Building a Data Privacy Compliance Program

Aaron Mendelsohn, Esq.
Program Manager – Data Privacy Compliance
October 26, 2011

Powering Business Worldwide

Celebrating 100 YEARS
Ideals that Endure

Agenda

- Determine Governance Structure
- Understand Regulatory Requirements
- Map Data Flows and Business Processes
- Develop Policies, Training, and Security Controls
- Select a Data Transfer Framework
- Establish a Monitoring and Reporting Structure

Determine Governance Structure

- Know the realities and politics of your organization
- Select a Global Privacy Leader
  - De facto Chief Privacy Officer
- Determine a reporting structure
  - Legal, Compliance, HR, IT
- Identify other key partners
  - Marketing, Supply Chain, Finance

Understand Regulatory Requirements

- Identify the countries and states your company has operations and conducts business
- Research and track the regulatory environments in each
- Monitor developments for key changes

Map Data Flows and Business Processes

- Identify types of data
  - Employee information
  - Sensitive information
- Perform a comprehensive mapping of data flows for all applications and business processes
  - Electronic and manual
  - Keep current – update regularly

Develop Policies, Training, and Security Controls

- Identify policies that govern private data
  - Work with the policy owners (Legal, IT, HR) to update, rework, or create policies as needed
- Develop a security and privacy awareness training for all employees
  - Target training to certain high-risk functions (HR, IT)
- Develop system level security controls for protecting the data.
  - Leverage existing frameworks for other compliance activities (SOX, HIPAA, ITAR, etc)

Select a Data Transfer Framework

- Safe Harbor
  - For transfer to the US only
  - Requires following the seven principles – notice, consent, onward transfer, access, security, data integrity, enforcement
  - http://export.gov/safeharbor
- Binding Corporate Rules
  - Relatively new worldwide governance model
  - Only internal/intra-company transfer of data
  - http://ec.europa.eu/justice/policies/privacy/binding_rules

Establish a Monitoring and Reporting Structure

- Conduct regular system validations
  - Use your data mapping inventory to prioritize
  - Remediate gaps and vulnerabilities
  - Report findings to executive management (CIO, CHRO, General Counsel, etc.)
- Third Party Compliance
  - How do you manage data privacy compliance with external business partners?
  - Utilize existing frameworks (BITS Shared Assessment, ISO, COBIT) or create your own assessment and process


EATON
Powering Business Worldwide