Data Security and Breach Notification Outside of the U.S.

Miriam Wugmeister
mwugmeister@mofo.com

November 2013
European Union: Data Security

• Reasonable organizational, technical, and administrative measures to protect data

• Very little guidance in most countries

• More detailed rules in:
  • Spain
  • Poland
  • Italy
  • Norway
Spain: Data Security

• Three Tiered System depending on the sensitivity of the data
  • Appoint Information Security Officer
  • Establish a written security program
  • Supervise service provider and contract
  • Implement technical and organizational measures to protect PI
  • Encryption of sensitive PI in transit
  • Implement access controls
  • Provide secure disposal of PI
Poland: Data Security

- Appoint Information Security Officer
- Establish a written security program
- Supervise service provider and contract
- Implement technical and organizational measures to protect data
- Implement access controls
- Provide secure disposal of PI
Latin America: Data Security

- Detailed rules in:
  - Argentina
  - Costa Rica
  - Mexico
  - Peru
  - Uruguay

- Nicaragua expected to issue additional regulations
Argentina: Data Security

- Three levels of security: High, Medium, Low
- Establish a written security program
- Encryption for transfers of sensitive data
- Supervise service provider and contract
- Implement access controls
- Provide secure disposal of PI
- Employee training
Costa Rica: Data Security

- DPA Registration of Security “Performance Protocol”
- Risk assessment
- Minimum reference security protocol for service providers
  - Requires binding and enforceable privacy and security policies, training manuals, audit procedures, procedures for receiving and responding to access, correction, consent revocation requests and complaints
- At least yearly updates to security measures for sensitive data
- Detailed inventories of data types, infrastructure, licenses, and processing and storage systems
- Documented procedures to supplement, preserve, modify, block, and suppress personal data onsite or in the cloud
Mexico: Data Security

- Administrative, physical and technical security measures
  - Internal supervision and monitoring system
  - External inspections or audit to check compliance with privacy policies.
  - Analyze causes of any violations and implement corrective, preventive and improvement actions

- Data Controller must consider taking the following actions:
  - prepare inventory of personal data and processing systems;
  - Conduct risk analysis
  - analyze possible security deficiencies
  - Conduct audits
  - Record the means used to store personal data

- Personnel training program to educate and generate awareness about obligations to protect personal data.
Peru: Data Security

• DPA to issue additional requirements
• Data encryption, digital signatures, and checksum verification to prevent unauthorized access, loss, or corruption during data transfers
Uruguay: Data Security

- Regular compliance audits required
- Different security levels assigned to users according to function
- Documented data access and processing procedures
- Restricted access for support, maintenance and testing activities; entry and exit control of support personnel
Asia/South Asia: Data Security

- Reasonable organizational, technical, and administrative measures to protect data
- More detailed rules in:
  - India
  - Japan
  - Korea
  - Taiwan
India: Data Security

- Reasonable security practices and procedures
  - Comprehensive documented program and policies
- In the event of a security breach, Government may require the organization to demonstrate that measures in the documented program have been implemented
- Organizations that have implemented IS/ISO/IEC 27001 standard or an approved code of best practices are deemed to have complied with reasonable security practices and procedures
  - Such standard or codes must be certified or audited on an annual basis by independent auditors approved by the Central Government.
Japan: Data Security

- Appoint data protection officer
- Perform Risk Assessment
- Supervise service provider and contract
- Implement technical and organizational measures to protect data
- Implement access controls
- Provide secure disposal of PI
Japan (cont’)

• Financial organizations must establish security regulations for:
  • acquisition and input; use and processing; storing and saving; transfer and transmission; deletion and abandonment; and responding to data breaches

• Financial organizations must also encrypt biometric data and save and store separately from other personal data
• Technical, administrative and physical security measures are required
• Encryption for selected data in transit and certain data at rest (unless mitigating controls in place)
• Internal administrative plan
• “Exert active efforts” to conduct the impact assessment if there is concern that personal data have been infringed
• Training at least twice a year for employees, outsourcing contractors, and developers
Korea (cont’)

• Policy to prevent illegal or unauthorized use of software
• Block access from unauthorized IP addresses
• Separate from the network an administrator’s PC access to a database server
• Change access passwords of Data Managers and other people at least every 3 months
• Perform vulnerability test against new and well-known vulnerabilities at least once per year
Taiwan: Data Security

• Central competent authority for the specified industry sector may require and specify the standards for a security maintenance plan or method of disposal of personal data

• Supervision of service providers required; periodic compliance checks; maintain supervision records
Common Elements of Data Security Program

- Appoint person to lead effort
- Conduct risk assessment
- Establish comprehensive written policy
- Train employees
- Supervise service providers
- Encryption of sensitive data
- Provide secure disposal
• US Executive Order was released on February 12, 2013, directing the U.S. government to take various steps to protect the nation’s critical infrastructure from cyber threats.

• On February 7, 2013, the European Commission published a proposed Directive on network and information security for “market operators”
Breach Notification Laws
Countries with Breach Notification Laws

- Austria
- Belarus
- Canada (Alberta)
- Colombia
- Costa Rica
- Germany
- Japan
- Korea
- Mexico
- Norway
- Philippines
- Russia
- Taiwan
- United Arab Emirates (DFIC)
- Uruguay
Applicable Law

• Breach Notification laws outside the US are data protection laws, not consumer protection laws
• Applicable law is generally law where the data controller is established, not where the individual resides
Japan Breach Notification Rules

**METI**
- Recommended but not mandatory
- Loss of any unencrypted personal data
- Regulator or APIPO to be notified about all breaches
- Notice to individuals in some cases
- Public announcement (in certain circumstances)
- Immediate notice when sensitive data involved

**FSA**
- Mandatory
- Loss of any personal data
- Immediate notice to regulator
- “Prompt” notice to individuals
- “Prompt” public announcement
Germany Breach Notification Rules

- Notification provisions
  - Loss of sensitive and financial data that may lead to “serious impediments for privacy and other interests”
  - Immediate notice to individuals
  - Immediate notice to regulators
  - Public announcement may substitute for individual notice when breach affects a broad public
Korea

- Any leak of Personal Data
- Notice to affected individuals
- Notice to government authorities for leaks involving 10,000 or more individuals
UAE (DFIC) Breach Notification Rules

- Security provisions in the Data Protection Law
  - Notice to regulator as soon as possible about any unauthorized intrusion
  - Notice to individuals not required
Uruguay

• The obligation to give notice is triggered by the knowledge of a data security breach that could affect the Individuals’ rights in a significant way.

  • Not clear to whom notice must be given
  • No exceptions
  • No content requirements
Uruguay Breach Notification Rules

• Regulations
  • Data controller and processor must report any security violations at any stage of processing that significantly affect the interests of the individual
  • Unclear to whom notice must be given
Countries with Voluntary Guidelines

• Canada, UK, Australia, and New Zealand
  • Notice to individuals when there is a risk of harm
  • Notice to regulators about any significant or material breaches
  • No defined data elements but sensitive and financial data are more likely to trigger obligation
  • Notification as soon as possible after containment

• Ireland
  • Notice to regulator about any unauthorized or accidental disclosures of personal information
  • Regulator to help determine if individual notices should be given

• Others: Bahamas, Belgium, Denmark, Hong Kong, and Mauritius
For More Information

• Privacy Library: www.mofoprivacy.com
• mwugmeister@mofo.com