BYOD Privacy and Security in Europe

LORENZ | International Lawyers

BYOD: Overview

BYOD Overview

- 38% of companies expect to stop providing electronic devices to their employees by 2016 (1)

- According to a 2013 survey conducted by Cisco, approximately 90% of all workers say they use their own personal smartphones, tablets or laptops in some work-related capacity, whether the practice is officially endorsed by their employers or not

(1) Wills, D. A. (2013, April 11). Bring your own device: The facts and the future. Gartner Research. Retrieved from http://www.gartner.com/DisplayDocument?id=2422315&ref=clientFriendlyUrl.

Europe v. the Rest of the World (I)

- BYOD is less popular in Europe than in the U.S.
  - European companies v. US companies having BYOD policy: 36% v. 68%
- BYOD is not significantly growing in Europe
  - 2013 v. 2014: 10% more companies have BYOD policy but equal amount (ci. 40%) is not planning to implement one in the near future
- BYOD is less popular in Europe than in the rest of the world
  - Average number of employees using own device in Asia: 78%

Europe v. Rest of the World (II)

BYOD is less popular in Europe:

- Culture
  - General expectation that employer provides tools to perform job;
  - Employees are more sensitive about limitations of their privacy and allowing space for data management software on personal devices
- Legal hurdles
  - Stricter rules on data protection and privacy result in more concerns and challenges for European enterprises when implementing BYOD.

Relevant Legislation: EU

- Privacy and Data Protection Regulation
  - Article 8 ECHR and national constitutions of EU member states
  - Data Protection Directive 95/46 and national laws implementing it
- Labor law
- Telecommunications regulations
  - E-privacy directive 2002/58 as amended and national implementing acts
  - Right to secrecy of telecommunication in Article 8 ECHR, national Constitution and/or national Telecom Acts
- Information security laws and standards

BYOD: Main Business Challenges

Liability: EU

Liability linked to data controller capacity:

- BYOD: employer is the data controller
- Non-compliance may result in:
  - Damages; and
  - Sanctions.
- Employer responsibilities versus employee rights

Data Security: EU

Importance:

- Data security is amongst the principal obligations of the management board of companies due to value of data

- No specific laws and regulations specifically dealing with BYOD information security – "adequate" technical measures
  - State-of-the-art
  - Sensitive nature of data
  - Measures should be in line with potential risks

- Data breach notification

Data Protection Compliance: EU

- Employer is responsible for processing of personal data on employee devices

- Important to ensure compliance with EU data protection principles as if personal devices are company owned

Monitoring: US v. EU

US

- Federal law permits employers to monitor employees' internet or e-mail usage under certain conditions
- Common challenges to monitoring State laws

EU

- Principal violation of employee's right to privacy and secrecy of telecommunication
- Balance with company's legitimate interests
- Conditions:
- Restrict to professional data
- Legitimate purpose
- Proportionality
- Transparency
- Rules on acceptable use
- Procedural requirements

Discovery Requests: US v. EU

US

- Discovery requests in litigation generally demand that a litigant produce all responsive data that is within its control.
- When an employee's personal device contains data that is responsive to discovery requests, employers are faced with questions about whether they are required—and permitted—to search their employees' devices for responsive data.
- Courts are generally reluctant to require the production of personal data on employees' personal devices unless there is a compelling need to do so.

EU

- Generally the concept of "discovery requests" does not exist.
- Processing of personal data to comply with discovery request requires legal basis
  - Foreign legal obligation not sufficient
  - Possibility to rely on company's legitimate interest if anticipated in BYOD policy

Post-Employment Relationship: US v. EU

EU Perspective:

- Need to recover, destruct or restrict access to company information as soon as the employee leaves the company
- In a non BYOD environment: Reclaim the corporate owned devices
- In a BYOD environment: Device remains property of the employee and cannot be claimed by the company.
- Solutions: (i) remote data management (wiping the data from the device), (ii) limit access rights to company information systems, and (iii) requiring former employees to return company data
- Issues with these solutions: Access to, requiring to hand over, or wiping such personal information potentially constitutes a violation of the employee's right to privacy and the secrecy of telecommunication.
- Approach: Reduce privacy expectations and liability risks by anticipating post-employment in BYOD policy

Post-Employment Relationship: US v. EU

US Perspective

- Need to recover, destruct or restrict access to company information as soon as the employee leaves the company
- In a BYOD environment: Device remains property of the employee and cannot be claimed by the company.
- Similar solutions as EU: (i) remote data management (wiping the data from the device), (ii) limit access rights to company information systems, and (iii) requiring former employees to return company data
- Key: Lay out post-employment process clearly in BYOD policy and follow policy – including potential risks associated with wiping company data.

BYOD: Managing Challenges

Organizational: BYOD or Not?

Risks

- Main risk is data security:
- Larger number of data
- Different device types
- Transfer of data
- Data leakage
- Personal use

Benefits

- Increase of productivity and efficiency
- Innovation
- Employee satisfaction
- Increase of flexibility
- Chance to embed privacy in the core of business activities and raise privacy standards

Develop, Implement & Enforce Policy: Purpose

- Raise Awareness
- Ensure Policy Enforceability
- Limit Employee's Privacy Expectations

Develop, Implement & Enforce Policy: Procedure

- Involve HR, IT, and Legal
- Involvement of Employees and their Representatives
- Communication to Employees
- Training Employees
- Monitoring and Audit Compliance
- Consistency with Existing Policies

Develop, Implement & Enforce Policy: Content (I)

Overview

- US: employers must clearly define employees' expectations of privacy on their personal devices used for business purposes.
  - Eliminate expectation of privacy or maintain the privacy of employees' personal data by identifying: (1) when an employer may access, monitor, wipe or disable an employee's device; (2) what data or folders the employer may access.
- EU

Develop, Implement & Enforce Policy: Content (II)

- Register Devices
- Limitation on Types of Devices (free choice, limited choice, no choice)
- Acceptable Use

Develop, Implement & Enforce Policy: Content (III)

- Monitoring and Access to Data on Device
- Data Breach Procedure
- Post-Employment Procedures
- Reimbursement
- Anticipate compliance with data protection requirements

Technical: Data Security Measures

In order to manage the risks related to BYOD the following measures should be considered:

- Internal security risk assessment
- Device configuration and settings
- Encryption
- Access controls for device and data/password protection and policy
- Secure transfer of data and connection to company network
- Maintenance and updating security on employee owned devices
- Use of a Data Loss Prevention System
- Preventing storage of data on the device or cloud environments
- Technical prevention of copying sensitive data on the device
- Data log for professional use
- Data loss prevention by frequent synchronization with/back up on company server.
- *Protect the information not the device!*

BYOD: Other Issues

Other Considerations

- Software licensing violations
- Tax implications
- Labor law issues
  - Telework
  - Working time restrictions
  - Health and safety requirements
- Sector specific requirements

BYOD: Future Challenges

Future Challenges

Evolution of BYOD

- Bring-Your-Own-Technology
  - Current and future technology

BYOD under the new EU Data Protection Regulation

- Accountability
- Data breach notification
- Right to be forgotten

Discussion and Q&A

What Client Surveys Say...

Legal 500 – 2013 (Privacy): Lorenz' business-minded team provides 'great service' and can call on relationships with law firms in other jurisdictions when running international compliance projects. It acts for blue-chip corporates across the insurance, transport and pharmaceuticals industries. Practice head Jan Dhont is 'knowledgeable', 'responsive', has 'great listening skills' and 'a practical approach'.

Legal500 2014 – Data Privacy: Lorenz is 'the best of the best' for data protection and privacy issues, according to one client. It advised a US pharmaceuticals company on a web-based tool relating to nutritional supplements, which included detailed work on privacy documents. Practice head Jan Dhont is 'the pre-eminent EU data protection expert', and all of the team's lawyers have 'industry depth and excellent communication skills'.

Legal 500 – 2012 (IT): Data protection is a particular area of expertise for Lorenz, which recently advised a US-based commercial insurer on ad hoc data privacy issues in human resources, international data transfers and the use of social media. Jan Dhont is the key partner.

Legal 500 – 2011 (Privacy): Lorenz is 'top notch' when it comes to complex EU data privacy problems, and provides 'prompt assistance' and 'practical, risk-assessed advice'. The team advises Fortune 100 and 500 companies on access requests and e-discovery. Practice head Jan Dhont is 'professional and concise.

We appreciate the opportunity to be of service to you.

LORENZ | International Lawyers

Regentlaan 37-40 Boulevard du Régent
1000 Brussels, Belgium
Telephone +32 2 239 2000 - Fax +32 2 239 2002
www.lorenz-law.com