

# Handlungsbedarf im Arbeitnehmerdatenschutz

## Teil 1: Arbeitnehmerdatenschutz rechtssicher gestalten

### 1. Position der vbw

Es steht außer Frage, dass der verantwortungsvolle Umgang mit sensiblen Daten immer gewährleistet sein muss. Die vbw – Vereinigung der Bayerischen Wirtschaft e. V. toleriert keine Verletzungen des Datenschutzrechts. Auf der anderen Seite müssen jedoch auch die berechtigten Belange der Wirtschaft Berücksichtigung finden.

Der verantwortungsvolle Umgang mit Daten ist Teil guter Unternehmensführung und Praxis in deutschen Unternehmen. Es darf nicht übersehen werden, dass es sich bei den bekannt gewordenen Missbrauchsfällen um Einzelfälle handelt, die bereits gegen die geltende Rechtslage verstoßen haben. Der weitaus überwiegende Teil der Unternehmen respektiert den Datenschutz und hält die bestehenden Regelungen ein.

Forderung der vbw ist es daher, die beiderseitigen Interessen in einen angemessenen Ausgleich zu bringen.

Das Bundesdatenschutzgesetz bietet den Arbeitnehmern bereits umfassenden Schutz. Zur Beseitigung von Rechtsunsicherheiten sind nach einer sorgfältigen Analyse der geltenden Rechtslage lediglich punktuelle Nachbesserungen nötig. Das Streben nach mehr Rechtssicherheit darf nicht zu Überregulierung mit unnötiger Bürokratie ohne praktischen Nutzen führen.

### 2. Hintergrund

Datenschutz ist in der heutigen Zeit wichtiger denn je. Auf gesellschaftlicher Ebene ist die Einstellung zum Schutz persönlicher Daten gespalten: Während im privaten Bereich viele Daten bereitwillig ins Internet gestellt oder zur Teilnahme an Gewinnspielen preisgegeben werden, wird auf die Datenerhebung und -verarbeitung im Arbeitsverhältnis sehr sensibel reagiert.

Die Unternehmen befinden sich in der schwierigen Lage, auf der einen Seite Compliance-Vorgaben erfüllen und Korruption bekämpfen zu müssen. Auf der anderen Seite müssen die gesetzlichen Vorgaben des Datenschutzrechts eingehalten werden. Dabei herrscht oft Rechtsunsicherheit, da es sich beim Datenschutzrecht um eine zersplitterte Materie handelt und eine Vielzahl von Gesetzen und die höchstrichterliche Rechtsprechung zu beachten sind. Die Entwicklungen in der Technologie ermöglichen sowohl Zugriffe auf Daten von außen als auch interne Kontrollen.

Zudem bedarf es stets einer Interessenabwägung im Einzelfall, weshalb die Unternehmen auf verlässliche gesetzliche Leitplanken angewiesen sind.

Durch die im letzten Jahr bekannt gewordenen Datenschutzskandale sah sich der Gesetzgeber aufgefordert, mit der Bundesdatenschutzgesetznovelle II den neuen § 32 zum Datenschutz im Beschäftigungsverhältnis in das Bundesdatenschutzgesetz aufzunehmen. Wenig Beachtung fand

die Tatsache, dass es sich dabei um einzelne Missbrauchsfälle handelte und das Vorgehen der betroffenen Unternehmen bereits gegen das zu dieser Zeit geltende Recht verstoßen hat. Wichtiger als eine Neuregelung ist daher die Gewährleistung des Vollzugs des geltenden Rechts.

Dennoch wurde im Koalitionsvertrag vereinbart, in das Bundesdatenschutzgesetz einen eigenen Abschnitt zum Arbeitnehmerdatenschutz aufzunehmen. Bei dieser Neuregelung ist darauf zu achten, eine Überregulierung zu vermeiden und den Unternehmen weiterhin die Möglichkeit zu geben, die für sie notwendigen Daten zu erheben und zu verarbeiten.

## Teil 2: Neuregelung des Arbeitnehmerdatenschutzes

Das Bundesinnenministerium hat Ende Mai 2010 einen Referentenentwurf zur Regelung des Beschäftigtendatenschutzes vorgelegt. Nach Abstimmung mit anderen Ressorts ist dieser am 25. August 2010 vom Kabinett verabschiedet worden. Die erste Lesung im Bundestag soll Mitte November stattfinden.

### 1. Zusammenfassende Bewertung des Gesetzentwurfs

Der Gesetzentwurf schränkt die Möglichkeiten der Datenerhebung, -verarbeitung und Nutzung für die Arbeitgeber im Vergleich zur geltenden Rechtslage ein.

Problematisch sind vor allem folgende Einschränkungen:

- Möglichkeit der Einwilligung der Beschäftigten nur in den gesetzlich vorgesehenen Fällen:
  - Datenerhebung über Bewerber bei Dritten
  - Ärztliche Untersuchung oder Eignungstest vor Begründung des Beschäftigungsverhältnisses
  - Speicherung von Bewerberdaten nach Ablehnung
  - Verwendung von Fotos

Nicht mehr möglich ist damit die Einwilligung beispielsweise in:

- Kontrollen, Spamfilterung und Archivierung von E-Mails bei erlaubter Privatnutzung
- Personaldatentransfer ins Nicht-EU-Ausland
- Datenübermittlung für Zusatzleistungen wie Gesundheitsvorsorgeprogramme oder Gruppenversicherungen
- Keine Befugnisse zur Durchführung präventiver, verdachtsunabhängiger Compliance-Maßnahmen; dies führt zum Konflikt mit gesetzlichen Vorschriften, die die Einführung von Kontrollsystemen fordern (z. B. § 91 Abs. 2 AktG, § 130 OWiG, § 33 Abs. 1 WpHG, § 9 Abs. 1 GwG, § 25a KWG)
- Keine ausreichende Ermächtigung zur Kenntnisnahme bzw. Kontrolle der E-Mail und Internetnutzung

- Es fehlt die für die Unternehmen dringend notwendige Vereinfachung der Datenübermittlung im Konzern und ins Ausland.
- Einschränkung von praxisgerechten Regelungen durch Betriebsvereinbarungen, da auch durch eine Betriebsvereinbarung nicht zu Ungunsten der Beschäftigten von den Regelungen des BDSG abgewichen werden darf.
- Das ausnahmslose Verbot der heimlichen Videoüberwachung ist nicht akzeptabel.
- Das vielfach verwendete Wort „erforderlich“ schränkt die Datenerhebung erheblich ein. Sinnvoller und praktikabler wäre stattdessen im gesamten Gesetzentwurf die Verwendung des Wortes „dienlich“.
- Die zahlreichen Informationspflichten bringen unnötige Bürokratie für die Unternehmen mit sich. Zudem bergen die hierdurch bedingten Datenversendungen erhöhte Risiken (z. B. „Datenmüll“ bei der Versendung von Datensammlungen).

Zudem orientiert sich der Entwurf am technischen Stand des Jahres 2010. Da die technische Entwicklung der Zukunft nicht absehbar ist, wäre es sinnvoll, möglichst wenige Anknüpfungen an konkrete technische Instrumente zu haben. Dies birgt die Gefahr der Bedeutungslosigkeit und des ständigen Änderungsbedarfs.

## 2. Bewertung der einzelnen Normen des Referentenentwurfs

### **§ 4 Zulässigkeit der Datenerhebung, -verarbeitung, -nutzung**

In § 4 Abs.1 BDSG wird die Klarstellung aufgenommen, dass Betriebs- und Dienstvereinbarungen andere Rechtsvorschriften im Sinne des BDSG sind.

Diese Klarstellung entspricht den Forderungen der vbw.

### **§ 27 Anwendungsbereich**

In den § 27 wird ein neuer Absatz hinzugefügt, wonach für Beschäftigtendaten die Vorschriften des zweiten, dritten und vierten Unterabschnitts gelten; dies auch dann, wenn die Daten nicht automatisiert oder dateigebunden erhoben, verarbeitet oder genutzt werden.

#### Forderungen der vbw:

- Klarstellung im Gesetzestext, dass § 28 BDSG neben den §§ 32ff BDSG anwendbar bleibt. Insbesondere die Interessenabwägungsklausel aus § 28 Abs. 1 S.1 Nr. 2 BDSG stellt eine wichtige Rechtsgrundlage für verschiedene Verarbeitungen von Mitarbeiter-

daten dar. Dies betrifft vor allem Fälle, in denen unklar ist, ob die Datenverarbeitung zum Zweck des Beschäftigungsverhältnisses erfolgt.

- Des Weiteren sollte die BDSG-Systematik erhalten bleiben und nur dateibezogene oder automatisierte Datenverarbeitung vom Anwendungsbereich des § 32 BDSG erfasst werden. Sonst wird aus § 32 BDSG eine vertragsrechtliche Regelung, die nur im Arbeitsverhältnis gilt.

### **§ 32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses**

Es wird detailliert geregelt, welche Daten der Arbeitgeber vor Begründung eines Beschäftigtenverhältnisses erheben darf. Das Fragerecht im Bewerbungsverfahren wird auf Daten beschränkt, die erforderlich sind, um die Eignung des Bewerbers für die vorgesehene Tätigkeit festzustellen. Sensible Daten dürfen nur unter den Voraussetzungen des § 8 Abs. 1 AGG erhoben werden.

Allgemein zugängliche Daten darf der Arbeitgeber nur erheben, wenn er den Beschäftigten vor der Erhebung darauf hingewiesen hat und kein schutzwürdiges Interesse am Ausschluss der Erhebung überwiegt. Ein schutzwürdiges Interesse überwiegt bei Daten aus sozialen Netzwerken; dies gilt nicht für soziale Netzwerke, die der Darstellung der beruflichen Qualifikation dienen.

#### Forderungen der vbw:

- Streichung der Hinweispflicht auf die Erhebung von allgemein zugänglichen Daten. Es handelt sich dabei um allgemein zugängliche Daten, die für jeden abrufbar sind und von deren Existenz der Betroffene Kenntnis hat.
- Konkretisierung der Abgrenzung zwischen sozialen Netzwerken, die der elektronischen Kommunikation dienen und solchen, die der Darstellung der beruflichen Qualifikation dienen. Die Abgrenzung ist in der Praxis für den Arbeitgeber schwierig.
- Streichung von Vorstrafen und laufenden Ermittlungsverfahren aus dem abschließenden Katalog in § 32 Abs. 2. Die in § 8 Abs. 1 AGG genannte Voraussetzung der Erforderlichkeit der Frage für die Besetzung des Arbeitsplatzes würde ansonsten wesentlich eingeschränkt.
- Zudem fehlt eine Rechtsgrundlage für den Abgleich von Bewerberdaten mit sogenannten Sanktionslisten. Die Legitimation hierfür sollte zumindest in die Gesetzesbegründung aufgenommen werden.

### **§ 32a Ärztliche Untersuchungen und Eignungstests vor Begründung eines Beschäftigungsverhältnisses**

Explizit geregelt werden gesundheitliche Untersuchungen und Eignungstests. Gesundheitliche Untersuchungen sind nach Einwilligung des Beschäftigten zulässig, wenn die Erfüllung bestimmter gesundheitlicher Voraussetzungen eine wesentliche und entscheidende berufliche Anforderung zum Zeitpunkt der Arbeitsaufnahme darstellt.

Ein Eignungstest darf durchgeführt werden, wenn er erforderlich ist, um festzustellen, ob der Beschäftigte zum Zeitpunkt der Arbeitsaufnahme für die vorgesehenen Tätigkeiten geeignet ist.

#### Forderung der vbw:

Die Voraussetzungen, unter denen gesundheitliche Untersuchungen zulässig sind - „wesentliche und entscheidende berufliche Anforderung“, sind zu eng. Auch im Interesse der Arbeitnehmer müssen mit Einwilligung des Bewerbers gesundheitliche Untersuchungen möglich sein, die zum Schutz der Arbeitnehmer zweckdienlich sind.

### **§ 32b Datenverarbeitung und -nutzung vor Begründung des Beschäftigungsverhältnisses**

Daten, die der Arbeitgeber ohne Datenerhebung erhält, dürfen nur verarbeitet und genutzt werden, wenn dies für die Tätigkeit oder die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist. Dies gilt nicht, wenn der Beschäftigte die Daten dem Arbeitgeber übermittelt hat, ohne dass der Arbeitgeber hierzu Veranlassung gegeben hat.

Bewerberdaten müssen gelöscht werden, wenn feststeht, dass ein Beschäftigungsverhältnis nicht begründet wird, außer der Bewerber willigt in eine weitere Speicherung ein.

#### Forderungen der vbw:

- Möglichkeit der Speicherung von Bewerberdaten bis zu sechs Monaten nach Abschluss des Bewerbungsverfahrens, um drohenden oder anhängigen Rechtsstreitigkeiten begegnen zu können (z. B. Ansprüche aus dem AGG) oder auf geeignete Bewerber zurückgreifen zu können, wenn die Stelle nach Ablauf der Probezeit neu besetzt werden soll.
- Die zur Identifikation eines Bewerbers erforderlichen Daten sowie der Vermerk, warum der Bewerber nicht eingestellt wurde, sollten für die Dauer von zwei Jahren gespeichert werden dürfen.
- Nicht praktikabel ist die Regelung, dass ohne Datenerhebung erlangte Daten nur dann genutzt werden dürfen, wenn es für die Tätigkeit oder die Entscheidung über die Be-

gründung des Beschäftigungsverhältnisses erforderlich ist. Datenbestände müssten nach dieser Vorschrift in „erforderliche“ und „nicht erforderliche“ Daten unterteilt werden. Der Begriff „erforderlich“ sollte daher durch „dienlich“ ersetzt werden.

### **§ 32c und § 32d Datenerhebung bzw. Datenverarbeitung und -nutzung im Beschäftigungsverhältnis**

Es werden Regelbeispiele aufgeführt, in denen die Erhebung von Beschäftigtendaten als erforderlich angesehen wird.

Gesundheitliche Untersuchungen und Eignungstests sind mit Einwilligung des Beschäftigten erlaubt, wenn sie erforderlich sind, um die Eignung des Beschäftigten zu überprüfen. Voraussetzung ist das Vorliegen tatsächlicher Anhaltspunkte, die Zweifel an der fortdauernden Eignung des Beschäftigten begründen oder der beabsichtigte Wechsel der Tätigkeit.

Die Verarbeitung und Nutzung von Beschäftigtendaten ist für die erforderlichen Zwecke zulässig. Daten, die der Arbeitgeber ohne Datenerhebung erlangt hat, darf er nur verarbeiten und nutzen, wenn dies erforderlich und nicht unverhältnismäßig ist.

Zur Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen wird nur noch ein automatisierter Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form zugelassen. Die Daten dürfen erst dann personalisiert werden, wenn sich ein Verdachtsfall ergibt.

Beschäftigtendaten dürfen nicht automatisiert zusammengeführt werden, um ein Gesamtbild der wesentlichen geistigen und charakterlichen Eigenschaften oder des Gesundheitszustands des Beschäftigten zu erstellen.

Dritte dürfen an sie übermittelte Daten nur zu dem festgelegten Zweck nutzen. Hierauf muss der Arbeitgeber den Dritten hinweisen.

#### Forderungen der vbw:

- Im § 32c die Streichung des Verweises auf § 32 Abs. 6 (Direkterhebung beim Beschäftigten). Dies ist gerade im Hinblick auf gesetzliche Auskunftspflichten (z. B. ELENA-Verfahren) nicht praktikabel.
- Ebenso sollte § 32c Abs. 2 ersatzlos gestrichen werden, da die Veränderung der Tätigkeit unter die Durchführung des Beschäftigungsverhältnisses in Abs.1 fallen. Die Regelung ist daher überflüssig.
- Die Voraussetzungen, unter denen gesundheitliche Untersuchungen zulässig sind, sind zu eng. Zur Einhaltung von Sicherheitsstandards und zur Vermeidung von Unfällen

len muss es für die Unternehmen möglich sein, routinemäßige Alkohol- und Drogenkontrollen durchführen zu können.

- Die anonymisierte Überprüfung eignet sich nur für präventive Kontrollen. Bei Vorliegen eines Verdachts sollte gleich eine Prüfung auf personenbezogener Basis durchgeführt werden dürfen.
- Ausdrückliche Klarstellung im Gesetzestext, dass verdachtsunabhängige Stichprobenkontrollen durchgeführt werden dürfen.
- Streichung des Abs. 5, da hierunter auch die Speicherung und Zusammenführung in einer elektronischen Personalakte fallen könnte.

### **§ 32e Datenerhebung ohne Kenntnis des Beschäftigten zur Aufdeckung und Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen im Beschäftigtenverhältnis**

Grundsätzlich darf der Arbeitgeber Beschäftigendaten nur mit Kenntnis des Beschäftigten erheben.

Ohne Kenntnis des Beschäftigten dürfen Daten nur zur Aufdeckung von Straftaten oder schweren Pflichtverletzungen sowie zur Verhinderung von damit im Zusammenhang stehenden weiteren Straftaten oder schweren Pflichtverletzungen erhoben werden. Die Erhebung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise erschwert oder weniger erfolgsversprechend wäre. Ist der Zweck nicht zu erreichen, ist die Maßnahme abzubrechen. Unzulässig ohne Kenntnis des Beschäftigten ist eine länger als 24 Stunden ununterbrochen bzw. vier Tage dauernde planmäßige Beobachtung, das Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes und der Einsatz besonderer technischer Mittel zu Beobachtungszwecken.

Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht erhoben, verarbeitet oder genutzt werden.

Die Datenerhebung unterliegt der Vorabkontrolle gem. § 4d Abs. 5 BDSG.

Der Grund der Speicherung der Daten und die Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden und ist spätestens am Ende des Kalenderjahrs, das dem Jahr der Dokumentation folgt, zu löschen.

#### Forderungen der vbw:

- Gesetzliche Klarstellung, dass auch rein präventive Maßnahmen ohne Vorliegen von tatsächlichen Anhaltspunkten zulässig sind, um den Compliance-Anforderungen der Unternehmen (z. B. § 91 AktG) gerecht zu werden.

- Auch bei Pflichtverletzungen, die keine außerordentliche Kündigung rechtfertigen, muss eine Datenerhebung erlaubt sein. Der Begriff der schwerwiegenden Pflichtverletzung ist hierfür zu eng. Die im Entwurf ersichtliche qualitative Schwelle scheint der Systematik aus dem öffentlichen Recht für staatliche Eingriffe entlehnt. Hier geht es jedoch um berechnete Interessen zwischen Vertragspartnern, Vertragsbrüche zu verhindern. Daher sollte die Datenerhebung bei der Verletzung sämtlicher dem Beschäftigten obliegenden vertraglichen Haupt- und Nebenpflichten erlaubt sein. Zudem weiß der Arbeitgeber meist erst nach Klärung des Sachverhaltes, welche Art der Pflichtverletzung vorliegt.
- In den Gesetzestext aufgenommen werden sollte zudem, dass der Verdacht gegen eine „Beschäftigtengruppe“ für die Datenerhebung ausreicht, da in der Praxis selten eine konkrete Person einer Straftat / Pflichtverletzung verdächtigt wird, sondern bestimmte Arbeitsbereiche oder Abteilungen. Dies findet sich bisher nur in der Gesetzesbegründung.
- Die Pflicht zur Vorabkontrolle generiert in der Praxis erhebliche Mehraufwände und sollte daher gestrichen werden.
- Die Regelung zur Dokumentation schafft zusätzlichen unnötigen bürokratischen Aufwand. Unklar ist zudem, in welcher Form die Dokumentation zu erfolgen hat. Hier sollte klargestellt werden, dass eine elektronische Dokumentation ausreicht.

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

Videoüberwachung ist zur Wahrung der aufgelisteten wichtigen betrieblichen Interessen zulässig, wenn kein schutzwürdiges Interesse der Betroffenen am Ausschluss der Datenerhebung besteht. Ausdrücklich verboten wird die Videoüberwachung von Betriebsstätten, die überwiegend zur privaten Lebensgestaltung des Beschäftigten dienen, sowie von Sanitär-, Umkleide- und Schlafräumen.

Die heimliche Videoüberwachung ist unzulässig.

Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet und muss spätestens am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt, gelöscht werden.

Die Videoüberwachung unterliegt der Vorabkontrolle gem. § 4d Abs. 5 BDSG.

#### Forderungen der vbw:

- Die Liste der wichtigen betrieblichen Interessen sollte keine abschließende Auflistung darstellen, sondern Regelbeispiele. Zudem sollte sie um den Punkt „Aufklärung von Straftaten“ ergänzt werden.

- Der Verweis auf § 32e und den Begriff der „schwerwiegenden“ Pflichtverletzung ist zu eng. Im Vorfeld der Überwachung ist meist noch nicht bekannt, in welchem Umfang Pflichtverletzungen vorliegen.
- Zudem sollte in Ausnahmefällen eine heimliche Videoüberwachung zur Aufklärung und Verhinderung von Straftaten oder Pflichtverletzungen zulässig sein, wenn die Erforschung eines Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.
- Ebenso fehlt eine Regelung zur rechtmäßigen Verwendung von Zufallsfunden anlässlich einer rechtmäßigen Videoüberwachung (z. B. ein anderer als der verdächtige Arbeitnehmer wird bei der Begehung einer Straftat aufgezeichnet).

### **§ 32g Ortungssysteme**

Ortungssysteme zur Bestimmung des geographischen Standorts dürfen grundsätzlich nur zur Sicherheit des Beschäftigten oder zur Koordinierung des Einsatzes des Beschäftigten eingesetzt werden. Die Ortung ist nur während der Arbeitszeit erlaubt. Der Einsatz des Ortungssystems muss für den Beschäftigten erkennbar sein. Der Arbeitgeber muss den Beschäftigten über den Umfang der Aufzeichnungen und deren Auswertung informieren. Ein Ortungssystem zum Schutz von beweglichen Sachen darf nicht erfolgen, solange der Beschäftigte die bewegliche Sache erlaubterweise nutzt.

Forderung der vbw ist, dass beim Einsatz von Ortungssystemen gewonnene Daten über rechtswidriges Verhalten der Beschäftigten zur Aufklärung von Straftaten oder Pflichtverletzungen verwendet werden dürfen.

### **§ 32h Biometrische Verfahren**

Biometrische Verfahren dürfen nur zur Autorisierung und zu Authentifikationszwecken benutzt werden. Für die Erhebung, Verarbeitung oder Nutzung zu anderen Zwecken ist die Einwilligung des Beschäftigten notwendig.

Forderung der vbw ist die Sicherstellung, dass Zugangskontrollsysteme, die gleichzeitig zur Zeiterfassung genutzt werden, nicht unter diese Regelung fallen. Die Daten müssen gem. § 32 d und e genutzt und verarbeitet werden dürfen.

### **§ 32i Nutzung von Telekommunikationsdiensten**

Es wird ausdrücklich geregelt, in welchen Fällen bei rein dienstlicher Nutzung von Telekommunikationsdiensten anfallende Verkehrsdaten erhoben, verarbeitet oder benutzt

werden dürfen. Für die inhaltliche Kontrolle von dienstlichen Telefondiensten ist die Einwilligung des Beschäftigten und des Kommunikationspartners notwendig.

Eine inhaltliche Kontrolle der rein dienstlichen Nutzung von Internet und E-Mail ist zulässig, soweit dies zur Durchführung des Beschäftigungsverhältnisses oder zum ordnungsgemäßen Betrieb und zur Datensicherheit erforderlich ist. Dies gilt auch soweit es für den ordnungsgemäßen Geschäftsbetrieb des Arbeitgebers in den Fällen einer Versetzung, Abordnung oder Abwesenheit erforderlich ist.

Private Daten und Inhalte darf der Arbeitgeber nur erheben, verarbeiten oder nutzen, wenn dies zur Durchführung des ordnungsgemäßen Geschäftsbetriebs unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat.

#### Forderungen der vbw:

- Klarstellung der Nichtanwendbarkeit des § 88 TKG auf Arbeitgeber bei erlaubter Privatnutzung von Internet und E-Mail; zumindest Zulässigkeit von (Stichproben-) Kontrollen auch ohne Einwilligung der Arbeitnehmer. Zudem muss die Möglichkeit der Regelung durch den Abschluss von Betriebsvereinbarungen, Tarifverträgen oder mit Einwilligung der Beschäftigten gesetzlich klargestellt werden.
- Bezüglich der Einwilligung in die Aufzeichnung von Telefonaten sollte eine Ausnahmeklausel für Notfälle (z. B. Anruf bei der Werksfeuerwehr) aufgenommen werden.
- Der Zugriff auf rein dienstliche E-Mails darf nicht beschränkt werden, da diese den Geschäftsbriefen gleichgestellt sind und immer auch eine Korrespondenz des Arbeitgebers darstellen. Zudem besteht häufig eine Archivierungspflicht gem. § 257 HGB.
- Verkehrsdaten müssen auch zur Durchführung des ordnungsgemäßen Dienst- und Geschäftsbetriebs sowie zur Verhinderung und Aufdeckung von Straftaten, Ordnungswidrigkeiten und Pflichtverletzung genutzt werden dürfen. Dies muss auch bei erlaubter Privatnutzung gelten, da diese ansonsten verboten werden müsste.

### **§ 32j Unterrichtungspflichten**

Bei Verletzungen der Regeln des BDSG besteht eine Unterrichtungspflicht des Arbeitgebers gegenüber dem Beschäftigten. Bei einer drohenden schwerwiegenden Beeinträchtigung von Rechten oder schutzwürdigen Interessen der Beschäftigten muss zudem die Aufsichtsbehörde unterrichtet werden.

Die Vorschrift verweist auf den bereits seit September 2009 geltenden § 42a BDSG. Allerdings listet § 42a BDSG besonders sensible Daten auf, bei deren Verlust eine Unterrichtungspflicht besteht. § 32i BDSG sieht diese Unterrichtungspflicht hingegen für alle Arten von Beschäftigtendaten vor.

Forderung der vbw: Die Unterrichtungspflicht aus § 42a BDSG ist auch für entsprechende Beschäftigtendaten ausreichend. Eine Sonderbehandlung durch Ausdehnung auf alle Arten von Beschäftigtendaten ist nicht begründbar und auch nicht notwendig.

### **§ 32k Änderungen**

Ändert der Arbeitgeber Daten, die er einem Dritten übermittelt hat, so muss er die Berichtigung, Löschung oder Sperrung dieser Daten dem Dritten unverzüglich mitteilen. Die Pflicht besteht ausnahmsweise nicht, wenn die Mitteilung zur Wahrung der schutzwürdigen Interessen der Beschäftigten nicht erforderlich ist.

Forderung der vbw:

- Ablehnung der Klausel, da sie zu einem erheblichen bürokratischen Aufwand in der Praxis führt. Die Relativierung „Wahrung der schutzwürdigen Interessen der Beschäftigten“ führt zu Rechtsunsicherheit in der Praxis.
- Sinnvoll wäre zumindest eine Klarstellung, dass nur Dritte in aktiver Geschäftsbeziehung zum Arbeitgeber gemeint sind.

### **§ 32l Einwilligung, Geltung für Dritte, Rechte der Interessenvertretung, Beschwerderecht, Unabdingbarkeit**

Die Möglichkeit zur individuellen Einwilligung der Beschäftigten wird auf die gesetzlich vorgesehenen Fälle beschränkt.

Die Vorschriften gelten für Dritte entsprechend, die für den Arbeitgeber beim Erheben, Verarbeiten und Nutzen von Beschäftigtendaten tätig werden.

Der Beschäftigte erhält ein Beschwerderecht bei der Aufsichtsbehörde, wenn der Arbeitgeber unbefugt Daten erhebt, verarbeitet oder nutzt und einer Beschwerde des Beschäftigten nicht unverzüglich abhilft.

Von den Vorschriften des Unterabschnitts darf nicht zu Ungunsten der Beschäftigten abgewichen werden.

Forderungen der vbw:

- Gesetzliche Klarstellung, dass die freiwillige Einwilligung des Beschäftigten in die Datenverarbeitung möglich ist. Diese Regelung widerspricht den allgemeinen Regeln des Schuldrechts, wonach auch im Arbeitsverhältnis die Abgabe freier Willenserklärungen möglich ist (z. B. Abschluss eines Aufhebungsvertrages). Sie behandelt Beschäftigte faktisch wie beschränkt Geschäftsfähige und schränkt die Möglichkeiten für praktikab-

le bedarfsgerechte Lösungen erheblich ein. Auch für den Arbeitnehmer positive Einwilligungen, z. B. in ein Gesundheitsvorsorgeprogramm wären ausgeschlossen.

- Streichung des Beschwerderechts bei der Aufsichtsbehörde. Der Betroffene kann bereits nach geltender Rechtslage jederzeit eine Eingabe an die Aufsichtsbehörde richten.
- Die Möglichkeit der praxis- und interessensgerechten Ausgestaltung durch Betriebsvereinbarungen und Tarifverträge darf nicht durch eine generelle Unabdingbarkeitsklausel eingeschränkt werden.

### Teil 3: Weitere Forderungen der vbw

Darüber hinaus fehlen notwendige Klarstellungen im BDSG:

#### – **Konzernprivileg**

Hinderlich für die Unternehmen ist die derzeitige Rechtslage, nach der die Datenübermittlung im Konzern nicht privilegiert ist und einzelne Konzernteile wie betriebsfremde Dritte behandelt werden. Für jeden Datentransfer ist daher ein eigener Erlaubnistatbestand notwendig.

Forderung der vbw: Im Rahmen einer Neuregelung müssen die Datenübermittlung im Konzern erleichtert und die wirtschaftlichen Zusammenhänge im Konzern berücksichtigt werden.

Vorschlag: Ergänzung eines neuen S. 2 in § 32 Abs. 1 BDSG, in dem die Datenübermittlung innerhalb eines Konzerns der Datenübermittlung im Unternehmen nach S. 1 gleichgestellt wird.

#### – **Internationaler Datentransfer**

Der Datentransfer in Länder außerhalb der EU unterliegt derzeit strengen Anforderungen, die den Unternehmen ein schnelles Agieren erschweren.

Forderung der vbw: Es sollten Rahmenbedingungen geschaffen werden, die den Datentransfer ins Ausland entbürokratisieren.

Vorschlag: Insbesondere sollte klargestellt werden, dass der Datentransfer ins Ausland innerhalb eines Konzerns durch (Konzern-)Betriebsvereinbarungen wirksam geregelt werden kann.

#### – **Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten**

Der Betriebsrat geht in vielen Bereichen mit Arbeitnehmerdaten um. Hierbei unterliegt er gegenwärtig keiner Kontrolle. Der Datenschutzbeauftragte hat nach verbreiteter Auffassung keine Kontrollbefugnisse für den Umgang des Betriebsrats mit Arbeitnehmerdaten.



Forderung der vbw: Der kontrollfreie Raum muss durch Befugnisse des betrieblichen Datenschutzbeauftragten gegenüber dem Betriebsrat geschlossen werden.

Vorschlag: Gesetzliche Klarstellung, dass das Kontrollrecht des betrieblichen Datenschutzbeauftragten auch den Umgang des Betriebsrats mit Arbeitnehmerdaten umfasst.

#### – **Erleichterungen bei der Auswahl des Datenschutzbeauftragten**

Das Bundesdatenschutzgesetz sieht vor, dass nur ein „zuverlässiger“ Datenschutzbeauftragter bestellt werden kann. Diese Zuverlässigkeit wird bei Interessenkonflikten mit der dienstlichen Tätigkeit verneint. Dies wird teils schon bei Beschäftigten angenommen, die in irgendeiner Weise personenbezogene Daten verarbeiten. Dies erschwert die Rekrutierung von kompetenten internen Personen, insbesondere bei kleinen und mittleren Unternehmen.

Forderung der vbw: Die Unternehmen müssen mehr Freiheit bei der Auswahl des Datenschutzbeauftragten erhalten. Nicht jede Tätigkeit des Beschäftigten in der Datenverarbeitung darf automatisch zu einem Interessenkonflikt führen.

Vorschlag: Gesetzliche Klarstellung, dass auch Beschäftigte, die sich mit der personenbezogenen Datenverarbeitung befassen, die erforderliche Zuverlässigkeit für die Tätigkeit als (arbeitsteiliger) Datenschutzbeauftragter aufweisen können, sofern keine konkreten Anhaltspunkte für einen Interessenkonflikt bestehen.

#### – **Eingeschränkte gerichtliche Überprüfbarkeit bei Betriebsvereinbarung mit Zustimmung des Datenschutzbeauftragten**

Im Bereich des Bundesdatenschutzgesetzes bestehen Selbstregulierungselemente, nämlich der Betriebsrat und der betriebliche Datenschutzbeauftragte. Diese sollten dafür verwendet werden, um mehr Rechtssicherheit zu gewinnen.

Forderung der vbw: Datenschutzrechtliche Vorgänge, die kollektivrechtlich erlaubt sind, sollten privilegiert werden und nur eingeschränkt gerichtlich überprüfbar sein.

Vorschlag: Stimmen Betriebsrat und betrieblicher Datenschutzbeauftragter einer bestimmten Datenerhebung, -verarbeitung oder -nutzung zu, ist die entsprechende Datenverarbeitung nur unzulässig, wenn sie offensichtlich rechtswidrig ist.

#### – **Erleichterungen bei der Auftragsdatenverarbeitung**

Die Auftragsdatenverarbeitung ist gerade für kleine und mittlere Unternehmen ein wichtiges Instrument, um Vorgänge wie z. B. die immer komplizierter werdende Lohn- und Gehaltsabrechnung durch externe Dienstleister erledigen zu lassen. Die seit 01. September 2009 geltenden Kontroll- und Dokumentationspflichten erschweren die Auftragsdatenverarbeitung erheblich.

The logo for the Bavarian Chamber of Commerce (vbw) is located in the top right corner. It consists of the lowercase letters 'vbw' in a white, sans-serif font, centered within a dark grey square. Below the letters, the text 'Die bayerische Wirtschaft' is written in a smaller, white, sans-serif font.

vbw

Die bayerische Wirtschaft

Forderung der vbw: Die Kontroll- und Dokumentationspflichten bei der Auftragsdatenverarbeitung müssen erleichtert werden.

Vorschlag: Hat der Auftragnehmer ein Qualitätssiegel oder erteilt er eine Datenschutzeselbstauskunft, dann muss dies die Kontroll- und Dokumentationspflichten vor Abschluss und während des Auftragsverhältnisses entbehrlich machen.

07. Oktober 2010