsvereinbarung zu regeln,[7] weil § 32h BDSG-E insoweit nur sehr allgemeine Vorgaben macht.[8] Die Grundüberlegung der Regelung bleibt aber zutreffend, da durch sie der Gefahr entgegengewirkt werden kann, dass grundrechtliche Schutzpositionen in Verhandlungen zwischen Arbeitgebern und Betriebsräten im Rahmen von Gesamteinigungen zu marginalen Verhandlungsposten werden.

3.2 Ausschluss der Einwilligung

Der weitgehende Ausschluss der Einwilligung in § 32l Abs. 1 BDSG-E[9] wirft zwei Fragen auf: Die nach der europarechtlichen Zulässigkeit und die nach der sachlichen Angemessenheit. Vorwegzuschicken ist, dass die praktische Bedeutung einer echten (das heißt freiwilligen und informierten) Einwilligung in der betrieblichen Praxis eingeschränkt ist. Zum einen wird es vielfach an der Freiwilligkeit fehlen, weil die Verweigerung der Einwilligung zu erheblichen Nachteilen für Beschäftige führen kann. Zum anderen erfordern betriebliche Abläufe im Allgemeinen ein hohes Maß an Einheitlichkeit, das nicht gewährleistet werden kann, wenn einzelne Beschäftigte die Einwilligung verweigern. Bei einer tatsächlich freiwilligen Entscheidung ist dies aber praktisch nie auszuschließen.

Zweifel an der Europarechtskonformität von § 32l Abs. 1 BDSG-E bestehen deshalb, weil Art. 7 lit. a der Datenschutzrichtlinie die Einwilligung als eigenständigen Erlaubnistatbestand nennt. Dies allein reicht −entgegen anderslautender Stimmen[10] − indes noch nicht aus, um die vorgeschlagene Regelung richtlinienwidrig werden zu lassen. Zwar hat der Europäische Gerichtshof der Datenschutzrichtlinie den Charakter einer Vollharmonisierung zugesprochen.[11] Das bedeutet aber lediglich, dass den nationalen Gesetzgebern nur die Spielräume zukommen, die die Richtlinie selbst ihnen gibt. In gewissen Grenzen sind sie daher befugt, Anforderungen zu typisieren, die von der Richtlinie selbst gesetzt werden.

---

7 S. beispielsweise die Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme des TeleTrusT e.V., http://www.teletrust.de/uploads/media/TeleTrusT-AG_Biometrie_BetriebsV_1.2.pdf.

8 Dazu noch unten 3.7.3.

9 Der Entwurf von BÜNDNIS 90/DIE GRÜNEN enthält eine vergleichbare Regelung in § 4 Abs. 1 Satz 1.

10 Mit diesem Argument *Forst*, RDV 2010, 150; *ders.*, NZA 2010, 1043, 1044; *Thüsing*, RDV 2010, 147,148 f.; *ders.*, NZA 2011, 16, 18 f.; *Rasmussen-Bonn/Raif*, GWR 2011, 80; ähnlich *Kort*, MMR 2011, 294, 299; für die Zulässigkeit *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729.

11 EuGH, Urteil vom 6.11.2003 - Rs. C-101/01 (Lindqvist/Schweden), MMR 2004, 95, 98 f.

Hierzu gehört auch die Freiwilligkeit der Einwilligung, an die die Datenschutzrichtlinie hohe Anforderungen stellt. Demzufolge muss es zulässig sein, wenn nationale Gesetzgeber in Konkretisierung des durch die Richtlinie vorgeschriebenen „hohen Schutzniveaus“[12] in bestimmten Lebensbereichen, in denen von einer Freiwilligkeit typischerweise nicht ausgegangen werden kann, die Möglichkeit einer Einwilligung generell ausschließen. Eine solche Situation ist im Arbeitsverhältnis weithin gegeben.

Aus den vorstehenden Erwägungen folgt allerdings auch, dass der nationale Gesetzgeber dort keine Einschränkungen machen darf, wo typischerweise gerade keine Unfreiwilligkeit vorliegt. Gemessen an diesem Kriterium erscheinen die ausdrücklich zugelassenen Einwilligungstatbestände des Entwurfs[13] zu eng. Dort, wo Beschäftigte gerade keinem starken Druck ausgesetzt sind, spricht auch kein sachlicher Grund für einen Ausschluss der Einwilligung. In der Literatur finden sich denn auch Beispiele wie das Angebot zum Abschluss einer betrieblichen Altersvorsorge[14] oder die Internetpräsentation von Wissenschaftlern und ihren Arbeitsergebnissen,[15] bei denen der Ausschluss der Einwilligung nicht angemessen wäre. Für derartige Fälle bedarf es einer Generalklausel, die die Einwilligung in bestimmten Fällen zulässt – allerdings nur bei Vorliegen bestimmter Mittel zur Sicherung der Freiwilligkeit. Dies könnte eine Beschränkung auf Fälle sein, in denen Beschäftigte selbst initiativ werden, oder ein freiwilliges Koppelungsverbot seitens des Arbeitgebers.

3.3 Rechtsschutzfragen

Der Regierungsentwurf bedarf hinsichtlich des Komplexes der Rechtsschutzfragen in mehreren Punkten der Überarbeitung.

3.3.1 Beschwerderecht

§ 32l Abs. 4 BDSG-E verlangt von Beschäftigten, sich vor einer Eingabe an die Datenschutzaufsichtsbehörde mit einer Beschwerde an den Arbeitgeber zu wenden. Dies ist eine Verschlechterung der Rechtsposition der Beschäftigten, sachlich nicht zu rechtfertigen und darüber hinaus europarechtswidrig. Es ist nicht zutreffend, dass der Entwurf ein Beschwerderecht neu einführt.[16] Nach aktueller Rechtslage hat jedermann gemäß § 38 Abs. 1 Satz 8 i.V.m. § 21 Satz 1 BDSG das Recht, sich an die Datenschutzaufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung

---

12 Erwägungsgrund 10.
13 Die Einwilligung wird in § 32 Absatz 6 Satz 4, § 32a Absatz 1 Satz 2, Absatz 2 Satz 2, § 32b Absatz 3, § 32c Absatz 3, § 32h Absatz 1 Satz 2, § 32i Absatz 2 Satz 1, § 32i Absatz 2 Satz 2 BDSG-E explizit zugelassen.
14 S. *Thüsing*, NZA 2011, 16, 19; kritisch auch *Beckschulze/Natzel*, BB 2010, 2368, 2374.
15 S. bei *Tinnefeld/Petri/Brink* (die die Regelung im Grundsatz befürworten), MMR 2010, 727, 729.
16 So aber *Beckschulze/Natzel*, BB 2010, 2368, 2374

seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Das gilt auch für Beschäftigte.[17]

Inhaltlich ist nicht einzusehen, warum Beschäftige selbst bei schweren Pflichtverletzungen des Arbeitgebers zunächst bei diesem um Abhilfe nachsuchen sollen.[18] In derartigen Fällen besteht das Risiko, dass die Beschäftigten von der Wahrnehmung ihrer datenschutzrechtlich garantierten Betroffenenrechte (die gemäß § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können) abgeschreckt werden. Europarechtlich sieht Art. 28 Abs. 4 der Datenschutzrichtlinie ein vorheriges internes Beschwerdeverfahren nicht vor, sondern gibt jedermann das Recht, sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden.[19]

§ 32l Abs. 4 BDSG-E sollte folglich ersatzlos gestrichen werden.

3.3.2 Whistleblower

Der Regierungsentwurf enthält keine ausdrückliche Regelung für „Whistleblower“. Das hat zur Folge, dass sich die Einrichtung einer Stelle für anonyme Beschwerden als rechtlich problematisch erweist, da keine Datenerhebungs- und -verarbeitungsbefugnis für die so erhobenen Daten existiert.

Rechtspolitisch wäre eine solche Regelung wünschenswert,[20] auch wenn – oder gerade weil – über den konkreten Inhalt unterschiedliche Auffassungen herrschen. Die Bedeutung hat sich gerade bei den so genannten Datenskandalen der letzten Jahre gezeigt, die zum Teil durch Whistleblower aufgedeckt wurden.[21] Für die USA sind entsprechende Regelungen nach dem Sarbanes-Oxley Act vorgeschrieben. Daneben hat auch die Art. 29-Gruppe ausdrücklich festgestellt, dass Whistleblower-Regelungen mit der Datenschutzrichtlinie vereinbar sind.[22] Eine entsprechende Norm sollte dabei auch diejenigen Daten erfassen, die im Betrieb über Dritte (insbesondere Kunden) verarbeitet werden.

---

17 S. *Petri*, in: Simitis (Fn. 4), § 38 Rn 3 m.w.N.; *Tinnefeld/Petri/Brink*, MMR 2010, 727, 735.

18 Kritisch auch *Wybitul*, Handbuch Datenschutz im Unternehmen, 2011, 523.

19 S.a. Stellungnahme der Neuen Richtervereinigung (abrufbar unter http://www.nrv-net.de/downloads_stellung/89.pdf), S. 9; Stellungnahme des ULD Schleswig-Holstein (abrufbar unter https://www.datenschutzzentrum.de/arbeitnehmer/20101012-stellungnahme.html).

20 Ebenso z.B. *Gola*, RDV 2010, 97, 99; *Tinnefeld/Petri/Brink*, MMR 2010, 727, 735; *Kort*, MMR 2011, 294, 296 f.; § 24 des Entwurfs von BÜNDNIS 90/DIE GRÜNEN enthält einen entsprechenden Vorschlag.

21 S. *Tinnefeld/Petri/Brink*, MMR 2010, 727, 728.

22 S. Art. 29-Gruppe, WP 117, Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität, abrufbar unter

3.3.3 Verbandsklagerecht

Im Konfliktfall ist das betriebliche Umfeld ein typisches Beispiel eines Machtgefälles, welches das Risiko birgt, dass Betroffene von Rechten, die ihnen zustehen, keinen Gebrauch machen. Selbstverständlich muss dem Einzelnen die subjektive Verfolgung von Rechten erhalten bleiben. Dies wird jedoch kaum je (und in Zukunft noch weniger)[23] zur Durchsetzung des Datenschutzrechts in größeren Zusammenhängen wie betrieblichen Abläufen führen. Hier bedarf es der Unterstützung durch professionelle Institutionen und Organisationen. Dies wird durch die Datenschutzbehörden in Teilen geleistet; diese arbeiten aber weithin an der Kapazitätsgrenze.

Zur Lösung bietet sich ein Rückgriff auf das Verbandsklagerecht an, das etwa im Verbraucher- und Umweltschutzrecht seit vielen Jahren ein anerkanntes Instrument zur kollektiven Wahrnehmung von Interessen ist. Ein derartiges Recht (etwa für Betriebsräte und Gewerkschaften) sollte auch bei Verstößen gegen die Datenschutzvorschriften im Betrieb gesetzlich verankert werden.[24] Zur Absicherung könnte ein Zulassungsverfahren eingeführt werden, in dem – ähnlich wie im Umweltrecht – Nachhaltigkeit, Zielrichtung und Dauerhaftigkeit der Tätigkeit überprüft werden.

3.4 Konzerndatenschutz

Die fehlende Regelung einer Verarbeitungs- und Übermittlungsbefugnis im Konzern und die Frage nach dem Verhältnis zur Auftragsdatenverarbeitung sind zwei der drängendsten Probleme des betrieblichen Datenschutzes, insbesondere weil die binäre Trennung zwischen Auftragsdatenverarbeitung und Funktionsübertragung in weiten Teilen nicht mehr der betrieblichen Wirklichkeit entspricht.

Insofern ist es einerseits zwar misslich, dass der Entwurf hierzu keine Regelung enthält.[25] Anderseits ist jedoch zu bedenken, dass nicht nur Zweifel an der europarechtlichen Zulässigkeit eines derartigen Vorhabens bestehen,[26] sondern die eigentlichen Probleme zudem bei solchen internationalen Konzernen bestehen, denen selbständige Unternehmen mit Sitz außerhalb des Geltungsbereichs der europäischen Datenschutzrichtlinie angehören. Abhilfe kann hier daher wohl nur auf europäischer Ebene geleistet werden.

---

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf: Basis ist Art. 7 (f) der Datenschutzrichtlinie.

23 S. perspektivisch *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, 198 f.

24 Vergleichbar dem Entwurf von BÜNDNIS 90/DIE GRÜNEN, § 23.

25 S.a. *Kort*, MMR 2011, 294, 297 f.; aus Perspektive der Aufsichtsbehörden s. den Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“, abrufbar unter http://www.rp-darmstadt.hessen.de/?cid=f8a680608c6fea87bbe406d0cc8eb0d0.

26 Z.B. *Thüsing*, NZA 2011, 16, 19, der allerdings nationale Spielräume bejaht.

Entscheidend gegen eine Regelung spricht im vorliegenden Zusammenhang schließlich, dass es beim Konzerndatenschutz zwar auch, aber nicht nur um die Verwendung von Daten der Beschäftigten geht – betroffen sind vielmehr auch die Daten von Kunden, Vertragspartnern, Behörden und sonstigen Dritten. Dass der Konzerndatenschutz einer Lösung bedarf, steht somit außer Frage, eine entsprechende Regelung sollte aus den genannten Gründen aber nicht gesondert in einem Abschnitt über den Beschäftigtendatenschutz erfolgen.

3.5 Bewerberauswahl und soziale Netzwerke

§ 32 Abs. 6 Satz 2 und Satz 3 BDSG-E bemühen sich um eine sachgerechte Lösung des Problems der sozialen Netzwerke. Die Norm ist aber in mehrfacher Hinsicht zweifelhaft. Soweit sie an schutzwürdige Interessen des Beschäftigten anknüpft, stellt sich das Problem, dass sich das Vorliegen derartiger Interessen jenseits des gesetzlich geregelten Falles der nicht-beruflichen sozialen Netzwerke regelmäßig erst aus der Information ergeben wird, die im Internet verfügbar ist. In diesem Fall hat der Arbeitgeber die relevante Information jedoch bereits zur Kenntnis genommen.

Soweit § 32 Abs. 6 Satz 3 BDSG-E dem Arbeitgeber untersagt, Daten aus privaten sozialen Netzwerken zu erheben, ist die Norm de facto unkontrollierbar[27] und wird deshalb mutmaßlich Placebo bleiben. Ein Effekt könnte höchstens insoweit eintreten, als entsprechende Informationen in gerichtlichen Verfahren nicht verwertet werden dürfen[28] oder Mitarbeiter in Personalabteilungen sich unter Berufung auf die Vorschrift gegen Anweisungen zur Erhebung von Daten aus privaten sozialen Netzwerken zur Wehr setzen können.

Insgesamt sendet § 32 Abs. 6 Satz 3 BDSG-E angesichts seiner fehlenden Durchsetzbarkeit ein falsches Signal an die Betroffenen: Es wird suggeriert, man könnte die Verwendung von Informationen dauerhaft kontrollieren, die sich einmal im Internet befinden. Dies wird zunehmend unrealistisch, und das gilt auch für die vorgeblich geschützten Räume „privater“ sozialer Netzwerke, in denen häufig hunderte von Kontakten Zugriff auf die Daten haben und diese weitergeben können.

3.6 Organisatorische und technische Seiten des Datenschutzes

Der Bereich der organisatorischen und technischen Aspekte des Datenschutzes ist im Regierungsentwurf deutlich zu schwach ausgeprägt. Erwägenswert erscheint der weitere Ausbau folgender Aspekte:

---

[27] Ebenso Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
[28] S. *Raif*, ArbRAktuell 2010, 617.

- Die Dokumentationspflichten, die derzeit lediglich in § 32d Abs. 3 Satz 2, § 32e Abs. 5 Satz 2 und Satz 3 BDSG-E gesetzlich verankert sind. Derartige Verpflichtungen sollten auch bei anderen eingriffsintensiven Maßnahmen vorgesehen werden.
- Die Vorabkontrolle nach § 4d Abs. 5 BDSG wird nur in ausgewählten Bereichen angeordnet und begegnet in der Art der Anordnung weiteren Bedenken. Der Anwendungsbereich der Norm beschränkt sich nämlich auf besondere Risiken, die etwa bei heimlicher Kontrolle oder bestimmten technisch elaborierten Maßnahmen wie „intelligenter" Videoüberwachung vorliegen.[29] Das wird beispielsweise in den Fällen des § 32e Abs. 5 BDSG-E nicht zwingend der Fall sein. Außerdem dürfte im Betrieb häufig die Ausnahmeregelung des § 4d Abs. 5 Satz 2 2. HS Var. 2 BDSG greifen.[30] Beide Aspekte werden die Verweisung substantiell beschränken. Wenn insoweit eine Rechtsfolgenverweisung beabsichtigt war, sollte dies entsprechend dem Vorschlag des Bundesrates[31] klargestellt werden. Vorzugswürdig wäre es demgegenüber allerdings, eine allgemeine Vorschrift zur Vorabkontrolle einzuführen.[32]

Schließlich gibt es einen Aspekt, der im Regierungsentwurf nicht beachtet wird, nämlich die Frage besonderer Datensicherheitsmaßnahmen. Bei einer Einfügung der Regelungen zum Beschäftigtendatenschutz in das Bundesdatenschutzgesetz greift insoweit die allgemeine Vorschrift des § 9 BDSG mit der entsprechenden Anlage. Die Anforderungen dieser Norm (und damit die Regelungstechnik über eine Generalklausel, die jede Form der Verarbeitung personenbezogener Daten erfasst) hat das Bundesverfassungsgericht allerdings in der Entscheidung zur Vorratsdatenspeicherung als nicht hinreichend beurteilt.[33] Die Anforderungen, die das Gericht insoweit aufgestellt hat, sind zwar nicht direkt auf den Umgang mit Daten im Betrieb anwendbar. In beiden Fällen geht es aber um die Speicherung von Daten mit erheblicher Sensibilität und von vielen Betroffenen (Streubreite), teilweise (bei der Speicherung von Telekommunikations-Verkehrsdaten) sogar um identische Datenarten. Insofern sind auch an die Maßnahmen der Datensicherheit im Bereich der nur mittelbaren Wirkung der Grundrechte (wie im Betrieb) hohe Anforderungen zu stellen. In der Folge der Entscheidung des Bundesverfassungsgerichts darf sich der Gesetzgeber

---

[29] Dazu *Hornung/Desoi*, K&R 2011, 153, 158.
[30] Stellungnahme des ULD Schleswig-Holstein (Fn. 19)
[31] BT-Drs. 17/4230, S. 34.
[32] Z.B. entsprechend dem Vorschlag von BÜNDNIS 90/DIE GRÜNEN, § 29.
[33] BVerfGE 125, 260; zur Frage der Datensicherheit s. *Roßnagel/Bedner/Knopp*, DuD 2009, 536 ff.; *Hornung/Schnabel*, DVBl. 2010, 824, 829.

insoweit nicht auf die betriebliche Praxis verlassen, sondern hat vielmehr selbst Vorgaben zu machen.[34]

3.7 Der Regelungskomplex der Überwachung und Kontrolle

Es ist zu begrüßen, dass sich die Entwürfe mit der besonders konfliktträchtigen Frage der Überwachung und Kontrolle der Beschäftigten im Detail auseinandersetzen und dabei auch relevante Fragen aus der Praxis entscheiden. Allerdings sollte man sich nicht der Hoffnung hingeben, dass damit ein Maß an substantieller Rechtsklarheit geschaffen wird, das die Ausfüllung durch die Arbeitsgerichtsbarkeit überflüssig macht. An vielen Stellen enthält der Regierungsentwurf etwa wertungs- und ausfüllungsbedürftige Begriffe wie „betriebliche Gründe“, „schwerwiegende Pflichtverletzung“, „erforderlich“, „unerlässlich“, „Kernbereich privater Lebensgestaltung“, „Anhaltspunkte für schutzwürdige Interessen der Betroffenen“ etc. Dies wird dazu führen, dass die Festlegung wichtiger Grundlinien für die Praxis schließlich doch Aufgabe der Gerichte sein wird. So bleibt etwa die genaue Bedeutung des Kernbereichsschutzes offen: § 32e Abs. 7 BDSG-E nennt nur den Begriff, und die Begründung[35] enthält keine weiteren Erläuterungen. Die relativ enge Definition des Bundesverfassungsgerichts[36] wird jedenfalls nur selten einschlägig sein.

Im Folgenden sollen einige Problempunkte dieses Regelungskomplexes bewertet werden.

3.7.1 Compliance und Screening

Die Regelung in § 32d Abs. 3 BDSG-E stellt eine Gewichtungsverschiebung zulasten des Schutzes der Beschäftigendaten dar. Die Gesetzesbegründung betont zwar zu Recht, dass sich Pflichten der Unternehmen zur Korruptionsbekämpfung und Compliance teilweise aus Spezialgesetzen ergeben.[37] Bislang ist aber offen – und wird vielfach bestritten – ob diese Verpflichtungen den datenschutzrechtlichen Pflichten der Arbeitgeber gegenüber den Beschäftigen vorgehen, oder ob umgekehrt das Datenschutzrecht gerade Grenzen für derartige Compliance-Vorschriften enthält. Der Entwurf gibt hier auf Seiten des Beschäftigendatenschutzes nach. Die in der Öffentlichkeit bekannt gewordenen Missbrauchsfälle zeigen indes, dass dieser Komplex einer deutlich einengenderen Regelung bedarf als der Entwurf dies bislang vorsieht.

Zunächst ist die Regelung in § 32d Abs. 3 BDSG-E nicht konsistent mit den Begrifflichkeiten und Zielrichtungen der datenschutzrechtlichen Konzepte der Anonymität und Pseudo-

---

[34] S. etwa die Vorschläge im Entwurf der SPD (§ 16 und § 17) und von BÜNDNIS 90/DIE GRÜNEN (§ 5).
[35] BT-Drs. 17/4230, S. 19.
[36] Verweis bei *Tinnefeld/Petri/Brink*, MMR 2010, 727, 732.
[37] BT-Drs. 17/4230, S. 18.

nymität.[38] Gemäß § 3 Abs. 6 BDSG bedeutet „anonymisieren“ das „Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“. Ausweislich § 32d Abs. 3 Satz 2 BDSG-E ist dies aber gerade nicht gemeint, da die Daten offenbar so behandelt werden sollen, dass eine Re-Personalisierung noch möglich ist. Pseudonymisieren meint gemäß § 3 Abs. 6a BDSG das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. Bei der Regelung in § 32d Abs. 3 BDSG-E wird indes weder das eine noch das andere beabsichtigt. Es kann deshalb keine Rede davon sein, dass die Pflicht zur Anonymisierung die Rechte der Beschäftigten hinreichend wahrt.[39] Die Begrifflichkeiten suggerieren vielmehr eine datenschutzfreundliche Lösung, die de facto nicht erreicht wird.

Der Regierungsentwurf enthält überdies keine definierte Anlassbeschreibung oder Verdachtsschwelle. Dies ist ausweislich der Gegenäußerung auch so beabsichtigt,[40] das heißt die Norm ist so zu lesen, dass das beschriebene Vorgehen anlasslos und dauerhaft zulässig ist. Dies ist eine potentiell außerordentlich weitreichende Verarbeitungsbefugnis, da – wie beschrieben – das Verfahren gerade weder eine Anonymisierung noch eine Pseudonymisierung im Rechtssinn beinhaltet und deshalb auch keinen echten Schutz bietet.

Wenn die Norm beibehalten wird, sollte sie enger gefasst werden. Hierfür bieten sich mehrere Möglichkeiten an:

- Um eine ubiquitäre, anlasslose und dauerhafte Kontrolle zu verhindern, sollte entsprechend dem Vorschlag des Bundesrates das Vorliegen tatsächlicher Anhaltspunkte verlangt[41] und die Variante der schweren Pflichtverletzung gestrichen werden. Keinesfalls sollte Stimmen gefolgt werden, die den Anwendungsbereich sogar noch über den der schweren Pflichtverletzung hinaus und in den präventiven Bereich hinein erweitern wollen.[42]

- Falls die anlasslose Datenerhebung beibehalten wird, sollte sie zumindest insoweit beschränkt werden, dass sie nur für besonders gefahrgeneigte Arbeitsbereichen wie Beschaffungsabteilungen zugelassen wird. Man kann dies aus Gesichtspunk-

---

38 S. *Heinson/Sörup/Wybitul*, CR 2010, 751, 755; *Schuler*, DuD 2011, 126, 127 f.; Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
39 So aber *Forst*, NZA 2010, 1043, 1046 f.
40 BT-Drs. 17/4230, S. 40.
41 BT-Drs. 17/4230, S. 32; ebenso *Rasmussen-Bonn/Raif*, GWR 2011, 80; Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
42 So aber *Kort*, Der Betrieb 2011, 651, 652 f.

ten der Verhältnismäßigkeit auch aus dem aktuellen Entwurf herauslesen.[43] Es sollte aber explizit geregelt werden.

- Ein allgemeines und verdachtsloses Screening von Beschäftigtendaten ist allenfalls dann zu rechtfertigen, wenn effektive technische und organisatorische Sicherungsmittel sowie eine Vorabprüfung[44] eingesetzt werden. Diese Anforderung erfüllt der Entwurf nicht.
- Eine echte Pseudonymisierung kann nur erreicht werden, wenn die Daten bei Dritten ausgewertet werden und der Arbeitgeber weder faktische noch rechtliche Möglichkeiten des Zugriffs auf die Zuordnungsregel hat und sicherstellt, dass lediglich konkrete Verdachtsfälle in den Verantwortungsbereich des Arbeitgebers gelangen.[45] Insofern wäre die Einbeziehung vertrauenswürdiger Dritter zu erwägen.
- Eine echte Anonymisierung kann ebenfalls eingesetzt werden, aber nicht in dem Sinne, in dem der Entwurf dies vorsieht. Anonyme Daten können – etwa zur Bestimmung korruptionsgefährdeter Arbeitsbereiche – analysiert werden, wenn keine Möglichkeit der Re-Individualisierung besteht. Stattdessen können im Fall von Auffälligkeiten (pseudonyme) Stichproben erfolgen.[46]

3.7.2 Videoüberwachung

Die Absicht einer Regelung der Videoüberwachung nicht öffentlich zugänglicher Bereiche ist zu begrüßen, weil es bislang an einer gesetzlichen Normierung hierzu fehlt.[47] Besonders positiv zu werten ist dabei die Anwendung auch auf Attrappen (§ 32f Ab s. 1 Satz 3 BDSG-E), deren subjektive Wirkung auf die Beschäftigten vielfach mit der einer echten Kamera identisch sein wird.

An einigen Stellen bedarf der Regierungsentwurf jedoch der Überarbeitung. Bei den Zulässigkeitsalternativen sollten § 32f Abs. 1 Satz 1 Nr. 2 und Nr. 7 BDSG-E gestrichen werden. Die Wahrnehmung des Hausrechts (Nr. 2) betrifft typischerweise nicht das Beschäftigtenverhältnis, sondern Dritte. Hinsichtlich Nr. 7 ist zumindest eine Präzisierung dahin geboten, dass eine Videoüberwachung nicht etwa standardmäßig zur Kontrolle der Arbeitsqualität zulässig ist. Dies wäre mit den Persönlichkeitsrechten der Beschäftigten nicht zu vereinbaren.[48] Dass die Gesetzesbegründung von den sieben Alternativen der Zulässigkeit lediglich eine (Nr. 3) etwas näher erläutert, ist wenig hilfreich. Als Ergänzung der

---

43 S. *Heinson/Sörup/Wybitul*, CR 2010, 751, 755.
44 Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
45 In diese Richtung *Heinson/Sörup/Wybitul*, CR 2010, 751, 755.
46 S. *Brink*/*Schmidt*, MMR 2010, 592, 594 f.
47 6b BDSG betrifft nur öffentlich zugängliche Bereiche.
48 Kritisch auch *Viotto*, AuR 2010, 433, 433; ULD Schleswig-Holstein (Fn. 19); *Seifert*, DuD 2011, 98, 103.

Zulässigkeitstatbestände wäre ein expliziter Ausschluss des Einsatzes zur Leistungskontrolle angemessen.[49]

Die Auflistung überwachungsfreier Räume in § 32f Abs. 2 BDSG-E sollte um einen expliziten Schutz auch von Pausenräumen ergänzt werden.[50] Hiergegen spricht jedenfalls nicht, dass derartige Räume von mehreren Personen genutzt werden;[51] selbstverständlich kann auch in diesem Fall ein so großes Schutzbedürfnis bestehen, dass der Ausschluss der Kontrolle gerechtfertigt ist. Keinesfalls sollten umgekehrt die Varianten der Sanitär-, Umkleide- und Schlafräume gestrichen werden.[52]

Zu der kontrovers diskutierten Frage des Verbots einer heimlichen Videoüberwachung ist zu bemerken: Dieses Verbot gilt nur für den Arbeitgeber. Soweit der Verdacht auf eine entsprechende Straftat vorliegt, kann dieser sich selbstverständlich an Staatsanwaltschaft und Polizei wenden. Bei Vorliegen eines entsprechende Anfangsverdachts dürfen dann gemäß § 100h Abs. 1 Satz 1 Nr. 1 StPO auch ohne Wissen der Betroffenen Bildaufnahmen hergestellt werden.

Sollte eine Änderung des absoluten Verbots erwogen werden, so wären aus verfassungsrechtlicher Sicht jedenfalls hohe Anforderungen zu formulieren: Zum einen für die materiellen Eingriffsvoraussetzungen (konkrete Anhaltspunkte für eine Straftat),[53] zum anderen für organisatorische Absicherungen: Beteiligungen des Betriebsrats, Dokumentationspflichten (Vorabkontrolle, Dokumentation des Überwachungsanlasses und der Durchführung der Überwachung) sowie für den Fall der Nichteinhaltung der materiellen und prozessualen Anforderungen ein explizites Beweisverwertungsverbot sowie die Aufnahme einer besonderen Sanktionsvorschrift in den Katalog des § 43 BDSG.

Abschließend bleibt anzumerken, dass bei Umsetzung dieser Anforderungen im Wesentlichen Anwendungsfälle verbleiben, die in den Zuständigkeitsbereich von Staatsanwaltschaft und Polizei fallen. Da insofern auch eine Durchführung der Maßnahme durch diese staatlichen Stellen möglich (und unter rechtsstaatlichen Gesichtspunkten sogar vorzugswürdig) ist, erscheint eine Veränderung des Entwurfs insgesamt verzichtbar.

---

[49] S. Stellungnahme der Neuen Richtervereinigung (Fn. 19), S. 7; ebenso der Entwurf von BÜNDNIS 90/DIE GRÜNEN, § 10 Abs. 1 Satz 1; a.A. *Kort*, MMR 2011, 294, 296.

[50] Ebenso der Vorschlag des Bundesrates, BT-Drs. 17/4230, S. 34.

[51] S. *Seifert*, DuD 2011, 98, 104 f.

[52] So aber *Heinson/Sörup/Wybitul*, CR 2010, 751, 757.

[53] Diese Verengung gegenüber der Rechtsprechung des BAG erscheint geboten. Das Gericht hat – zu weitgehend – die heimliche Überwachung auf Basis der bisherigen Rechtslage auch bei schweren Pflichtverletzungen für zulässig erklärt, s. BAG NJW 2003, 3436, 3437.

3.7.3 Biometrie

§ 32h BDSG-E ist so weit und generisch gefasst, dass auf ihn in der Form des Entwurfs verzichtet werden kann. Er bietet gegenüber den Regelungen der §§ 32c, 32d BDSG-E de facto keine präziseren Leitlinien Die Komplexität der verschiedenen biometrischen Charakteristika, Systeme und Verfahren und der mit ihnen verbundenen Rechtsfragen im Betrieb[54] ist so groß, dass mit einer derart allgemein gefassten Norm wenig gewonnen ist. Zumindest müssten bestimmte zulässige oder unzulässige Einsatzfelder oder Einsatzmodalitäten beschrieben und Regeln für den Umgang mit biometrischen Daten vorgegeben werden.

3.7.4 Telekommunikationsdienste

§ 32i BDSG-E befasst sich nur mit einer Hälfte des schwierigen Problems der Kontrolle von Telekommunikationsdiensten am Arbeitsplatz, und zwar mit der weniger problematischeren.

Der Fall der ausschließlich beruflichen oder dienstlichen Nutzung ist zwar ebenfalls komplex, im Ergebnis aber unproblematischer als die Überwachung von Diensten, wenn eine private Nutzung gestattet ist. Der von § 32i BDSG-E geregelte Fall ist in der Praxis der bei weitem leichter zu bewältigende, der aber insbesondere bei der Internetnutzung immer unrealistischer wird. Die eigentlichen Probleme und kontroversen Rechtsfragen entstehen dann, wenn eine private Nutzung ganz oder in Grenzen zugelassen ist. Hierzu schweigt der Entwurf.[55] Auch die Gesetzesbegründung enthält noch nicht einmal Anhaltspunkte zur Lösung des Problems. Die Gegenäußerung[56] verweist (de lege lata zutreffend) auf das Telekommunikationsgesetz, dessen Regelungen aber ersichtlich für das Problem der privaten Nutzung betrieblicher Telekommunikationsanlagen nicht geschaffen wurden und für dieses Problem auch nicht adäquat sind.

§ 32i Abs. 4 Satz 2 BDSG-E sollte gestrichen werden. Weder aus dem Gesetz noch aus der Begründung ist ersichtlich, was genau mit „private Daten“ gemeint ist. Ein anerkennenswertes Interesse von Arbeitgebern an der Kenntnisnahme privater Daten und Inhalte der Telekommunikation ist nicht ersichtlich.[57]

---

[54] S. z.B. *Hornung/Steidle*, AuR 2005, 201 ff.; *Hornung*, AuR 2007, 398 ff.; allgemein zu den Verhältnismäßigkeitskriterien *Hornung*, Die digitale Identität, 2005, 178 ff.

[55] Kritisch dazu z.B. *Heinson/Sörup/Wybitul*, CR 2010, 751, 757 ff.; *Kort*, MMR 2011, 294 f.; *Wybitul* (Fn. 18), 503.

[56] BT-Drs. 17/4230, S. 42.

[57] Ebenso *Forst*, NZA 2010, 1043, 1048.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 E

Prof. Dr. Gregor Thüsing, LL.M. (Harvard), Universität Bonn

Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes BT-Drucks. 17/4230 et. alt.

I. Ein wichtiger Schritt nach vorne

Zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Regelung des Beschäftigtendatenschutzes gab es bereits erste kritische Stimmen. Insbesondere der Bundesrat hat in seiner Stellungnahme umfangreiche Änderungen eingefordert.[1] Doch bei aller Kritik im Detail ist der Entwurf ein wesentlicher Schritt nach vorne hin zu einem besseren Beschäftigtendatenschutz. Beschäftigtendatenschutz ist Persönlichkeitsschutz; Persönlichkeitsschutz ist ernst zu nehmen. Die Bundesregierung kommt nun einer Forderung nach, die seit mehr als 30 Jahren erhoben wird; detaillierte gesetzliche Regelungen zum Arbeitnehmerdatenschutz Die Regierungskoalition hat sich in ihren Koalitionsvereinbarungen darauf geeinigt „praxisgerechte Regelungen für Bewerber und Arbeitnehmer [zu] schaffen und gleichzeitig Arbeitgebern eine verlässliche Regelung für den Kampf gegen Korruption an die Hand [zu] geben."[2] Gemessen an dieser Messlatte – Rechtssicherheit und Praxistauglichkeit – kann der vorliegende Entwurf wesentliche Impulse für einen besseren und bewussteren Umgang mit Daten in der betrieblichen Wirklichkeit geben. All dies vorweg soll daher nicht hervorgehoben werden, wo der Entwurf uneingeschränkt zu begrüßen ist, sondern nur auf die Stellen hingewiesen werden, wo Verbesserungen möglich sind.

II. Anwendungsbereich

Missverständlich ist zunächst die Regelung des Anwendungsbereichs. Der neue § 27 Abs. 3 BDSG-E macht deutlich, dass es sich um Datenverarbeitung von Beschäftigtendaten „für Zwecke des Beschäftigtenverhältnisses" handeln soll.

[1] BT-Drucksache 535/10 v. 05.11.10.
[2] Koalitionsvertrag zwischen CDU, CSU und FDP S. 106, abrufbar unter www.cdu.de/doc/pdfc/091026-koalitionsvertrag-cducsu-fdp.pdf

Dem § 27 wird folgender Absatz 3 angefügt:

„(3) Für das Erheben, Verarbeiten und Nutzen von Beschäftigtendaten durch den Arbeitgeber für Zwecke eines früheren, bestehenden oder zukünftigen Beschäftigungsverhältnisses gelten die Vorschriften des zweiten, dritten und vierten Unterabschnitts. Satz 1 gilt auch, wenn Beschäftigtendaten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden."

Entsprechend lautet dann auch die Abschnittsüberschrift vor den §§ 32 ff. BDSG-E. Mit dieser Begrenzung passen aber zahlreiche Rechtfertigungsvorschriften der §§ 32 ff BDSG-E nicht, die hier Rechtfertigungstatbestände anführen, die sich gerade nicht auf Zwecke des Beschäftigtenverhältnisses beziehen, nicht, s. etwa § 32f Abs. 1 Nr. 1,2,3,5,6,7 BDSG-E:

§ 32f
Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung nicht öffentlich zugänglicher Betriebsgelände, Betriebsgebäude oder Betriebsräume (Betriebsstätten) mit optisch-elektronischen Einrichtungen (Videoüberwachung), die auch zur Erhebung von Beschäftigtendaten geeignet ist, ist nur zulässig

1. zur Zutrittskontrolle,
2. zur Wahrnehmung des Hausrechts,
3. zum Schutz des Eigentums,
4. zur Sicherheit des Beschäftigten,
5. zur Sicherung von Anlagen,
6. zur Abwehr von Gefahren für die Sicherheit des Betriebes,
7. zur Qualitätskontrolle,

soweit sie zur Wahrung wichtiger betrieblicher Interessen erforderlich ist und wenn nach Art und Ausmaß der Videoüberwachung keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Datenerhebung überwiegen. Der Arbeitgeber hat den Umstand der Videoüberwachung durch geeignete Maßnahmen erkennbar zu machen. § 6b Absatz 3 und 4 gilt entsprechend. Die Sätze 1 und 2 gelten entsprechend, wenn von einer Einrichtung lediglich der Anschein einer Videoüberwachung ausgeht.

Andere Bespiele sind § 32i Abs. 1 Nr. 1 und 2 BDSG-E. Das kann nicht stimmen, denn für andere Zwecke als Zwecke des Beschäftigtenverhältnis sollen diese Normen ja gar nicht anwendbar sein, können also auch keine Rechtfertigung für diese Fälle aussprechen

III. Einstellung

§ 32 Abs. 1 BDSG-E enthält eine Regelung zur Datenerhebung, die systematisch einerseits wohl zu

weit, andererseits zu eng ist: „Der Arbeitgeber darf den Namen, die Anschrift, die Telefonnummer und die Adresse der elektronischen Post eines Beschäftigten iSd § 3 Abs. 11 Nr. 7 1 Alt. vor Begründung eines Beschäftigungsverhältnisses erheben. Weitere personenbezogene Daten darf er erheben, soweit die Kenntnis dieser Daten erforderlich ist, um die Eignung des Beschäftigten für die vorgesehenen Tätigkeiten festzulegen. Er darf zu diesem Zweck insbesondere Daten über die fachlichen und persönlichen Fähigkeiten, Kenntnisse und Erfahrung sowie über die Ausbildung und über den bisherigen beruflichen Werdegang des Beschäftigten erheben“. Name, Anschrift, Telefonnummer und Adresse der Bewerber werden damit zu gänzlich ungeschützten Daten. Solch vogelfreie Daten kannte das BDSG bislang nicht. Das überrascht, warum sollte der Arbeitgeber diese Speicherung etwa vornehmen, wenn er gar nicht beabsichtigt, einen Bewerber einzustellen? Soweit er im Übrigen Daten erheben kann, allein, um die Eignung des Bewerbers zu beurteilen, greift dies zu kurz. § 32 BDSG in der aktuellen Fassung spricht richtig nicht von der Erforderlichkeit zur Prüfung der Eignung, sondern von der Erforderlichkeit für die Entscheidung über die Einstellung. Das ist ein anderer Bezug. Darf etwa zukünftig nicht mehr nach den Gehaltsvorstellungen im Vorfeld der Vertragsanbahnung gefragt werden? Auch dies ist eine Datenerhebung und über die Eignung des Bewerbers sagt sie nichts, viel mehr über seine Bereitschaft, seinerseits ein Beschäftigungsverhältnis zu begründen. Eine kluge Rechtsprechung mag zukünftig entscheiden, dass auch die Bereitschaft, für ein bestimmtes Entgelt zu arbeiten, Bestandteil der Eignung des Mitarbeiters ist. Dies würde zum richtigen Ergebnis führen – denn alles andere wäre sinnwidrig –, würde dem Wortlaut des Gesetzes aber widersprechen. Der Gesetzgeber sollte sagen, was er meint, und es beim bisherigen Bezugspunkt des § 32 BDSG belassen.

Dasselbe gilt für § 32a Abs. 2 BDSG. Danach darf der Arbeitgeber Eignungstests durchführen. Der ist denkbar weit gefasst: „Der Arbeitgeber darf die Begründung des Beschäftigungsverhältnisses von einer sonstigen Untersuchung oder Prüfung abhängig machen, wenn die Untersuchung oder Prüfung wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung erforderlich ist, um festzustellen, ob der Beschäftigte zum Zeitpunkt der Arbeitsaufnahme für die vorgesehenen Tätigkeiten geeignet ist (Eignungstest). Der Beschäftigte muss in den Eignungstest nach Aufklärung über dessen Art und Umfang sowie in die Weitergabe des Ergebnisses des Eignungstests an den Arbeitgeber eingewilligt haben. Der Eignungstest ist nach wissenschaftlich anerkannten Methoden durchzuführen, sofern solche bestehen. Dem Beschäftigten ist das Ergebnis des Eignungstests mitzuteilen. Sind Eignungstests ganz oder teilweise durch Personen durchzuführen, die einer beruflichen Schweigepflicht unterliegen, darf dem Arbeitgeber insoweit nur mitgeteilt werden, ob der Beschäftigte nach dem Ergebnis des Eignungstests für die vorgesehenen Tätigkeiten geeignet ist“. Dieser Test ist entsprechend § 32 Abs. 2 S. 3 BDSG-E „nach wissenschaftlich anerkannten Methoden durchzuführen,

sofern solche bestehen“. Wie ist es zukünftig mit der Arbeitsprobe eines Mitarbeiters? Soll die nur zulässig sein, wenn sie wissenschaftlichen Kriterien folgt oder der Arbeitgeber nachweisen kann, dass es für diese Art von Prüfung keine wissenschaftlichen Kriterien gibt? Die Formulierung des Gesetzes öffnet Spielraum für zahlreiche Klagen. Ein Bewerber, der abgewiesen wurde, mag Schadensersatz wegen Verletzung des Rechts auf informationelle Selbstbestimmung einklagen, weil ein Eignungstest, dem er unterzogen wurde, zwar vom Arbeitgeber als solide angesehen wurde, aber nicht wissenschaftlich untermauert wurde. Wieso soll einem Arbeitgeber, der selbst nicht wissenschaftlich arbeitet, die Verpflichtung auferlegt werden, Eignungstests nur nach wissenschaftlichen Methoden durchzuführen?

Schließlich erstaunt § 32 Abs. 2 BDSG-E. Danach darf nur nach Vorstrafen gefragt werden, wenn der Maßstab des § 8 AGG erfüllt wäre. Der aber ist ganz und gar eng. Entscheidend ist, ob die Tätigkeit mit diesem Merkmal überhaupt ausgeübt werden kann. *Testfrage* ist: Wäre die Stelle dauerhaft unbesetzt geblieben, wenn sich nur Arbeitnehmer ohne das geforderte Differenzierungsmerkmal beworben hätten? Nur dort, wo das männliche oder weibliche Geschlecht, das Alter oder die Religion nicht bloß erwünschte Nebeneigenschaft ist, sondern der Arbeitnehmer gerade dafür bezahlt wird, es Bestandteil seiner entgoltenen Leistung ist, ist das Merkmal eine wesentliche und entscheidende berufliche Anforderung.[3] Danach dürfte die Frage nach Vorstrafen durchgängig ausgeschlossen sein, erst recht nach laufenden Ermittlungsverfahren. Denn ein Mensch kann sich ändern, und ihm zu unterstellen „Wer einmal klaut, klaut immer“ ist sicherlich unzulässig. Deshalb wird vorgeschlagen, diese beiden Merkmale aus § 32 Abs. 2 BDSG-E zu streichen. Das aktuelle Recht ist hier sehr viel vernünftiger.[4]

IV. Verdeckte Videoüberwachung

Die verdeckte Videoüberwachung soll nach § 32f Abs. 1 S. 2 BDSG-E generell unzulässig sein. Dies ist ein Novum des Arbeitnehmerdatenschutzes, dass nicht die Erhebung bestimmter Daten unzulässig sein soll, sondern allein bestimmte Mittel der Erhebung unabhängig von ihrer Erforderlichkeit und Verhältnismäßigkeit. Das Ergebnis kann kurios sein. Gerade weil die Videoüberwachung unzulässig wäre, wäre der Arbeitgeber ggf. berechtigt, weitergehende Eingriffe in das Recht auf informationelle Selbstbestimmung seiner Mitarbeiter zu tätigen. Gilt bereits jetzt, dass eine verdeckte Videoüberwachung nur zulässig ist, soweit es kein milderes Mittel zur Aufklärung gibt, wären zukünftig andere Mittel zulässig, die den Arbeitnehmer vielleicht stärker betreffen, aber ohne technische

[3] Ausführlich MünchKomm-*Thüsing,* § 8 AGG Rn. 10 m.w.N.
[4] LAG Hamm v. 10.3.2011 – 11 Sa 2266/10; HWK-*Thüsing,* 4. Aufl. 2010, § 123 BGB Rn. 13.

Hilfsmittel auskommen. Der Arbeitgeber dürfte daher unter Umständen einen Detektiv einstellen, der eine Observierung oder Nachfragen bei den Kollegen vornimmt, die den einen oder anderen Arbeitnehmer in ein schlechtes Licht rücken könnten. Dogmatisch richtig wäre es, nicht generell unzulässige Mittel zu schaffen, sondern allgemein den Maßstab der Verhältnismäßigkeit ernst zu nehmen und – wie in Vorentwürfen des neueren Rechts – die Verhältnismäßigkeit klar durch Vorgaben des Gesetzgebers zu strukturieren. Die Alternative wäre, die Polizei zu bitten, eine Videoüberwachung anzuordnen, was oftmals schon deswegen nicht erfolgreich sein wird, weil diese aus Opportunitätsgründen von einer Überwachung absehen kann. Im Übrigen ist es fraglich, ob der Arbeitgeber sich den Betriebsfrieden dadurch zerstören will, dass er die Polizei, unter Umständen sogar regelmäßig, in den Betrieb zur Aufklärung möglicher Straftaten einbezieht. Noch einmal: Was hier geschaffen wurde, ist rechtssystematisch falsch und rechtspolitisch kontraproduktiv: *es führt zu stärkeren Eingriffen in das Recht auf informationelle Selbstbestimmung, nicht schwächeren. Das bisherige Recht sollte daher beibehalten werden.*[5]

V. Betriebsvereinbarung als Rechtfertigung

Größerer Handlungsbedarf noch besteht bei der Betriebsvereinbarung als Instrument der Rechtfertigung einer Datenverarbeitung. Diese ist bislang in der Rechtsprechung des BAG als andere Rechtsvorschrift iSd § 4 Abs. 1 BDSG anerkannt.[6] Sie ist damit eigenständige Rechtfertigungsgrundlage und ist nicht am BDSG zu überprüfen (*sic*!). Grenzenlose Eingriffe in das Recht auf informationelle Selbstbestimmung der Beschäftigten sind damit dennoch nicht verbunden, haben doch die Betriebsparteien die Verantwortung, die Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu wahren, § 75 Abs. 2 BetrVG. Dieser Prüfungsmaßstab ist zwar durchaus ernst zu nehmen, führt aber nicht zu einer Übertragung der Regelung des BDSG eins zu eins. Insbesondere ist es den Betriebsparteien damit möglich, die materiellen Schutzkriterien des BDSG („Erforderlichkeit“ und „Verhältnismäßigkeit“) durch prozentuale Kriterien zu ersetzen: Ist eine Betriebsvereinbarung etwa dahin ausgelegt, dass bestimmte Datenverarbeitungen nur zulässig sind nach vorheriger Information, Konsultation, und Zustimmung des Betriebsrates, so führt dies im Regelfall zu einem angemessenen Umgang mit Arbeitnehmerdaten. Und der Arbeitgeber hat dann Rechtssicherheit, dass sein Verhalten zulässig ist und damit einen Anreiz zu einer solchen Betriebsvereinbarung zu kommen. Dies führt zu einem bewussten, überlegten und angemessenen Umgang mit Daten – und das ist gut so.

---

[5] Ausführlich BAG 26.8.2008 - 1 ABR 16/07 sowie LAG Köln v. 8.11.2010 - 6 Sa 817/10.

[6] BAG v. 27.5.1986 – 1 ABR 48/84, BAGE 52, 88; v. 30.8.1995 – 1 ABR 4/95, BAGE 80, 366; v. 20.12.1995 – 7 ABR 8/95, BAGE 82, 36; ; hierzu *Thüsing,* Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 102.

Dieser Anreiz könnte zukünftig nicht mehr bestehen. Allerdings ist eine Änderung des § 4 Abs. 1 BDSG geplant, die die bisherige Rechtsprechung zum BDSG scheinbar vollauf bestätigt. Dem § 4 Abs. 1 soll angefügt werden: „Andere Rechtsvorschriften im Sinne des Gesetzes sind Betriebs- und Dienstvereinbarung". In der Begründung heißt es dann in der Tat, dass die bisherige Rechtsprechung des BAG bestätigt werden soll. Dem widerspricht jedoch diametral die Begründung zum § 32l Abs. 4 BDSG-E. Danach darf von den Vorschriften dieses Abschnitts nicht zu Ungunsten der Beschäftigten abgewichen werden. Die Begründung hierzu verweist recht geschwätzig darauf, dass dies auch für Betriebs- und Dienstvereinbarungen gelten soll. Das eine ist mit dem anderen unvereinbar. Wenn Betriebsvereinbarungen eigenständige Rechtsvorschriften sind, wie es § 4 Abs. 1 BDSG ausdrücklich sagt, dann kann sie nicht am BDSG gemessen werden - ebenso wie andere (staatliche) Gesetze, die eine Spezialnorm gegenüber dem BDSG darstellen, nicht am Maßstab des BDSG ihrerseits überprüft werden. Würde man die Erläuterung zu § 32 l Abs. 4 BDSG-E ernst nehmen, so wäre die Anerkennung in § 4 Abs. 1 BDSG schlichtweg sinnlos. Es sollte daher im weiteren Gesetzgebungsverfahren deutlich gemacht werden, dass der Gesetzgeber die Betriebsparteien nicht entmündigen will und ihnen zutraut, einen angemessenen betriebsspezifischen Arbeitnehmerdatenschutz zu formulieren. Es entspricht guter arbeitsrechtlicher Übung, Gesetze zur Abdingbarkeit durch Betriebsvereinbarungen zu öffnen (siehe z.B. § 7 Arbeitszeitgesetz) und dem Grundsatz der Subsidiarität, die praxisgerechte Lösungen erlaubt.

Will man nicht ganz so weit gehen, so empfiehlt sich eine Negativliste, bei der eine Abweichung durch Betriebsvereinbarung nicht möglich sein soll, etwa bei § 32 – 32a BDSG-E, weil hier das Arbeitsverhältnis noch nicht begründet wurde, und der Arbeitnehmer die Betriebsvereinbarung dadurch noch nicht personell legitimiert hat – oder aber § 32f BDSG-E, weil es sich hier um einen besonders sensiblen Sachverhalt handelt. Vorgeschlagen wird daher folgende Regelung in § 32l Abs. 5 BDSG-E:

> „Von § 32 bis § 32b, § 32e und § 32f darf in Tarifverträgen, Betriebs- und Dienstvereinbarungen nicht zuungunsten des Beschäftigten abgewichen werden. Soweit hierdurch von anderen Regelungen dieses Unterabschnitts zu Ungunsten des Beschäftigten abgewichen wird, haben diese Vereinbarungen die sich aus den allgemeinen Grundsätzen des Arbeitsrechts und Persönlichkeitsschutzes ergebenden Beschränkungen zu beachten."

VI. Einwilligung als Rechtfertigung

Gleiches lässt sich dann für die Einwilligung des Arbeitnehmers als Rechtfertigung sagen. Diese soll zukünftig als eigenständiges Rechtfertigungsinstrument gänzlich wegfallen und nach § 32 l Abs. 1 BDSG-E, nur dort, wo die § 32 ff. BDSG-E die Einwilligung ausdrücklich anerkennen – das ist jeweils

nur als zusätzliches Kriterium zur Erforderlichkeit nicht aber zur eigenständigen Rechtfertigung – soll sie eine Bedeutung haben. Das Ganze ist deswegen kaum überzeugend, weil die Fälle, in denen §§ 32 ff. BDSG-E die Einwilligung nennen, gerade typischerweise Fälle fehlender Freiwilligkeit sind. Soll etwa der Arbeitnehmer im Vorfeld der Bewerbung einwilligen, dass der Arbeitgeber auch Dritte über die Qualifikationen des Bewerbers befragen kann (vorgesehen in § 32 Abs. 6 BDSG-E), so ist dies typischerweise eine Situation, in der eine Freiwilligkeit gerade nicht gegeben ist. Welchen Sinn hier die Anwendung haben soll, ist unklar, insbesondere aber kann es sich hier nicht um eine Einwilligung handeln, die den Erfordernissen des § 4a BDSG entspricht.

Der generelle Ausschluss des § 4a BDSG sollte überdacht werden. Danach sind Einigungen ohnehin nur wirksam, dort wo sie auf der freien Entscheidung des Arbeitnehmers beruhen, der seinerseits auf den Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen ist. Das Schriftlichkeitserfordernis dient dem Schutz vor übereilter Zustimmung; die jederzeitige Widerruflichkeit ermöglicht es, noch einmal über die gegebene Zustimmung nachzudenken. Wenn all diese Kriterien gegeben sind, spricht nichts dagegen, die Einwilligung als Rechtfertigung zuzulassen. Hierfür streiten schon europarechtliche und verfassungsrechtliche Überlegungen:

- Der Arbeitnehmerdatenschutz schützt das Recht auf informationelle Selbstbestimmung des Arbeitnehmers. Das Recht auf informationelle Selbstbestimmung ist Bestandteil des allgemeinen Persönlichkeitsrechts.[7] Über das allgemeine Persönlichkeitsrecht kann der Berechtigte – wie über jedes andere Grundrecht – aber verfügen. Es gelten die Grundsätze der Grundrechtsausübung durch Grundrechtsverzicht: Soweit ich über ein Grundrecht freiwillig und informiert verfüge ohne den Kernbereich des Menschenwürdegehalts anzutasten, ist dieser Wille gerade als eine Möglichkeit der Wahrnehmung des Grundrechts zu akzeptieren.[8] Es gibt keinen Grund dafür, den Datenschutz gegen den zu schützen, der durch den Datenschutz geschützt ist. Es wäre vielmehr eine Beschränkung der Grundrechte des Arbeitnehmers, die der Rechtfertigung bedarf – und die fehlt, wo der Entschluss des Arbeitnehmers tatsächlich freiwillig, informiert und jederzeit widerruflich erfolgt.

- In gleiche Richtungen deuten europarechtliche Überlegungen. Die Einwilligung ist nach Art. 7 lit. a der Richtlinie 95/46/EG ausdrücklich als Rechtfertigung der Datenverarbeitung vorgesehen. Im Bereich des Arbeitsverhältnisses hierdrauf gänzlich zu verzichten, wird die Rechtfertigungsmöglichkeiten der Richtlinie also nicht ausschöpfen. Dies wäre nur dann zulässig, wenn eine Übererfüllung der

[7] Grundlegend BVerfG vom 15.12.1983 – 1 BvR 209/83, NJW 1984, 419.
[8] Siehe hierzu allgemein Sachs/*Sachs*, GG vor Art. 1 Rn. 57.

Schutzvorgaben der Richtlinien unproblematisch möglich wäre. Da aber die Richtlinie nicht allein den Schutz der betroffenen Dateninhaber beabsichtigt, sondern darüber hinaus – ausweislich etwa der Erwägungsgründe 8 und 9 der Richtlinie – den freien und ungehinderten Datenfluss in Europa fördern soll, wäre der Ausschluss des § 4a BDSG eine Friktion mit der Folge der Erschwernis dieser Ziele, für die auch europarechtlich eine Rechtfertigung erforderlich wäre. Diese ist wiederum nicht ersichtlich, wo die Einwilligung tatsächlich freiwillig informiert und jederzeit widerruflich erfolgt.

- Im Übrigen wäre sonst zu fragen, warum bei Beamten weiterhin aufgrund spezialrechtlicher Vorgabe mit Einwilligungen gearbeitet werden soll (etwa bei der Beihilfebearbeitung), und damit eine Rechtfertigung möglich sein soll, die beim Arbeitnehmer nicht wirksam wäre.

Der Gesetzgeber tut daher gut daran, die Einwilligung nicht gänzlich zu verbieten, sondern vielmehr darauf zu beschränken, wo tatsächlich von einer Freiwilligkeit ausgegangen werden kann. Dies ist im Arbeitsverhältnis vielleicht nicht allzu oft gegeben, deshalb aber anzunehmen, sie sei nie gegeben,[9] ist falsch. Dies mag schon das folgende Beispiel illustrieren: Will der Arbeitgeber etwa seinen Mitarbeitern eine betriebliche Altersversorgung ermöglichen, wird dies oftmals durch einen externen Versorgungsträger durchgeführt. Der wiederum benötigt persönliche Daten für seine Arbeit. Allgemeine Praxis ist bislang, dass hierfür eine Einwilligungserklärung des Arbeitgebers eingeholt wird, auf deren Grundlage der Versorgungsträger arbeitet. Dies wird zukünftig unzulässig sein. Würde der Arbeitnehmer aber sich selber unmittelbar an den Versicherer wenden, wäre die Einwilligungserklärung wirksam. Wieso? Die Ungleichbehandlung beider Vertragsbeziehungen ist sachwidrig und führt in dem spezifischen Bereich der betrieblichen Altersversorgung zu einem administrativen Aufwand, den man bei anderen Versicherungsverträgen nicht als erforderlich angesehen hat.

Will der Gesetzgeber sich die Mühe machen und die Einwilligung als Rechtfertigung im Arbeitsrecht nicht ausschließen, sondern sachgerecht und fallgerecht konkretisieren, würde sich etwa folgender neuer § 4a Abs. 2 BDSG anbieten:

> „(2) Bei der Einwilligung eines Beschäftigten ist von einer freien Entscheidung nur auszugehen, wenn das strukturelle Ungleichgewicht des Beschäftigungsverhältnisses keinen Einfluss auf die Erklärung hat. Hiervon ist regelmäßig nur auszugehen, wenn -
> - die Einwilligung erst erteilt wurde, nachdem sich die verantwortliche Stelle bereits verbindlich für die Begründung eines Beschäftigungsverhältnisses bereit erklärt hat;
> - dem Beschäftigten ausreichend Zeit zur Entscheidung gegeben wird, mindestens aber drei Tage;

[9] So in der Tat z.B. *Schaar,* MMR 2001, S. 644.

- der Beschäftigte die Möglichkeit hat, Rücksprache mit Dritten zu halten;
- der Beschäftigte auf die Möglichkeit der Rücksprache mit Dritten hingewiesen wurde."

Eine andere – zweitbeste Lösung – wäre es ebenso wie bei der Betriebsvereinbarung hier eine Negativliste zu formulieren im Hinblick auf die Normen, die auch durch Einwilligung nicht zum Nachteil des Arbeitnehmers abbedungen werden können. Denkbar ist auch eine Positivliste, die sich auf § 32c, d und i BDSG-E bezieht.

VII. Konzernsachverhalte

Die Begründung des Gesetzesvorschlags weist ausdrücklich darauf hin, dass das „immer wieder angesprochene Thema der Einräumung von vereinfachten Übermittlungsmöglichkeiten im Rahmen von Unternehmenszusammenschlüssen… in diesem Gesetzesentwurf keiner abschließenden Lösung zugeführt werden" konnte. Das ist recht wohlwollend gesprochen: Denn es wurde überhaupt keiner Lösung zugeführt. Der Bundesrat sieht das Problem und fordert die Bundesregierung auf, die Fragen des Konzerndatenschutzes bei auf EU-Ebene anstehenden Verhandlungen zu einer Reform der EG-Datenschutzrichtlinie einzubringen und in absehbarer Zeit einen Gesetzesentwurf zur konzerninternen Datenübermittlung vorzulegen.[10] Die Augen richten sich hier auf Europa, da die Datenschutzrichtlinie kein Konzernprivileg kennt und es in vergangenen Diskussionen um ihre Novellierung sich entsprechende Vorschläge nicht durchsetzen konnten.[11]

Wo rechtspolitischer Wille ist, wäre aber bereits jetzt ein Handeln möglich. Wie hoch die europarechtliche Hürde ist, ist schwierig zu ermessen: Generell ist festzustellen, dass die Konzerndimensionalität einer Regelung in vielen europäischen Richtlinien nicht beachtet wird und oftmals überlegt wird, ob die Vorgaben, die Brüsseler Regelungen für Unternehmen in Unternehmensverbünden umzusetzen sind.[12] Es empfiehlt sich für das weitere Procedere eine genaue Analyse der Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung verantwortliche Stelle" und „Auftragsverarbeiter" der Art. 29-Arbeitsgruppe zu versuchen und daraus eine konzernspezifische Definition der verantwortlichen Stelle entwickeln.[13] Die Arbeitsgruppe weist zu Recht daraufhin, dass es mehrere verantwortliche Stellen für die Verarbeitung von Daten geben kann und lotet zahlreiche

[10] BR-Drucksache 535/10 v. 05.11.10 S. 2, 4.
[11] Hierzu Mitteilung der Europäischen Kommission vom 4. November 2010: Gesamtkonzept für den Datenschutz in der Europäischen Union, S. 18, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:DE:PDF.
[12] S. hierzu nur im Bereich des Arbeitsrechts die vorsichtigen Anträge des GA *Bot* im Verfahren Albron Catering v. 3.6.2010 - C-242/09..
[13] Abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf..

Grenzbereiche dieser letztlich deutungsoffenen Begriffe aus. Selbst wer aber eine Ergänzung des § 3 Abs. 7 BDSG nicht das Wort reden will und eine konzernspezifische Definition der verantwortlichen Stelle nicht versuchen will, der kann dennoch vereinfachte Übermittlungen im Konzern zur Verfügung stellen. So sind etwa die Erfordernisse der Auftragsdatenverarbeitung nach § 11 BDSG nicht sämtlich europarechtlich vorgegeben. Hier könnte so etwas wie eine „Auftragsdatenverarbeitung light" für den spezifischen Bereich der Konzerne und ihrer Beschäftigtendaten formuliert werden. Eben dies müsste insbesondere etwa für gemeinsame Betriebe mehrer Unternehmen iS. des § 1 Abs. 2 BetrVG gelten, könnte aber auch auf Konzernsachverhalte insgesamt ausgedehnt werden. Sollte der Gesetzgeber sich hierzu nicht durchringen können, eine wie auch immer genannte Konzernklausel aufzunehmen, sollte er wenigstens in § 28 BDSG ausdrücklich festlegen, dass bei einer Abwägung der beiderseitigen Interessen auch Konzernbelange berücksichtigt werden können.[14] Wer es sich zur Aufgabe gestellt hat, den Arbeitnehmerdatenschutz einer praxisgerechten und rechtssicheren Lösung zuzuführen, darf diesen wichtigen Bereich nicht aussparen. Dies gilt umso mehr, wenn Konzernbetriebsvereinbarungen und gleichlautende Einwilligungserklärungen der Arbeitnehmer zukünftig keine rechtfertigende Wirkung mehr haben sollen. Dies macht die Regelungen der Konzerndimensionalität des Datenschutzes umso dringlicher. Der Vorschlag der Fraktion Bündnis 90/ Die Grünen, ist daher als Ausgangspunkt einer Regelung zu begrüßen: 8BT-Drucks. 17/4853, S. 8):

> (2) Die Übermittlung von Beschäftigtendaten zwischen rechtlich selbständigen Unternehmen innerhalb von Konzernverbünden ist nur zulässig, soweit sie zur Wahrung eines betrieblichen Interesses, das in unmittelbarem Zusammenhang mit dem Beschäftigungsverhältnis steht, erforderlich ist und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Vor oder bei der Übermittlung muss das übermittelnde Unternehmen den Betroffenen Zweck und Ausmaß mitteilen. Zweck, Ausmaß und andere Modalitäten der Übermittlung können auf Grundlage dieses Gesetzes auch durch Betriebsvereinbarung geregelt werden, soweit dadurch das Schutzniveau dieses Gesetzes nicht unterschritten wird.

Geeigneter scheint mir noch folgende Formel:

§ 32d Abs. 6 BDSG-E

„Die Übermittlung von Beschäftigtendaten innerhalb eines Konzerns im Sinne des § 18 Aktiengesetzes ist zur Durchführung des Beschäftigtenverhältnisses zulässig, soweit keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden und ein angemessenes Schutzniveau in den betreffenden konzernangehörigen Unternehmen besteht. Einzelheiten können durch

[14] S. hierzu auch *Thüsing*, RDV 2010, S. 149.

Betriebsvereinbarung geregelt werden."

Die Normierung der Konzerndimensionalität kann damit als Ausgestaltung der Datenverarbeitung auf Grundlage einer Interessenabwägung erfolgen, die Art. 7 f) der EG-Datenschutzrichtlinie (RL95/46/EG) als generellen Erlaubnistatbestand vorsieht.

VIII. Überwachung Telekommunikation

Überdenkenswert ist weiterhin auch die Regelung in § 32i BDSG-E, in der die Überwachung der Telekommunikation normiert wird. Dies ist momentan ein besonders konfliktreiches Feld, in der Rechtsicherheit nicht immer gegeben ist.[15]

Die Grenzen der Überprüfbarkeit sind hier gänzlich unklar. Das gilt insbesondere für den Regelungsgehalt des § 32i Abs. 4 BDSG-E: „Nach Abschluss einer Telekommunikation gelten für die Erhebung, Verarbeitung und Nutzung der Daten und Inhalte die §§ 32c und 32d [d.h. die allgemeinen Regelungen zur Datenerhebung und Datenverarbeitung und Nutzung im Beschäftigungsverhältnis]. Der Arbeitgeber darf private Inhalte nur erheben, verarbeiten und nutzen, soweit dies zur Durchführung eines ordnungsgemäßen Dienst- und Geschäftsbetrieb unerlässlich ist und die Beschäftigten hierauf schriftlich hingewiesen hat." Hier bleibt nicht nur offen, wie dieser schriftliche Hinweis zu erfolgen hat (generell am Anfang des Beschäftigtenverhältnisses? Im Hinblick auf jede Erhebung und Verarbeitung gesondert?). Vielmehr greift die Regelung ins Leere. Gespeichert, und damit erhoben werden die Daten schon während der laufenden Kommunikation, dort kann also nie Abs. 4 greifen. Die übrigen Absätze dieser Vorschrift gelten nicht für erlaubte Privatkommunikation. Für erlaubte Privatnutzung fehlt jede Regelung. Sollte hier das TKG eingreifen, so wird diese Sichtung aufgrund des strengen Maßstabs fast unmöglich. So läuft er leer. Bislang ist es so, dass in der Praxis oftmals geraten wird, die private Nutzung zu verbieten und konsequent dieses Verbot zu überwachen, damit die Kontrollmöglichkeiten des Arbeitgebers nicht eingeschränkt werden. *Dies ist für alle Beteiligten misslich*. Datenschutz wird zum Nachteil des Arbeitnehmers. Klargestellt werden sollte die Nicht-Anwendbarkeit des TKG auch bei erlaubter Privatnutzung verbunden mit einer Anpassung des Absatz 4. Dies wäre unproblematisch möglich, entspricht dies doch bereits durchaus einigen Judikaten und beachtlicher Stimmen in der Literatur *de lege lata*.[16] Ob dies dann durch Festlegung im TKG erfolgt oder aber im BDSG, ist dann

[15] Ausführlich *Thüsing*, Arbeitnehmerdatenschutz und Compliance, Rn. 198 ff.

[16] Vgl. etwa VGH Kassel, Beschl. v. 16.5.2009 - 6 A 2672/08.Z, NJW 2009, 2470, 2471 f.; OLG Karlsruhe v. 10.1.2005 – 1 Ws 152/04, MMR 2005, 178, 179 f.; ausdrücklich offen gelassen wurde der Streit in: VG Frankfurt/Main v. 6.11.2008 – 1 K 628/08.F (3), CR 2009, 125 f.; VGH Hessen v. 19.05.2009 – 6 A 2672/08.Z, NJW 2009, 2470, 2471; *Barton*, CR 2004, 305, 310; *Gramlich*, RDV 2001, 123, 124; *Haußmann/Krets*, NZA 2005, 259, 260; *Schimmelpfennig/Wenning*, DB 2006, 2290 ff.

Frage der gesetzgeberischen Ästhetik.[17] Vorgeschlagen wird folgende Regelung in § 32i Abs.5 BDSG-E:

> „Allein durch die kostenlose Gewährung der privaten Nutzung von Email und Internet wird der Arbeitgeber nicht Diensteanbieter im Sinne der § 3 Nr. 6 Telekommunikationsgesetz. Bei erlaubter Privatnutzung darf der Arbeitgeber dienstliche Inhalte nur erheben, verarbeiten und nutzen, soweit der Arbeitnehmer hierin eingewilligt hat oder dies zur Durchführung eines ordnungsgemäßen Dienst- und Geschäftsbetrieb erforderlich ist und die Beschäftigten zuvor hierauf schriftlich hingewiesen hat. Private Inhalte dürfen nur erhoben werden, soweit dies erforderlich ist um festzustellen, dass es sich nicht um dienstliche Inhalte handelt. Eine Verarbeitung oder Nutzung privater Inhalte ist unzulässig““

[17] S. hierzu auch *Thüsing,* Arbeitnehmerdatenschutz und Compliance Rn. 220 ff. mit umfassenden Nachweisen.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 F

Dr. Philipp Kramer
Rechtsanwalt, Hamburg
Vorstand der Hamburger Datenschutzgesellschaft
Lehrbeauftragter Universität Hamburg
Lehrbeauftragter Hochschule Ulm

Stellungnahme zu

- **BT-Drucksache 17/4230**
- **BT-Drucksache 17/69**
- **BT-Drucksache 17/4853**
- **BT-Drucksache 17/121**
- **BT-Drucksache 17/779**
- **Ausschussdrucksache 17(4)255**

betreffend Beschäftigtendatenschutz

zur Anhörung 40. Sitzung des Bundestagsinnenausschusses (17. Wahlperiode)

20. Mai 2011/sh

Übersicht

A. Ausgangspunkt / Fragestellung / Vorbemerkungen
B. Rechtliche Bewertung
1. Vorzug eines Artikelgesetzes
2. Einfache Struktur mit Fallgruppen
3. Abgrenzung der bereichsspezifischen Beschäftigtendatenschutzregeln
4. Gestaltungsbefugnisse der Betriebs-/Tarifparteien
5. Verarbeitungseinwilligung des Beschäftigten
6. Private Nutzung von Telekommunikationsdiensten
7. Geschäftsdatenanalyse (Screening)
8. Inkrafttretensregelung
9. Andere, Beschäftigtendatenverarbeitung vorsehende Gesetze

A. Ausgangspunkt / Fragestellung / Vorbemerkungen

Das Datenschutzrecht soll erneut geändert werden. Standen 2009 das Werbedatenschutzrecht, der Schuldnerdatenschutz und die Vorschriften zum Schutz vor dem „Abstempeln“ als schlechter Schuldner auf der Tagesordnung, geht es dieses Mal um den Schutz der Beschäftigten. Sie sollen davor bewahrt werden, dass der Arbeitgeber Informationen über sie, die von der Bewerbung bis zur Leistungsabwicklung anfallen, übermäßig nachteilig verwendet werden.

Der **Grund für neue Beschäftigtendatenschutzvorschriften** wird von den Bundestagsfraktionen weitgehend einheitlich darin gesehen, für die Rechtsunterworfenen mehr Transparenz zu schaffen. Es soll also **leichter erkennbar sein, welcher Umgang mit Beschäftigtendaten zulässig ist und welcher nicht**. Als Motiv wird mehr oder weniger deutlich die Reaktion auf immer wieder aufkommende Pressemeldungen zu Bespitzelungen von Beschäftigten ins Feld geführt. Das ist mit Rücksicht

auf die sich in der Öffentlichkeit ergebenden teils klaren, teils diffusen Befürchtungen nachvollziehbar. **Sich diesem Bedarf nach Klarheit zu stellen und gesetzgeberisch aktiv zu werden, ist ein berechtigtes Motiv des Gesetzgebers.**

Die nachfolgende Stellungnahme konzentriert sich auf die gegenwärtig in Diskussion befindlichen Hauptpunkte. Nicht ausführlich erläutert sind folgende Themen:

- **Videoüberwachung ohne Kenntnis des Beschäftigten**

  Allein der Regierungsentwurf sieht hier ein vollständiges Verbot vor. Er nimmt also an, dass eine Videoüberwachung ohne Kenntnis des Beschäftigten niemals verhältnismäßig sein kann. Diese dafür erforderliche Typisierung eines immer überwiegenden Beschäftigteninteresses stößt auf erhebliche rechtliche Zulässigkeitsbedenken. Bei klaren Verdachtsmomenten und konkretisierten Verhältnismäßigkeitsanforderungen kann eine zeitbegrenzte Videoüberwachungsmaßnahme das im Verhältnis zur dauerhaften offenen Videoüberwachung oder zum Detektiveinsatz verhältnismäßigere Mittel sein. So auch die weiteren vorliegenden Entwürfe, die Maßnahmen dieser Art in begrenzten Fällen zulassen (§ 11 Absatz 2 BDatGE-SPD; § 10 Absatz 3 BDatGE-Bündnis 90/DIE GRÜNEN).

- **Telekommunikationsdatenerfassung dienstlich**

  Der Regierungsentwurf erkennt die besonderen Beschäftigtendatenverarbeitungserfordernisse in Unternehmen wie Callcentern (§ 32i Absatz 2 BDSG-RegE) und lässt die Inhaltsdatenverarbeitung unter bestimmten Voraussetzungen zu. Im Rahmen der Steuerung solche Unternehmen oder Unternehmensteile, die mit Kundendienst zu tun haben, ist auch die Verkehrsdatenerfassung für die Einsatzsteuerung zwingend. Als ein Weniger zur Inhaltsdatenverarbeitung liegt die entsprechende Befugnis des Arbeitgebers zwar nach dem Regierungsentwurf nahe; doch ist sie nicht ausdrücklich geregelt.

- **Konzernregelung**

  Innerhalb des Konzerns erfolgen mannigfaltige Übermittlungen personenbezogener Daten, auch von Beschäftigtendaten. Einige dieser Übermittlungen lassen sich nicht im Wege der Auftragsdatenverarbeitung, beispielsweise als Dienstleistungen eines Shared Service Centers, darstellen. Angesichts der Absicht detaillierter Beschäftigtendatenschutzregeln sollte eine klärende Konzernregelung eingeführt werden. Es kann auf dieser Reformstufe nicht um ein Konzernprivileg gehen. Das EU-Datenschutzrecht sieht das nicht vor, sondern sieht Konzerne datenschutzrechtlich als Ansammlung rechtlich selbständiger Einheiten. Eine EU-datenschutzkonforme Vorgehensweise kann in Anlehnung an die Verbundverfahren der Landesdatenschutzgesetze ausgestaltet werden. Formulierungen der Landesgesetze lauten hier beispielsweise „wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist“ (§ 4a LDSG Nordrhein-Westfalen; § 17 Absatz 1 Satz 1 LDSG Mecklenburg-Vorpommern). Das Hinzutreten der Vorabkontrolle im Regelfall könnte vorgesehen werden.

B. Rechtliche Bewertung

1. Vorzug eines Artikelgesetzes

Fragestellung
Es besteht keine Einigkeit, ob ein gesondertes Gesetz den Beschäftigtendatenschutz regeln soll. Was ist vorzuziehen: Ein bereichsspezifisches Beschäftigtendatenschutzgesetz oder spezielle Vorschriften im bestehenden BDSG?

Fazit aus Sicht des Datenschutzbeauftragten
Eine ausgelagerte Regelung in einem eigenen Gesetz führt in der Praxis zu einem Anwendungserschwernis. Ein Beschäftigtendatenschutzgesetz würde nicht abschließend gelten, sondern immer wäre das Zusammenspiel mit anderen Vorschriften zu prüfen. Diese Prüfung ist für den Nichtjuristen, der als Datenschutzbeauftragter häufig anzutreffen ist, besonders schwer. Zudem ist schon jetzt eine Zersplitterung des Datenschutzrechts in verschiedene Spezialgesetze und Maßstäbe zu beobachten. Ein weiteres Gesetz befördert bereichsspezifische Abwägungen, bevor in vielen ungeklärten Fragen ein Konsens herbeigeführt worden ist.

Im Einzelnen
Die Vorschriften über den Beschäftigtendatenschutz ließen sich in einem Arbeitsgesetzbuch kodifizieren, wenn es ein solches gäbe. Demgegenüber gibt es ein allgemeines Datenschutzrecht mit dem Bundesdatenschutzgesetz. Systematisch liegt es daher näher, dort auch die neuen Vorschriften über den Beschäftigtendatenschutz unterzubringen. Dafür spricht auch, dass der Gesetzgeber bereits ein eigenes Werbedatenschutzrecht im Bundesdatenschutzgesetz § 28 Absatz 3 -3b geregelt hat. Für eine Aufnahme der neuen Vorschriften ins Bundesdatenschutzgesetz spricht auch, dass anderenfalls die allgemeine Regelung des BDSG, nämlich §§ 1-11 einschließlich der Anlage zu § 9, in ein neues Gesetz aufgenommen werden müssten. Diese Konsequenz ziehen auch die Entwürfe der SPD-Fraktion und der Bündnis 90/DIE GRÜNEN-Fraktion nicht, sondern verweisen teilweise auf Vorschriften des BDSG. **Die vereinheitlichende**

Klammer, also die gemeinsame Fortentwicklung der Rechtsgrundsätze des informationellen Selbstbestimmungsrechts durch die Rechtsanwender würde erheblich erschwert. Wie schon beim Telemediengesetz birgt ein Vorgehen mit einem eigenen Beschäftigtendatenschutz die Wahrscheinlichkeit, dass sich die Rechtsgebiete, allgemeines Datenschutzrecht und Beschäftigtendatenschutz, unterschiedlich entwickeln. Auch das ließe sich noch, je nach politischer Auffassung, gutheißen. Nicht im Sinne des Datenschutzes wirkt sich jedoch dann eine Entwicklung in unterschiedlichen Gesetzen aus, wenn wichtige Grundfragen des Datenschutzes – wie heute – nicht geklärt sind. So fehlt bisher eine allgemein akzeptierte Grundregel, wann Kontrollmaßnahmen durch eine Videoüberwachungsanlage zulässig sind. Betritt man als Verbraucher einen Shop mit höherwertigen Waren, so wird mehr und mehr eine solche Anlage installiert sein; wie inzwischen in vielen U- und S-Bahnen. Sollte nun tatsächlich ein Spezialrecht dafür geschaffen werden, wenn der Verbraucher jedenfalls zugleich auch Beschäftigter des entsprechenden Shops ist? Müssen nicht für beide Fälle ähnliche Grundsätze gelten, wann das Kontrollinteresse das Interesse am Unbeobachtetsein überwiegt? Natürlich kann es sich ergeben, dass zugunsten der Beschäftigten angesichts ihres ständigen Aufenthalts in Shops stärkere Einschränkungen zum Tragen kommen. Doch was soll der dafür geltende Maßstab sein? Die arbeitsgerichtliche Rechtsprechung hat hier bereits durch verschiedene Fallentscheidungen eine Messlatte geschaffen, die durchaus auf andere Videoüberwachungsbereiche erstreckt werden könnte.

2. Einfache Struktur mit Fallgruppen

Fragestellung
Alle Gesetzesentwürfe sind bestrebt, möglichst konkrete Regelungen zu schaffen. Sollte dieser Weg umgesetzt werden?

Fazit aus Sicht des Datenschutzbeauftragten

a) Konkrete Regelungen sind zu begrüßen, wenn sie leicht verständlich formuliert werden können und formuliert sind.

b) Soweit die konkrete Regelung mit neuen vagen – wertausfüllungsbedürftigen – Begriffen einhergeht, ist der Rückgriff auf bestehende vage Begriffe vorzuziehen.

c) Es ist zu berücksichtigten, dass der Gewährträger des Datenschutzes – neben den Datenschutzaufsichtsbehörden – der behördliche und betriebliche Datenschutzbeauftragte ist. Dieser verfügt nicht zwingend über fundierte Kenntnis des und Übung mit dem juristischen Handwerkszeug. Zudem ist er häufig nicht hauptberuflich als Datenschutzbeauftragter tätig. Soll er seine Gewährsfunktion effektiv wahrnehmen können, bedarf es gerade im Datenschutzrecht der Beachtung des Gebots des leicht verständlichen Gesetzes.

Im Einzelnen

Für den Juristen ist es mit seinem Handwerkszeug relativ leicht möglich, die Gesetzentwürfe zu lesen, zu verstehen und anzuwenden. Quantitativ fällt auf, dass die Gesetzentwürfe eine erhebliche Zahl zusätzlicher Vorschriften für das Beschäftigtendatenschutzrecht vorsehen. Das kommt beispielsweise dadurch zustande, dass für die Datenerhebung und Datenverwendung vor und im Beschäftigungsverhältnis eine Vielzahl von Einzelvorschriften geschaffen wird. Bisher lässt das Bundesdatenschutzgesetz einen Datenumgang für private Unternehmen nur mit einer **Erlaubnis nach der Rechtfertigungsquintas** vor. Daten personenbezogener Art dürfen dann verarbeitet werden,

(1) wenn ein **Spezialgesetz** dies anordnet oder vorsieht;
(2) wenn die Daten **allgemein zugänglich** sind, sofern die berechtigten Interessen des Betroffenen gewahrt werden;
(3) wenn es für ein **Rechtsgeschäft** oder in Vorbereitung eines solchen erforderlich ist;

(4) wenn das Datenumgangsinteresse gewichtiger ist als das Geheimhaltungsinteresse (Informationelles Selbstbestimmungsrecht) des Betroffenen (**Güterabwägung**) oder
(5) wenn eine wirksame **Einwilligung** des Betroffenen vorliegt.

Diese Anforderungen sind in §§ 4 Absatz 1 und 28 Absatz 1 BDSG geregelt. Die nunmehr angestrebte Komplexität von Erlaubnistatbeständen für den Umgang mit Beschäftigtendaten mag aufgrund der Brisanz von pressewirksamen Beschäftigtendatenkontrollen erforderlich sein. Es bleibt jedoch aus Sicht des Datenschutzbeauftragten zu wünschen, dass auf eine **Minimierung der Vorschriften, auf übereinstimmende Begriffe an den verschiedenen Stellen und eine stringente Gliederung** Acht gegeben wird.

Diese Forderung von Systematik, Klarheit und Lesbarkeit des Gesetzes hat im Datenschutzrecht seine besondere Bewandtnis. Die Einhaltung der datenschutzrechtlichen Vorschriften wird bei privaten Unternehmen – wie auch teilweise bei Behörden – durch bestellte Datenschutzbeauftragte kontrolliert. Neben den staatlichen Aufsichtsbehörden – in der Bundesrepublik vorwiegend als Landesdatenschutzbeauftragte eingerichtet – gibt es eine **unabhängige Stelle im Unternehmen bzw. in der Behörde**, die fachlich unabhängig die Einhaltung der Gesetze und der Datensicherheitsanforderungen kontrolliert. Dabei hat der Datenschutzbeauftragte zwei Aufgaben. Er muss sich erstens um die richtige Rechtsanwendung kümmern und zweitens dafür Sorge tragen, dass die Technik und die Anweisungen an die Beschäftigten hinreichende Sicherheit der Daten gewährleistet. **Weder der Jurist noch der IT-Spezialist allein** ist also in der Lage, ohne weitere Kenntnisse neben seinem Kernbereich die Kontrollfunktion des Datenschutzbeauftragten angemessen zu erfüllen. Er muss sich also auf mindestens zwei Gebieten auf dem aktuellen Stand halten. Das Fehlen einer klaren Ausbildung oder einer eindeutigen Anforderung eines Berufsabschlusses führt zudem dazu, dass es keinen Schwerpunktberuf für die Tätigkeit des Datenschutzbeauftragten gibt. In der Vergangen-

heit und auch heute noch kommen viele Datenschutzbeauftragte aus dem Bereich der IT oder der Revision. Sie verfügen dann typischerweise nicht über eine ausführliche Ausbildung, die aufzeigt, wie man mit gesetzlichen Vorschriften umgeht und sie auslegt. Andererseits ist unsere Gesellschaft mehr und mehr auf solche Fachleute angewiesen, die nicht nur die gesetzlichen Regeln verstehen, sondern auch wissen, wie beispielsweise eine Software wie Google Analytics, ein Cookie oder ein soziales Netzwerk arbeitet. Entwickelt der Gesetzgeber die Datenschutzgesetze in ihrem Inhalt nicht nur weiter, sondern werden sie über das zwingend erforderliche Maß komplexer, so **droht die Funktion des unabhängigen Datenschutzbeauftragten auszutrocknen**.

Eine Vielzahl neuer Vorschriften kann für die Beschäftigten das teilweise ausdrücklich erwünschte höhere Schutzniveau schaffen. Voraussetzung dafür ist allerdings, dass die Vorschriften **leicht verständlich** bestimmte Lebenssachverhalte der Beschäftigtenwelt regeln. Wenn es beispielsweise heißt,

- länger als 24 Stunden ohne Unterbrechung (§ 32e Absatz 4 Satz 1 Nr. 1 BDSG-RegE);
- „gilt nicht für den Einsatz von Ferngläsern und Fotoapparaten“ (§ 32e Absatz 4 Satz 1 Nr. 3 BDSG-RegE);
- „Beschäftigte haben das Recht, Erklärungen zum Inhalt der Personalakte abzugeben.“ (§ 20 Absatz 3 Satz 1 BDatGE-SPD);

handelt es sich um leicht verständliche Formulierungen. **Demgegenüber** bringen **nicht leicht verständliche Regelungen** wie

- „Der Arbeitgeber darf Beschäftigtendaten verarbeiten und nutzen, soweit sie nach § 32, 32a oder 32c erhoben worden sind, dies erfor-

derlich ist […] zur Erfüllung anderer Zwecke, für die der Arbeitgeber sie nach den Vorschriften dieses Unterabschnitts [i.e. Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses] hätte erheben dürfen, und dies nach Art und Ausmaß im Hinblick auf den Zweck verhältnismäßig ist.“ (§ 32d Absatz 1 BDSG-RegE);

- „Der Arbeitgeber darf Beschäftigtendaten nicht in einer Weise verwenden, dass sie ein Gesamtbild der wesentlichen geistigen und charakterlichen Eigenschaften (Persönlichkeitsprofil) oder Gesundheitsdaten (Gesundheitsprofil) der Beschäftigten ergeben können. (§ 10 Absatz 2 BDatGE-SPD; ähnlich § 32d Absatz 5 BDSG-RegE);

erhebliche Rückfragen mit sich, die Rechtsanwender wie Arbeitgeber, Betroffene wie Aufsichtsbehörden und letztlich die Gerichte beantworten müssen. Wenn neue Regelungen geschaffen werden, die eben nicht **leicht verständlich den** Lebenssachverhalt der Beschäftigtenwelt erfassen und mit einer Rechtsfolge ausstatten, sollte von den generellen Regelungen nicht abgewichen werden. Andernfalls besteht das gesteigerte Risiko, dass neue vage – wertausfüllungsbedürftige – Rechtsbegriffe verwendet werden. Über diese neuen Begriffe müssten sich zunächst die Rechtsanwender im rechtsstaatlichen Prozess gewissermaßen einigen. Der Rechtsfortbildung wäre zwar Entwicklungspotential eröffnet. Zugleich würde jedoch eine Rechtsunsicherheit befördert, die die Fraktionen des Deutschen Bundestags gerade vermeiden wollen. Gelingt es dem Gesetzgeber nicht, eine bestimmte Fragestellung des Datenumgangs im Beschäftigungsverhältnisses präzise zu erfassen und/oder kann er die Rechtsfolge nur mit vagen Begriffen regeln, wie

> „nur zulässig, soweit Art und Ausmaß im Hinblick auf den Zweck verhältnismäßig sind“ (§ 32c Absatz 4 BDSG-RegE),

führt die Einführung neuer Tatbestands- oder Rechtsfolgenbeschreibungen, hier Anforderung der Verhältnismäßigkeit (schon § 32 Absatz 1 Satz 2 BDSG), zu höherer Rechtunsicherheit. Der Gesetzgeber sollte auf die bekannten Regelungsmaßstäbe zurückgreifen, hier den Erforderlichkeitsmaßstab. Sicher, auch für die bekannten vagen Begriffe ist das letzte Wort der Begriffsbeschreibung nicht gefallen. Doch hat man sich hier dem Begriffen bereits genähert. Das gilt namentlich für die generelle Datenumgangsbefugnis. Sie bestimmt sich für Bundesbehörden wie für private Unternehmen nach dem Maßstab der „Erforderlichkeit“ (§§ 13 Absatz 1, 14 Absatz 1 Satz 2, 15 Absatz 1 Nr. 1, 16 Absatz Nr. 1 BDSG; § 28 Absatz 1 Satz 1 Nr. 2, Absatz 2 Nr. 2, Absatz 3 Satz 2 BDSG). Dieser primäre Maßstab des Datenschutzrechts wird bis heute nicht einheitlich verstanden. Fest steht, dass nur ein für einen bestimmten Zweck geeigneter und zweckmäßiger Datenumgang erforderlich sein kann. Im Übrigen reicht die Auslegung von „Nützlichkeit“ (*Gola/Schomerus*, BDSG, § 28 Rn. 15) über „keine zumutbare Alternative“ (*Schaffland/Wiltfang*, BDSG, § 28 Rn. 110) bis zur „Unverzichtbarkeit“ (*Simitis-Sokol*, BDSG, § 3 Rn. 26). Letztlich steht hinter dem Erforderlichkeitsmaßstab die Abwägung. Ohne vorangegangene **Zweckbestimmung, die dem gesamten Datenschutzrecht rechtfertigungsimmanent ist**, kommt eine Bestimmung dessen, was in die Abwägung einzufließen hat, nicht in Betracht. Im Rahmen der Aufnahme des Verhältnismäßigkeitsprinzips in § 32 Absatz 1 Satz 2 BDSG ist dieser strukturierende und klärende Rechtsgedanke auch von der Literatur aufgenommen worden (Taeger/Gabel-Zöll, BDSG, § 32 Rn. 17, 46; Gola/Schomerus, BDSG, § 32 Rn. 27; Thüsing, Arbeitnehmerdatenschutz, Rn. 70; ausführlich zur Betriebsvereinbarung BAG, Beschluss vom 26. 8. 2008 - 1 ABR 16/ 07). Der Arbeitgeber muss für die Abwägung festlegen und in Textform dokumentieren, für welchen Zweck die Beschäftigtendaten erhoben, verarbeitet und genutzt werden sollen. Sodann ist zu prüfen, ob die Datenverarbeitung diesen Zweck ermöglicht. Darüber hinaus dürfen dem Arbeitgeber keine angemessenen milde-

ren Mittel zur Verfügung stehen, die gleichermaßen wirksam den Zweck erreichen lassen. **In einem letzten Schritt ist zu ermitteln, ob nicht das Geheimhaltungsinteresse des Beschäftigten mit Rücksicht auf dessen verfassungsrechtliche Anerkennung stärker wiegt als das Verwendungsinteresse des Arbeitgebers.** Hierbei ist zu prüfen, ob das Ausmaß des Eingriffs in das informationelle Selbstbestimmungsrecht in einem angemessenen und zumutbaren Verhältnis zum vom Arbeitgeber erzielten Zweck steht.

Bei der Forderung, zumindest statt neuer, bereits gegebene wertausfüllungsbedürftige Begriffe zu verwenden, ist der Gewährträger des Datenschutzes zu berücksichtigen. Ob ein konkretes Unternehmen datenschutzkonform handelt, wird von den Datenschutzaufsichtsbehörden aus Ressourcengründen selten geprüft. Auch der Betroffene wird – von eklatanten einzelnen Missbrauchsfällen abgesehen – einfache oder formale Datenschutzverstöße kaum zur Kenntnis nehmen und um das Abstellen des Zustands bitten. Soweit der Betriebsrat datenschutzrechtliche Kenntnis hat, wird er sich vermutlich für den Beschäftigtendatenschutz betriebsverfassungsrechtlich einsetzen. Im Übrigen gewährt der unparteiische Sachwalter „behördlicher / betrieblicher Datenschutzbeauftragter“ datenschutzkonforme Zustände. Er kontrolliert die Verarbeitungen personenbezogener Daten auf der Basis von Verarbeitungsinventuren. Dazu werden die Orte und Systeme personenbezogener Datenverarbeitung im Unternehmen inventarisiert. Die nachfolgende rechtliche Kontrolle setzt voraus, dass er im Umgang mit den Datenschutzvorschriften vertraut ist. Diese Kontrolle durch den Datenschutzbeauftragten wird allerdings mehr und mehr daran scheitern, wenn Datenschutzbeauftragte ohne juristisches und lange geübtes Spezialwissen an neue, vage Vorschriften herangehen müssen. Der Trend zum juristischen Datenschutzbeauftragten ist schon jetzt klar erkennbar. Für den Rechtsteil des Datenschutzes mag diese Entwicklung zu begrüßen sein. Doch der juristische Datenschutzbeauftragte hat typischerweise nicht die zweite notwendige Qualifikation des Datenschutzbeauftragten, ein tieferes Verständnis von den technischen und organisatorischen Informationssicherheitsmaßnahmen. Das Berufsbild des Datenschutzbeauftragten ist durch diese Doppelqualifikation geprägt. **Nur der Erhalt des Zugangs zur Tätigkeit des**

Datenschutzbeauftragten aus rechtlichen und technisch-organisatorischen Qualifikationen gewährleistet die dauerhafte Kompetenz dieser Einrichtung des Datenschutzbeauftragten. Der gegenseitige Austausch von technischem und juristischem Verständnis ist von maßgeblicher Bedeutung und darf nicht durch eine juristische Schwerpunktsetzung verlagert werden.

3. Abgrenzung der bereichsspezifischen Beschäftigtendatenschutzregeln

Fragestellung

Werden Spezialvorschriften zum Beschäftigtendatenschutz geschaffen, muss für den Anwender klar sein, wann die Spezialvorschriften und wann allgemeine Datenschutzvorschriften gelten. Ist das Gesetz hier hinreichend deutlich?

Fazit aus Sicht des Datenschutzbeauftragten

Die mit dem Arbeitspapier der Berichterstatter der Koalitionsfraktionen eingebrachte Änderung des § 27 Absatz 3 BDSG „Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Beschäftigten für andere, außerhalb des Beschäftigungsverhältnisses liegende Zwecke“ bringt mehr Klarheit, wann neue Spezialvorschriften und wann das bisherige Recht anzuwenden ist.

Im Einzelnen

Beschäftigtendaten sind erforderlich, um das Beschäftigungsverhältnis mit seinen **Hauptpflichten** überhaupt durchzuführen. Alle Daten, die für die Leistungserbringung und die Entgeltzahlung benötigt werden, dürfen nach den vorliegenden Entwürfen verarbeitet werden. Daher ist es danach erlaubt, die Stamm-, Lohnsteuer- und Sozialversicherungsdaten im Rahmen des Beschäftigungsverhältnisses zu verarbeiten.

Im Rahmen der Unternehmensführung werden Beschäftigtendaten auch für **organisatorische, soziale und personelle Zwecke** verwendet, die nur **mittelbar mit dem Beschäftigungsver-**

hältnis verbunden sind. Dazu gehören die Verwendung von Beschäftigtendaten für

- Personalplanungsmaßnahmen, die aus der Perspektive des Unternehmens durchgeführt werden,
- gezielte Aus- und Fortbildungsmaßnahem,
- unternehmens-/gruppeninterne Arbeitsprofile zur Projektteambildung,
- Bescheinigungen, die nicht gesetzlich geregelt, sondern vom Beschäftigen gewünscht werden, beispielsweise für ausländische Gerichte,
- statistische Analysezwecke, denen der Zugriff auf personenbezogene, noch nicht anonymisierte Beschäftigtendaten vorausgeht,
- Zutritts- und Zugangsberechtigungssysteme.

Auch soweit es um **bloße Nebenpflichten und deren Kontrolle** geht, wird allerdings nicht durchgängig die Auffassung vertreten, dass die Verarbeitung zur Nebenpflichterfüllung zur Durchführung des Beschäftigungsverhältnisses erforderlich sei. Ein Datenumgang zur Erfüllung von Pflichten bzw. Wahrnehmung von Rechten und deren Kontrolle sieht allein BDSG-RegE mit § 32c Absatz 1 Satz 1 Nr. 3 und BDatGE-SPD mit § 8 Absatz 2 Satz 1 vor (zur Wahrnehmung von Rechten). BDatGE-Bündnis 90/DIE GRÜNEN verzichtet auf eine Regelung für die Verarbeitung von Beschäftigtendaten für freiwillige Zwecke und für allgemeine Kontrollzwecke.

Auch erfolgt der Umgang mit Beschäftigtendaten für diverse freiwillige, teils vertraglich fixierte Leistungen gegenüber den Beschäftigten. Dazu gehören unter anderem

- Geburtstagsgrüße,
- Weiterbildungsangebote,

- Rabattierung beim Personaleinkauf,
- Essenszuschuss,
- rabattierte Kantinennutzung,
- Firmenwagen mit Fuhrparkmanagement (einschließlich Ordnungswidrigenkeitenverwaltung),
- Fahrtkostenzuschuss,
- Busdienste,
- Zur-Verfügung-Stellung eines Parkplatzes,
- firmenorganisierte Gesundheitsmanagementsysteme,
- Zuschüsse für die Mitgliedschaft in Sporteinrichtungen,
- freiwillige betriebliche Altersversorgungssysteme,
- Firmenkreditkarte für Firmen- und Privatnutzung,
- Betriebskindergarten,
- sonstige Betreuung von Kindern der Beschäftigten,
- Beratung von Beschäftigten in Familien-, Schuldner- oder Suchtsachen,
- Arbeitgeberdarlehen,
- Sterbekasse für Hinterbliebene des Beschäftigten,
- die Zusendung von Informationen an den Beschäftigten nach Hause.

Die Aufzählung zeigt Leistungen, die durch eine unterschiedliche Nähe zum Beschäftigungsverhältnis gekennzeichnet sind. Häufig wird man sie nur als „**anlässlich eines Beschäftigungsverhältnisses durchgeführt**“ bezeichnen können. Soweit diese Leistungen erbracht werden, muss deren Gewährung schon aus handelsrechtlichen Gründen nachvollzogen werden können. Auch Haftungsgründe können eine Erfassung von Daten der

Beschäftigten und gegebenenfalls von Familienmitgliedern erforderlich machen.

Die Vielzahl der möglichen Zwecke ließe sich von den bereichsspezifischen Vorschriften kaum vollständig erfassen. Da freiwillige soziale Leistungen eines Unternehmens heute insbesondere mit den Mitteln der elektronischen Datenverarbeitung durchgeführt und kontrolliert werden, wäre ihre Verwaltung und damit ihr Zur-Verfügung-Stellen datenschutzrechtlich nahezu unmöglich gemacht. Es bedürfte dann Hilfskonstruktionen. All diese Leistungen müssten als Neben- und Treupflichten von der vertraglichen Rechtfertigung gedeckt werden können. Diese Rechtsunsicherheit und die Hilfskonstruktionen führen jedoch dazu, dass für jede Verarbeitung von Beschäftigtendaten für diese Zwecke Rechtsunsicherheiten im Bereich des Datenschutzrechts entstünden. Die Begründung zum bestehenden § 32 BDSG hat dieses Verarbeitungserfordernis bereits erfasst und zum Ausdruck gebracht,

> „Für andere Zwecke [i.e. außerhalb von Zwecken des Beschäftigungsverhältnisses] können auch im Verhältnis von Arbeitgeber und Beschäftigten die Vorschriften des Bundesdatenschutzgesetzes und anderer Gesetze, die eine Datenerhebung, -verarbeitung und -nutzung erlauben oder anordnen, weiterhin Anwendung finden.“ (BT-Drs. 16/13657, S. 21).

Die vorgeschlagenen Gesetzesentwürfe sehen dagegen fast ausnahmslos für freiwillige Leistungen ohne Rechtsposition keine Befugnis vor, die dafür erforderlichen Daten zu verarbeiten. Dabei dürfte kaum in Frage zu stellen sein, dass der Arbeitgeber die für die Durchführung der freiwilligen Leistung erforderlichen Beschäftigtendaten verarbeiten darf. Allerdings bestimmt § 4 Absatz 1 Satz 3 BDatGE-SPD, wenn auch ohne ausdrücklichen Bezug zu den allgemein Datenschutzvorschriften der §§ 4, 28 BDSG:

> „Rechtsvorschriften, die das Erheben und Verwenden von Beschäftigtendaten zu anderen Zwecken erlauben oder anordnen, werden durch dieses Gesetz nicht berührt."

Das Arbeitspapier der Berichterstatter der Koalitionsfraktionen trägt diesem Datenverarbeitungserfordernis Rechnung, in dem es eine klarstellende Regelung in § 27 Absatz 3 BDSG-RegE einbringt. Zusätzlich sollte zur Vermeidung von Widersprüchen vorgesehen werden, dass das bereichsspezifische Beschäftigtendatenschutzrecht auch bei **außerhalb des Beschäftigungsverhältnisses liegende Datenverwendungszwecke** Anwendung findet, wenn es ausdrücklich in den bereichsspezifischen Vorschriften erwähnt ist.

> „Für das Erheben, Verarbeiten und Nutzen von Beschäftigtendaten durch den Arbeitgeber für Zwecke eines früheren, bestehenden oder zukünftigen Beschäftigungsverhältnisses gelten die Vorschriften des zweiten, dritten und vierten Unterabschnitts. **Für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Beschäftigten für andere, außerhalb des Beschäftigungsverhältnisses liegende Zwecke, finden die übrigen Bestimmungen des Gesetzes Anwendung.** Satz 1 gilt auch, wenn Beschäftigtendaten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden **oder wenn die Beschäftigtendatenverarbeitung im zweiten, dritten und vierten Unterabschnitt ausdrücklich geregelt ist.**"

Damit ist ausdrücklich der Weg zur Güterabwägung (Erlaubnis der Datenverarbeitung bei schwerer wiegendem Unternehmensinteresse nach § 28 I 1 Nr. 2 BDSG) für die Beschäftigtendatenverarbeitung eröffnet. Die Erhebung von nützlichen, doch nicht gebotenen Beschäftigtendaten für die freiwilligen Leistungen ist gesperrt.

4. Gestaltungsbefugnisse der Betriebs-/Tarifparteien

Fragestellung

Darf aufgrund von rechtssetzenden Betriebs- / Dienstvereinbarungen oder Tarifverträgen von den Standards des bereichsspezifischen Beschäftigtendatenschutzrechts abgewichen werden?

Beispiele

Betriebsvereinbarungen Arbeitszeiterfassung, SAP, E-Learning, Call Center, Data-Loss-Prevention.

Fazit aus Sicht des Datenschutzbeauftragten

Datenschutzgestaltende Betriebs- / Dienstvereinbarungen und Tarifverträge entsprechen dem Gedanken des Betriebsverfassungsgesetzes und ermöglichen die Mitwirkung der Beschäftigten an datenschutzkonformen Lösungen über den Wortlaut der auslegungsbedürftigen Begriffe des Beschäftigtendatenschutzrechts hinaus. Eine zwingende Beteiligung des Datenschutzbeauftragten sichert, dass der datenschutzmäßige unabhängige Sachverstand in die Betriebsvereinbarung einfließt.

Im Einzelnen

Die Befugnis, mit dem Mittel der Betriebs- / Dienstvereinbarung oder eines Tarifvertrags von den bereichsspezifischen Vorschriften abzuweichen, wird von allen Entwürfen vorgesehen (§ 4 Absatz 1 Satz 2 BDSG-RegE; § 4 Absatz 1 Satz 1 BDatGE-Bündnis 90/DIE GRÜNEN) oder doch vorausgesetzt (§§ 18 Absatz 1 Satz 2, 18 Absatz 2 Satz 2 BDatGE-SPD). Diese gesetzliche Regelung ist zu begrüßen, da sie rechtssystematisch folgerichtig ist. Trotz Vertragsbezeichnung sind Betriebsvereinbarungen doch Normen, da sie grundsätzlich alle Arbeitnehmer erfassen (§ 77 Absatz 4 Satz 1 BetrVG):

> „Betriebsvereinbarungen gelten unmittelbar und zwingend."

Wie sonstige Normen auch müssen Betriebsvereinbarungen verhältnismäßig sein. Die mit der Vereinbarung vorgesehene Beschäftigtendatenverarbeitung muss unter Berücksichtigung des informationellen Selbstbestimmungsrechts geeignet, erforderlich und zumutbar sein, um den von den Vertragsparteien erstrebten Zweck zu erreichen.

Der Regierungsentwurf gibt hier zu rechtlichen Bedenken Anlass, wenn er formuliert, dass von allen Beschäftigtendatenschutzvorschriften „nicht zu Ungunsten der Beschäftigten abgewichen" werden dürfe. Das könnte dahingehend verstanden werden, dass den Betriebs- und Tarifparteien **ihre verfassungsrechtlich gebundene Gestaltungsbefugnis genommen werden solle**. Es wäre jedoch eine erhebliche Beschränkung der Gestaltungsbefugnisse der Betriebs- und Tarifvertragsparteien, wenn der Gesetzgeber ihnen im Datenumgang jegliche Befugnis absprechen würde.

Unabhängig davon würde ein Verbot von gestaltenden Betriebsvereinbarungen und Tarifverträgen für den Datenumgang die weiteren Wirkungen dieser Instrumente dauerhaft zurückweisen. Sie schaffen nach der Erfahrung in größeren Betrieben Transparenz, in dem die Parteien weit genauer als das Gesetz ausführlich beschreiben, welche Beschäftigtendatenverarbeitung zulässig ist und welche nicht. Auch konkrete Verwertungsverbote werden ausgesprochen. Teilweise konkretisieren sie auch Datenschutzvorschriften.

Außerdem würde die **Ordnungsfunktion des Betriebs-/Personalrats beim Beschäftigtendatenschutz** in ihrer Bedeutung abnehmen. Soweit Datenschutzvorschriften die Beschäftigten betreffen, kommt ihm zwar unabhängig von Betriebsvereinbarungen eine Überwachungsaufgabe zu.

> Der Betriebsrat hat folgende allgemeine Aufgaben: (1) darüber zu wachen, dass die zugunsten der Arbeitnehmer

> geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden;“ (§ 80 Absatz 1 Nr. 1 BetrVG)

Die Einhaltung sehr abstrakt-genereller Rechtsnormen ist für den Betriebsrat im Betriebsalltag allerdings nicht immer leicht zu kontrollieren. Ohne Betriebsvereinbarungen zum Beschäftigtendatenschutz würde seine Kontrollaktivität in diesem Bereich rechtstatsächlich vermutlich abnehmen. Gerade kurze und klare Betriebsvereinbarungen ermöglichen demgegenüber eine **effizientere Kontrolle, da der kontrollierende Betriebsrat die umzusetzenden Normen unmittelbar mit beeinflusst hat**. Seine gewisse Gewährfunktion wird damit leichter umsetzbar. Doch wenn mit der Betriebsvereinbarung, wie mit einer Dienstvereinbarung oder einem Tarifvertrag, von den gesetzlichen Beschäftigtendatenschutzregeln nicht zu Ungunsten abgewichen werden darf, droht das „Aus“ der Betriebsvereinbarung zum Beschäftigtendatenschutz, da angesichts der vielen vagen, wertausfüllungsbedürftigen Begriffe im geplanten Beschäftigtendatenschutzrecht das Risiko rechtswidriger Vereinbarungen hoch sein würde.

Zudem ist zu beachten, dass die „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ der zwingenden Mitbestimmung und damit im Zweifel einer Betriebs-/Dienstvereinbarung unterworfen sind (§ 87 Absatz 1 Nr. 6 BetrVG). Da sie jedoch auch regelmäßig mit einer personenbezogenen Beschäftigtendatenverarbeitung einhergehen, würde das Verbot der „Datenschutzgestaltung per Betriebs-/Dienstvereinbarung“ zu einem unlösbarem Dauerkonfliktfeld führen.

Der Gesetzgeber sollte daher die Gestaltungsbefugnisse der Betriebs- und Tarifvertragsparteien und die Grundsätze der Rechtsprechung des Bundesarbeitsgerichts, verhältnismäßige Bindung der Vereinbarungen, in seiner neuen Regelung klarstellen indem er in § 32l Absatz 5 formuliert:

> **„Von den Vorschriften dieses Unterabschnitts darf durch Betriebs- / Dienstvereinbarungen und Tarifverträgen auch zu Ungunsten der Beschäftigten abgewichen werden, wenn**
> **a) kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt [Alt.: sofern Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig ist] und**
> **b) der Arbeitgeber dem Beschäftigten die Regelung durch geeignete Maßnahmen zugänglich gemacht hat.**
> **Als Indiz für eine verhältnismäßige Regelung gilt insbesondere, dass die Beschäftigten einen angemessenen Ausgleich für die Beschränkung ihrer Persönlichkeitsrechte erhalten**“.

Dabei ist zu beachten, dass der Ausgleich einen datenschutzmäßigen Bezug hat. Insbesondere per Betriebs-/Dienstvereinbarung dokumentierte und kontrollierbare Verfahren der Beschäftigtendatenverarbeitung unter Einschluss von Kontrollmöglichkeiten des Datenschutzbeauftragten und des Betriebs-/Personalrats tragen dazu bei, ein Mehr an faktischem Datenschutz zu schaffen.

Alternativ kommt eine Liste solcher, gattungsmäßig bezeichneter Beschäftigtendatenverarbeitungen in Betracht, die besonders sensibel sind und bei denen von vornherein kaum ein verhältnismäßiges Abweichen durch Betriebs- / Dienstvereinbarung oder Tarifvertrag angenommen werden kann.

Zudem ist zu empfehlen, die Einhaltung der vorgenannten Anforderungen durch eine vorherige Prüfung des Datenschutzbeauftragten verfahrensmäßig zu sichern. Die Datenverarbeitung

aufgrund einer solchen Betriebsvereinbarung und damit deren Verhältnismäßigkeit könnten als weiterer Kontrollpunkt der Vorabkontrolle nach § 4d Absatz 5 BDSG unterworfen werden (wie es der BDSG-RegE selbst bereits für die Datenerhebung ohne Kenntnis des Betroffenen, für die Datenerhebung durch Ortungssysteme, durch biometrische Verfahren ausdrücklich vorsieht).

> „Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn
>
> 1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
> 2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,
> 3. **durch eine Betriebs- / Dienstvereinbarung oder einen Tarifvertrag von den Vorschriften des Zweiten Unterabschnitts des Dritten Abschnitts dieses Gesetzes zu Ungunsten des Beschäftigten abgewichen wird**,
>
> es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.“

5. Verarbeitungseinwilligung des Beschäftigten

Fragestellung

Ist der Ausschluss der Einwilligung als Rechtfertigung einer Datenverwendung sachgerecht, wenn lediglich einzelne Erlaubnisse für mögliche Einwilligungen ausgesprochen werden?

Beispiele

Arbeitgeber fragt nach der Einwilligung, die Bewerbungsunterlagen im Konzern an potentiell suchende Konzerngesellschaften weiterzureichen; Beschäftigter willigt ein, dass ein Portraitfoto in der Firmenbroschüre erscheint, dass sein Kurzlebenslauf im Web erscheint.

Fazit aus Sicht des Datenschutzbeauftragten

Die Einwilligung wird selten das Mittel der Wahl sein, weil die gesetzliche Generalklausel mit ihrer Freiwilligkeitsanforderung für Einwilligungen ein erhebliches Schutzniveau schafft. Im Zweifel werden Unternehmen diese Rechtfertigungsgrundlage meiden, weil die Rechtsunsicherheit schnell zur Unwirksamkeit der Einwilligung führt. Für Situationen, in denen die Freiwilligkeit typischerweise nicht gegeben ist, mag der Gesetzgeber die typisierte Unfreiwilligkeit durch Einwilligungsverbot feststellen. Soweit diese Typisierungen nicht möglich sind, bleibt als abgeschwächte Regelungsvariante die Bezugnahme auf eine die Einwilligung ergänzende Verhältnismäßigkeitsprüfung.

Im Einzelnen

Datenverarbeitungen sind auch zulässig, wenn der Betroffene in sie eingewilligt hat. Schon heute sind die Anforderungen in die wirksame Einwilligung derart umfangreich, dass eine wirksame Einwilligung selten zu erlangen sein wird. Neben der Schriftlichkeit kommt es vor allem auf die Erläuterung der Datenverarbeitung an, genauer auf den Zweck. Der Betroffene muss Anlass, Ziel und Folgen seiner Einwilligung abschätzen können (*Simitis-Simitis*, BDSG, § 4a Rn. 70), „wissen, was mit den Daten geschehen soll“ (*Gola/Schomerus*, BDSG, § 28 Rn. 15). Und hinzu tritt das weitere Erfordernis der freiwilligen Ertei-

lung. Das Bundesverfassungsgericht BVerfG (Kammerbeschluss, 23.10.2006, 1 BvR 2027/02) stellt darauf ab, **ob der Betreffende noch „eigenverantwortlich und selbständig" seinen informationellen Selbstschutz sicherstellen kann**. Zudem steht bei Unternehmen die grundsätzliche Widerruflichkeit der Einwilligung einer Datenverarbeitung auf der Basis einer Einwilligung entgegen, sofern nicht der Widerruf treuwidrig ist.

Angesichts dieser Umstände **stellen Unternehmen praktisch selten auf die Einwilligung als Rechtfertigungsgrundlage ab**. Die unternehmerische Wertschöpfung soll nicht auf rechtsunsicheren und zudem einseitigen widerruflichen Erklärungen der Beschäftigten beruhen. Insofern kommt die Einwilligung hauptsächlich in Betracht, wenn es um die Nebenverarbeitung von Beschäftigtendaten geht.

Der Regierungsentwurf wie BDatGE-Bündnis 90/DIE GRÜNEN sehen die Beschränkung der Einwilligung im Beschäftigungsverhältnis auf bestimmte Datenverarbeitungen ausdrücklich vor. Im Übrigen sei die Rechtfertigung durch Einwilligung ausgeschlossen (§ 32l Absatz 1 BDSG-RegE; § 4 Absatz 1 Satz 1 BDatGE-Bündnis 90/DIE GRÜNEN).

Der Regierungsentwurf erfasst folgende Fälle als Ausnahme.

- Dritterhebung von Beschäftigtendaten,
- Gesundheitsprüfung,
- Eignungstest,
- längere Aufbewahrung von Bewerbungsunterlagen,
- jeweils im Bewerbungsverfahren,
- Fotos,
- Telekommunikationsinhalte bei dienstlicher Nutzung (mit/ohne Ankündigung),

BDatGE-Bündnis 90/DIE GRÜNEN erlaubt die Einwilligung in folgenden Fällen.

- Dritterhebung von Beschäftigtendaten im Bewerbungsverfahren,

- Gesundheitsprüfung, Test auf übertragbare vorhandene Krankheiten, medizinische und psychologische Befunde,
- Alkohol- und Drogentests,
- längere Aufbewahrung von Bewerbungsunterlagen,
- Weitergabe vor allem in Konzernen,
- Weitergabe bei Betriebsübergang,
- Fotos, wobei zusätzlich noch eine Güterabwägung vorzunehmen ist,
- Telekommunikationsinhalte bei dienstlicher Nutzung (mit Ankündigung).

Demgegenüber regelt BDatGE-SPD in Einzelfällen eine Einwilligungsmöglichkeit ausdrücklich und spricht sich außerhalb des Gesetzesentwurfstexts allgemein gegen „‘erzwungene‘ freiwillige Einwilligungen“ aus.

Geht es um Beschäftigtendatenverarbeitung **für Zwecke des Beschäftigungsverhältnisses** kommt eine konkretisierende Beschränkung der Einwilligung durchaus in Betracht. **Einer generellen Einschränkung mit Öffnungsklausel für bestimmte Fälle steht jedoch entgegen, dass die EU-Datenschutzrichtlinie jedenfalls keinen allgemeinen Ausschluss der Einwilligung vorsieht.** Ausschlüsse setzen typisierende Fallgruppen voraus, bei denen der Gesetzgeber typisierend unterstellt, dass die Anforderungen an eine Einwilligung gemäß § 4a BDSG nicht gegeben sind. Diese Typisierung fehlt dem Gesetz, wenn es mit einer Positivliste zulässiger Einwilligungsfälle arbeitet, wie sie der Regierungsentwurf und BDatGE-Bündnis 90/DIE GRÜNEN vorsieht. Ganz praktisch ergeben sich Fälle, bei denen der Ausschluss nicht durch eine typisierte Unfreiwilligkeit gekennzeichnet ist. So fehlt es beispielsweise an einer typisierten Unfreiwilligkeit, wenn der Beschäftigte nach Kündigung seine Einwilligung in die weitere Nutzung seines gemischt genutzten Firmen-E-Mail-Postfachs oder in die Löschung seines Homeverzeichnisses gibt.

Die Beibehaltung des strengen Grundsatzes der Einwilligungszulässigkeit nach § 4a BDSG mit einer typisierten Liste von verbotenen Einwilligungstatbeständen wäre demgegenüber denkbar.

6. Private Nutzung von Telekommunikationsdiensten

Fragestellung

Nahezu unlösbare Konflikte produziert die Inanspruchnahme von E-Mail und WEB durch die Beschäftigten für private Zwecke. Genügen die vorgeschlagenen Vorschriften dem Bedürfnis nach Rechtsklarheit unter Wahrung des Fernmeldegeheimnisses?

Beispiele

Beschäftigter ist berechtigt, die dienstliche E-Mail-Funktion auch für private Mails zu nutzen. Der SPAM-Filter-Betreiber schaut sich jedoch in Einzelfällen einzelne Mails an, um SPAM von anderen Mails zu unterscheiden. Im Urlaub gibt der Beschäftigte seinem Kollegen das Passwort, damit dieser die dienstlichen E-Mails bearbeiten kann. Der überblättert zwar private E-Mails, doch es ist für ihn unvermeidlich, grob die Inhalte privater E-Mails zur Kenntnis zu nehmen. Im Fall eines Zugriffproblems erhält der Beschäftigte Unterstützung von der IT. Der Mitarbeiter IT stellt zufällig fest, dass der Nutzer strafrechtsrelevante Inhalte in seinem E-Mail-Postfach hat.

Fazit aus Sicht des Datenschutzbeauftragten

Angesichts des Fernmeldegeheimnisses ist es schwer, eine interessengerechte und verfassungskonforme Lösung zu finden. Der Regierungsentwurf schafft hier mit § 32i Absatz 4 Satz 2 eine – wenn auch streng beschränkte – Möglichkeit, die private Nutzung zuzulassen, ohne dass sich das Unternehmen mit der Entscheidung für eine Privatnutzung seiner Beschäftigten handlungsunfähig macht.

Im Einzelnen

Vielfach finden sich in Unternehmen keine oder nur lückenhafte Regeln zum Umgang mit den Firmengeräten und Firmenaccounts zu privaten Zwecken. Die geübte private Nutzung führt den Arbeitgeber im Zweifel in die Rolle des Diensteanbieters mit einem Unterworfensein unter das Fern-

meldegeheimnis. Bei jedwedem Zugriff auf den auch privat genutzten Account des Beschäftigten droht die Verletzung des Fernmeldegeheimnisses. Zugriffe lassen sich jedoch praktisch nachvollziehbar nicht verhindern, wenn es geht um

a) die steuer- und handelsrechtlich gebotene Vorhaltung von elektronischen Dokumenten,
b) den Zugriff, um Datensicherheitsrisiken zu erfassen,
c) den Zugriff auf E-Mails bei Abwesenheit des Account-haltenden Beschäftigten,
d) die Kontrolle, weil strafrechtswidriger oder grob vertragswidriger Umgang mit der Privatnutzungsbefugnis zu vermuten ist oder
e) den Betrieb von SPAM-Filtern.

Die herrschende Meinung sieht als Lösung nach gegenwärtiger Rechtslage nur die Option, den Beschäftigten – gegen den Kommunikationstrend in der Gesellschaft – die Nutzung des Accounts für private Zwecke ausdrücklich zu untersagen und die Einhaltung dieses Verbots zu kontrollieren. Dieses Vorgehen liegt weder im überwiegenden Interesse der Arbeitgeber noch der Beschäftigten. Daher bedarf es einer gesetzlichen Regelung, die einen Interessenausgleich unter Beachtung des verfassungsrechtlich geschützten Fernmeldegeheimnisses (Art 10 Absatz 1 GG) herbeiführt.

Der Regierungsentwurf schafft mit § 32i Absatz 4 Satz 2 BDSG-RegE eine Lösung.

> „Der Arbeitgeber darf private Daten und Inhalte nur erheben, verarbeiten und nutzen, wenn dies zur Durchführung des ordnungsgemäßen Dienst- oder Geschäftsbetriebes unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat.“

Die Datensicherheitsanforderungen sind durch die Befugnisse des § 100 TKG erfasst. Regelungslücken verbleiben für die Kontrollmöglichkeiten für strafrechtswidrige oder grob vertragswidrige Privatnutzung durch den Beschäftigten (siehe oben Fall d). Hier wäre eine Lösung innerhalb der vorhandenen bereichsspezifischen Datenschutzregeln des TKG denkbar.

Der BDatGE-SPD mit § 14 Absatz 4 lässt die Konfliktlage mit einer Bestätigung des Fernmeldegeheimnisses ungelöst, fixiert andererseits – anders als das TKG – eine zeitliche Löschfrist für TK-Daten, die aus Datensicherheitsgründen gespeichert sind (§ 14 Absatz 5 Satz 2). BDatGE-Bündnis 90/DIE GRÜNEN sehen mit § 12 Absatz 5 und 6 ähnliche Regelungen wie BDatGE-SPD vor, wobei nur eine typisierte Löschfrist normiert werden soll.

7. Geschäftsdatenanalyse (Screening)

Fragestellung

Erfassen die Vorschläge zum Beschäftigtendatenumgang bei Geschäftsdatenanalysen die geübten Sachverhalte?

Beispiele

Ein Unternehmen gleicht die Kontonummern seiner Beschäftigten, die jedenfalls technisch verfügungsbefugt sind, mit den Kontonummern ihrer Lieferanten ab; ein weiterer Abgleich sucht die Vermögensverfügungen heraus, bei denen die Vollmachtsgrenzen betragsmäßig zu mehr als 95% in Anspruch genommen worden sind; Logfiles werden von Netzwerküberwachungssystemen zum Erkennen von Angriffen eingesetzt; gewartete Maschinen zeichnen die Wartungsaktivitäten auf.

Fazit aus Sicht des Datenschutzbeauftragten

Die Problematik wird allein vom Regierungsentwurf erfasst. Allerdings verkürzt der Regierungsentwurf die mit einem Screening verbundene Beschäftigtendatenverarbeitung auf die Ermittlung von Strafrechtsverstößen und schwerwiegenden Pflichtverletzungen. Es sollte dringend klargestellt werden (sie-

he unten), dass Screeningmaßnahmen unabhängig von einer Beschäftigtenkontrolle stattfinden. Da mit dem Screening durch die Zuordnungsmöglichkeit eine Beschäftigtenkontrolle verbunden oder gegebenenfalls beabsichtigt ist, muss flankierend ein datenschutzkonformer Umgang geregelt werden. Dem wird der Regierungsentwurf gerecht, in dem er ein Pseudonymisierungsgebot festschreibt. Die Kontonummer wie die Beschäftigten-ID kann ein Pseudonym darstellen, solange sie im Unternehmen nicht allgemein bekannt ist.

Im Einzelnen
Im Tagesgeschäft eines Unternehmens fallen täglich eine Vielzahl von Geschäftsdaten und Daten aus den Buchhaltungssystemen an. Während im sehr kleinen Unternehmen diese Daten noch durch die Geschäftsleiterhand steuer- und prüfbar sind, fällt diese Möglichkeit mit zunehmender Unternehmensgröße weg. Damit droht dem Unternehmen der Fehlgebrauch und der Missbrauch von Verfügungen, die sich auf die Vermögens-, Finanz- und Ertragslage des Unternehmens auswirken. Teilweise ist ein internes Kontrollsystem verbindlich. Es ist **darauf gerichtet, die Vorgaben der Geschäftsleitung zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit zu steuern**. Auch Maßnahmen zum Schutz des Vermögens und damit zur Verhinderung und Aufdeckung von Vermögensschädigungen, zur Verlässlichkeit der Rechnungslegung sowie zur Einhaltung maßgeblicher rechtlicher Vorschriften gehören dazu.

Neben organisatorischen Vorgaben ist auch der Fluss der Geschäftsdaten zu kontrollieren. Soweit mit diesen Geschäftsdaten Beschäftigtendaten verbunden sind, liegt eine Beschäftigtendatenverarbeitung vor. Die öffentliche Diskussion um Screeningmaßnahmen mit Beschäftigtenbezug hat dazu geführt, dass der Regierungsentwurf und der BDatGE-Bündnis 90/DIE GRÜNEN hierfür ausdrückliche Vorschriften vorsehen. BDatGE-Bündnis 90/DIE GRÜNEN stellt allerdings allein die Recherche zu einzelnen Beschäftigten in den Vordergrund und kommt zu einer Einschränkung auf konkrete Verdachtsfälle (§ 11 Absatz 1). Völlig ungeregelt bleibt damit die normale Geschäftsdatenanalyse, die begleitend innerhalb eines Unternehmens letztlich auch immer auf einzelne Beschäftigte zurückge-

führt werden kann, sofern nicht der Beschäftigtenbezug endgültig – vor allem durch Anonymisierung – aufgehoben wird. Er ist daher mit den gesetzlichen Kontrollpflichten des Unternehmens nicht vereinbar.
Durch die heutige Technologie ist es in vielen Fällen nicht zu verhindern, dass der Beschäftigtenbezug bei geschäftlichen Handlungen des Beschäftigten zumindest herstellbar ist. Allein die Tätigkeit eines Wartungstechnikers ist heute über sein Betreuungsgebiet und die automatischen Aufzeichnungen von komplexen Maschinen erkennbar. Gerade im Gesundheitsbereich sehen Regelungen wie die GCP(Good Clinical Practice)-Verordnung vor, wie klinische Studien mit Arzneimitteln am Menschen durchzuführen sind und welche personenbezogenen Daten, auch von Beschäftigten, langjährig (10 Jahre) vorzuhalten sind. Letztlich geht es um Qualitätskontrollen im Interesse der Gesundheit betroffener Patienten. Auch einfache Qualitätsmanagementsysteme sehen rückführbare Kontrollen vor. In diesen Fällen kommt es nicht darauf an, aufgrund eines konkreten Verdachts zu ermitteln. Vielmehr geht es um die ständige Überwachung von bestimmten Qualitätsanforderungen.

Diese präventiven Überwachungsmaßnahmen können daher schon rechtlich nicht verboten werden, ohne anderen gesetzlichen Vorgaben oder daraus entwickelten Standards zu widersprechen. So ist auch das Screening nicht in erster Linie auf die Ermittlung von rechtswidrigen Handlungen gerichtet, sondern auf die Dokumentation, dass die Geschäftsleiter die Sorgfalt eines ordentlichen Geschäftsmannes angewendet haben.

Auf der anderen Seite haben Beschäftigte berechtigte Geheimhaltungsinteressen. Da Screeningmaßnahmen prinzipiell alle transaktionsbeteiligten Beschäftigten betreffen können, erfassen sie auch völlig ordnungsgemäß handelnde Beschäftigte. Aus Datenschutzsicht besteht die überwiegende Meinung, dass deren Daten nicht ohne überwiegendes Interesse verarbeitet werden. Fehlt das ex post, stellt sich also nachträglich heraus, dass kein ordnungswidriges Verhalten vorliegt, hätten ihre Transaktionen nicht überwacht werden müssen. Da jedoch Screeningmaßnahmen präventiv erfolgen, kann es nicht auf eine nachträgliche Betrachtung ankommen. Dennoch fällt der Datenschutz nicht weg. Mit dem Mittel der Pseudonymisierung

stellt das bisherige BDSG eine Technik zur Verfügung, die verhindert, dass ein bestimmter Datensatz von sich aus unmittelbar einem bestimmten Beschäftigten zugeordnet ist.

Der Regierungsentwurf wird dieser ausgleichenden Gestaltung weitgehend gerecht, wenn er wie folgt formuliert.

> „Der Arbeitgeber darf zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen durch Beschäftigte im Beschäftigungsverhältnis […] einen automatisierten Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form mit von ihm geführten Dateien durchführen." (§ 32 Absatz 3 Satz 1)

Allerdings ist er nicht konsequent. Er erkennt die präventive Funktion dieser Screenings, wenn es heißt „Ergibt sich ein Verdachtsfall …" (§ 32 Absatz 3 Satz 2). Der Regierungsentwurf geht also davon aus, dass das Screening selbst noch nicht verdachtsbezogen ist, beschränkt jedoch das Screening auf die Erforschung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen. Das Ergebnis eines einzelnen Screenings ist jedoch nicht zwingend auf eine Straftat oder eine schwerwiegende Pflichtverletzung bezogen. Erst die weitere manuelle Auswertung kann dann eine schwerwiegende Pflichtverletzung ergeben. Doch bis zu diesem Auswertungsergebnis steht ein solcher Verdacht nicht fest. Insofern ist eine Beschränkung auf Straftaten oder anderen schwerwiegenden Pflichtverletzungen nicht sachgerecht. Der Regierungsentwurf berücksichtigt nicht hinreichend den Zweckbindungsgrundsatz des BDSG. Bei enger Auslegung führt die Formulierung dazu, dass ein Screening immer die Unsicherheit in sich trägt, dass das gefundene Ergebnis jedenfalls nicht für sich allein Straftaten oder andere schwerwiegende Pflichtverletzungen begründet. Denn das Screening richtet sich in erster Linie immer auf die Analyse einzelner Datensätze zu Geschäftsprozessen. Setzt sich die enge Auslegung durch, droht das „Aus" der Rechtmäßigkeit des Screenings, sofern nicht das Unternehmen seine Screenings

immer unter den Vorbehalt der Ermittlung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen stellt.

Diese Verengung der Rechtfertigung von Screeningmaßnahmen auf Ermittlungsmaßnahmen gegen Beschäftigte sollte mit einer modifizierten Formulierung des § 32d Absatz 1 Satz 2 und Satz 3 klargestellt werden.

> Der Arbeitgeber darf zur **ordnungsgemäßen Überwachung seiner Geschäftsprozesse automatisierte Analyseverfahren einsetzen. Soweit dabei Beschäftigtendaten verwendet werden, sind diese zu pseudonymisieren oder zu anonymisieren. Ergibt sich ein Verdacht einer Straftat, insbesondere nach den §§ 266, 299, 331 bis 334 des Strafgesetzbuchs, oder einer anderen schwerwiegenden Pflichtverletzung durch einzelne Beschäftigte**, dürfen die Daten personalisiert werden. Der Arbeitgeber hat die näheren Umstände, **die ihn zu einer Personalisierung nach Satz 1 veranlassen,** zu dokumentieren. Die Beschäftigten sind vor den Maßnahmen über Inhalt, Umfang und Zweck des automatisierten Abgleichs zu unterrichten.“

8. Inkrafttretensregelung

Fragestellung

Ist die kurze Inkrafttretensfrist von 6 Monaten sachgerecht?

Fazit aus der Sicht des Datenschutzbeauftragten

Die Umsetzungsfrist sollte zumindest 1 Jahr betragen.

Im Einzelnen

Die vorgesehenen Änderungen machen eine umfassende Revision der unternehmensinternen Prozesse aus Datenschutzsicht erforderlich. Auch Betriebsvereinbarungen werden auf den Prüfstand zu stellen sein. Der Regierungsentwurf und BDatGE-SPD sehen ein Inkrafttreten sechs Monate nach Verkündung im Bundesgesetzblatt vor. BDatGE-Bündnis 90/DIE GRÜNEN regelt trotz umfangreicher Änderungen ein sofortiges Inkrafttreten mit Verkündung.

Die konkreten Inhalte der Beschäftigtendatenschutzregeln waren für die Adressaten bisher nicht absehbar. Im Gesetzgebungsverfahren des Bundestages sind noch Änderungen zu erwarten, die sich wesentlich auf die Rechte und Pflichten der Beschäftigten und Arbeitgeber und damit auch der Betriebs- und Personalräte auswirken. Soweit es um die Frage des „Ja“ oder „Nein“ zu einer Datenverarbeitung geht (Verbote bestimmter Beschäftigtendatenverwendung) und auch keine Ersatzmaßnahmen erforderlich sind, bedarf es keiner großen Umsetzungsfrist. Sobald dagegen Dokumentationspflichten, mit Beschäftigteninformationspflichten, Prüfungspflichten des Datenschutzbeauftragten und Betriebs- und Dienstvereinbarungen betroffen sind, ist eine sechsmonatige Umsetzungsfrist im Rahmen der Betroffenenprozesse nicht realistisch.

Das Fehlen einer Umsetzungsfrist für die neuen Regeln zur Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz aus dem Jahre 2009 hat gezeigt, dass unrealistische Umsetzungszeiträume hinsichtlich des gesetzgeberischen Ziels eindeutig kontraproduktiv sind. So gab es im Jahre 2009 seitens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und der Landesdatenschutzaufsichtsbehörden höchst unterschiedliche Vorstellungen, wie viel Zeit man den Unternehmen für die Umsetzung der neuen Regeln einräumt; nicht im Sinne einer Umsetzungsfrist (vom Gesetz nicht vorgesehen), sondern im Sinne eines Absehens von einer Kontrolle (Duldung alter Zustände). Das Fehlen einer Frist führte sogar zu einem Auslegungsargument. Wenn der Gesetzgeber keine Umsetzungsfrist oder eine nicht passende vorsieht, sei eine gesetzliche Vorschrift im Zweifel so auszulegen, dass keine Anpassung erforderlich sei, weil der Gesetzgeber andernfalls auf eine angemessene Frist nicht verzichtet hätte.

9. Andere, Beschäftigtendatenverarbeitung vorsehende Gesetze

Fragestellung

Wie sind andere gesetzliche Vorschriften zu berücksichtigen, die eine Beschäftigtendatenverarbeitung verlangen?

Fazit aus Sicht des Datenschutzbeauftragten

Die Beschäftigtendatenschutzvorschriften sollten um einen Satz ergänzt werden, der deutlich macht, dass eine Beschäftigtendatenverarbeitung erlaubt ist, wenn andere gesetzliche Vorschriften sie erforderlich machen.

Im Einzelnen

Das Datenschutzrecht ist eine Querschnittsmaterie. Es legt sich gewissermaßen über fast alle Gebiete gesetzlicher Regelungsbereiche, weil dieser typischerweise mit einer Verarbeitung personenbezogener Daten einhergeht. Verbietet das Datenschutzrecht eine bestimmte Verarbeitung, so ergibt sich eine Kollision, wenn andere Gesetze die fragliche Datenverarbeitung erforderlich machen. Beispiel: bankenaufsichtsrechtliche Kontrollpflichten wie Pflichten zu Risikoüberwachungsprozessen (§ 25a Absatz 1 Satz 2 Nr. 1b) und zur Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstiger strafbarer Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können (§ 25c KWG). Diese Kollisionen gilt es interessengerecht zu lösen. Hierzu könnte unter anderem Sachverstand zuständiger Behörden genutzt werden; wie beispielsweise der BaFin. BDatGE-Bündnis 90/DIE GRÜNEN (§ 4 Absatz 1 Satz 1) berücksichtigt in seiner zweiten Fassung die Datenverwendungserfordernisse aus anderen Gesetzen mit der Formulierung

> „soweit […] eine andere Rechtsvorschrift dies erlaubt, ausdrücklich anordnet […]“.

Der Regierungsentwurf erkennt die Problematik, verweist allerdings auf eine Prüfung im weiteren Gesetzgebungsverfahren. BDatGE-SPD (§ 4 Absatz 1 Satz 2) löst den Konflikt nicht, sondern verlangt, dass das andere Gesetz die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses erlauben oder anordnen müsse. Doch selbst in aktuellen gesetzlichen Regelungen – wie beispielsweise zur Beschäftigtenkontrolle bei möglichen Insidergeschäften von Beschäftigten (§ 33 WpHG) – fehlt eine ausdrückliche Erwähnung von Beschäftigtendatenverwendung. Sie setzen diese voraus.

Die endgültigen Vorschriften zum Beschäftigtendatenschutz müssen daher eine Regelung aufweisen, die dem Rechtsanwender vorgibt, wie Kollisionsfälle zu lösen sind. Da auch sonstige Gesetze den Grundrechten unterworfen sind, bietet sich die Heranziehung des Verhältnismäßigkeitsgrundsatzes an.

Dr. Philipp Kramer
Rechtsanwalt

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 G

DVD Deutsche Vereinigung für Datenschutz e. V.

Rheingasse 8 - 10
53113 Bonn

Telefon: 0228/22 24 98
Telefax: 0228/24 38 470

dvd@datenschutzverein.de
www.datenschutzverein.de

Berlin/Bonn, den 17.05.2011

Verfasser : Sönke Hilbrans, Berlin
Rechtsanwalt und Fachanwalt für Strafrecht

Öffentliche Anhörung im

Innenausschuss des Deutschen Bundestages

zum Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes

BT-Drucksache 17/4230 u. a.

am 23.05.2011

Schriftliche Stellungnahme

Die folgenden Ausführungen befassen sich im Wesentlichen mit dem Gesetzentwurf der Bundesregierung für ein Gesetz zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230 vom 15.12.2010) und dem Arbeitspapier der Berichterstatter der Koalitionsfraktionen vom 10.05.2011. Diese Auswahl erfolgt allein im Hinblick auf den Verlauf des Gesetzgebungsverfahrens und möge nicht als Ablehnung der Gesetzentwürfe BT-Drs. 17/69 und BT-Drs. 17/4853 verstanden werden.

I. Allgemeines

Der Gesetzentwurf der Bundesregierung verfolgt das Ziel, praxisgerechte Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen, die Datenverarbeitung auf das zu Zwecken des Beschäftigungsverhältnisses Erforderliche zu beschränken, Beschäftigte wirksam vor Bespitzelungen am Arbeitsplatz zu schützen und gleichzeitig Arbeitgebern verlässliche Grundlagen für die Erfüllung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand zu geben. Diese Ziele verfehlt der Gesetzentwurf, weil

- er keine klare gesetzliche Differenzierung zwischen den mit personenbezogenen Daten von Beschäftigten verfolgten Zwecken trifft,
- daher informationelle Gewaltenteilung in Betrieb und Unternehmen nicht geschaffen wird,
- schutzwürdige Interessen von Beschäftigten im Wesentlichen vermittels allgemeiner Verhältnismäßigkeitserwägungen oder in der Praxis nicht abgrenzungsscharfer Generalklauseln geschützt werden sollen,
- effektive Verfahrensregelungen und Sanktionen zum Schutz der Beschäftigten vor Datenschutzverstößen (etwa Zustimmungsvorbehalte für den betrieblichen Datenschutzbeauftragten, Verwertungsverbote) nicht geschaffen werden.

Dagegen zielt der vorgelegte Entwurf auf Vorschriften, welche eine Überwachung und Ausforschung von Beschäftigten rechtlich absichern würden, die nach geltendem Recht unzulässig wären. In der Sache würden damit Datenschutzverstöße, welche noch in jüngster Zeit als Skandale gewertet wurden, legalisiert. Demgegenüber werden fortschrittliche Initiativen, welche Beschäftigte vor sachlich nicht angezeigten Eingriffen in ihre Persönlichkeitsrechte wirksam schützen könnten, nicht aufgegriffen. Auch hätte sich eine Gestaltung des Beschäftigtendatenschutzes in einem besonderen, von dem Bundesdatenschutzgesetz geschiedenen Gesetz empfohlen.

II. Zu den Regelungen des Entwurfs der Bundesregierung (BT-Drs. 17/4230) im Einzelnen:

1. § 32 BDSG-E: Datenerhebung von Bewerbern

a.) (§ 32 Abs, 2 BDSG-E): Die Anpassung der Erhebung sensibler Daten von Bewerbern an die Voraussetzungen des § 8 Abs. 1 AGG ist – anders als im Arbeitspapier der Berichterstatter der Koalitionsfraktionen vom 10.05.2011 befürchtet – nicht mit einer Ausweitung des Anwendungsbereichs des Allgemeinen Gleichbehandlungsgesetzes verbunden und in der Sache zu begrüßen. Es empfiehlt sich allerdings, im Hinblick auf den bestehenden und auch von der EU- Datenschutzrichtlinie geforderten gesetzlichen Schutz besonderer Arten personenbezogener Daten (§ 3 Abs. 9, § 28 Abs. 6 – 9 BDSG u. a.), die verschiedenen Schutzsysteme für besonders zu schützende Daten aneinander anzupassen. Im Hinblick darauf und auf die etablierte Rechtsprechung deutscher und europäischer Gerichte sollte eine Erhebung von Bewerberdaten über eine Gewerkschaftszugehörigkeit und Schwangerschaft generell verboten werden.

b.) (§ 32 Abs. 6 S. 2 und 3 BDSG-E): Der Zugriff von Arbeitgebern auf veröffentlichte Informationen bedarf einer Regulierung. Veröffentlichungen können von den Betroffenen ebenso wenig effektiv kontrolliert werden wie Einträge in kommerziellen Datenbanken (etwa von Auskunfteien). Es liegt auch auf der Hand, dass von den Betroffenen in jüngerer Zeit selbst veröffentlichte Daten nicht den gleichen Schutzbedarf auslösen wie Daten, die schon lange zurückliegende Sachverhalte abbilden oder von Dritten in Unkenntnis oder gegen den Willen der Betroffenen erhoben und veröffentlicht werden. Das von Arbeitgeberseite regelmäßig wiederholten Bedürfnis nach der Erhebung und Verarbeitung veröffentlichter Daten wird von dem Gesetzentwurf nur unzureichend kanalisiert. Die in Abs. 6 S. 2 und 3 abgebildeten Arbeitgeberinteressen fallen in ihrer Wertigkeit erheblich hinter denen zurück, die § 4 Abs. 2 S. 2 BDSG für die Abweichung von dem Prinzip der offenen Direkterhebung im Allgemeinen voraussetzt. Für diese Privilegierung von Arbeitgebern gegenüber anderen Datenverarbeitern ist kein zwingender Grund ersichtlich. Auch sind sowohl die allgemeine Zugänglichkeit von Daten (Abs. 6 S. 2) als auch die Zweckbestimmung von sozialen

Netzwerken (Abs. 6 S. 3 2. Halbsatz) im Einzelfall nicht treffsicher zu bestimmen. So ist die Allgemeinzugänglichkeit von Daten bspw. in bestimmten Datenbanken in anderem datenschutzrechtlichen Kontext umstritten. Eine Hinweispflicht für den Arbeitgeber (Abs. 6 S. 2) zieht keinen effektiven verfahrensrechtlichen Schutz nach sich und wirft auch die Frage auf, ob die Informationspflicht nach Art. 11 EU-Datenschutzrichtlinie hinreichend umgesetzt wurde.

Der Entwurf ist daher zu überarbeiten mit dem Ziel, die Umgehung des gesetzlichen Primats der offenen Direkterhebung (§ 4 Abs. 2 S. 1 BDSG) auf Fälle zu beschränken, in denen Zweifel an der Vereinbarkeit der Erhebung mit dem allgemeinen Persönlichkeitsrecht der Bewerber nicht bestehen. Dies können Fälle nach Abs. 6 S. 3 1. Halbsatz sein.

c.) (§ 32 Abs. 6 BDSG-E): Der Gesetzentwurf untertrifft dass erforderliche Schutzniveau auch, soweit Bewerberdaten bei sonstigen Dritten erhoben werden dürfen. Denn gerade bei sonstigen Dritten – etwa früheren Arbeitgebern, Auskunfteien usw. – gespeicherte personenbezogene Daten sind regelmäßig einer effektiven Kontrolle durch die Betroffenen entzogen. Auch wenn die besonderen Formbestimmungen für die datenschutzrechtliche Einwilligung (§ 4a Abs. 1 BDSG) eingehalten werden, ist eine freiwillige Einwilligung in die Erhebung von Bewerberdaten bei Dritten praktisch nicht vorstellbar. Der Streit um ein bestehendes Fragerecht wird auf diesem Wege von dem Gesetzgeber allenfalls auf den Streit um eine bestehende Freiwilligkeit verlagert, ohne dass Rechtssicherheit geschaffen würde. Da es Arbeitgebern in den Fällen, in denen ein dringendes Informationsbedürfnis besteht, regelmäßig frei steht, von den Betroffenen selbst die erforderlichen Daten zu erheben – und sich etwa Zeugnisse vorlegen zu lassen – bedarf es einer für die Persönlichkeitsrechte der Betroffenen höchst gefährlichen Regelungen wie § 32 Abs. 6 S. 4 BDSG-E nicht.

2. § 32a BDSG-E: Ärztliche Untersuchungen und Eignungstests

a.) (§ 32a Abs. 1 BDSG-E): Die verkürzende Anlehnung an § 8 Abs. 1 AGG bei der Regelung betriebsärztlicher Einstellungsuntersuchungen geht insoweit fehl, als auch die gesundheitlichen Voraussetzungen im Hinblick auf die Bedingungen der Ausübung einer Tätigkeit untersucht werden können sollen. Denn soweit arbeitsmedizinische Voraussetzungen am Arbeitsplatz eingehalten werden, bedarf es eines spezifischen Abstellens auf die Bedingungen der Ausübung einer Tätigkeit nicht und reicht es aus, die Tauglichkeit des Bewerbers im Hinblick auf die objektiven allgemeinen gesundheitlichen Voraussetzungen der Tätigkeit zu prüfen.

b.) (§ 32a Abs. 2 BDSG-E): Der Entwurfstext will die Prüfung der Eignung eines Bewerbers für eine auszuübende Tätigkeit in jedweder Hinsicht eröffnen. Um eingriffsintensive, im Ergebnis sachlich nicht mehr gerechtfertigte Eignungstests insbesondere jenseits bestehender anerkannter wissenschaftlicher Methoden zu unterbinden, ist die Durchführung solcher Tests auf die Ermittlung einer objektiven fachlichen Eignung zu beschränken. Eine Einwilligung nach § 32a Abs. 2 S. 4 BDSG-E kann, da der Bewerber faktisch jenseits des Abbruchs des Bewerbungsverfahrens keine Wahlfreiheit bei der Teilnahme an Eignungstests hat, die persönlichkeitsrechtlichen Mängel des Entwurfs nicht heilen.

3. § 32b BDSG-E: Verarbeitung und Nutzung von Bewerberdaten

Die Löschungspflicht nach § 32b Abs. 3 BDSG-E ist zu schärfen: Der nach der Gesetzesbegründung nur deklaratorisch verstandene Verweis auf § 35 Abs. 2 S. 2 BDSG in § 32b Abs. 3 BDSG-E kann entfallen. Auf diese Weise werden angesichts des differenzierten normativen Programms von § 35 Abs. 2 S. 2 BDSG Auslegungsschwierigkeiten vermieden.

Dagegen besteht Anlass, in § 32b Abs. 3 BDSG-E den Hinweis aufzunehmen, dass eine Einwilligung in die weitere Speicherung von Bewerberdaten nach Abschluss des Bewerbungsverfahrens lediglich für Zwecke nach § 32b Abs. 2 S. 1 Nr. 1 BDSG-E und nur für einen von dem Bewerber zu bestimmenden Zeitraum Geltung haben soll.

4. § 32c BDSG-E: Datenerhebung im Beschäftigungsverhältnis

a.) Allgemeines: Auch die dem Innenausschuss nunmehr vorliegende Entwurfsfassung lässt Zweifel an dem Zweckprogramm der Verarbeitung und Nutzung von Beschäftigtendaten aufkommen: Zwar beschreiben § 32c Abs. 1 S. 2 Nr. 1 und 2 BDSG-E noch definierte Zwecke, so dass eine Datenerhebungsbefugnis auf diese Zwecke bezogen und beschränkt verstanden werden kann. Demgegenüber ist jede generelle Erlaubnis zur Erhebung von Beschäftigtendaten zwecks Wahrnehmung allgemein bestehender Rechte des Arbeitgebers einschließlich der Verhaltens- oder Leistungskontrolle (§ 32 Abs. 1 S. 2 Nr. 3 BDSG-E) in sich nicht differenziert. Da auch auf der Verwendungsebene (§ 32d Abs. 1 Nr. 2 BDSG-E) keinerlei Differenzierung erfolgt, handelt es sich um eine Erhebungsgeneralklausel ohne normatives Eigengewicht. In der Sache dürften, soweit das Direktionsrecht des Arbeitgebers reicht, zu beliebigen Zwecken mit Bezug zur Beschäftigung Daten erhoben werden. Damit bekennt sich § 32c Abs. 1 S. 2 Nr. 3 BDSG-E zu einem gleichsam Globalzweck von Beschäftigtendaten im Arbeitsverhältnis. Diese Zweckbeschreibung untertrifft die verfassungsrechtlichen Anforderungen an eine an den Grundsätzen der Verhältnismäßigkeit, Datensparsamkeit und informationellen Gewaltenteilung orientierten Datenschutzgesetzgebung.

b.) (§ 32c Abs. 1 S. 3 BDSG-E): Datenerhebung unter Umgehung des Betroffenen

Die Ausführungen zu § 32 Abs. 6 S. 4 BDSG-E gelten entsprechend. Es sollte bei der allgemeinen Regel nach § 4 Abs. 2 BDSG bleiben.

c.) (§ 32c Abs. 3 BDSG-E): Ein Recht des Arbeitgebers, ärztliche Untersuchungen und Eignungstests im Hinblick auf eine (von dem Arbeitgeber) beabsichtigte Versetzung oder Umsetzung zu verlangen, geht zu weit. Ein praktisches Bedürfnis nach einer Erweiterung der bisherigen gesetzlichen Regeln des Arbeitsschutzes durch § 32c Abs. 3 Nr. 1 BDSG-E ist nicht ersichtlich. Die Möglichkeit, schon durch von dem Arbeitgeber bloß kund getane Absicht ein intrusives Datenerhebungsprogramm auszulösen (Abs. 3 Nr. 2), eröffnet erhebliche Missbrauchsmöglichkeiten. Eine Selektion von Beschäftigten nach Gesundheit oder – fachlichen wie unsachlichen - Eignungskriterien muss grundsätzlich unterbunden werden, zumal die arbeitsrechtliche Praxis ohne eine solche Regelung auskommt. Arbeitnehmern steht es ggf. frei, sich unternehmensintern auf eine andere Stellen zu bewerben und dadurch die Rechtsfolgen von § 32a ff BDSG-E auszulösen. § 32c Abs. 4 BDSG kompensiert diesen Mangel nicht, weil das Zweckprogramm von § 32c Abs. 3 BDSG-E keine Einschränkung erfährt.

5. Datenverarbeitung und –nutzung im Beschäftigungsverhältnis

a.) (§ 32d Abs. 1 und Abs. 2 BDSG-E): Der Entwurf bekennt sich mit § 32d Abs. 1 Nr. 1 und 2 BDSG-E, wie bereits mit § 32c Abs. 1 S. 2 Nr. 3 BDSG-E, zu einem gleichsam Globalzweck von Beschäftigtendaten im Arbeitsverhältnis (vergl. auch die insoweit schonungslos offene Entwurfsbegründung zu § 32d Abs. 4 BDSG-E). Damit relativiert der Entwurf mit Wirkung für alle im Beschäftigungsverhältnis erhobenen Daten den Grundsatz der Zweckbindung und klaren Zweckbestimmung jeder Datenverarbeitung. Auch und gerade für die Verarbeitung von im Verlauf des Arbeitsprozesses, bei der Erbringung der Arbeitsleistung oder sonst im Betrieb angefallene Beschäftigtendaten (Abs. 2) ist eine Beschränkung der Datenverarbeitung auf den Zweck, zu dem die Daten generiert wurden, dringend angezeigt.

Da der Gesetzentwurf damit – auch entgegen Ansätzen in der arbeitsgerichtlichen Rechtsprechung zum allgemeinen Persönlichkeitsrecht – innerhalb einer verantwortlichen Stelle (§ 3 Abs. 7 BDSG) keine Nutzungsbeschränkungen vorsieht, fehlt es an tragfähigen Ansätzen für informationelle Gewaltenteilung im Unternehmen. Eine wesentliche

verfassungsrechtliche Forderung an jede verfassungskonforme Datenverarbeitung, nämlich die auch organisatorische Differenzierung der Zweckverfolgung, wird sehenden Auges verfehlt.

Die Erinnerung an den Grundsatz der Verhältnismäßigkeit (§ 32d Abs. 1 Nr. 3 BDSG-E) fügt dem normativen Programm des Entwurfs nichts hinzu, sondern wiederholt nur einen für alle Eingriffe in das allgemeine Persönlichkeitsrecht geltende Selbstverständlichkeit.

Da der Entwurf auf eine umfassende Regelung zielt, sollte in Absatz 1 klargestellt werden, dass die allgemeinen Regelungen des Bundesdatenschutzgesetzes (etwa nach § 28 Abs. 1 BDSG) keine Anwendung finden, mithin Beschäftigtendaten nur unter den Voraussetzungen von § 32d BDSG-E verarbeitet oder genutzt werden dürfen.

b.) (§ 32d Abs. 3 BDSG-E): Die Vorschrift legalisiert die unternehmensinterne Rasterfahndung, die in der Vergangenheit den Kern viel beachteter Datenschutzskandale ausgemacht hat und im öffentlichen Bereich bzw. zur Strafverfolgung nur unter qualifizierten Voraussetzungen und mit Zustimmung eines Richters zulässig wäre. Das gesetzliche Programm der Rasterfahndung legt mit der ausdrücklichen Erlaubnis einer Repersonalisierung (§ 32d Abs. 3 S. 2 BDSG-E) offen, dass allenfalls mit pseudonymisierten, weiterhin aber im Rechtssinne personenbezogenen Daten gearbeitet werden soll (vergl. nur § 3 Abs. 1 BDSG). Auch die Formel für die nachträgliche Unterrichtung der Beschäftigten (§ 32d Abs. 3 S. 4 BDSG-E) greift zu kurz. Zwar lehnt sie sich an das Recht der Strafverfolgung und Gefahrenabwehr an, jedoch hat gerade diese Form in der Vergangenheit eine verbreitete Auslegung dergestalt erfahren, dass bereits das Bekanntwerden der Anwendung einer bestimmten Methode den Zweck der Erhebung gefährden sollte. Da Maßnahmen nach § 32d Abs. 3 BDSG-E der Aufdeckung von zurückliegenden Pflichtverletzungen und nicht der Gefahrenabwehr dienen sollen, wäre im Falle ihrer gesetzlichen Legalisierung bereits eine Unterrichtung der Beschäftigten nach Ende der Maßnahme und/oder bei Repersonalisierung der verwendeten Daten möglich und auch angezeigt.

Auf dieses skandalumwitterte Instrument sollte der Gesetzgeber aber im Ergebnis verzichten. Diejenigen Unternehmen, welche von solchen Maßnahmen noch profitieren wollen, sollten das Verantwortungsbewusstsein aufbringen, im Wege der Betriebsvereinbarung die Rechtsgrundlagen für unabweisbare betriebliche Sicherheitsanwendungen zu schaffen.

c.) (§ 32d Abs. 4 BDSG-E): Datenübermittlung an Dritte, welche nach dem Zusammenhang der Vorschrift offenbar nach den schon für die Verarbeitung und Nutzung durch den Arbeitgeber zu weit geratenen § 32d Abs. 1 und 2 BDSG-E zulässig sein soll, sind von Gesetzes wegen an strengste Voraussetzungen zu binden. Die auch von der Entwurfsbegründung angenommene Freiheit des Arbeitgebers, zu jedem mit dem Beschäftigungsverhältnis verbundenen Zweck Beschäftigtendaten an Dritte übermitteln zu dürfen (vergl. Begründung zu Abs. 4 und oben zu a.)), verfehlt bei Weitem den gebotenen Schutz des Persönlichkeitsrechts der Betroffenen.

Der Entwurf verzichtet damit nicht nur auf ein Mindestmaß an Übermittlungsschutz für die Beschäftigten. Es fehlt auch an elementaren verfahrensrechtlichen Sicherungen: Lediglich die Mitteilung an dem Empfänger über den Zweck übermittelter Daten reicht dazu bei Weitem nicht aus, zumal ein trennscharfer legitimer Übermittlungszweck gerade in dem gesetzlichen Zweckprogramm nach § 32d Abs. 1 BDSG nicht identifiziert werden kann. Ferner fehlt es an der obligatorischen Kennzeichnung übermittelter Daten als Beschäftigtendaten, ohne welche der Übermittlungsempfänger die besondere Schutzwürdigkeit dieser Daten gar nicht verfahrenstechnisch absichern könnte. Weitere verfahrensrechtliche Sicherungen, wie etwa eine obligatorischen Benachrichtigung der Betroffenen, fehlen ebenfalls.

Der Entwurf ist daher durch ein enges, gesetzlich bestimmtes Zweckprogramm der Übermittlung von Beschäftigtendaten zu ergänzen.

6. § 32e BDSG-E: Heimliche Datenerhebung zur Bekämpfung von Straftaten u. a.

a.) (§ 32 Abs. 1 S. 2 BDSG-E): Mit § 32 Abs. 1 S. 2 BDSG in der geltenden Fassung hat der Gesetzgeber in Einklang mit der etablierten arbeitsrechtlichen Rechtsprechung eine eng gefasste Vorschrift geschaffen, welche heimliche Datenerhebungen in notwehrähnlicher Lage ausnahmsweise rechtfertigt. Dieser Regelungsgedanke wird nunmehr über den Verdacht von Straftaten hinaus erweitert auf sonstige arbeitsvertragsrechtliche Pflichtverletzungen, die zu einer Kündigung aus wichtigem Grund (§ 626 BGB) führen könnten. Damit bekennt sich der Gesetzentwurf ausdrücklich zur Anwendung heimlicher Mittel auch in denjenigen Fällen, in denen zwar kein nennenswerter Schaden für den Arbeitgeber oder Dritte eingetreten ist bzw. droht, gleichwohl aber eine Pflichtverletzung eine Kündigung rechtfertigt (sog. Maultaschenkündigung). Wenn sich aber die Bedeutung einer potentiellen Verfehlung aus arbeitsvertragsrechtlichen Wertungen ableitet, emanzipiert sich das Gesetz von dem Rechtsgüterschutz als Eingriffsrechtfertigung und geht die auch zusätzliche Verhältnismäßigkeitsschranke nach § 32e Abs. 3 S. 1 BDSG-E ins Leere. Der Gesetzgeber ist, wenn er nicht eine potentiell verfassungswidrige Blankettermächtigung für eingriffsintensive heimliche Datenerhebungen schaffen will, aufgefordert, das Zweckprogramm nach § 32e Abs. 2 Nr. 1 BDSG-E auf Straftaten oder sonstige Pflichtverletzungen zu beschränken, welche einen erheblichen Schaden für den Arbeitgeber oder Dritte nach sich ziehen (können). Arbeitsvertragsrechtlich zulässige Kündigungen werden dadurch nicht ausgeschlossen, können aber nicht ohne Weiteres mittels hochgradig eingriffsintensiver Ausnahmeinstrumente herbeigeführt werden.

Die Verfolgung von Zielen einer betrieblichen inneren Sicherheit durch die Arbeitgeber selbst bedarf im Übrigen nicht der umfangreiche Legalisierung, die ihr der Entwurf zubilligt: Es steht verantwortungsbewussten Arbeitgebern auch nach dem Entwurf frei, durch Betriebsvereinbarung zu einer auf die Spezifika des jeweiligen Unternehmens abgestimmten Feinabstimmung von unternehmerischen Bedürfnissen und den Persönlichkeitsrechten der Beschäftigten zu kommen. Die von der Gesetzesbegründung als Anwendungsbeispiel angesprochene Aufdeckung von Korruptionsnetzwerken unter maßgeblicher Beteiligung von Unternehmen außerhalb des Arbeitgebers ist nicht etwa ein plastisches Beispiel dafür, dass exstensive Datenerhebungen unter Einschluss von Dritten zwingend erforderlich sind.

Vielmehr illustrieren derartige Fallkonstellationen, dass Arbeitgeber nur durch frühzeitiges Einschalten der Polizei in der Lage sind, forensisch verwertbare Beweise zu erheben und zu sichern. Es ist daran zu erinnern, dass es im Rechtsstaat die Justiz ist, welche zuständig ist für die Verfolgung von Straftaten und ihre Sanktionierung. Nur so, und nicht durch eine Legalisierung unternehmerischer Eigeninitiative, können die Voraussetzungen für ein rechtsstaatliches Verfahren zum Schutz der Belange der Unternehmen geschaffen und gesichert werden.

b.) (§ 32e Abs. 4 BDSG-E): Das Erhebungsmethodenarsenal bei heimlichen Ermittlungen nach § 32e Abs. 2 BDSG-E wird von § 32e Abs. 4 BDSG-E nur ansatzweise beschränkt. Offenbar sollen weiterhin Privatdetektive, Observationen innerhalb und außerhalb von Betriebsgeländen, beliebige Anfragen bei Dritten und die Nutzung aller im Unternehmen angefallenen personenbezogenen Daten zulässig sein. Nicht geregelt ist ferner die Folge von Übertretungen der in sich schon vagen Einschränkungen nach § 32e Abs. 4 S. 1 BDSG. Der Gesetzentwurf kann dies nur ausgleichen, indem er sich zu Verwendungs- und Verwertungsverboten für im Widerspruch zur gesetzlichen Regel erhobene Daten bekenn.

c.) (Verfahrensrechtliche Absicherungen, § 32e Abs. 3 S. 2 – 4, Abs. 5 – 7 BDSG-E): Die verfahrensrechtlichen und materiell-erhebungsrechtlichen Absicherungen nach § 32e Abs. 3 S. 2 – 4, Abs. 5 – 7 BDSG-E sind im Grundsatz zustimmungswürdig. Sie greifen aber angesichts der Eingriffstiefe, welche die geregelten Maßnahmen entfalten könnten, zu kurz: So fehlt es weiterhin an einer Vorschrift, welche ausdrücklich verbietet, heimliche Datenerhebung gegen andere als die verdächtigen Beschäftigten zu richten und mehr als unvermeidbar Daten über Dritte zu erheben, welche nicht Beschuldigte sind.

Während staatlicher Rechtsgüterschutz und Straftatenbekämpfung in ein dichtes Geflecht rechtsstaatlicher Kontrolle und Verwendungsregelungen eingebunden sind, verzichtet der Entwurf auf verfahrensrechtliche Sicherungen unter Einschaltung unabhängiger Kontrollorgane. Die nach der Entwurfsbegründung nur als deklaratorische Erinnerung gedachte Anspielung auf die Vorabkontrolle nach § 4d Abs. 5 BDSG (§ 32e Abs. 5 S. 4 BDSG-E) kompensiert diesen Mangel nicht. Denn sie schöpft das Potential der

Vorabkontrolle bei weitem nicht aus: Die Vorabkontrolle ist nach § 4d Abs. 5 BDSG an spezifische, auslegungsfähige Voraussetzungen gebunden. Die effektive Kompensation der Heimlichkeit von Ermittlungen nach § 32e Abs. 2 BDSG-E kann nur durch Vorabkontrolle und zusätzliche obligatorische Einbindung von Betriebsräten, bei Ermangelung solcher durch Einbindung der Aufsichtsbehörden sichergestellt werden.

Zu einer Überwachungsfreiheit der Kommunikation mit Betriebsrat, Personalrat, Jugend- und Auszubildendenvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragten oder betriebsinternen theologischen oder medizinischen Beratungsstellen bekennt sich der Gesetzentwurf in der Gesetzesbegründung an anderer Stelle (BT-Drs. 17/4230, S. 20 zu § 32i Abs. 1 BDSG-E). Dieser Grundsatz ist allgemein für die betriebliche Datenerhebung – deklaratorisch – gesetzlich festzuschreiben.

Schließlich fehlt es sowohl in § 32e BDSG-E wie bei allen Datenerhebungsbefugnissen nach dem Entwurf an der effektiven Absicherungen auf der Verwendungs- und Verwertungsebene (s, schon oben zu b.). Der Entwurf sollte zumindest Regelungen dergestalt aufnehmen, dass Kündigungen oder sonstige arbeitsvertragsrechtliche oder zivilrechtliche Folgen von dem Arbeitgeber nicht auf Daten gestützt werden können, welche unter Verstoß gegen § 32e Abs. 2 – 7 BDSG-E und andere wesentliche Schutzvorschriften erhoben wurden. Solange ein Sanktionsapparat für Datenschutzverstöße des Arbeitgebers lediglich theoretisch existiert, bleibt die Erkennung und Bestimmung schutzwürdiger Interessen der Beschäftigten ebenso allein Sache des Arbeitgebers wie etwa die Bestimmung von Anlass und Streubreite bzw. Stichprobengröße heimlicher Nutzungen zu Sicherheitszwecken (vergl. auch § 32i Abs. 1 BDSG-E, dazu sogleich). Mangels trennscharfer Verbote kann nach geltendem Verfahrensrecht die Auslegung der Generalklauseln und Ermessensvorschriften des Bundesdatenschutzgesetzes durch den Arbeitgeber nur in exzessiven Missbrauchsfällen sicher in eine Sanktion oder gar ein verfahrensrechtliches Verwertungsverbot münden. Die Risiken der Rechtsanwendung durch den Arbeitgeber verbleiben nach dem Entwurf einmal mehr bei den Arbeitnehmern.

d.) (§ 32e Abs. 5 S. 5 BDSG-E): Die Unterrichtung der Zielpersonen heimlicher Maßnahmen greift zu kurz. Vielmehr sind alle Betroffenen von heimlichen Erhebungen zu unterrichten. (Zum Wegfall der Zweckgefährdung als Unterrichtungsvoraussetzung siehe schon oben zu 5. b.)).

7. § 32f BDSG-E (Videoüberwachung)

a.) (§ 32f Abs. 1 S. 1 BDSG-E): Videoüberwachung steht, auch wenn sie offen erfolgt, nach der an den persönlichkeitsrechtlichen Grenzen der unternehmerischen Gestaltungsfreiheit und damit unmittelbar an Verfassungsrecht orientierten Rechtsprechung des Bundesarbeitsgerichts unter erheblichem Rechtfertigungsdruck. Das von dem Entwurf eröffnete gesetzliche Zweckprogramm der Videoüberwachung ist demgegenüber konturenschwach und kann sich nur bei oberflächlicher Betrachtung auf zwingende betriebliche Interessen und hochrangige Rechtsgüter stützen.

Besonders augenfällig wird diese Emanzipation vom bestehenden Recht an dem Erhebungszweck der Qualitätskontrolle: Dieser lässt sich schon nicht hinreichend von der Verhaltens- oder Leistungskontrolle unterscheiden. Eine Videoüberwachung zu diesem Zweck erwiese sich auch gleichsam automatisch als schwerwiegender und unverhältnismäßger Eingriff in das Persönlichkeitsrecht der Betroffenen. Da jede Videoüberwachung der Erbringung der Arbeitsleistung den Kern des menschlichen Verhaltens im Betrieb betrifft, sind Überwachungen von Arbeitsplätzen stattdessen von Verfassungs wegen möglichst auszuschließen.

Die zusätzlichen Voraussetzungen nach Abs. 1 S. 1 werden sich als wirkungslos erweisen: Da die Qualitätskontrolle immer ein „wichtiges betriebliches Interesse" im Sinne der Vorschrift sein kann, läuft der Entwurf auch bei wortgetreuer Beachtung der Vorschrift Gefahr, sich an den verfassungsrechtlichen Grenzen zulässiger Persönlichkeitsrechtseinschränkungen in der Arbeitswelt zu vergehen. Dagegen spricht auch nicht die von dem Gesetzentwurf gewählte Einschränkungen, dass keine Anhaltspunkte

dafür bestehen dürfen, dass schützwürdige Interessen der Betroffene am Ausschluss der Datenerhebung überwiegen (Abs. 1 S. 1 a.E.). Zwar ist gegen eine Berücksichtigung schon von an Anhaltspunkten für schutzwürdige Interessen nichts zu erinnern. Die Orientierung am Ausschluss der Überwachung greift allerdings an dieser Stelle zu kurz. Denn angesichts des weiten Gestaltungsspielraums des Arbeitgebers bei der Gestaltung technischer Überwachung ist der Totalverzicht (Ausschluss der Datenerhebung) die falsche Referenzgröße. Tatsächlich wäre die Orientierung an der konkret von dem Arbeitgeber beabsichtigten Datenerhebung richtig. Auch ist ein Überwiegen schutzwürdiger Interessen der Betroffenen angesichts des Zweckkatalogs von § 32f Abs. 1 S. 1 BDSG-E nicht angemessen. Eine Videoüberwachung hätte aus Gründen der Verhältnismäßigkeit bereits dann auszubleiben, wenn schutzwürdige Interessen beeinträchtigt würden (vergl. auch das Regelungsmodell in § 32f Abs. 3 BDSG-E).

b.) (§ 32f Abs. 2 S. 2 BDSG-E): Die Freistellung von Überwachung müsste klarstellend auch auf sonstige Sozialräume erstreckt werden.

c.) (§ 32f Abs. 3 BDSG-E): Der Vorschrift fehlt bisher jede zeitliche Beschränkung der Videoüberwachung. Das Bundesarbeitsgericht hat auf die Gefahr permanenten Überwachungsdrucks durch auch nur zeitweilige Videoüberwachung eindrucksvoll hingewiesen und ihre persönlichkeitsrechtliche Unerträglichkeit verdeutlicht. Für jede, auch offene, Videoüberwachung ist daher von vorneherein festzuhalten und auch bekannt zu machen, in welchem zeitlichen Umfang sie erfolgt, wann und zu welchen konkreten Zwecken eine Speicherung erfolgen soll und aus welchem Anlass. Da § 32f Abs. 1 BDSG-E sich seinem Wortlaut nach nur als Erhebungsvorschrift versteht, fehlt es dem Entwurf dagegen sogar an einer gesetzlichen Legitimation für eine Speicherung. Aus welchen Gründen und zu welchen Zwecken eine Speicherung erforderlich ist, wäre konsequenterweise gesetzlich zu regeln. Dabei müsste, verbreiteter Regelungstechnik im öffentlichen Bereich folgend, eine nur durch überwiegende konkrete Verwendungsinteressen im Einzelfall durchbrochene kurze Speicherungshöchstdauer festgelegt werden.

8. § 32h BDSG-E (biometrische Verfahren)

Ungeachtet einer zunehmenden Verbreitung biometrischer Verfahren zu Identifikationszwecken ist die Erhebung und Verarbeitung biometrischer Daten weiterhin mit einem empfindlichen Eingriff in das Persönlichkeitsrecht der Betroffenen verbunden. Wie kein anderes Merkmal sind biometrische Daten unveränderlich mit dem Betroffenen verknüpft. Ihre Verwendung zu betrieblichen Identifikationszwecken ist daher, zumal für gewöhnliche betriebliche Nutzungen ausreichend technische Alternativen zur Verfügung stehen, auf das zwingend erforderlich Maß zu beschränken in Fällen, in denen gleichwirksame Methoden nicht zur Verfügung stehen.

Der Entwurf stellt demgegenüber den Einsatz biometrischer Verfahren in das Ermessen des Arbeitgebers, zumal die Formel nach § 32h Abs. 1 S. 1 a.E. BDSG-E keine effektive Schranke darstellt (s. oben 7. b.)).

9. § 32i BDSG-E (Nutzung von Telekommunikationsdiensten)

a.) (Vorbemerkung): Das gesetzliche Regelungsmodell, welches auf die ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubte Nutzung von Telekommunikationsdiensten abstellt, erweist sich als nur eingeschränkt praxisrelevant. Aus guten Gründen vermeiden Arbeitgeber eine Beschränkung der Nutzung ihrer Telekommunikationstechnik auf ausschließlich berufliche oder dienstliche Zwecke, zumal dies mit dem unternehmerischen Bedürfnis nach einer kommunikativen, weltgewandten und informierten Belegschaft kollidieren müsste. In Zeiten, in denen gerade auch von Arbeitnehmerinnen und Arbeitnehmern erwartet wird, in weit höherem Maße als früher kommunizierend zur Verfügung zu stehen, erschiene ein Verbot von privater Mitbenutzung geschäftlicher Telekommunikationsanlagen als veraltet.

Gleichwohl erweist schon die Regelung des datenschutzrechtlich einfachen Falles der nur zu beruflichen oder dienstlichen Zwecken erlaubte Nutzung betrieblicher Telekommunikationsinfrastruktur als äußerst schwierig. Der Entwurf verfehlt eine konsistente und angemessene Lösung.

b.) (Datenverarbeitung vor und nach Abschluss eines Telekommunikationsvorgangs):

Der Gesetzentwurf verfehlt mit der Unterscheidung von Datenerhebung während und nach dem Telekommunikationsvorgang schon eine konsistente Regelung und ist neu zu fassen: Die Entwurfsfassung leidet an einem durch Auslegung nicht mehr zu behebenden Formierungsmangel. Während § 32i Abs. 1 – 3 BDSG-E offenbar die Erhebung bzw. Speicherung von Daten aus Telekommunikationsvorgängen während laufender Telekommunikation betreffen sollen, sieht § 34i Abs. 4 BDSG-E für die Erhebung, Verarbeitung und Nutzung von Daten nach Abschluss eines Telekommunikationsvorgangs die Geltung der allgemeinen Regeln nach §§ 32c und 32d BDSG-E vor. Abgesehen von den Inhaltsdaten von Sprachtelefonie sind aber alle bei der Nutzung von Telekommunikationsanlagen anfallenden Daten – insbesondere Telekommunikationsverbindungsdaten und Inhaltsdaten von betrieblichen Emails - nach Abschluss der Telekommunikation noch vorhanden. Eine Beschränkung der Erhebung bzw. Speicherung, wie sie § 32i Abs. 1 und Abs. 3 BDSG-E vornehmen, wird nach dem Entwurf mithin mit dem Moment gegenstandslos, in dem die Telekommunikation beendet ist. § 32i Abs. 4 S. 1 BDSG-E erweist sich daher als sinnwidrig.

c.) (§ 32i Abs. 1 BDSG-E): Die stichprobenartige oder anlassbezogen gezielte Leistungs- oder Verhaltenskontrolle mittels Telekommunikationsverbindungsdaten (§ 32i Abs. 1 S. 1 Nr. 3 BDSG-E) kommt in ihrer Überwachungsintensität einer Videoüberwachung gleich und ist abzulehnen. Die Gesetzesbegründung legt dazu offen, dass das persönlichkeitsrechtlich kritische Potential der Auswertung von Verbindungsdaten – nämlich die Erstellung von Kommunikationsprofilen und deren Auswertung – Arbeitgebern zukünftig zugänglich sein soll. Während die Rechtsprechung die Speicherung und Verarbeitung von Telekommunikationsverbindungsdaten zu anderen als Abrechnungszwecken nur in eng begrenzten Ausnahmefällen hinnimmt, zielt der Gesetzentwurf mit der Erlaubnis zu stichprobenartige oder anlassbezogene Kontrollen darauf, allenfalls flächendeckende oder

jeden vernünftigen Anlasses entbehrende Kontrollen auszuschließen. Da es an einer begleitenden Kontrolle der Telekommunikationsüberwachung durch eine unabhängige Stelle und der ausdrücklichen Anordnung einer Vorabkontrolle für eine konkrete Auswertungsmaßnahme (wie etwa in § 32e Abs. 5 S. 4 BDSG-E) fehlt, bleibt es dem Zufall bzw. der Gefährdungseinschätzung des Arbeitgebers nach § 32i Abs. 1 S. 2 BDSG-E überlassen, ob den Betroffenen die Auswertung ihrer Telekommunikation bekannt wird oder nicht. Eine derart ungeregelte Arbeitnehmerüberwachung hätte in einer freiheitlichen Betriebsverfassung keinen Platz.

d.) (§ 32i Abs. 2 BDSG-E): Die Erhebung und Verwendung der flüchtigen Inhalte von Sprachtelefonie wird gemeinhin zu den sensibelsten Eingriffen in das Persönlichkeitsrecht und die Telekommunikationsfreiheit (Art. 10 Abs. 1 GG) der Betroffenen gerechnet. Nach geltendem Recht sind arbeitgeberseitige Inhaltskontrollen von Telefonaten grundsätzlich verboten und nur ausnahmsweise hinzunehmen, wenn sie offen erfolgen und qualifizierte Bedürfnisse des Arbeitgebers sie unentbehrlich machen. So hat die Rechtsprechung etwa das offene Mithören in Callcentern zu Ausbildungszwecken im Einzelfall hingenommen. Daran will offenbar § 32i Abs. 2 S. 1 BDSG-E anschließen, welcher das heimliche Mithören von Telefonaten jenseits der Call-Center-Regelung (§ 32i Abs. 2 S. 2 BDSG-E, dazu sogleich) verbietet.

Nicht verständlich ist daher, dass ausgerechnet für diesen höchst eingriffsintensiven Überwachungseingriff nach dem Entwurf eine Einwilligung eingeholt können werden soll. Von einer freiwilligen, ohne Zwang abgegebenen Einwilligung in das hohe Opfer des Verzichts auf die Telekommunikationsfreiheit kann unter diesen Umständen nicht ausgegangen werden, zumal der Arbeitnehmer keine angemessene Kompensation oder sonstigen Anreiz für eine Mitwirkung erhält und lediglich von der Vermeidung von Nachteilen motiviert sein kann. Unter diesen Umständen ist und bleibt die Freiheit der Einwilligung des Arbeitnehmers, was sie bisher schon in den allermeisten Fällen war: Wunschdenken. Kann der Arbeitnehmer daher, ungeachtet einer formellen Einwilligung, der Überwachung tatsächlich nicht ausweichen, ist die Berechtigung zur Inhaltskontrolle zwecks Wahrung von Arbeitgeberinteressen der Übergang in eine Totalüberwachung der Inhalte der Telekommunikation und verfassungswidrig.

e.) (§ 32i Abs. 2 S. 2 BDSG-E): Auch die Call-Center-Regelung übergeht, indem sie „im Einzelfall" eine dem Beschäftigten nicht erkennbare Gesprächsüberwachung erlaubt, das persönlichkeitsrechtliche Verbot der heimlichen Telefonüberwachung im Arbeitsverhältnis. Dieser Eingriff kann auch nicht dadurch in seiner Eingriffsintensität abgefedert werden, dass die Beschäftigten vorab abstrakt über die Möglichkeit der Überwachung informiert werden. Denn auch insoweit entsteht durch die Möglichkeit jederzeitigen Mithörens ein Überwachungsdruck, der die Persönlichkeitsrechte der Betroffenen stranguliert. Dass die Anwendung technologisch anspruchsvoller und besonders eingriffsintensiver Auswertungsmethoden wie der automatisierten Worterkennung oder der automatisierten Analyse des emotionalen Gesprächsverlaufs den Betroffenen – und damit auch den Geschprächspartnern – mitgeteilt werden muss, sieht der Entwurf über dies nicht vor.

f.) (§ 32i Abs. 3 BDSG-E): Zur Nutzung von Inhalten sonstiger Telekommunikationsdienste – insbesondere Email, Videodienste – gilt das zu § 32i Abs. 1 BDSG-E Gesagte (s. oben c.).

10. Modifikationen des allgemeinen Teils des Bundesdatenschutzgesetzes (§ 32l BDSG-E)

a.) (§ 32l Abs. 1 BDSG-E): Ein gesetzlicher Kanon einwilligungsfähiger Verarbeitungen ist ungeachtet überwiegend bedenklicher Vorschläge des Entwurfs die richtige Antwort für die strukturelle Unterlegenheit der Beschäftigten gegenüber dem Arbeitgeber. Wohl nur der Gesetzgeber kann auch eine den Vorgaben der EU-Datenschutzrichtlinie genügende Festlegung treffen. Für eine weitere Flexibilisierung des Gesetzesvorbehalts für Einwilligungen im Arbeitsleben, wie sie die Berichterstatter der Koalitionsfraktionen im Arbeitspapier vom 10.05.2011 anregen, besteht auch kein praktisches Bedürfnis. Detaillösungen lassen sich einerseits kollektiv-rechtlich erzielen. Andererseits kann der Arbeitgeber zur Datenerhebung auf die gesetzlichen Verarbeitungsgeneralklauseln zurück greifen, wenn schutzwürdige Belange der Beschäftigten im Einzelfall nicht gefährdet sein

sollen. Denn eine Datenerhebung ohne bestehendes unternehmerisches Bedürfnis kann unterbleiben und bedarf daher auch keiner Einwilligung.

b.) (§ 32l Abs. 4 BDSG-E): Der Entwurf will mit dieser Vorschrift offenbar eine vereinzelt gebliebene Rechtsprechung fortschreiben, nach welcher die Mitteilung von Verstößen des Arbeitgebers gegen Gesetz und Recht an Strafverfolgungs- oder Aufsichtsbehörden eine Pflichtverletzung im Arbeitsverhältnis darstellen soll. Ein solches Privileg für verantwortliche Stellen, welche als Arbeitgeber i. S. § 3 Abs. 13 S. 1 BDSG-E grundsätzlich besondere Schutzpflichten gegenüber den Beschäftigten haben, ist sachlich nicht gerechtfertigt. Wer selbst von Persönlichkeitsrechtsverletzungen betroffen ist oder von solchen Kenntnis hat, muss sich ohne Weiteres an die dafür gesetzlich zuständigen Stellen wenden können, anstatt von dem Gesetzgeber für die Mauer des Schweigens über Datenschutzverstöße von Arbeitgebern in die Pflicht genommen zu werden. Es kann das Recht, Aufsichtsbehörden einzuschalten, auch im Konfliktfall nicht davon abhängig gemacht werden, ob tatsächlich Anhaltspunkte für einen Verdacht i. S. § 32l Abs. 4 BDSG bestanden haben oder nicht. Dies gilt insbesondere auch für öffentliche Stellen, welche Arbeitgeber i. S. § 3 Abs. 13 BDSG-E sind. Ebenso wenig ist den Beschäftigten zuzumuten, ohne Beistand der Aufsichtsbehörde oder Dritter zu beurteilen, ob im Einzelfall eine Abhilfe tatsächlich geschaffen wurde und ob diese unverzüglich erfolgt ist. Die im Arbeitsverhältnis strukturell drohende Sanktionslosigkeit von Datenschutzverstößen wird durch die Entwurfsfassung damit weiter abgesichert. Dem sollen weit reichende Duldungspflichten der Beschäftigten bei heimlichen und/oder eingriffsintensiven Datenerhebungen gegenüberstehen.

Die Vorschrift, welche auch eine effektive behördliche Strafverfolgung behindert, ist daher ersatzlos zu streichen. Klarstellend sollte § 6 Abs. 1 BDSG um das Recht der jederzeitigen Anrufung von Aufsichtsbehörde und Datenschutzbeauftragten ergänzt werden. Eine verfahrensrechtliche Waffengleichheit zwischen Arbeitgeber und Beschäftigtem und unter den Betriebsparteien und die effektive Wahrnehmung nicht nur von datenschutzrechtlichen Ansprüchen würden sonst ernsthaft in Frage gestellt.

b.) (§ 32l Abs. 5 BDSG-E): Die in Zusammenhang mit § 32l Abs. 3 BDSG-E (Unberührtheit der Rechte der Interessenvertretung der Beschäftigten) und § 6 Abs. 1, Abs. 3 BDSG zu sehende Vorschrift ist als lange fällige Klarstellung in einem ausdauernd geführten Streit zu begrüßen.

Berlin, den 17.05.2011

Sönke Hilbrans

Prof. Dr. Peter Wedde

Direktor der Europäischen Akademie der Arbeit
in der Universität Frankfurt am Main
Professor für Arbeitsrecht und
Recht der Informationsgesellschaft

EUROPÄISCHE AdA
EUROPÄISCHE AKADEMIE DER ARBEIT
IN DER UNIVERSITÄT FRANKFURT AM MAIN

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 H

Stellungnahme

für die Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 23. Mai 2011 in Berlin zum Thema Beschäftigtendatenschutz

A. Einleitung

Mit dem Entwurf der Bundesregierung zu einem Gesetz zur Regelung des Beschäftigtendatenschutzes vom 15.12.2011 sowie mit den alternativen Entwürfen der SPD vom 25.11. 2009 und des BÜNDNIS 90/DIE GRÜNEN vom 22.2.2011 liegen drei unterschiedliche Regelungskonzepte vor, die sich dem Thema „Beschäftigtendatenschutz“ widmen. Dass eine so intensive Befassung mit dem Thema erfolgt, ist vor dem Hintergrund zahlreicher Praxisprobleme im Bereich des Beschäftigtendatenschutzes ohne Einschränkung zu begrüßen. Besonders positiv zu

bewerten ist das mit allen Gesetzesvorschlägen verfolgte Ziel, die Datenschutzrechte von Beschäftigten klar herauszuarbeiten und zu stärken.

Der Regierungsentwurf hat nach der amtlichen Begründung zum Ziel, praxisgerechte Regelungen für Beschäftigte und Arbeitgeber zu schaffen, die klarstellen, dass nur solche Daten erhoben, verarbeitet und genutzt werden dürfen, die für das Beschäftigungsverhältnis erforderlich sind. Mit den Neuregelungen sollen Beschäftigte an ihrem Arbeitsplatz zudem wirksam vor Bespitzelungen geschützt werden. Gleichzeitig sollen Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und für den Kampf gegen Korruption an die Hand gegeben werden.[1] Die auf Beschäftigte bezogenen Elemente dieser Zielsetzung sind ohne Einschränkung zu begrüßen. Nicht zu verkennen ist weiterhin, dass es legitime Informationsinteressen von Arbeitgebern gibt, die normativ geregelt werden müssen. Der vorliegende Gesetzentwurf erfüllt allerdings die selbst gesetzten Anforderungen bezüglich des Schutzes der Beschäftigten nur unzureichend.

Vor diesem Hintergrund beschränkt sich die folgende Stellungnahme auf Themenfelder, in denen Defizite für den Schutz der Beschäftigten bestehen bzw. denen in der betriebspraktischen Debatte eine herausragende Bedeutung zukommt. Sie stellt den Gesetzentwurf der Bundesregierung (im Folgenden: Regierungsentwurf) in den Mittelpunkt der Bewertung.

---

1 BT-Drs. 17/4230, S. 1.

B. Stellungnahme

Die Stellungnahme bezieht sich auf die folgenden Themenfelder:

1. Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Betriebsvereinbarungen.
2. Zulässigkeit der Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Einwilligungen der Beschäftigten.
3. Erhebungsbefugnisse in der Bewerbungsphase.
4. Ärztliche Untersuchungen.
5. Videoüberwachung.
6. Verdeckte Datenerhebung und Auswertung vorhandener Daten.
7. Zugriff auf Telekommunikationsdaten.
8. Compliance.
9. Unternehmensübergreifende Datenverarbeitung in Konzernen.

1. Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Betriebsvereinbarungen

Der Regierungsentwurf sieht durch die Ergänzung zu § 4 Abs. 1 BDSG ausdrücklich vor, dass Betriebs- und Dienstvereinbarungen datenschutzrechtliche Erlaubnisnormen für die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten sein können. Diese normative Klarstellung ist zu begrüßen. Die Präzisierung des datenschutzrechtlichen Schutzbereichs durch kollektivrechtliche Regelungen ist gängige und bewährte Praxis.

Bei der Ausgestaltung von kollektivrechtlichen Regelungen müssen die Betriebsparteien die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer schützen und fördern. Diese Vorgabe ist in § 75 Abs. 2 BetrVG ausdrücklich normiert. Hieraus leitet sich für kollektivrechtliche Regelungen mit Bezug zum Beschäftigtendatenschutz ab, dass sie Eingriffe in Persönlichkeitsrechte

nur ausnahmsweise und nur so schonend wie möglich zulassen dürfen. Die Bewertung des hiernach zulässigen Regelungsrahmens konfrontiert die Betriebsparteien und insbesondere Betriebsräte nach geltendem Recht oft mit der Frage, welche mit Eingriffen in das Persönlichkeitsrecht der Beschäftigten verbundenen Erhebungen, Verarbeitungen und Nutzungen überhaupt noch durch eine Betriebsvereinbarung geregelt werden können. In der Praxis geht es beispielsweise um die Weitergabe von Daten von im Bereich der klinischen Forschung beschäftigten Medizinern an US-amerikanische Zertifizierungsstellen oder um die umfassende Auswertung von Daten im Zusammenhang mit zivilrechtlichen Streitigkeiten in Großbritannien.

Derartige Unklarheiten bezüglich der kollektivrechtlichen Regelungsbefugnis werden durch die Vorgabe in § 32l des Regierungsentwurfs vermieden, nach der von den neuen Vorschriften zum Beschäftigtendatenschutz nicht zu Ungunsten der Beschäftigten abgewichen werden darf. Diese Regelung ist grundsätzlich zu begrüßen. Sie ist praktikabel und hindert die Betriebsparteien in der betrieblichen Praxis nicht daran, einzelne Tatbestände aus dem datenschutzrechtlichen Regelungsfeld in Betriebsvereinbarungen bezogen auf die konkrete betriebliche Situation zu präzisieren.

Die Einführung einer Regelung, nach der Betriebsvereinbarungen von den neuen Vorgaben des Beschäftigtendatenschutzes zu Ungunsten der Beschäftigten von den Regelungen des Regierungsentwurfs abweichen könnten, wäre problematisch. Eine solche Öffnungsklausel hätte zur Folge, dass der Grundschutz, der durch das neue Gesetz geschaffen wird, in der betrieblichen Praxis sofort wieder reduziert bzw. unterlaufen werden könnte.

Für Arbeitgeber und Betriebsräte würde zudem aus einer solchen Öffnungsklausel vor dem Hintergrund der komplexen neuen Gesetzessituation eine arbeitsintensive und rechtlich anspruchsvolle Herausforderung folgen. Sie müssen mit Blick auf § 75 Abs. 2 BetrVG bei Verhandlungen einerseits bewerten, welche Ab-

weichungen zu Ungunsten der Beschäftigten noch zulässig sein könnten. Andererseits müssten sie die einschlägige Rechtsprechung berücksichtigen wie etwa die Aussagen des BAG zur fehlenden Auswahlmöglichkeit beim Bestehen mehrerer Kontrollalternativen. Arbeitgeber müssen hiernach die Alternative auswählen, die so wenig wie möglich in Grundrechte der Beschäftigten eingreift.[2]

Vor diesem Hintergrund ist die Gefahr nicht von der Hand zu weisen, dass es bei der Einfügung einer Öffnungsklausel, die Anpassungen unterhalb des gesetzlichen Standards zulässt, zu betrieblichen Regelungen kommen kann, die unangemessen weit in die Rechte von Beschäftigten eingreifen. Damit würde das erklärte Ziel der Gesetzesnovelle, nämlich der Schutz der Beschäftigten, verfehlt.

Sollte es bezogen auf bestimmte betriebliche Sachverhalte die Notwendigkeit abweichender Regelungen durch Betriebsvereinbarungen geben (etwa im Bereich der betrieblichen Altersversorgung), sollte eine klare Rechtssituation durch abschließende beispielhafte Erlaubnisnormen im neuen Gesetz hergestellt werden statt durch Öffnungsklauseln.

2. Zulässigkeit der Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Einwilligungen der Beschäftigten

In der arbeitsrechtlichen Debatte zum Thema Beschäftigtendatenschutz wird bezüglich des Rückgriffs auf Einwilligungen immer wieder darauf verwiesen, dass Freiwilligkeit aufgrund der unterschiedlichen Durchsetzungskraft der Parteien im Regelfall nicht gegeben ist. Probleme werden insbesondere in der Anbahnungsphase gesehen, weil Bewerber hier Einwilligungen praktisch nicht verweigern können, wenn sie ihre Einstellungschancen wahren wollen. Dass die Befürchtung berechtigt ist, dass es zu „unfreiwilligen Einwilligungen“ kommt, ist in den letzten

---

[2] Vgl. hierzu etwa BAG vom 26.8.2008 - 1 ABR 16/07, BAGE 127, 276-297

Jahren an zahlreichen Beispielen für unangemessene Gesundheits-, Blut- oder Urintests deutlich geworden.

Nach Abschluss eines Arbeitsvertrags stellt sich die Situation für Beschäftigte vertraglich zwar sicherer, tatsächlich aber in vielen Fällen vergleichbar dar. Um den Arbeitsplatz oder Aufstiegschancen zu sichern, stimmen Beschäftigte entsprechenden Anforderungen ihrer Arbeitgeber oft entgegen eigener Interessen zu. Häufig ist dieses Problem etwa im Zusammenhang mit von Arbeitgeber gewollten Zugriffen auf die persönlichen E-Mail-Accounts von Beschäftigten oder bezüglich der Umleitung eingehender elektronischer Post auf von Arbeitgebern bestimmte Vertreter gegeben.

Vor diesem Hintergrund ist die abschließende Begrenzung in § 32l Abs. 1 des Regierungsentwurfs für die Einholung freiwilliger Einwilligungen als Grundlage für die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten auf die in den Regelungen der §§ 32 bis 32l genannten Fälle grundsätzlich positiv zu bewerten. Sie stellt einen guten Ansatz dar, um Beschäftigte davor zu schützen, Einwilligungen in die Erhebungen, Verarbeitungen oder Nutzungen ihrer personenbezogenen Daten nur deshalb zu erteilen, weil sie Sorge davor haben, sonst berufliche Nachteile zu erleiden.

Die Regelung in § 32l Abs. 1 des Regierungsentwurfs steht nicht im Widerspruch zu Artikel 7 Buchstabe a) der Europäischen Datenschutzrichtlinie. Dort ist nämlich als Verarbeitungsvoraussetzung festgelegt, dass die betroffene Person „*ohne jeden Zweifel*“ ihre Einwilligung gegeben hat. Genau diese Zweifelsfreiheit besteht im Beschäftigungsverhältnis nicht.

Kritisch fällt eine Auseinandersetzung mit den Einzelregelungen aus, in denen die Einwilligung zugelassen werden soll. Insbesondere in der Bewerbungsphase ist es Beschäftigten, die ihre Einstellungschancen wahren wollen, praktisch unmöglich, eine nach § 32 Abs. 6 Satz 4 des Regierungsentwurfs zulässige Einwilligung in die Erhebung von sonstigen Daten bei Dritten nicht zu erteilen.

Problematisch sind in diesem Zusammenhang auch die durch § 32 Abs. 6 Satz 2 erweiterte Erhebungsbefugnisse von Arbeitgebern bezüglich allgemein zugänglicher Daten. Hieraus folgt, dass Bewerber auch dann um eine Einwilligung gebeten werden könnten, wenn der mögliche Arbeitgeber die bei der nach neuem Recht zulässigen Recherche im Internet gewonnenen Informationen durch Anfragen bei Dritten spezifizieren möchte. Da § 32 Abs. 1 Satz 2 als Erhebungsgrund ganz allgemein die „Eignung des Beschäftigten für die vorgesehene Tätigkeit" nennt und keine Begrenzung auf berufsspezifischen Fähigkeiten oder Kenntnissen enthält, könnten Bewerber in diesem Zusammenhang um Zustimmung dazu gebeten werden, weitere Daten von einem privaten Ermittler erheben zu lassen. Hieran könnte etwa ein Flughafenbetreiber interessiert sein, der im Internet Hinweise darauf gefunden hat, dass ein Bewerber in einer Initiative gegen ein Erweiterungsvorhaben aktiv sein könnte.

Vergleichbare Probleme bestehen bezüglich der Freiwilligkeit einer Einwilligung bei ärztlichen Untersuchungen (§ 32a Abs. 1) oder bezüglich der Erhebung, Verarbeitung oder Nutzung der Inhalte von Telekommunikationsdiensten, die zu beruflichen Zwecken verwendet werden (§ 32i Abs. 2). Diese Beispiele deuten darauf hin, dass der Regierungsentwurf die Rechte der Beschäftigten in diesen Punkten nicht stärkt.

Die restriktive Regelung in § 32l Abs. 1 des Regierungsentwurfs, die Einwilligungen nur in einer abschließend genannten Zahl von Fällen zulässt, kann in der betrieblichen Praxis zu Problemen führen, wenn es Konstellationen gibt, in denen Einwilligungen unstreitig auf freiwilliger Basis erteilt werden. Beispielhaft sei auf die Übermittlung von Beschäftigtendaten an Dritte im Rahmen internen Aktienkaufprogrammen verwiesen.

Um derartige Einwilligungen auch in Zukunft möglich zu machen, könnte eine Öffnung der Regelung in § 32l Abs. 1 des Regierungsentwurfs zur Vermeidung erfolgen, wenn flankierende Schutzmaßnahmen normativ verankert würden.

Hierzu könnte die verbindliche Vorgabe gehören, dass über den im künftigen BDSG genannten Einwilligungstatbestände weitere Einwilligungen nur zulässig sind, wenn als Ergebnis einer neutralen Bewertung zu Ungunsten der Beschäftigten keine Abweichungen vom Schutzstandard des Beschäftigtendatenschutzes gegeben sind.

Weiterhin könnte normativ zu Lasten der Arbeitgeber für Streitfälle eine Beweislastumkehr vorgesehen werden, wenn sie aus einer Einwilligungen Rechte herleiten wollen. Vorbild für eine solche Regelung könnte § 22 AGG sein. Schließlich könnte die Wirksamkeit einer eingeforderten freiwilligen Einwilligung daran gekoppelt werden, dass im Rahmen eines Mitbestimmungsverfahrens eine Prüfung durch den Betriebsrat erfolgt ist. Wo dieser nicht gewählt ist, könnte die Prüfung stattdessen durch den betrieblichen Datenschutzbeauftragt oder durch die zuständige staatliche Aufsichtsbehörde vorgenommen werden.

3. Erhebungsbefugnisse in der Bewerbungsphase

Die Zulässigkeit der Datenerhebung in der Bewerbungsphase wird grundlegend in § 32 des Regierungsentwurfs geregelt. Die hiernach möglichen Datenerhebungen sind sehr weit gefasst. Dies macht schon die in § 32 Abs. 1 Satz 2 des Regierungsentwurfs zu findende Formulierung deutlich, nach der die Erhebung von Daten in der Bewerbungsphase erlaubt ist, „*um die Eignung des Beschäftigten*“ festzustellen. Der allgemeine Begriff der Eignung geht über die intendierte Feststellung der fachlichen Eignung hinaus. Hierauf bezogen lässt sich eine Begrenzung der Erkenntnismöglichkeiten des Arbeitgebers zwar aus § 32 Abs. 7 des Regierungsentwurfs herleiten. Hiernach ist die die Zulässigkeit der Datenerhebung daran gebunden, dass Art und Ausmaß der Datenerhebung im Hinblick auf den Zweck verhältnismäßig sind. In der Praxis generiert diese normative Unklarheit aber die Notwendigkeit der Präzisierung durch die Rechtsprechung.

Bezogen auf die angestrebte Verbesserung des Beschäftigtendatenschutzes ist auch die Regelung in § 32 Abs. 6 Satz 2 des Regierungsentwurfs kritisch zu bewerten. Hiernach können Arbeitgeber allgemein zugängliche Daten über Beschäftigte erheben, wenn sie hierauf vor der Erhebung hingewiesen haben. Ausreichend würde es sein, wenn der entsprechende Hinweis sich etwa in der Stellenausschreibung finden würde. Ist diese Voraussetzung erfüllt, könnten Arbeitgeber Informationen über Bewerber im Internet mittels Suchmaschine legal sammeln. Für Bewerber hat diese normative Situation zur Folge, dass sie nicht wissen, welche der über sie im Internet verfügbaren und möglicherweise von Dritten ohne ihre Kenntnis eingestellten Daten ein Arbeitgeber berücksichtigt hat.

Praktisch lässt sich die Möglichkeit der beschriebenen Internetrecherchen aus technischer Sicht nicht mehr verhindern. Auf der normativen Ebene ist aber trotz dieser Möglichkeiten eine Regulierung der Zulässigkeit dieses Vorgehens vorstellbar. Die Situation gleicht strukturell bezüglich des technisch möglichen Herunterladens etwa der Situation bei urheberrechtlich geschützter Musik und der hierzu erfolgten normativen Regulierung.

Soll Beschäftigtendatenschutz im Angesicht der bestehenden technischen Möglichkeiten trotzdem gesichert werden, könnte die Zulässigkeit von Internetrecherchen über Bewerber mit der Schaffung adäquater Informationsrechte verbunden werden. In diesem Zusammenhang ist zu bedenken, dass Beschäftigte nach geltendem Recht gegenüber einem Arbeitgeber, der entsprechende Internetrecherchen durchführt, gemäß § 33 Abs. 1 Satz 1 BDSG einen Rechtsanspruch auf Benachrichtigung haben über die Art der Daten, die gespeichert wurden, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle. Hieraus können sie einen Informationsanspruch ableiten, der sie im konkreten Fall möglicherweise in die Lage versetzt, Ansprüche nach dem AGG geltend zu machen.

Ein effektiver Beschäftigtendatenschutz durch Schaffung einer Transparenz über das Wissen, das Arbeitgeber über Bewerber im Rahmen von Internetrecherchen erwerben können, würde demnach voraussetzen, dass Beschäftigte konkret über die verwendeten Suchbegriffe und die aufgesuchten Seiten informiert werden. Dies ließe sich etwa durch die Verpflichtung zur Protokollierung der Suchvorgänge und zur Übermittlung der Protokolle an Bewerber realisieren.

4. Ärztliche Untersuchungen

Der Umgang mit ärztlichen Untersuchungen sowie mit der Anforderung von Blut- und Urinproben wurde in zahlreichen Fällen aus den letzten Jahren datenschutzrechtlich als unzulässig oder zumindest als kritisch bewertet. Erinnert sei nur an Bluttests bei Bewerbern für Tätigkeiten bei Rundfunkanstalten oder Automobilherstellern, die durch die Art der Tätigkeit in Verwaltungsbereichen nicht gerechtfertigt waren. Ähnlich verhält es sich mit „Reihenurinuntersuchungen“ bei Bewerbern um eine Ausbildungsstelle vor Abschluss eines Ausbildungsvertrags wurden in der öffentlichen Debatte kritisch hinterfragt.

Vor diesem Hintergrund ist die Aufnahme einer Regelung zur Zulässigkeit ärztlicher Untersuchungen in § 32a Abs. 1 des Regierungsentwurfs grundsätzlich zu begrüßen. Allerdings zeigt die Norm schon deshalb keine klaren Grenzen der Zulässigkeit auf, weil sie in der zweiten Regelungsalternative von Abs. 1 Satz 1 ärztliche Untersuchungen zur Feststellung der Erfüllung bestimmter gesundheitlicher Voraussetzungen auch bezüglich der Bedingungen der Ausübung einer Tätigkeit zulässt. Dies schafft Auslegungsspielräume, die kontraproduktiv zur angestrebten Verbesserung der datenschutzrechtlichen Situation von Bewerbern sind. Angestrebt werden sollte deshalb eine klarere Begrenzung auf Untersuchungen, die aus objektiver Sicht eine Limitierung auf solche Untersuchungen beinhaltet, die wegen der Art der auszuübenden Tätigkeit eine wesentliche und entscheidende Bedingung für deren Ausübung sind. Gleichzeitig sollte festgeschrieben werden,

dass Arbeitgeber das bezogen auf Persönlichkeitsrechte der Beschäftigten mildeste Mittel der ärztlichen Untersuchung wählen müssen.

Bezüglich zulässige ärztlicher Untersuchungen innerhalb von Beschäftigungsverhältnissen enthält § 32c Abs. 3 Nr. 2 des Regierungsentwurfs die Möglichkeit, dass ärztliche Untersuchungen auch im Zusammenhang mit dem beabsichtigten Wechsel einer Tätigkeit oder eines Arbeitsplatzes verlangt werden können. Diese Regelung eröffnet Arbeitgebern Handlungsspielräume, die arbeitsrechtlich nicht nachzuvollziehen sind. Aus Blick des Beschäftigtendatenschutzes ist bezogen auf § 32c Abs. 3 des Regierungsentwurfs insgesamt eine Begrenzung auf die Fälle notwendig, in denen ärztliche Untersuchungen gesetzlich vorgeschrieben sind. Darüber hinausgehende Untersuchungsverlangen könnten durch ein Verfahren der Vorprüfung einer von Arbeitgebern gewollten Einwilligung durch Betriebsräte, betriebliche Datenschutzbeauftragte oder staatliche Aufsichtsbehörden rechtlich flankiert werden.[3]

5. Videoüberwachung

Die Fälle unzulässiger Videoüberwachung von Beschäftigten bei einem großen Lebensmitteldiscounter waren im April 2008 der Ausgangspunkt einer sich schnell intensivierenden Debatte um die Notwendigkeit einer Verbesserung des Beschäftigtendatenschutzes. In der Folgezeit gab es zahlreiche weitere Beispiele unzulässiger Videoüberwachung, etwa bei einem Lebensmittelproduzenten. Die arbeits- und datenschutzrechtliche Bewertung dieser Fälle hat das Fehlen einer gesetzlichen Regelung zur Videoüberwachung in nicht öffentlich zugänglichen Betriebsstätten verdeutlicht. Vor diesem Hintergrund ist die Aufnahme von § 32f in den Regierungsentwurf zu begrüßen.

---

[3] Vgl. hierzu die Ausführungen zu Kapitel 2 / Seite 8.

Kritisch ist anzumerken, dass durch § 32f des Regierungsentwurfs die Handlungsmöglichkeiten von Arbeitgebern gegenüber denen aus § 6b BDSG erweitert werden. Dies wird am Beispiel der durch § 32f Abs. 1 Nr. 7 möglichen Erhebung von Beschäftigtendaten zur Qualitätskontrolle deutlich. Unter dieses Tatbestandsmerkmal ließe sich etwa auch die permanente Beobachtung von Produktionsmitarbeitern subsumieren, wenn etwa ein Zulieferbetrieb mit einem Abnehmer ein „Null-Fehler-Konzept" vereinbart hat und diesem gegenüber durch Videoaufzeichnung im Streitfall nachweisen können will, dass alle Beschäftigten jeden Handgriff richtig gesetzt haben. Gemessen an der Rechtsprechung des BAG zur Videoüberwachung, die permanente „Totalkontrollen" für den Regelfall ausschließt[4], wäre ein solches Vorgehen derzeit unzulässig. Es könnte vor dem Hintergrund der neuen Rechtsgrundlage von der Rechtsprechung künftig als zulässig erachtet werden, wenn das überwiegende schutzwürdige Interesse der Betroffenen am Ausschluss der Datenerhebung, das im letzten Halbsatz von § 32f Abs. 1 Satz 1 des Regierungsentwurfs ausdrücklich genannt ist, im konkreten Fall negiert würde.

In der betrieblichen Praxis wird weiterhin die in § 32f Abs. 1 Satz 2 des Regierungsentwurfs enthaltene Verpflichtung des Arbeitgebers zur Kenntlichmachung der Videoüberwachung durch geeignete Maßnahmen zu Problemen führen. Mit Blick auf die Rechtsprechung, die Beschäftigten zur Wahrung ihrer Persönlichkeitsrechte auch im Betrieb kontrollfreie Bereiche zuspricht[5], wird es nicht ausreichend sein, nur pauschal auf den Umstand der Videoüberwachung hinweisen. Ergänzend muss in Situationen, in denen die Abgrenzung von berechtigt kontrollierten Bereichen und kontrollfreien Zonen für Beschäftigte nicht eindeutig ist, durch weitere Maßnahmen wie beispielsweise farbliche Kennzeichnung auf dem Fussboden einer Halle oder eines Büros verdeutlicht werden, wo gefilmt wird und wo nicht.

---

4 Vgl. etwa BAG vom 14.12.2004 - 1 ABR 34/03, RDV 2005, 216

5 Vgl. BAG vom 14.12.2004, a.a.O.

Abschließend sei die Bemerkung erlaubt, dass das vielfach formulierte Ziel des Gesetzgebers, heimliche Videoüberwachungen ausschließen zu wollen, sich derzeit gesetzestechnisch noch dezent im Hintergrund hält. Das Verbot heimlicher Videoüberwachung wird in § 32f selbst nämlich nicht ausdrücklich genannt, sondern muss aus § 4e Abs. 4 Nr. 3 i.V.m. Abs. 2 des Regierungsentwurfs hergeleitet werden, weil die Videoüberwachung als ein sonstiges besonderes technisches Mittel zu qualifizieren ist, mit dem die Erhebung ohne Kenntnis der Betroffenen unzulässig ist.

6. Verdeckte Datenerhebung und nachträgliche Auswertung vorhandener Daten

Eine Reihe bekannter Fälle unzulässiger Datenerhebung und Datenverarbeitung der letzten Jahre erfolgte mit dem Ziel der Aufdeckung von Straftaten oder schwerwiegender Pflichtverletzungen ohne Kenntnis der Beschäftigten und teilweise auch ohne gesetzeskonforme Einschaltung der zuständigen Betriebsratsgremien. Herausragende Aufmerksamkeit fanden insbesondere entsprechende Vorgänge bei der Telekom AG und der Bahn AG.

Neben der unzulässigen heimlichen Videoüberwachung hat die Reihe heimlicher Datenerhebungen und Datenverarbeitungen die Notwendigkeit einer Verbesserung des Schutzes der Beschäftigten verdeutlicht. Vor diesem Hintergrund überrascht es, dass der Gesetzentwurf Arbeitgebern durch § 32d Abs. 3 weitgehende Befugnisse zugesteht, vorhandene Daten mit dem Ziel der Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen zu verarbeiten. Der Regierungsentwurf bleibt damit hinter dem Stand der geltenden Regelung in § 32 Abs. 1 Satz 2 BDSG zurück, die zum 1. September 2009 als erste Reaktion auf die zahlreichen Fälle von Datenmissbrauch in das Gesetz eingefügt wurde. Voraussetzung einer Erhebung, Verarbeitung oder Nutzung ist nach dieser Norm, dass *„zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass*

der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat". Die geplante Regelung stellt aus Sicht der Beschäftigten damit nur eine Verschlechterung gegenüber der bisherigen Gesetzessituation dar.

An dieser Feststellung ändert sich auch durch das vorgesehene Verarbeitungsverfahren nichts, das zunächst einen anonymen oder pseudonymen Abgleich vorsieht und erst im Verdachtsfall eine Personalisierung vorsieht. Die Durchführung entsprechender Datenabgleiche steht nach dem derzeitigen Gesetzesvorschlag im alleinigen Ermessen des Arbeitgebers. Insoweit ist eine ausgewogene Inhaltskontrolle nicht garantiert.

Die in § 32d Abs. 3 des Regierungsentwurfs enthaltenen Tatbestandsvoraussetzungen, durch die eine „Personalisierung" gerechtfertigt würde, sind nicht präzise gefasst. Diese Aussage gilt insbesondere hinsichtlich der Zulässigkeit eines Datenabgleichs mit dem Ziel der Aufdeckung schwerwiegender Pflichtverletzungen. Der Gesetzestext zielt diesbezüglich wohl auf das Vorliegen der Voraussetzungen einer Kündigung aus wichtigem Grund gemäß § 626 BGB ab. Diesbezüglich ist zu bedenken, dass die Schwelle für eine solche Kündigung auch nach der im „*Fall Emmely*" zu Gunsten der gekündigten Klägerin ergangenen Entscheidung des BAG[6] nicht übermäßig hoch ist.

Im Ergebnis gesteht die Regelung in § 32d Abs. 3 des Regierungsentwurfs Arbeitgebern weitergehende Rechte zu als die bisherige Rechtssituation. Sie gefährdet damit in der Praxis auch funktionierende Betriebsvereinbarungen, die mit dem Ziel getroffen wurden, einerseits Arbeitgeber vor Straftaten und schwerwiegenden Pflichtverletzungen zu schützen und andererseits die Rechte von Beschäftigten zu wahren.

Besonders kritisch ist in diesem Zusammenhang die Regelung in § 32e Abs. 2, nach der Arbeitgeber in den dort abschließend genannten Fällen Beschäftigten-

---

[6] BAG vom 10.06.2010 - 2 AZR 541/09, NZA 2010, 1227.

daten auch ohne Kenntnis der Beschäftigten erheben dürfen. Voraussetzung ist auch hier, dass Tatsachen den Verdacht begründen, dass im Beschäftigungsverhältnis eine Straftat oder eine andere schwerwiegende Pflichtverletzung begangen wurde. Diese Regelung ist durch den letzten Halbsatz von Abs. 2 sowohl „repressiv“ bezüglich der Aufdeckung begangener Straftaten oder Pflichtverletzungen als auch „präventiv“ bezüglich der Verhinderung weiterer ausgestaltet. Die neue Vorschrift bleibt bezüglich der tatbestandlichen Voraussetzungen hinter den bereits angesprochenen weitergehenden Anforderung in § 32 Abs. 1 Satz 2 BDSG zurück.

Die Erhebung von Daten zu Zwecken der Aufdeckung oder Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverstößen im Beschäftigungsverhältnis steht gemäß § 32e Abs. 3 des Regierungsentwurfs unter dem Vorbehalt der Verhältnismäßigkeit. Weiterhin muss die Erforschung auf andere Weise erschwert oder weniger erfolgversprechend sein. Diese Regelung nimmt die Vorgaben der Rechtsprechung des BAG zum Persönlichkeitsschutz nur unzureichend auf.

Das propagierte Ziel, den Beschäftigtendatenschutz zu verbessern, wird durch die §§ 32d Abs. 3 und § 32e Abs. 2 des Regierungsentwurfs weit verfehlt. Arbeitgebern werden nach dieser Norm vielmehr zu Zwecken der Ermittlung und Identifikation von Straftaten und schwerwiegenden Pflichtverletzungen datenschutzrechtliche Kompetenzen eingeräumt, die weitreichender sind als bisher.

Ergebnis dieser Regelung wäre, dass die Zahl von Datenschutzverstößen gegenüber Beschäftigten abnimmt. Dies aber nur deshalb, weil sich Zahl und Umfang erlaubter Eingriffe in die Persönlichkeitsrechte der Beschäftigten erhöhen.

7. Zugriff auf Telekommunikationsdaten

Die Zugriffsmöglichkeiten von Arbeitgebern auf die Daten, die bei der Nutzung von betrieblichen Telekommunikationseinrichtungen anfallen, ist in der betrieblichen Praxis ein zentrales und oft auch kontroverses Diskussionsthema für Arbeitgeber, Betriebsräte und Arbeitnehmer.

Debattiert wird zunächst über die Notwendigkeit und Zulässigkeit des Zugriffs auf dienstliche Daten. Einvernehmen besteht in diesem Punkt zumeist dazu, dass Arbeitgeber bestimmte Daten aus gesetzlichen oder betrieblichen Gründen benötigen. Hierzu gehören insbesondere Geschäftsdaten, die nach steuerrechtlichen Grundsätzen vorgehalten werden müssen.

Das Einvernehmen endet, wenn es um die Verwendung anderer Daten wie insbesondere der geschriebenen und empfangenen E-Mails geht. Soweit die private Nutzung betrieblicher Systeme verboten ist, wird teilweise die Auffassung vertreten, dass dann Arbeitgebern die Einsicht in die E-Mails zusteht. Vor diesem Hintergrund wird teilweise auch eingefordert, bei Abwesenheit alle eingehenden E-Mails an einen Vertreter umzuleiten. Dieser Auffassung wird entgegen gehalten, dass es auch im dienstlichen Rahmen persönliche Kommunikationsvorgänge gibt, die sich der Kenntnis des Arbeitgebers oder direkter Vorgesetzter entziehen müssen wie etwa die Korrespondenz zwischen einem Arbeitnehmer und dem Betriebsrat, dem betrieblichen Datenschutzbeauftragten oder der Personalabteilung in einer individuellen Einkommenssteuerangelegenheit.

Verschärft wird die Diskussion um die Zulässigkeit der Zugriffe auf Daten aus dem Bereich der Nutzung von Telekommunikationsdiensten, wenn die private Nutzung betrieblicher Systeme erlaubt bzw. nicht ausdrücklich verboten ist. In diesen Fällen setzen insbesondere die anwendbaren Vorgaben des TKG Zugriffen der Arbeitgeber auf Inhaltsdaten praktisch absolute Grenzen, sofern keine wirksame Einwilligung der Beschäftigten besteht.

Die vorstehend skizzierten Fragen löst § 32i des Regierungsentwurfs nicht oder nur begrenzt, da es sich auf die ausschließlich dienstliche Nutzung beschränkt. Aber auch in diesem Rahmen wird keine Rechtsklarheit bezüglich des besonders zu schützenden Bereichs der „persönlichen dienstlichen Kommunikation“ geschaffen. Das Verbot der Erhebung, Verarbeitung und Nutzung der persönlichen Daten, die etwa aus einem E-Mail-Verkehr mit einem Betriebsrat oder dem zuständigen Personalreferenten resultieren, muss im Einzelfall aus der Abwägung zwischen den Interessen des Arbeitgebers und den schutzwürdigen Interessen der Beschäftigten abgeleitet werden. Diese Abwägung findet sich in § 32i des Regierungsentwurfs mehrfach wieder.

Die Bewertung der zutreffenden Durchführung der notwendigen Interessenabwägung obliegt damit im Ergebnis ebenso der Rechtsprechung wie das Setzen von notwendigen Begrenzungen. Rechtsklarheit wird damit nicht erzeugt.

8. Compliance

Teile der Neuregelungen des Regierungsentwurfs sind dazu bestimmt, die Grundlagen für die Durchsetzung von Compliance-Anforderungen der Arbeitgeber zu sein. Insbesondere die Regelung in § 32d Abs. 3 des Regierungsentwurfs soll eine Grundlage für die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen darstellen.[7]

Unklar bleibt allerdings, wofür dieser Begriff steht. Zum Regierungsentwurf findet sich in den Materialien die folgende Definition: „*Compliance bedeutet in diesem Zusammenhang die Einhaltung aller relevanten Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes.*“ [8]

---

7 Vgl. BT-Drs. 17/4230, S. 18.

8 Vgl. a.a.O.

Setzt man diese Definition bei der Interpretation der Vorschrift voraus, werden Arbeitgebern im Rahmen von Compliance-Aktivitäten weitgehende Befugnisse eingeräumt, um Datenerhebungen und Datenverarbeitungen gemäß § 32d Abs. durchzuführen. Unter den Voraussetzungen von § 32e Abs. 2 des Regierungsentwurfs könnte dies ggf. auch ohne Kenntnis der Beschäftigten, also „heimlich“ erfolgen.

Dies ist in der betrieblichen Praxis immer dann höchst problematisch, wenn Richtlinien oder Selbstverpflichtungen von Arbeitgebern einseitig gestaltet und vorgegeben werden. So sieht sich beispielsweise derzeit der zuständige Betriebsrat in einem großen europäischen Unternehmen mit einem Code of Compliance konfrontiert, der Beschäftigten weitgehende Verhaltensvorgaben macht. Diese Vorgaben sind wiederum maßgeblich durch Regeln der europäischen Konzernspitze geprägt, die ihren Sitz in einem anderen europäischen Land hat. Die Einhaltung der Vorgaben soll auch durch Auswertungen personenbezogener Daten in den verwendeten elektronischen Systemen kontrolliert werden. Die beabsichtigten Kontrollen haben nach der übereinstimmenden Meinung von Arbeitgeber und Betriebsrat derzeit in Deutschland keine Rechtsgrundlage. Die Konzernspitze hat dem Betriebsrat deshalb gerade mitgeteilt, dass die Einführung zur Vermeidung rechtlicher Unklarheiten erst nach Verabschiedung des hier zu diskutierenden Gesetzes erfolgen soll. Auf der Grundlage von § 32d Abs. 3 des Regierungsentwurfs hält sie die geplanten Kontrollen für zulässig.

9. Verarbeitungsregeln in Konzern

Der Regierungsentwurf enthält derzeit keine Erweiterung zur Zulässigkeit der unternehmensübergreifenden Verarbeitung in Konzernen. Eine solche Regelung wird indes in der Diskussion immer wieder gefordert.

Für eine solche Regelung spricht aus Sicht von Unternehmen und Konzernen die Vereinfachung von Verarbeitungsvorgängen gerade in Großkonzernen wie bei-

spielsweise eine Zentralisierung der Verarbeitung von Finanz-, Vertriebs- oder Personaldaten in zentralen Systemen. Derartige Zentralisierungen sind indes nach dem geltenden BDSG schon heute zulässig, beispielsweise auf der Grundlage von Aufträgen gemäß § 11 BDSG. Sie finden auf dieser Basis auch in vielen Fällen rechtskonform statt. Insoweit gibt es grundlegende Zweifel an der Notwendigkeit einer solchen Ergänzung.

Ein Sinn für eine solche Erweiterung erschließt sich aber aus der Praxis: Betriebsräte und betriebliche Datenschutzbeauftragte, die im Rahmen ihrer Aufgaben mit der Bewertung unternehmensübergreifender Systeme befasst sind, stellen in einer nicht geringen Zahl von Fällen fest, dass innerhalb von Konzernen eine unternehmensübergreifende Datenverarbeitung erfolgt, ohne dass die nach § 11 BDSG notwendigen Aufträge vertraglich abgesichert sind. Liegen entsprechende Verträge vor, erfüllen sie teilweise nicht die zwingenden Formvorgaben des § 11 BDSG oder sind aus anderen Gründen rechtsfehlerhaft.

Betriebsräte haben am Abschluss von Verträgen nach § 11 BDSG mit Blick auf den im Rahmen ihrer gesetzlichen Mitbestimmungsrechte angestrebten Persönlichkeitsschutz von Beschäftigten ein großes Interesse. Nur auf diesem Weg können sie bei unternehmensübergreifenden Verarbeitungen überprüfen und sicherstellen, ob etwa der Regelungsinhalt von Betriebsvereinbarungen zu IT-Systemen auch für Auftragnehmer verpflichtend ist. Sind etwa bestimmte Auswertungen nach einer Betriebsvereinbarung im Betrieb oder Unternehmen verboten, muss dies vertraglich auch mit einem Auftragnehmer vereinbart werden. Entsprechende Gestaltungen können Betriebsräte auf der Basis bestehender Mitbestimmungsrechte derzeit noch durchsetzen.

Würde die Schaffung einer konzernweiten Berechtigung zur Verarbeitung von Daten zum Wegfall der Notwendigkeit des Abschlusses von Aufträgen nach § 11 BDSG führen, hätte dies aus kollektivrechtlicher Sicht zur Folge, dass Betriebsräte das vorstehend beschriebene Regelungsinstrument ersatzlos verlieren. Betriebs-

vereinbarungen, die mit dem Ziel des Persönlichkeitsschutzes getroffen werden, könnten vor diesem Hintergrund leerlaufen, wenn es innerhalb von Konzernen keine wirksamen Begrenzungen auf zulässige Verarbeitungen gibt. Erfolgt die unternehmensübergreifende Verarbeitung grenzüberschreitend, hätten Betriebsräte in Konzernen noch nicht einmal mehr die Möglichkeit der Einbindung eines Konzernbetriebsrats.

Die Schaffung der Möglichkeit, innerhalb von Konzernstrukturen unternehmensübergreifende Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten einzuführen, würde damit unmittelbar die Mitwirkungs- und Mitbestimmungsrechte von Betriebsräten schwächen, ohne dass es vor dem Hintergrund der Möglichkeiten nach § 11 BDSG für eine solche Novelle einen zwingenden Grund gibt. Auch in diesem Punkt wird damit das Regelungsziel eines besseren Beschäftigtendatenschutzes verfehlt.