




Datenschutz und Arbeitnehmer

SAP – Fachtagung 2008 vom 13.-15. Februar 2008
SAP im betrieblichen Spannungsfeld

Tanja Jost
beim Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Übersicht

- 
1. Einleitung
 2. Gefahren für die Persönlichkeitsrechte der Beschäftigten am einzelnen Arbeitsplatz
 3. Personaldatenflüsse in Konzernen – national und international
 4. Regelungen zum Arbeitnehmerdatenschutz

Auf dem Weg zum gläsernen Mitarbeiter?

- Gesundheitsdaten im Arbeitsleben
- Internet- und E-Mail-Nutzung am Arbeitsplatz
- Videoüberwachung am Arbeitsplatz
- Chipausweise im Arbeitsalltag
- Biometrie am Arbeitsplatz

- Gesundheitsdaten sind besondere Arten von personenbezogenen Daten und unterliegen einem speziellen Schutz
- Neue Diagnosemöglichkeiten und einfachere molekulargenetische Untersuchungsmethoden führen zu Begehrlichkeiten bei Arbeitgebern
- Der Arbeitgeber darf bei Einstellungen keine genetischen Untersuchungen verlangen oder nach genetischen Dispositionen fragen

Internet- und E-Mail-Nutzung am Arbeitsplatz

- Durch Internet- und E-Mail-Nutzung entstehen zahlreiche Datenspuren - auch beim Arbeitgeber
- Selbst bei rein dienstlicher Nutzung ist eine lückenlose Überwachung unzulässig, nur Stichproben sind erlaubt
- Private Nutzung von Internet und E-Mail kann an bestimmte Bedingungen geknüpft werden. Regelungen sollten in Betriebs- bzw. Dienstvereinbarungen verbindlich festgelegt werden
- Protokollierung ist nur für bestimmte Zwecke zulässig



Videoüberwachung am Arbeitsplatz

- Videoüberwachung in Arbeitsbereichen führt oft beiläufig oder zielgerichtet zu einer Mitarbeiterkontrolle
- Zentraler Wertungsmaßstab bei der Beurteilung der Zulässigkeit einer Videoüberwachung ist immer die Verhältnismäßigkeit – d.h. sie muss erforderlich sein und Mittel-Zweck-Relation muss eingehalten sein
- Videoüberwachung von öffentlich zugänglichen Räumen, d.h. Räumen mit Publikumsverkehr, richtet sich nach § 6b BDSG:
 - Wenn Videoüberwachung aus Sicherheitsinteressen zulässig, muss sie als arbeitsplatzimmanent hingenommen werden



Videüberwachung am Arbeitsplatz

- wenn Mitarbeiter nicht eigentlicher Beobachtungsgegenstand sind, keine Auswertung zum Zwecke einer Leistungs- und Verhaltenskontrolle
- Zwecke der Videüberwachung müssen im Vorhinein festgelegt und in einem Verfahrensverzeichnis jedem Interessierten offen gelegt werden
- Videüberwachung von Arbeitsstätten ohne Publikumsverkehr richtet sich nach § 28 BDSG: Zulässigkeit nur bei besonderen Sicherheitsinteressen des Arbeitgebers:
 - Diebstahlschutz bei konkretem Verdacht
 - Transparentes Verfahren, Mitbestimmung Personalrat
 - Verwertungsverbot bei rechtswidriger Videüberwachung

- Einsatz im Rahmen der Zeiterfassung und Zutrittsregelung
 - Gefahr der Bildung von betriebsinternen Bewegungsprofilen
- Einsatz als Zahlungsmittel in der Kantine, bei Serviceeinrichtungen und beim Zugang zum PC
 - Gefahr der Bildung von Konsum-, Interessen- und Tätigkeitsprofilen
- Grundsätzlich zulässig, aber keine zweckfremde Nutzung erlaubt
- In Betriebs-/Dienstvereinbarungen sollten möglichst dezentrale Speicherung der Daten festgelegt und detaillierte Zugriffskonzepte geregelt werden

- Fingerabdruck-, Iris-, Stimm- oder Gesichtserkennung werden in den gleichen Bereichen verwendet wie Chipausweise
- Größere Gefahr der Profilbildung, weil lebenslange Bindung der biometrischen Merkmale an eine bestimmte Person
 - Daher möglichst keine Speicherung biometrischer Merkmale in einer Datenbank, sondern nur auf dem Chip
- Verknüpfung von Biometrie und Videoüberwachung kann zu einer Totalüberwachung führen
- Auch hier: Detaillierte Festlegung von Rechten und Pflichten in Betriebs-/Dienstvereinbarungen

Personaldatenflüsse in Konzernen – national und international

Übersicht:

- **Problem:**
Intensiver Austausch von Mitarbeiterdaten zwischen Mutterkonzern und Tochterunternehmen
- **Datenschutzrechtliche Beurteilung:**
Datenschutzrecht kennt kein Konzernprivileg, es handelt sich um eine Datenübermittlung an „Dritte“ gemäß den Bestimmungen des BDSG
- Regelung durch Betriebsvereinbarung möglich
- Sonderregelung bei Vorliegen einer Auftragsdatenverarbeitung
- Regelungen bei international agierenden Unternehmen

- Voraussetzungen für die Datenübermittlung nach dem BDSG:
 - Einwilligung der Mitarbeiter (§ 4 Abs. 1 BDSG)
oder
 - Datenübermittlung dient der Zweckbestimmung des Vertragsverhältnisses (§ 28 Abs. 1 S. 1 Nr. 1 BDSG)
oder
 - Datenübermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle (§ 28 Abs. 1 S. 1 Nr. 2 BDSG)
- Regelung durch Betriebsvereinbarung kann Erlaubnisnorm nach BDSG ersetzen



Personaldatenfluss im Rahmen einer Auftragsdatenverarbeitung

- Keine Datenübermittlung an „Dritte“, wenn es sich bei dem Personaldatenfluss um Auftragsdatenverarbeitung handelt
- Bei Auftragsdatenverarbeitung wird einem „Dritten“ als Auftragnehmer die technische Abwicklung übertragen, während die inhaltliche Verantwortung beim Auftraggeber verbleibt
- Probleme im Verhältnis zwischen Mutterkonzern und Tochterunternehmen, wenn Tochterunternehmen der Auftraggeber ist (z.B. zentrale Personalverwaltung)
 - Datenschutzkontrolle der Tochter beim Mutterkonzern
 - Kontrollrechte der Mitarbeitervertretung

Personaldatenfluss im Rahmen von Personalinformationssystemen

Beispiel: Skill-Datenbanken

- Personaldaten werden heute überwiegend in Personalinformationssystemen verwaltet
- Skill-Datenbanken enthalten hochsensible Daten und können zum gläsernen Mitarbeiter führen
- Anzustreben ist der verstärkte Einsatz von Systemen, die auf freiwilliger Teilnahme der Mitarbeiter basieren

Personaldatenfluss bei international agierenden Unternehmen

- Auch im internationalen Bereich gibt es kein Konzernprivileg
- Datenübermittlungen innerhalb des Europäischen Binnenmarktes nicht problematisch, da das Datenschutzniveau innerhalb der Mitgliedstaaten vergleichbar ist (§ 4b Abs. 1 BDSG)
- Datenübermittlungen an einen Drittstaat richten sich nach § 4b Abs. 2 BDSG:
Prüfung, ob dort ein angemessenes Datenschutzniveau gewährleistet ist

Personaldatenfluss bei international agierenden Unternehmen

- Wenn kein angemessenes Schutzniveau im Drittstaat vorliegt, sind Datenübermittlungen nur zulässig bei:
 - Einwilligung der Betroffenen
 - unveränderter Verwendung von Standardvertragsklauseln, die von der EU-Kommission anerkannt wurden
 - Ausnahmegenehmigung durch Datenschutzaufsichtsbehörde, wenn ausreichende Garantien zugunsten der Betroffenen vorliegen in Form von:

Vertragsklauseln oder verbindlichen Unternehmensregelungen
(s. hierzu Arbeitspapiere der Art.29 Gruppe – abrufbar auf der
Homepage der EU-Kommission

http://ec.europa.eu/justice_home/fsj/privacy/index_de.html

- „Safe Harbour“- Regelung mit den USA

- Keine speziellen gesetzlichen Regelungen vorhanden
- Lösung über Einwilligung problematisch, da keine Freiwilligkeit im Verhältnis zum Arbeitgeber
- Gewährleistung des Persönlichkeitsrechts durch Betriebs-/Dienstvereinbarungen
- Auch keine europäische Lösung in Sicht



Vielen Dank für Ihre Aufmerksamkeit!

Tanja Jost

**beim Bundesbeauftragten
für den Datenschutz und
die Informationsfreiheit
Husarenstr. 30
D-53117 Bonn**

Tel: 0228 - 81995313

E-Mail: Tanja.Jost@bfdi.bund.de

