Der Gesetzentwurf zum Beschäftigtendatenschutz aus Sicht des BITKOM

Erfurt, 31. Mai 2011

Übersicht

I. Anforderungen an den Beschäftigtendatenschutz

II. Änderungsbedarf bei einzelnen Regelungen

III. Fazit

I. Anforderungen an den Beschäftigtendatenschutz

- Fairer Ausgleich zwischen Arbeitgeber und Beschäftigteninteressen
- Beschäftigten sollen vor unberechtigten Eingriffe in ihre Persönlichkeitssphäre geschützt sein und ihre Rechte anhand klarer Regeln erkennen können.
- Moderne Arbeitsprozesse ohne bürokratische Hürden – für Arbeitgeber wie Beschäftigte
- Berücksichtigung unterschiedlicher Arbeits- und Abhängigkeitsverhältnisse
- Keine Widersprüche zu anderen gesetzlichen Verpflichtungen von Unternehmen.

II. Änderungsbedarf

1. Direkterhebung im Beschäftigungsverhältnis
2. Einwilligung
3. Private Nutzung von Telekommunikationsdiensten
4. Soziale Netzwerke
5. Gesellschaftsübergreifende Datenweitergabe
6. Vereinbarkeit mit Compliance-Vorschriften
7. Übergangsfrist
8. Verhältnis Datenschutzbeauftragter - Betriebsrat

1. Direkterhebungsgrundsatz (innerhalb eines bestehenden Beschäftigungsverhältnisses)

- Direkterhebungsgrundsatz soll auch im Rahmen eines bestehenden Beschäftigungsverhältnisses gelten.

  =>personenbezogene Daten zur Durchführung des Beschäftigungsverhältnisse nur direkt beim Beschäftigten einholen.

- Das ist angesichts der Vielzahl von Bezügen, in denen der Beschäftigte in seinem Arbeitsverhältnis steht, oft nicht praktikabel und auch für den Beschäftigten nicht vorteilhaft.

1. Direkterhebungsgrundsatz

- So ist es Beschäftigten schwer zu vermitteln, dass sie Daten, die bereits bei einem Unternehmensteil vorliegen, an andere Teile jeweils wieder neu weitergeben müssen. **Beispiel:** Kontonummer liegt bei Lohnbuchhaltung vor, muss aber für Reisekostenabrechnung an anderer Stelle wieder neu hinterlegt werden.

- **Beispiel:** Für eine frei werdende Stelle innerhalb eines Konzernunternehmens wird nach einem qualifizierten Nachfolger gesucht – in Frage kommende Bewerber werden zunächst ohne ihr Wissen genannt, um spätere Enttäuschung oder Konkurrenzverhalten zu verhindern. Das ginge nach der vorgesehenen Regelung nicht.

2. Einwilligung § 32l

- Problem für die Zukunft:

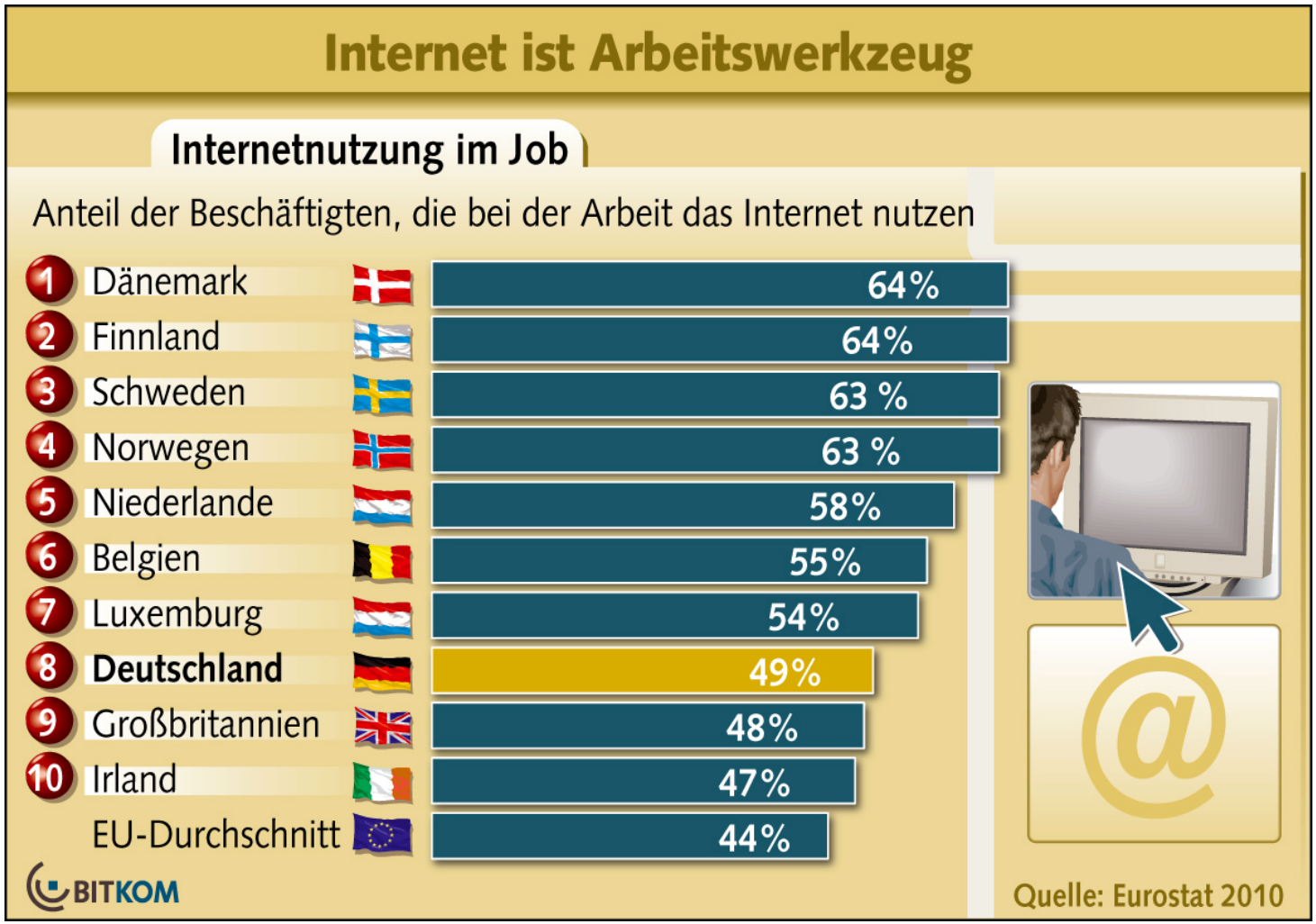
  Es ist nicht vorhersehbar, was für Fälle in Zukunft auftreten könnten, bei denen der Arbeitgeber Daten des Beschäftigten benötigt

- Problematisch schon jetzt:

  Datenerhebungen für vorteilhafte freiwillige Leistungen für den Beschäftigten, z.B. Gesundheitsförderungsprogramme oder Beteiligungsprogramme

  - Beispiel: Aktienprogramm eines Unternehmens für Mitarbeiter

Internetnutzung im Job



3. Nutzung von Telekommunikationsdiensten

- Regelung für die private Nutzung von Telekommunikationsdiensten fehlt – geregelt sind nur die Befugnisse des Arbeitgebers bei rein dienstlicher Nutzung.
- Viele Arbeitgeber werden die private Nutzung des Email-Accounts komplett verbieten, wenn die Einwilligung in die (beschränkte) Untersuchung von Telekommunikationsvorgängen nicht mehr zulässig ist.
- Durch beschränkte Einwilligungsmöglichkeit ist auch Einwilligung in die Erhebung von Verkehrs- und Inhaltsdaten im Rahmen von Telekommunikationsvorgängen (wie vom BfDI empfohlen) nicht mehr zulässig.

3. Telekommunikationsdienste

- § 32i sollte außerdem regeln, dass der Arbeitgeber bei Urlaub und Krankheit oder nach Beendigung des Arbeitsverhältnisses auf Telekommunikationsdaten und Telemediendaten zugreifen kann, sofern dies aus betrieblichen Gründen notwendig erscheint.
- Oft ist es notwendig Status von Tätigkeiten des Mitarbeiters zu klären, um ggf. dringende Aufgaben durch andere Mitarbeiter bearbeiten zu lassen.

4. Informationen über Bewerber aus sozialen Netzwerken

- Nicht von statischem Verständnis sozialer Netzwerke ausgehen!
- Abgrenzung zwischen Netzwerken, die *„zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind*“, und solchen, die „*der elektronischen Kommunikation dienen“*, schwierig. **Beispiel:** Facebook wird zunehmend auch beruflich genutzt.
- Auf **„allgemeine Zugänglichkeit“** abstellen. Begriff „soziale Netzwerke“ ist zu eng und auch ein Stück weit willkürlich – das Gleiche könnte auch für Blogs und abgeschlossene Foren gelten.
- Transparenz und Einhaltung der Nutzungsbedingungen des sozialen Netzwerkes sicherstellen.

§ 32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses

Regierungsentwurf:

(6) ... **Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind**. …

(7) Die Datenerhebung ist nur zulässig, wenn Art und Ausmaß im Hinblick auf den Zweck verhältnismäßig sind.

BITKOM-Vorschlag:

(6) **…Die schutzwürdigen Interessen des Beschäftigten überwiegen in der Regel auch, wenn der Arbeitgeber die Daten als Nutzer eines sozialen Netzwerks unter Nichteinhaltung der mit ihm vereinbarten Nutzungsbestimmungen erhebt oder er bei der Erhebung von Daten anderer Nutzer seine berufliche Zielsetzung nicht erkennbar macht….**

4. Soziale Netzwerke

Ohnehin gelten für diese Fallgestaltungen ja auch

- die Hinweispflicht des Arbeitgebers auf die Erhebung personenbezogener Daten aus allgemein zugänglichen Quellen,
- die Beschränkung dieser Erhebung (Absatz 1) auf personenbezogene Daten, deren Kenntnis zur Eignungsfeststellung erforderlich ist,
- die Sonderregelungen für besonders sensible Daten und Bereiche in den Absätzen 2 bis 5,
- die notwendige Abwägung zwischen schutzwürdigen Belangen des Beschäftigten und des Arbeitgebers (Absatz 6 Satz 2),
- das Erfordernis der Verhältnismäßigkeit nach Art und Zweck,
- die Auskunftsrechte des Beschäftigten gegenüber dem Arbeitgeber nach § 34 BDSG.

5. Regelung zur gesellschaftsübergreifenden Weitergabe von Beschäftigtendaten

- Organisationsstrukturen in Konzernen oder auch kleineren Unternehmensgruppen sind zunehmend gesellschaftsübergreifend ausgestaltet.
- Innerhalb von Matrixstrukturen sind Beschäftigte oft Vorgesetzten unterstellt, die nicht Beschäftigte derselben Gesellschaft sind.
- Das deutsche Datenschutzrecht erkennt das arbeitsteilige Zusammenwirken und dessen wirtschaftliche Einheit nicht an.
- Klare Regelung besser als heutiger unklarer Zustand – Betriebsvereinbarungen sind nicht für alles eine Lösung

6. Kompatibilität mit Compliance-Verpflichtungen

- Compliance = Einhaltung von Gesetzen und Pflichten im Unternehmen
- Beispiele für solche Gesetze und Pflichten im Rahmen einer ordnungsgemäßen Unternehmensführung sind :
  - Deutscher Corporate Governance Kodex
  - Kontrollpflichten zur Terrorbekämpfung
  - Kontrollpflichten aus Aktien- und GmbH-Gesetz
  - Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland (IDW)

6. Kompatibilität mit Compliance-Vorschriften

- Ziel vieler Vorschriften:
  Verhinderung u. ggf. Aufdeckung von Korruption und Betrug im Unternehmen (z.B. § 91 Abs.2 AktG).
- Umsetzung: üblicherweise stichprobenartige, verdachtsunabhängige Kontrollen oder automatisierte Abgleiche
- Die Vorschrift § 32d Abs. 3 sollte nicht nur die **Aufklärung von begangenen** Straftaten/anderen schwerwiegenden Pflichtverletzungen, sondern auch die „**Verhinderung** weiterer Straftaten oder schwerwiegender Pflichtverletzungen“ umfassen. Ansonsten sind präventive Maßnahmen nicht zulässig.
- In § 32 c Abs. 1 Satz 2 Nr. 1 sollten Kontroll- und Prüfpflichten mit aufgenommen werden.

6. Kompatibilität mit Compliance-Vorschriften

- Verdeckte Erhebung von Daten nach § 32 e Abs. 2 Nr. 1 nur beim Vorliegen von Tatsachen, die Verdacht auf Straftat o. schwerwiegende Pflichtverletzung begründen, die zu Kündigung aus wichtigem Grund berechtigen würden.
- Erschwert v.a. Präventivmaßnahmen, weil für diesen Fall bereits große Wahrscheinlichkeit für die Begehung der Straftat oder Pflichtverletzung gegeben sein muss. Dann geht es meist nur noch um Überführung.
- Verdeckte Datenerhebung als Präventivmaßnahme ist damit praktisch ausgeschlossen.

7. Übergangsfrist

- 6 Monate sind zu knapp.
- Übergangsfrist von mindestens 1 Jahr vorsehen.
- Prozesse müssen umgestellt werden.
- Nicht nur die jetzt gerade vorgestellten Punkte sind ja geändert, sondern auch einige weitere, die ebenfalls eine Umstellung von Prozessen nach sich ziehen.

8. Verhältnis Datenschutzbeauftragter - Betriebsrat

- Betriebsrat ist Teil der verantwortlichen Stelle ist => fällt in Regelungsbereich des BDSG. Datenverarbeitung hat auch im Betriebsrat stark zugenommen.
- Aufgrund seiner besonderen Stellung ist Kontrolle durch den Datenschutzbeauftragten nicht ohne weiteres möglich.
- Zuständigkeiten und Verantwortungsbereiche klar im Gesetz festlegen.
- Die arbeitsgerichtliche Rechtsprechung, dass der Datenschutzbeauftragte wegen der Unabhängigkeit des Betriebsrates nicht berechtigt ist, dessen Umgang mit personenbezogenen Daten zu kontrollieren, ist problematisch.

8. Verhältnis DSB - Betriebsrat

- **BITKOM-Vorschlag:** Einführung einer Geheimhaltungspflicht des betrieblichen Datenschutzbeauftragten und gesonderte Berichtswege für diesen Bereich.
- **Vorschlag des Bundesrates:** Möglichkeit eines eigenen Beauftragten für den Datenschutz innerhalb des Betriebsrates
  - könnte in der Praxis zu Kompetenzkonflikten führen.
  - Im Sinne eines durchgängigen Datenschutzkonzepts sollte die Kontrolle einheitlich erfolgen.

Fazit

- Noch einige Änderungen für mehr Praxistauglichkeit erforderlich.
- Keine Orientierung an „Skandalen“, sondern an der Arbeitswirklichkeit – in all ihren Facetten.
- Praxistauglichkeit ist essentiell damit Vorschriften auch eingehalten werden (können).
- Gesetzgeber muss die unterschiedlichen gesetzlichen Vorgaben für Unternehmen „harmonisieren“.

Vielen Dank für Ihre Aufmerksamkeit!

Susanne Dehmel
s.dehmel@bitkom.org

BITKOM - Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10 A, 10117 Berlin-Mitte
Internet: www.bitkom.org