

## **Stellungnahme zu Fragen des Arbeitnehmerdatenschutzes anlässlich der Anträge 16/11376, 16/9101, 16/9311, 16/12670**

### **1. Allgemeine Bewertung**

Angesichts langjähriger Erfahrung bei der Datenschutzberatung von Arbeitnehmersvertretungen und betrieblichen Datenschutzbeauftragten unterstütze ich, auch im Namen der Deutschen Vereinigung für Datenschutz e.V., das grundsätzliche Anliegen, ein Arbeitnehmerdatenschutzgesetz zu verabschieden.

In der Praxis zeigt sich seit langem, dass das Bundesdatenschutzgesetz zwar theoretisch auch für den betrieblichen Bereich eine solide Grundlage bietet, aber dennoch dem besonderen Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer nicht gerecht wird. Die Unbestimmtheit mancher Begriffe, wie zum Beispiel der Zweckbestimmung, um nur ein Beispiel zu nennen, führt in der betrieblichen Praxis häufig zu unakzeptabler, aber phantasievoller Definitionsjonglage des Arbeitgebers. Wird erst einmal so etwas Schwammiges wie „Optimierung von Abläufen“ als Zweckbestimmung akzeptiert, so lassen sich hernach alle auf dieser Grundlage gesammelten Beschäftigtendaten (Tastenschläge, minutiöse Überwachung von Außendienstmitarbeitern, sogar die Zahl der Toilettengänge) für fast alle denkbaren Auswertungen einsetzen, ohne, formal gesehen, den ursprünglichen Zweck zu ändern. Dass einigen Arbeitgebern sowohl bei der Sammlung als auch bei der Auswertung die Erfordernis der Abwägung mit den Persönlichkeitsrechten der Beschäftigten abhanden gekommen scheint, kann nun seit einigen Monaten auch öffentlich in den Medien verfolgt werden. Gerade diese Fähigkeit zur Abwägung ist zur Anwendung des BDSG jedoch unerlässlich. Da Unternehmen aus unterschiedlichsten Gründen diese Abwägung seit langen Jahren nicht vornehmen oder vornehmen können, scheint die Konkretisierung der Datenschutzprinzipien für den Arbeitsbereich der einzig erfolgversprechende Weg.

Soll ein Arbeitnehmerdatenschutzgesetz erfolgreich anwendbar sein, so muss es auf den Grundlagen des BDSG aufbauen und durch konkrete betriebliche Regelungen einen Mehrwert für den Datenschutz erzielen. Es muss sich an der betrieblichen Praxis orientieren und festlegen, wie die Prinzipien „Verbot mit Erlaubnisvorbehalt“, „Erforderlichkeit“, „Zweckbindung“ und „Transparenz“ in Bezug auf den Umgang mit Arbeitnehmerdaten umzusetzen sind. Ein zweites BDSG, bei dem nur die Worte „Betroffener“ durch „Beschäftigte“ und „verantwortliche Stelle“ durch „Arbeitgeber“ ersetzt würden, wäre nicht wünschenswert.

Da ein Arbeitnehmerdatenschutzgesetz in diesem Sinne eine bereichsspezifische Ergänzung des BDSG darstellt und nicht das BDSG ersetzen soll, erscheint es nicht sinnvoll, bereits im BDSG geregelte Sachverhalte nochmals ohne weitere Konkretisierung „abzuschreiben“. Dies ist nicht nur unnötig, es stiftet auch insofern Verwirrung als der fälschliche Eindruck entstehen könnte, mit Verabschiedung eines Arbeitnehmer-Datenschutzgesetzes sei das BDSG für den Umgang mit Beschäftigtendaten nicht mehr einschlägig.

Als unbedingte Nebenpflicht zur Verabschiedung eines Arbeitnehmerdatenschutzgesetzes erscheint die Ausstattungsverbesserung der Aufsichtsbehörden und aktives Sanktionieren von Verstößen gegen Grundpflichten (Bestellung bDSB, Meldepflicht, Schulungspflicht, Erstellung Verfahrensverzeichnis,...)

## 2. Überflüssiges

Beispielhaft, jedoch in Bezug auf die vorgelegten Anträge nicht abschließend, im Folgenden Regelungsvorschläge, die entweder konkretisiert oder aufgrund ihrer Verankerung im BDSG nicht im AN-DSG Eingang finden sollten, da sie bereits eindeutig heutiger Rechtslage entsprechen:

- Mit personenbezogene Daten darf auch heute schon nur nach Verpflichtung auf § 5 BDSG und Datenschutz-Unterweisung umgegangen werden [11376]
- Die Gleichstellung personenbeziehbarer Daten mit personenbezogenen Daten [11376] ist auch heute schon unstrittig. Strittig ist allerdings, wann ein Datum (Beispiel IP-Adresse) personenbeziehbar ist. Gerade hierzu wäre eine Klarstellung im betrieblichen Umfeld wünschenswert, die auf die Zugriffsmöglichkeiten des Arbeitgebers Bezug nimmt.
- Das Fragerecht im Bewerbungsverfahren verbietet auch heute schon viele Fragen, z. B. nach einer Schwangerschaft [9311].
- Die Rechte der Arbeitnehmervertretungen auf Information und Mitbestimmung sind bereits heute in BetrVG, PersVG und weiteren ausführlich geregelt [9311]

## 3. Schädliches

Folgende Regelungsvorschläge stellten sogar eine Verschlechterung der heutigen Rechtslage dar und sollten so keinesfalls umgesetzt werden:

- Die Beschränkung des Geltungsbereichs auf Regelungen zur Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung personenbezogener Daten [11376] nimmt aus nicht offensichtlichen Gründen die Löschung und Sperrung als Verarbeitungsphasen aus. Gerade zur Löschung (Fristen, Löschkonzepte, Löschanprüche) sollte ein gutes Arbeitnehmerdatenschutzgesetz aber konkrete Aussagen treffen.
- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist auch heute schon nur nach Identifizierung einer Zulässigkeitsgrundlage (Arbeitsvertrag, sonstiger Vertrag, Einwilligung) zulässig [11376]. Zur Problematik des Ausklammern von Löschung und Sperrung siehe oben. Das „Interesse des Betroffenen“ als zusätzliche Zulässigkeitsgrundlage einzuführen, würde den bekannten, problematischen Interpretationskunststücken Tür und Tor öffnen.
- Die Verknüpfung der Zulässigkeit der Verarbeitung mit dem Vorliegen eines nicht näher spezifizierten Datenschutzkonzepts [11376] ist wenig hilfreich. Es gibt keine allgemein akzeptierte Definition, welchen Inhalt und Umfang ein Datenschutzkonzept haben muss und die geforderte Dokumentation der Zugriffsrechte und Sicherheitsmaßnahmen ist weit weniger als nach heutiger Rechtslage im Verfahrensverzeichnis gemäß § 4g (2) BDSG vor Aufnahme einer Verarbeitung zu dokumentieren ist.
- Solange Betriebsräte kein Mitbestimmungsrecht bei der Bestellung des/der Datenschutzbeauftragten haben, ist es nicht akzeptabel, den Betriebsrat der Aufsicht des betrieblichen Datenschutzbeauftragten zu unterwerfen [11376], da dies die gesetzlich

garantierte Unabhängigkeit des Betriebsrats gefährdet (siehe hierzu auch BAG-Urteil 1 ABR 21/97).

- Ein Konzernprivileg zu konstatieren, gar ein europäisches [12670], geht hinter die Schutzregelungen des BDSG zurück, das aus gutem Grund ein solches Privileg ausdrücklich nicht vorsieht, da in heutigen Konzern- und Unternehmensstrukturen die Verflechtungen eine Grenzziehung (als Übermittlungsschranken) nicht mehr ermöglichen. Die Einführung eines Konzernprivilegs käme einem Dambruch gleich, der die unkontrollierbare Verteilung von Beschäftigtendaten zur Folge hätte.

Aus praktischer Sicht erscheinen einige der vorgeschlagenen Regelungen aufgrund der Gestaltung heutiger IT-Systeme weder umsetzbar noch hilfreich:

- Die Definition der Personalakteninhalte als „in unmittelbarem inneren Zusammenhang mit dem Beschäftigungsverhältnis stehend“ [12670] ist nebulös und wenig hilfreich. Auch Änderungsbelege in SAP (z. B. an der Hotline: wer hat wann welche Störungsmeldungen aufgenommen) erfüllen je nach Arbeitsaufgabe diese Definition – und sind doch alles andere als klassische Personalakteninhalte.  
Die geforderte technische und organisatorische Trennung bestimmter, besonders sensibler Beschäftigtendaten („Personalaktenqualität“) von weiteren Beschäftigtendaten [11376, 9311] erscheint realitätsfremd. Damit wäre kein SAP-System mehr legal zu betreiben, da derartige Systeme gerade so aufgebaut sind, dass zu einer Person unterschiedliche Datenklassen existieren, die jedoch immer an zentralen Stammdaten festgemacht werden. Aus Datenschutzsicht ist aber auch gar nicht entscheidend, dass die Datenklassen getrennt geführt werden (mit heutiger IT stellt eine Zusammenführung aus getrennten Systemen ohnehin kein Problem dar), sondern dass die Berechtigungssysteme feingranulare Einstellungen erlauben – und entsprechend dem „need-to-know“-Prinzip genutzt werden.
- Gesundheitsdaten unterfallen bereits heute den besonderen Daten gem. § 3 (9) BDSG. Eine Klarstellung erscheint insofern nicht erforderlich. Die Beschränkung der Verarbeitung von Gesundheitsdaten auf Personen, die der ärztlichen Schweigepflicht unterliegen [11376], würde es jedem Meister verunmöglichen, die Krankmeldungen seiner Schichtarbeiter zur Kenntnis zu nehmen.
- So sehr die Begrenzung des Einsatzes opto-elektronischer Geräte wünschenswert ist, so wenig kann man das Verbot der Verhaltensüberwachung generell durchhalten. Leitstände, sicherheitsrelevante Meldezentralen, Rechenzentren und anderer sind auf den Einsatz angewiesen – und zwar gerade zur Überwachung des Verhaltens. Eine fallunterscheidende Nutzungsbegrenzung ist daher zum Schutz der Betroffenen unbedingt erforderlich.
- Bei Zulässigkeit privater Nutzung die (nicht abdingbare!) Geltung des Fernmeldegeheimnisses und der entsprechenden TKG-Bestimmungen zu verlangen, würde bei jedem sicherheitsbewussten Unternehmen zu sofortigem Verbot privater Nutzung führen. Denn der sichere Betrieb einer IT-Infrastruktur in einem Unternehmen erfordert Schutzmechanismen, Protokollierungen und Sicherungskopien, die mit dem Fernmeldegeheimnis nicht vereinbar sind. Da andererseits auf der technischen Ebene private nicht von dienstlicher Nutzung zu unterscheiden ist, könnte eine private Nutzung nicht mehr toleriert werden. Unabhängig davon, dass dies auch mit Revisions- und

Überprüfungspflichten eines Unternehmens kollidiert, scheint dieser Vorschlag realitätsfern. Sinnvoller wäre stattdessen eine Klarstellung, dass ein Unternehmen gerade nicht als Telekommunikationsdiensteanbieter im Sinne des TKG gilt, dass aber für die transparente Gestaltung der Netzüberwachung und die betriebsöffentliche Dokumentation der Überwachungsmaßnahmen strenge, willkürverhindernde Vorschriften gelten.

#### 4. Erforderliches

Die folgenden Regelungsvorschläge sind, soweit sie aus den Anträgen stammen, im Sinne einer Konkretisierung des Arbeitnehmerdatenschutzes ausdrücklich zu begrüßen oder wären aus praktischer Sicht dringend erforderlich:

- Die Abkoppelung des Schutzes betroffener Beschäftigter von formalen Anstellungsverhältnissen und die Einbeziehung von Bewerber/innen, Leiharbeitnehmern, Freiberuflern etc. [9311, 11376]  
Zusätzlich sollten Beschäftigte von Fremdfirmen (z. B. Subunternehmer) für die Dauer ihres Arbeitseinsatzes bei einem Auftraggeber geschützt sein (z. B. bei der Fragestellung, ob man Beschäftigte von Fremdfirmen stärker durch Videoüberwachung kontrollieren darf als die eigenen Mitarbeiter/innen). Außerdem sind Auftragnehmer davor zu schützen, dem Auftraggeber eine direkte Kontrolle ihrer Beschäftigten zu gestatten (was z. B. in vielen Branchen von Automobilzulieferern bis zu Sachbearbeitungsbüros üblich ist).
- Das Verbot, alle gesetzlich garantierten Rechte Beschäftigter durch Rechtsgeschäft, also auch durch Betriebsvereinbarungen einzuschränken [11376]. Allerdings ist eindeutig zu spezifizieren, was eine zulässige „Verbesserung“ sein kann. Es sollte eindeutig geklärt werden, unter welchen Voraussetzungen eine Betriebsvereinbarung Zulässigkeitsgrundlage für eine automatisierte Verarbeitung sein kann (enger Bezug zur Erbringung der Arbeitsleistung, kein konkurrierendes Individualrecht etc.)
- Die Festschreibung von Mitbestimmungsrechten der Arbeitnehmervertretung für alle vom Arbeitnehmerdatenschutzgesetz erfassten Verarbeitungen. Die Festlegungen sollten sich an der Begrifflichkeit des BetrVG (mitbestimmen, beraten, vorschlagen) orientieren und keine neuen, unkonkreten Begriffe (z. B. abstimmen) einführen.
- Eine Konkretisierung und Ausgestaltung des Verfahrensverzeichnis gemäß § 4 d (2) BDSG derart, dass der Detaillierungsgrad für Arbeitnehmerdaten im Verzeichnis erhöht wird und das Verzeichnis mitbestimmungspflichtig wird.
- Die Verarbeitung und Nutzung von Beschäftigtendaten aus Protokolldateien (Serversysteme, Arbeitsplatzrechner) sollte der besonderen Zweckbindung gemäß § 31 BDSG unterfallen, nur dem ordnungsgemäßen Betrieb der Systeme dienen und ausschließlich den mit dem Betrieb direkt betrauten Personen zugänglich sein.
- Die Einrichtung einer paritätisch besetzten Schiedsstelle analog zur Einigungsstelle gem. BetrVG erscheint sinnvoll. Besetzung und Kostenträgerschaft sollten konkretisiert werden.

- Die Stärkung der Position betrieblicher Datenschutzbeauftragter ist zu begrüßen [11376]. Gleiches gilt für die Sanktionierung bei Nichtbestellung [9311] und bei fehlender Unterrichtung [12670]. Zusätzlich zu dem vorgeschlagenen Kündigungsschutz sollten verbindliche Mengengerüste bzgl. personeller und kapazitiver Unterstützung vorgesehen werden.
- Dem Betriebsrat sollte ein Mitbestimmungsrecht bei der Bestellung des betrieblichen Datenschutzbeauftragten eingeräumt werden [9311]. Die Voraussetzungen für eine Abberufung des Datenschutzbeauftragten sollten klar geregelt und in Fällen möglich sein, in denen der Datenschutzbeauftragte seine Aufgaben nicht ordnungsgemäß versieht.
- Konkrete Schutzvorschriften, insbesondere Verschlüsselungserfordernisse für bestimmte Arten von Daten (Online-Bewerbungen, Personalakten etc., Versand per E-Mail) [9311, 11376] sind erforderlich, da die Bereitschaft von Unternehmen, personenbezogene Daten in öffentlichen Netzen durch angemessene, sichere Verfahren vor unberechtigter Einsichtnahme zu schützen, generell zu schwach ausgeprägt ist.
- Eine Klarstellung, dass BDSG und BetrVG subsidiär neben einem Arbeitnehmerdatenschutzgesetz bestehen [12670], erscheint zur Klarstellung hilfreich. Es sollte außerdem klargestellt werden, wie das Verhältnis zu gesetzlichen oder sonstigen Normen zur IT-Sicherheit zu gestalten ist, die die Verarbeitung von Beschäftigtendaten verlangen (z. B. Forensische Analysen, Whistleblowing, EU-Sanktionslistenscanning, Sarbanes-Oxley Act u.s.w.).
- Die Einsatzmöglichkeiten von Videokameras im nicht-öffentlichen Betriebsbereich sollte, unabhängig von allen anderen sinnvollen Einschränkungen, nur zulässig sein, wenn im Herrschaftsbereich des AG (kein „Vermietervideo“).
- Die Rahmenbedingungen für Taschenkontrollen, Röntgenkontrollen sollten so konkretisiert werden, dass strenge Bedingungen formuliert und eine Aufzeichnung elektronischer Daten untersagt sind.
- Dem Arbeitgeber muss verboten sein, in den privaten Bereich der Beschäftigten einzudringen (z. B. durch Privatdetektive).
- Bewegungsdaten sollten einer strengen Zweckbindung und einer kurzen Löschfrist unterworfen werden (Location Based Services, GPRS, GSM u.ä. die für Flottenverwaltung, Dispositionssteuerung u.ä. verwendet werden.)
- Dem Betriebsrat sollte eine Mitbestimmung bei allen Löschfristen eingeräumt werden, die nicht gesetzlich geregelt sind.
- Die Gestaltungsanforderungen an Auftrags-DV-Verträge innerhalb von Konzernen (z. B. zur Erbringung von Personalbüro-Dienstleistungen) müssen konkretisiert werden, so dass notwendige Regelungsinhalte (Auftragsbeschreibung, Weisungsdurchsetzung, Kontrollrecht, Beschreibung der Schutzmaßnahmen etc.) ablesbar sind. Es sollte konkret geregelt werden, welche Verarbeitungen innerhalb eines Konzerns überhaupt als Auftrags-Datenverarbeitung gem. § 11 BDSG organisiert werden dürfen.

- Daten, die ein Betriebsarzt im Rahmen seiner rechtmäßigen Tätigkeit im Unternehmen über Beschäftigte erhebt (die also bis auf die Pflicht zur Mitteilung von arbeitsverhindernden Sachverhalten der Schweigepflicht unterliegen) dürfen nicht in Systemen des Arbeitgebers abgelegt werden, es sei denn, durch Verschlüsselung ist der alleinige Zugriff des Betriebsarztes sicher gestellt.
- Erlaubter Umfang und Zweck von Aufzeichnungen bei Rückkehrergesprächen gem. § 84 SGB IX sollten konkretisiert werden.
- Betriebsrat und Datenschutzbeauftragter sollten das ausdrückliche Recht erhalten, sich jederzeit, ohne dem Vorwurf der Illoyalität ausgesetzt zu sein, an die Aufsichtsbehörde zu wenden.

Karin Schuler, Datenschutz & IT-Sicherheit  
Kronprinzenstr. 76  
53173 Bonn

stv. Vorsitzende der Deutschen Vereinigung für Datenschutz e.V.  
Bonner Talweg 33-35  
53113 Bonn  
Tel. 0228/24 20 733,  
Fax. 0228/24 20 734,  
schuler@datenschutzverein.de