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

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