Westfälische
Wilhelms-Universität
Münster

Privacy protection in the workplace in Germany

PAW Conference, Pécs, April 2-3, 2012

WWU Münster

Dr. Pascal Schumacher

Institute for Information, Telecommunications and Media Law (ITM)

Agenda

I. Introduction

II. General overview on data protection law in Germany

III. Specifics on privacy in the workplace

IV. What's next: 2010-draft bill

Recent data protection scandals in German companies

General overview on data protection law in Germany

Laws

- Constitution: “right to information self-determination”
- Federal Laws: Data Protection Act, Telecommunications Act, Telemedia Act, Social Securities Code, etc.
- States (Länder): 16 Data Protection Acts

Basic system of Data Protection

- General rule: processing of personnel data is generally prohibited, unless it is exceptionally allowed
- Permissions:
  - Free individual consent
  - Legal provisions

Institutional control mechanisms

- Individual self-protection; inhouse supervision; external supervising agencies (Data Protection Commissioner)

- **Data Protection Officer** ("DPO")
  - Reports directly to the CEO; must be allowed to carry out his function free of interference; may not be penalized for his actions; and can only be fired in exceptional circumstances
  - Task: ensure compliance with data protection-relevant legal provisions
  - Technical and legal knowledge and reliability; no conflict of interests within the company
  - Problem: no provisions for "Group DPO" that oversees a group of companies

Specifics on privacy in the workplace

Explicit free consent (more and more questioned)

Legal permissions, especially Sec. 32 DPA:

(1) An employee's personal data may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be collected, processed or used to investigate crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime, and the employee does not have an overriding legitimate interest in ruling out the possibility of collection, processing or use, and in particular the type and extent are not disproportionate to the reason.

(2) ...

Specifics on privacy in the workplace

"Employees" (Sec. 3 XI No. 7 DPA)

- regular employees,
- trainees,
- persons participating in labor market rehabilitation measures,
- persons employed under the Youth Volunteer Service Act,
- persons comparable to employees due to their economic dependence, including home-based workers and those of similar status,
- applicants for employment and those whose employment has ended
- ...

Basic rule: collection and use of data needs to be **necessary and proportionate**

Application process

Health data

- more strict than for any other personal information
- relevance for the respective concrete workplace
- questions about pregnancy: right-to-lie

Data published on the internet

- general principles apply: information “generally accessible”?
- internet search engines
- social networks? Networks “designed to convey professional information” vs. “private networks”?

During the employment

Admissible data

- Information on gender, marital status, education, training, qualification and language skills, sickness and absence

Flow of personnel data in corporate groups

- No privileges for inter-company relationships
- Consent
- Purpose of the contractual relationship (Sec. 28 I 1 no. 1 DPA)
- Justified interests of the controller (Sec. 28 I 1 no. 2)

Regulation by a works agreement

- Corporate group agreements, collective agreements or works agreements
- No undercutting of the level of protection guaranteed by DPA

Problematic issues

Biometrics and chip identity cards in every day working life

- use and connection for other purposes than the business-related ones is not admissible; decentralized storage

Internet and e-mails at the workplace

- automated complete monitoring not permissible
- random and contemporary analysis of the log data is legal
- use for private purposes: conditions as to the time frame, the allowed areas and controls are legal

Video surveillance

- publicly accessible areas vs. not publicly accessible areas
- central yardstick: proportionality

What's next: 2010-draft bill

- Restriction of consent in employment contexts
- Data protection officer
- Impact on compliance measures and internal investigations
- Collection of data published on the internet
- Monitoring of emails
- Video surveillance
- Collective agreements as additional legal basis for data transfers

Thanks for your attention!

Institute for

Information, Telecommunications and Media Law (ITM)

at the University of Münster, Faculty of Law

Dr. Pascal Schumacher

Leonardo-Campus 9
D-48149 Münster

Tel: +(49) 251 – 83 386 50
Fax: +(49) 251 – 83 386 44

E-Mail: schumacher@uni-muenster.de

http://www.itm.uni-muenster.de