GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERUNG e.V.

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

zu den Anträgen

a) *Rechte der Beschäftigten von Discountern verbessern*
(BT-Drucksache 16/9101)

b) *Persönlichkeitsrechte abhängig Beschäftigter sichern – Datenschutz am Arbeitsplatz stärken*
(BT-Drucksache 16/9311)

c) *Datenschutz für Beschäftigte stärken*
(BT-Drucksache 16/11376)

d) Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern
(BT-Drucksache 16/12670)

erstellt von

Rechtsanwalt Andreas Jaspers,

Geschäftsführer der GDD e.V.

Gesellschaft für Datenschutz
und Datensicherung 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. Ausgangssituation

Der Schutz von Arbeitnehmerdaten ist in Deutschland nicht ungeregelt. Neben den bereichsspezifischen gesetzlichen Regelungen findet das Bundesdatenschutzgesetz auch auf die Verwendung von Arbeitnehmerdaten Anwendung. Zudem ist der Arbeitnehmerdatenschutz auch durch betriebliche Regelungen, insbesondere durch Betriebsvereinbarungen, geregelt. Weiterhin hat die Rechtsprechung das Persönlichkeitsrecht im Arbeitsverhältnis konkretisiert.

Gegenstand einer Kodifizierung des Arbeitnehmerdatenschutzes sind zunächst die bestehenden materiellen Regelungslücken. Weiterhin ist der Einsatz der modernen Informations- und Kommunikationstechnik im Arbeitsverhältnis mit Blick auf die Gewährleistung des Persönlichkeitsrechts von Arbeitnehmern zukunftsweisend datenschutzkonform auszugestalten.

II. Evidente Regelungslücken

1. 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.

2. 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.

3. Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten

Der unzulässigen Verwendung von Mitarbeiterdaten kann dadurch wirksam begegnet werden, dass die interne Kontrollinstanz der Unternehmen eine rechtliche und unternehmenspolitische Stärkung erhält. Die innerbetriebliche Selbstkontrolle in den Unternehmen wird vom betrieblichen

Datenschutzbeauftragten wahrgenommen, den bereits Unternehmen zu bestellen haben, die zehn oder mehr Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Insbesondere bedarf es einer Effektivierung der präventiven Arbeit des Datenschutzbeauftragten.

Naturgemäß können die Datenschutzbeauftragten ihrem gesetzlichen Auftrag zur Hinwirkung auf die Einhaltung der Datenschutzvorschriften nicht gerecht werden, wenn sie über die Datenverarbeitungen nicht rechtzeitig informiert werden. Insofern ist auf die bestehende Gesetzeslage hinzuweisen, wonach der Datenschutzbeauftragte über Vorhaben der automatisierten Verarbeitung rechtzeitig zu unterrichten ist, damit er die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen überwachen kann. In Ergänzung zur Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen zählt die gesetzlich vorgeschriebene Vorabkontrolle im Fall von besonders risikobehafteten Datenverarbeitungen zu den Aufgaben des Datenschutzbeauftragten. Eine Pflicht zur Vorabkontrolle besteht derzeit insbesondere in Fällen der Verarbeitung sensitiver Daten bzw. im Rahmen der Erstellung von Persönlichkeitsbewertungen. Die aktuellen Datenschutzskandale geben Anlass dazu, explizit alle Überwachungssysteme und -maßnahmen generell der Vorabkontrolle mit entsprechender schriftlicher Freigabeerklärung durch die Datenschutzbeauftragten zu unterziehen.

Umstritten ist, ob eine gesetzeswidrig unterbliebene Vorabkontrolle überhaupt spürbare Rechtsfolgen nach sich zieht. Es sollte gesetzlich klargestellt werden, dass ein Übergehen des Datenschutzbeauftragten sanktioniert wird. Dies hätte zur Folge, dass Verarbeitungen, die ohne das notwendige Vorabkontrollverfahren durchgeführt werden, als Ordnungswidrigkeiten oder Straftaten verfolgt werden könnten. Durch eine solche Aufwertung der Kompetenzen des Datenschutzbeauftragten würde auch dessen Verantwortung im Unternehmen steigen. Deshalb ist im Interesse der Gewährleistung einer unabhängigen Überprüfung der Zulässigkeit der Verarbeitung und Weitergabe personenbezogener Daten auch die Rechtsstellung des Datenschutzbeauftragten im Unternehmen zu stärken.

Seiner unabhängigen Kontrollaufgabe kann der Datenschutzbeauftragte nur dann nachkommen, wenn der Bestand seines Arbeits- oder Dienstverhältnisses vom Ergebnis der Überprüfung nicht berührt wird. Insoweit ist ein Sonderkündigungsschutz für den betrieblichen Datenschutzbeauftragten notwendig. Hierzu gibt es bereits einen Gesetzentwurf der Bundesregierung (BT-Drucks. 16/12011). Zugleich erfordert eine Erweiterung des Aufgaben- und Kompetenzbereichs des Datenschutzbeauftragten eine Ausweitung seiner zeitlichen und wirtschaftlichen Ressourcen für diese Tätigkeit. Es ist davon auszugehen, dass durch eine entsprechende Stärkung des Datenschutzbeauftragten Skandale, sofern diese nicht einen kriminellen Hintergrund haben, vermieden werden können und damit das Grundrecht auf informationelle Selbstbestimmung der Mitarbeiter erheblich gestärkt werden kann.

III. Gesetzliche Konkretisierungen

Das bestehende Datenschutzrecht ist weitgehend technikneutral. Der Einsatz moderner Informations- und Kommunikationstechniken im Arbeitsverhältnis ist bisher auf Grundlage unbestimmter Rechtsbegriffe und Interessenabwägungen zu entscheiden. Angesichts der rasanten Technikentwicklung ist dieser gesetzgeberische Ansatz auch weiterhin zu verfolgen.

Unabhängig hiervon kann es in einzelnen Zweifelsfällen angezeigt sein, gesetzgeberische Zielvorgaben für die Beurteilung der Zulässigkeit des Einsatzes der modernen Techniken im Arbeitsverhältnis aufzustellen.

1. Medizinische Untersuchungen

Medizinische Untersuchungen sollten nur zulässig sein, wenn sie mit Blick auf die auszuübende Tätigkeit zwingend notwendig sind. Dies ist insbesondere bei gefahrgeneigter Arbeit der Fall. Gentests sind mit Ausnahme der im Gendiagnostikgesetz geregelten Ausnahmetatbestände im Arbeitsverhältnis regelmäßig unzulässig.

2. Nutzung biometrischer Daten

Biometrische Daten im Arbeitsverhältnis dürfen grundsätzlich nur der Identitätskontrolle dienen. Der allgemeine datenschutzrechtliche Grundsatz der Datenvermeidung und der Datensparsamkeit gebietet es, dass biometrische Daten unter der alleinigen Kontrolle des Betroffenen stehen und ausschließlich zum Vergleich verarbeitet werden dürfen. Die Nutzung bedarf der Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten, deren gesetzlicher Anwendungsbereich insoweit auszuweiten ist.

3. Überwachungssysteme

Überwachungssysteme wie der Einsatz der Videotechnik oder andere Systeme mit vergleichbarer Eingriffsmöglichkeit in die informationelle Selbstbestimmung wie RFID oder GPS dürfen grundsätzlich nicht zu Zwecken Leistungskontrolle und Leistungsbemessung eingesetzt werden. Dies gilt insbesondere für Verfahren des Data Mining zum Zwecke der Mitarbeiterkontrolle und der Erstellung von Persönlichkeitsprofilen. Der gesetzliche Anwendungsbereich der Regelung zur Videoüberwachung in § 6b BDSG sollte nicht wie bisher auf „öffentlich zugängliche Räume“ beschränkt bleiben. Vielmehr ist die Vorschrift mit ihren Zulässigkeits- und Transparenzregeln auf den Einsatz der Videotechnik insgesamt zu erstrecken. Der Einsatz von Systemen, die eine Mitarbeiterüberwachung ermöglichen, sind generell der gesetzlichen Vorabkontrolle durch den Datenschutzbeauftragten zu unterwerfen.

4. Screening von Mitarbeitern

Das Screening von Mitarbeitern zum Zwecke der Prüfung von Compliance-Anforderungen darf nur unter Beachtung der Grundsätze der Verhältnismäßigkeit und der Datensparsamkeit durchgeführt werden. Für legitime Kontrollzwecke ist insbesondere vom Einsatz von Verfahren der Pseudonymisierung Gebrauch zu machen. Die Kontrollfrequenz und der betroffene Personenkreis bedarf der Begrenzung nach Erforderlichkeitsgesichtspunkten. Auch hier empfiehlt sich eine generelle Vorabkontrollpflicht.

5. Nutzung der Informations- und Kommunikationstechnik am Arbeitsplatz

Der Einsatz und die Kontrolle der Informations- und Kommunikationstechnik am Arbeitsplatz, insbesondere die Nutzung von Telefon, E-Mail und Internet, ist im Wege der Selbstregulierung, ggf. durch Betriebsvereinbarungen, gestaltbar. Dabei muss es dem Arbeitgeber möglich bleiben, wahlweise die Privatnutzung der IuK-Technik zu verbieten oder eine eingeschränkte Nutzung für private Zwecke durch den Arbeitnehmer zu erlauben. Hier haben sich bereits verschiedene Vorgehensweisen etabliert, die den jeweiligen betrieblichen Bedürfnissen Rechnung tragen. Nur für den ungeregelten Zustand verbleibt hinsichtlich der Reichweite des Fernmeldegeheimnisses mit Blick auf die Privatnutzung eine Rechtsunsicherheit bezüglich der Kontrollmöglichkeiten für legitime Zwecke durch den Arbeitgeber. Hier kann durch den Gesetzgeber klargestellt werden, dass auch bei Zulassung der Privatnutzung der Informations- und Kommunikationstechnik am Arbeitsplatz eine Kontrolle zur Aufdeckung von Straftaten und Missbrauch zulässig ist.

IV. Regelung des Arbeitnehmerdatenschutzes

Dass es wegen vorbezeichneter Gesetzeslücken und Empfehlungen für eine gesetzliche Konkretisierung des Arbeitnehmerdatenschutzes zwangsläufig eines eigenständigen Arbeitnehmerdatenschutzgesetzes bedarf, ist nicht zwingend. Hier kämen alternativ auch Regelungen im Bundesdatenschutzgesetz oder im Betriebsverfassungsgesetz in Betracht. Der Gesetzgeber sollte darauf achten, das Datenschutzrecht nicht durch neue bereichsspezifische Gesetze weiter zu zersplittern. Vielmehr sollte das Bundesdatenschutzgesetz als zentrales Gesetz, das die wesentlichen Datenschutzthemen regelt, auch die Grundlagen des Arbeitnehmerdatenschutz beinhalten. Die umfassende Geltung des Gesetzes bei der Verarbeitung von Personaldaten kann dadurch erreicht werden dass sein Anwendungsbereich sich hier nicht auf automatisierte oder dateigebundene Verarbeitungen beschränkt. Dadurch würden eine Reihe von ansonsten in einem Arbeitnehmerdatenschutzgesetz erforderliche Doppelregelungen vermieden.

Bonn, den 4. Mai 2009