

Global Data Privacy

May 19, 2009



1. What is data privacy?

A Definition of Data Privacy

Data privacy is the relationship between the collection and dissemination of personally identifiable information, the individual's expectation of protection against unauthorized access, and the associated technical, legal and regulatory issues surrounding them.

1. What is data privacy?

Major Issues in Data Protection and Privacy

- Damage to reputation
- Loss of business
- Fines
- Sanctions



3. Data Protection and Privacy in the United States vs. the European Union

Privacy Laws Overview:

There are a number of industry-specific and other US laws focused on privacy, data protection and ID theft prevention.

Industry/Type of Data Specific

Financial Services Specific Privacy Legislation

Gramm-Leach-Bliley Act (GLBA)

Fair and Accurate Credit Transactions Act of 2003 (FACT Act)

- Disposal Rule
- Identity Theft Red Flags Rule
- Affiliate Marketing Rule

State Opt-in Statutes (e.g., CA, AK, IL, ND, VT)

Pharma and Health Care Specific Privacy Legislation

Health Insurance Portability Administrative Act (HIPAA)

Prohibitions on pharmaceutical sales and marketing practices (TX SB 11; CA AB 715; NH HB 1346)

Various State healthcare and medical marketing restrictions

CA Medical Info. Consent Act (SB 1633)

Telecommunications

Telephone Records and Privacy Protection Act

Govt-Specific Privacy and Data Protection Legislation

eGov Act

Omnibus Spending Act for FY2005
Global Data Privacy
PricewaterhouseCoopers Israel

Generally Applicable

Marketing Privacy

E-Mail – CAN-Spam Act

Telemarketing - Telemarketing Sales Rule

Fax – Junk Fax Prevention Act; Telephone Consumer Protection Act (TCPA)

Web - CA Online Privacy Protection Act

Wireless – TCPA

Disclosure -- California Personal Information: Disclosure to Direct Marketers Act (SB 27)

Data Protection Legislation

Breach/Notice Statutes

California Security Safeguards Act (AB 1950)

NYSE's Listed Company Manual, § 303A, ¶ 10.

Social Security Number Laws

3. Data Protection and Privacy in the United States vs. the European Union

A Comparison of US and EU Approaches to Data Protection and Privacy

	United States	European Union and Elsewhere
Legislative Approach	<ul style="list-style-type: none"> • Sectoral Approach. Based mainly on Fair Information Practice Principles <ul style="list-style-type: none"> • Notice, Choice, Access, Security (and Enforcement) 	<ul style="list-style-type: none"> • Omnibus Approach. Based mainly on OECD Guidelines <ul style="list-style-type: none"> • Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability)
Types of Personal Information Covered	<ul style="list-style-type: none"> • Financial - GLBA/FCRA/FACT Act • Health Care - HIPAA • Children - COPPA • Privacy Marketing Laws • Security Breach and Disclosure 	<ul style="list-style-type: none"> • All Types of Personal Data. EU Data Protection Directive and Other Global Laws
Scope	<ul style="list-style-type: none"> • Primarily Consumers 	<ul style="list-style-type: none"> • Consumers, Employees and Business-to-Business
Enforce-ment Body	<ul style="list-style-type: none"> • Federal Trade Commission • State Attorneys General • FCC, Industry Trade Groups • Private and Class Actions 	<ul style="list-style-type: none"> • Data Protection Authorities • Labor Works Councils/Union Bodies • Private Rights of Actions
Registration and Data Transfers	<ul style="list-style-type: none"> • No restrictions on transfers across country borders • No filing requirements 	<ul style="list-style-type: none"> • Transfer out of EEA only with “Adequate Protections” • Often database and transfer filings

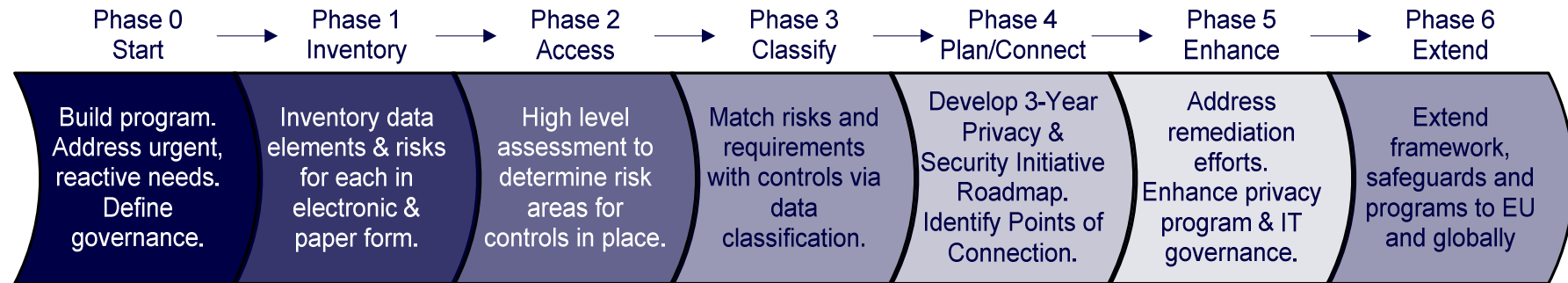
4. How Data Privacy Affects You

Who Should Care?

- Privacy Office (CPO)
- Internal Audit
- HR
- Physical Security
- Security/IT
(CISO/CSO/CIO/CTO)
- Legal and Compliance
- Risk
- Business Operations



Building a Privacy Program



Key Privacy Compliance Services

- Draft policies
- PII Inventory
- Heat Map Analysis
- Prioritization
- 3 Year Roll-Out Plan
- Eliminate PII
- Data Mapping
- Draft Charter
- Controls Inventory
- Data Mapping
- Draft Charter
- Safe Harbor
- Vendor Program
- Model Contracts
- Data Transfer Plan
- Benchmark

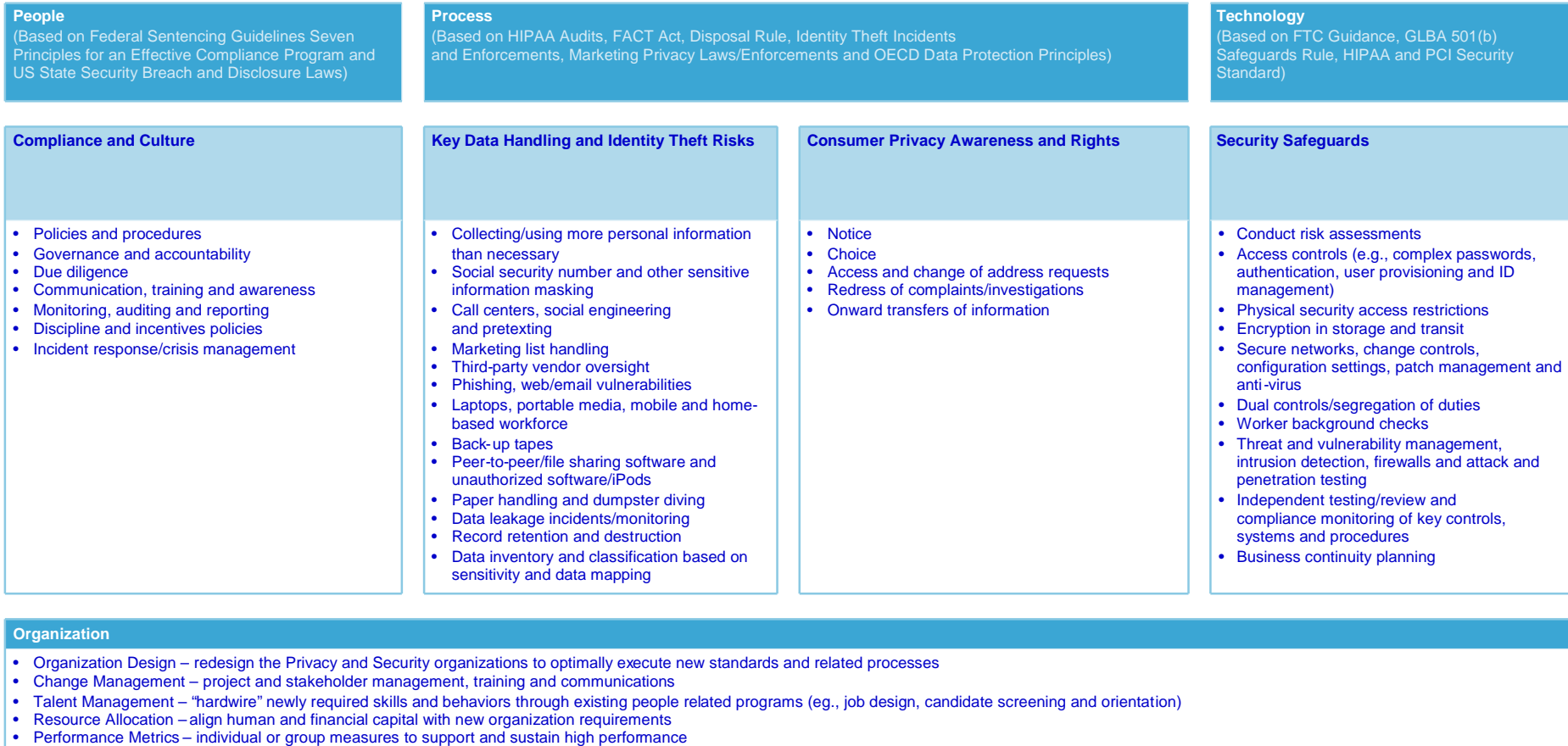
Key Data Loss Functions

- Sensitive Data Discovery (e.g., SSN, PCI, SOX, Driver's License)
- Sensitive Data Discovery (e.g., SSN, PCI, SOX, Driver's License)
- Endpoint Protection (USB Drive, CDs, Laptops, Other)
- Network Communication Analysis (Monitor, Filter and Block)
- Document Management (eDiscovery and Records)
- Email Encryption (rules based)

PwC's Integrated Framework

People, Process, Technology and Organization – 40 Elements

- Below: many of the common elements of a privacy and identity theft prevention programs
- Used by leading companies and successfully tested with regulators.



Globalization - What Our Clients Are Doing

Cross Border Regulatory Issues

- **Mapping Key Transborder Data Flows.** Emphasis on data lifecycle – collection, storage, access, use, external/internal transfers/sharing and retention/destruction
- **Inventory Compliance Requirements.** While EU requirements are substantial, many financial institutions have been developing approaches to increasingly integrate global requirements
- **Leverage Data Leakage Tools to Identify Improper Transfers.** Identify or quarantine suspected potentially improper data transfers

Globalization - What Our Clients Are Doing

- **Considering Global Compliance or Risk Management Strategies**
 - **Compliance Approaches.** Safe Harbor Certification, Intra-Group Agreements, Model Contracts, Binding Corporate Rules
 - **Develop Transborder Dataflow/Transfer Policy or Guidelines.** Providing guidance, training and audit support often promotes heightened compliance
 - **Elimination of Sensitive or Other Data from Business Processes.** To minimize incidents of non-compliance, unnecessary data elements are eliminated
 - **Masking.** Certain data elements masked or records de-identified except where a person has a legitimate reason to know

Globalization - The Trend Toward Safe Harbor

Cross Border Regulatory Rules and Compliance Options

Develop and Maintain a Privacy or Safe Harbor Policy

- **(1) Notice.** Global or EU applicable privacy policy or EU notice statements to ensure accurate, comprehensive, and visible to data subjects
- **(2) Choice.** Covers consent, permission, data use limitations/opt-out strategies and special treatment for "Sensitive Personal Data"
- **(3, 4, and 5) Access, Data Integrity and Enforcement.** Addresses areas related to existing processes or controls, if applicable, to meet Access, Data Integrity and Enforcement requirements needed to cover a Safe Harbor election

Globalization - The Trend Toward Safe Harbor

- **(6) Security.** Maintain administrative, technical and administrative safeguards and controls designed to address appropriate security requirements for US and EU applications that capture or process data subject to the certification
- **(7) Onward Transfer.** Establish safeguards and controls ensuring any onward transferee or third party that can access the data subject to the certification will maintain comparable safeguards or has also made a Safe Harbor election

Annual Re-Certification and Training