

Zehn Thesen zum Arbeitnehmerdatenschutz

Ein Positionspapier des Social and Labor Affairs Committee von AmCham Germany

Die Informationstechnik hat in der Arbeitswelt einen immensen Stellenwert. Ihre Bedeutung wird künftig noch zunehmen. Im Hinblick auf die Anonymität der elektronischen Datenverarbeitung und die mit ihr verbundenen umfangreichen Nutzungs- und Missbrauchsmöglichkeiten wird seit Langem eine gesetzliche Regelung des Arbeitnehmerdatenschutzes gefordert. Das Bundesministerium des Innern hat am 1. April 2010 ein Eckpunktepapier zum Beschäftigtendatenschutz vorgelegt. Ein Referentenentwurf wird derzeit innerhalb der Bundesregierung abgestimmt. Vor dem Hintergrund der bevorstehenden Gesetzesnovelle stellt AmCham Germany zehn Thesen zum Arbeitnehmerdatenschutz zur Diskussion und plädiert für eine Regelung, die den Bedürfnissen international operierender Unternehmen und ihren Arbeitnehmern gleichermaßen gerecht wird:

1) Die berechtigten Interessen multinationaler Unternehmen und ihrer Arbeitnehmer sind zu berücksichtigen.

Die Regelungen zum Arbeitnehmerdatenschutz haben einen sachgerechten Ausgleich zwischen dem Schutz des Persönlichkeitsrechts der Arbeitnehmer einerseits und den berechtigten Arbeitgeberinteressen andererseits zu finden. Dabei ist zu berücksichtigen, dass international operierende Unternehmen immer höheren Compliance-Anforderungen (z.B. den Standards der US-amerikanischen Börsenaufsicht SEC) genügen und zu diesem Zweck allgemeine Verhaltensregelungen (wie Codes of Conduct) sowie Kontroll- und Berichtssysteme (wie Ethics Hotlines) implementieren müssen. Internationale Konzerne haben zudem ein berechtigtes Interesse an einem effektiven, einheitlichen und wirtschaftlichen Personalmanagement, weil dies der Unternehmensgruppe und den dort beschäftigten Arbeitnehmern zugute kommt. Dabei sind ein konzern einheitliches Personalmanagement, zentrale Trainings- und Schulungsprogramme, Talent Management und ein konzerninterner Arbeitsmarkt wichtige Bestandteile, die nicht an überhöhten Datenschutzerfordernissen scheitern dürfen. Daher sollten die Neuregelungen zum Arbeitnehmerdatenschutz ein Konzernprivileg zumindest dann anerkennen, wenn datenschutzrechtliche Mindeststandards wie in der EU gewahrt sind, z.B. wenn innerhalb des Konzerns Datenschutzrichtlinien bzw. IT-Standards gelten, die von einer Datenschutzbehörde der EU oder eines Mitgliedsstaats genehmigt wurden, oder wenn die EU-Standardvertragsklauseln genutzt werden.

2) Das Harmonisierungsprinzip der EU-Datenschutzrichtlinie sollte beachtet werden.

Die neuen Regelungen zum Arbeitnehmerdatenschutz sollten nicht über den europäischen Schutzstandard hinausgehen. Insoweit ist zu beachten, dass die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) der Angleichung der Rechtsvorschriften in den Mitgliedstaaten dient, um Hemmnisse für die Wirtschaftstätigkeiten auf Gemeinschaftsebene sowie Wettbewerbsverfälschungen zu verhindern (vgl. Erwägungen (7) und (8) der Richtlinie).

Gerade für international agierende Unternehmen ist ein einheitlicher Schutzstandard innerhalb der EU im Hinblick auf die Voraussehbarkeit und Berechenbarkeit der rechtlichen Rahmenbedingungen von erheblicher Bedeutung.

3) Der Geltungsbereich der Regelungen zum Arbeitnehmerdatenschutz darf nicht ausufern, sondern ist in erster Linie auf elektronische Datenverarbeitung zu begrenzen.

Der Geltungsbereich der Regelungen zum Arbeitnehmerdatenschutz sollte im Einklang mit der EU-Datenschutzrichtlinie sowie mit § 1 Abs. 2 Nr. 3 BDSG stehen und sich in erster Linie auf die Erhebung, Verarbeitung und/oder Nutzung von Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien beschränken. Eine Regelung – wie im jüngst eingeführten § 32 Abs. 2 BDSG –, welche jegliche Handlung erfasst, die eine Erhebung, Nutzung oder Verarbeitung von Beschäftigtendaten darstellt, ist nicht sachgerecht. Danach müsste nahezu jede Handlung des täglichen (Geschäfts-)Lebens auf ihre datenschutzrechtliche Zulässigkeit überprüft werden ist, wie z.B. die Frage eines Vorgesetzten an einen Mitarbeiter, wo sich sein Kollege gerade aufhält, jegliche Kommunikation mit oder über einen Beschäftigten, das zufällige Mithören eines Gesprächs oder Telefonats eines Arbeitnehmers und sogar jedes bewusste oder unbewusste Beobachten eines Mitarbeiters durch den Vorgesetzten. Eine derartige Regelung geht viel zu weit und ist kaum praktikabel. Die Praxis benötigt einen klar definierten Anwendungsbereich. Dies gilt umso mehr, wenn mit der Unzulässigkeit von Datenerhebungen oder -verwendungen Strafen oder andere Sanktionen verbunden sind.

4) Unternehmen brauchen praxiserichte und verständliche Regelungen.

Die gesetzlichen Neuregelungen zum Arbeitnehmerdatenschutz sollten sich nicht auf die Wiedergabe zahlreicher unbestimmter Rechtsbegriffe (wie z.B. "erforderlich", "verhältnismäßig") beschränken, welche die vorzunehmende Interessenabwägung zwischen dem Persönlichkeitsrecht des Arbeitnehmers und den berechtigten Interessen des Arbeitgebers oder von Dritten offenlässt. Damit wäre für die Praxis keinerlei Gewinn an Rechtssicherheit und Rechtsklarheit verbunden. Notwendig wäre vielmehr, dass das Gesetz für bestimmte Fallkonstellationen (wie z.B. den Einsatz von Videoüberwachung, die Kontrolle der E-Mail- und Internet-Nutzung durch Arbeitnehmer) die Wertungsentscheidung selbst trifft oder bei Verwendung unbestimmter Rechtsbegriffe zumindest möglichst viele Regelbeispiele angibt, aus denen Wertungen für die gesetzlich nicht geregelten Fälle abgeleitet werden können.

Unter dem Gesichtspunkt der Compliance sind Arbeitgeber häufig verpflichtet, präventiv tätig zu werden. Die Unternehmensleitung oder der Compliance Officer darf nicht in die Situation geraten, dass sie bzw. er bei Beachtung der datenschutzrechtlichen Vorschriften sich andererseits einer Beihilfe durch Unterlassen zu im Unternehmen begangenen Straftaten strafbar macht, weil wirksame Kontrollen unterlassen wurden.

5) Es sollte eine verbindliche Anrufungsauskunft bei den Aufsichtsbehörden geschaffen werden.

Im Hinblick auf die mit unbestimmten Rechtsbegriffen verbundenen Wertungsfragen und der daraus folgenden Rechtsunsicherheit für die Unternehmenspraxis sollte für Arbeitgeber die Möglichkeit einer schnellen, verbindlichen Voranfrage bei den Datenschutzbehörden – ähnlich der Anrufungsauskunft bei den Finanzämtern – geschaffen werden.

6) Die Betriebsvereinbarung als Rechtsgrundlage für die Erhebung und Verwendung von Arbeitnehmerdaten zu mit dem Arbeitsverhältnis verbundenen Zwecken ist von großer praktischer Bedeutung.

Die Möglichkeit für die Betriebsparteien, mit dem Abschluss einer Betriebsvereinbarung eine "andere Rechtsvorschrift" im Sinne des § 4 Abs. 1 BDSG und damit eine Rechtsgrundlage für die Erhebung, Verarbeitung und/oder Nutzung von Arbeitnehmerdaten zu schaffen, ist für die Praxis von erheblicher Bedeutung. Diese Möglichkeit muss aufrechterhalten werden. Arbeitgeber und Betriebsrat (bzw. Gesamt- oder Konzernbetriebsrat) sind in der Lage, entsprechend dem Gebot vertrauensvoller Zusammenarbeit (§ 1 Abs. 2 BetrVG) die berechtigten Interessen des Arbeitgebers und das Persönlichkeitsrecht des Arbeitnehmers (§ 75 Abs. 2 BetrVG) unter Berücksichtigung der besonderen Situation des Betriebs, Unternehmens bzw. Konzerns zu einem sachgerechten Ausgleich zu bringen.

7) Das Verhältnis Betriebsrat – Datenschutzbeauftragter sollte stimmig geregelt werden.

Der Datenschutzbeauftragte ist ein unabhängiger (interner oder externer) Sachverständiger, der den Arbeitgeber und Betriebsrat bei der Einhaltung der datenschutzrechtlichen Vorschriften beraten kann und soll. Ein Betriebsratsmitglied kann wegen der Gefahr von Interessenskonflikten nicht gleichzeitig Datenschutzbeauftragter sein. Der Betriebsrat sollte nicht die Rolle eines Ersatzdatenschutzbeauftragten wahrnehmen, sondern sich der Sachkunde des Datenschutzbeauftragten bedienen. Insoweit ist zu erwägen, bei den datenschutzrechtlich relevanten Mitbestimmungsrechten (wie z.B. § 87 Abs. 1 Nr. 6, § 94 BetrVG) den Datenschutzbeauftragten zum obligatorischen, nicht stimmberechtigten Mitglied einer Einigungsstelle zu machen. Dies würde auch der Beschleunigung der betrieblichen Mitbestimmung dienen, was gerade bei Sachverhalten, in denen sich IT- und Datenschutzfragen stellen, sachgerecht wäre, weil diese in der Praxis oft eilbedürftig sind.

Abzulehnen sind daher Forderungen nach einem gesonderten Beauftragten für Arbeitnehmerdatenschutz neben dem betrieblichen Datenschutzbeauftragten, der in Abstimmung mit dem Betriebsrat bestellt und abberufen wird. Dies führt in der Praxis zu unlösbaren Kompetenzkonflikten.

8) Die freiwillige Einwilligung des Arbeitnehmers als Rechtsgrundlage für eine Erhebung, Verarbeitung und/oder Nutzung von Arbeitnehmerdaten ist unabdingbar.

Jeder Arbeitnehmer sollte selbst über seine Datenlage entscheiden können. Auch im Arbeitsverhältnis und bei dessen Anbahnung kann eine wirksame freiwillige Einwilligung erteilt werden. Arbeitnehmer sind durch das geltende Arbeitsrecht (wie z.B. das Kündigungsschutzgesetz und die AGB-Kontrolle vorformulierter Regelungen gemäß §§ 305 ff. BGB) so umfangreich geschützt, dass nicht generell davon ausgegangen werden kann, sie könnten keine wirksame Einwilligung erklären, die auf ihrer "freien Entscheidung" (vgl. § 4a Abs. 1 Satz 1 BDSG) beruht. Andernfalls würde man die betroffenen Arbeitnehmer entmündigen. Möchte man den Grundsatz der Freiwilligkeit der Einwilligung stärken, kommt die gesetzliche Regelung eines Koppelungsverbots in Betracht (vgl. auch § 28 Abs. 3b BDSG, § 95 Abs. 5 TKG). Z.B. könnte man die Einwilligung mangels Freiwilligkeit für unwirksam erklären, wenn der Arbeitgeber die Einwilligung an den Arbeitsvertragsabschluss oder eine sonstige Begünstigung koppelt. Ferner sollte gesetzlich klargestellt werden, ob und inwieweit § 94 BetrVG für formularmäßige Einwilligungen in die Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten gilt.

9) Arbeitgeber sind keine IT-Diensteanbieter. Eine sachgerechte Kontrolle der E-Mail- und Internet-Nutzung muss dem Arbeitgeber stets möglich sein.

Die Qualifizierung der Arbeitgeber als Diensteanbieter im Sinne des § 3 Nr. 6 und 24 TKG bzw. § 2 Satz 1 Nr. 1 TMG für den Fall, dass die private Nutzung von E-Mail und Internet durch die Arbeitnehmer zugelassen oder wissentlich geduldet wird, ist nicht sinnvoll. Der Arbeitgeber muss in der Lage sein, einerseits dem Nutzungsinteresse der Arbeitnehmer entgegenzukommen und andererseits eine Missbrauchskontrolle durchführen zu können. Im IT-System des Arbeitgebers gespeicherte E-Mails müssen für den Arbeitgeber wie Geschäftspost einsehbar sein, falls sie nicht erkennbar ausschließlich die Privatsphäre des Arbeitnehmers betreffen. Dies um so mehr, als es der Arbeitnehmer selbst in der Hand hat, zu entscheiden, ob nach Abschluss des Übertragungsvorgangs eine private E-Mail im IT-System des Arbeitgebers gespeichert bleibt oder nicht. Eine Regelung in Deutschland, die dazu führt, dass jedem Arbeitgeber nur geraten werden kann, die private Nutzung von E-Mail und Internet zu verbieten, ist insbesondere nicht im Interesse der Arbeitnehmer.

10) Die Regelungen zum Arbeitnehmerdatenschutz sollten systematisch stimmig sein.

Die neuen Regelungen zum Arbeitnehmerdatenschutz sollten in sich stimmig sein und sich in die Systematik zum übrigen Arbeitsrecht einfügen. Insoweit ist am Begriff des "Arbeitnehmers" und nicht des "Beschäftigten" (vgl. § 3 Abs. 11 BDSG n.F.) festzuhalten. Wird das Fragerecht des Arbeitgebers gesetzlich normiert, sollte das Verhältnis zwischen der Zulässigkeit der Datenerhebung und den Benachteiligungsverboten nach dem AGG eindeutig geregelt werden.

**American Chamber of Commerce in Germany e.V.
(AmCham Germany)**

Mit etwa 3.000 Mitgliedern ist AmCham Germany die größte bilaterale Wirtschaftsvereinigung in Europa. Die in ihr organisierten Unternehmen repräsentieren circa 130 Milliarden Euro Investment und 800.000 direkte Arbeitsplätze. Die Kammer versteht sich als Kommunikationsbrücke zu Investoren in den Vereinigten Staaten. Im Vordergrund ihrer Tätigkeit steht die Förderung der deutsch-amerikanischen Wirtschaftsbeziehungen und des Wirtschaftsstandorts Deutschland.

Chair Social and Labor Affairs Committee

Gert Schröder
Director, Labour Relations
United Parcel Service Deutschland Inc. & Co. OHG

Co-Chair Social and Labor Affairs Committee

Caroline Bitsch
Partner
JUSTEM Rechtsanwälte

AmCham Staff Contact

Eva Funhoff
Specialist, Government & Press Relations
American Chamber of Commerce in Germany e.V.
Börsenplatz 7-11
60313 Frankfurt am Main
T +49 69 92 91 04-41
F +49 69 92 91 04-11
E efunhoff@amcham.de