Data Protection & Privacy

Cindi Smith-Durham, Esq.
Managing Corporate Counsel, Alcatel-Lucent USA Inc.

Joseph LaVela, Esq.
Privacy and Compliance Counsel, Alcatel-Lucent

May 14, 2010

Agenda

• Data Privacy – Overview, Recent Developments and Trends
• Data Privacy Compliance Program Structure
• Privacy and Global Outsourcing
• Questions and Answers
Privacy can be defined “as the rights and obligations of individuals with respect to the collection, use, retention and disclosure of personal information” (AICPA, 2006).
Legal Framework - United States

United States – laws focus mostly on prevention of identity theft and protection of specific types of personal information (esp. health data)

Federal Laws:

- U.S. Constitution
- Financial Information: Gramm Leach Bliley Act
- Heath Information: HIPPA Privacy Law and Regulations and HITECH amendments
- Protection of children using computers: COPPA
- Federal Wiretap Act, ECPA & Stored Communications Act
- The Cable Communications Policy Act of 1984, etc.

Local and State Privacy & Data Protection Laws:
- Exist in at least 46 states
- Focus on prevention of data breaches involving specific data types, and notification/remediation in case of breaches
- Anti-Spam laws
- Numerous other bills introduced in States, Counties and Municipalities

Legal Framework – EU/EEA

- Directive 95/46/EC - applies to any “processing” of personal data, both terms defined very broadly

- Personal Data: Any information relating to an identified or identifiable natural person (“data subject”)


- Processing: Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
Legal Framework – EU/EEA

Compliance Requirements for Processing of Personal Data:

The philosophy of the data privacy laws is that **any processing of personal data is forbidden except where expressly permitted.**

Permitted if:

- the data subject has **unambiguously** given his consent
  - Must be free and informed
  - Employees generally cannot give a valid consent
- Or if the processing is necessary
  - For performance of a contract with the data subject
  - For compliance with a legal obligation to which the controller is subject
  - To protect the vital interests of the data subject
  - For performance of a task in the public interest or exercise of official authority
  - For the purposes of the legitimate interests pursued by the controller or the third party to whom the data are disclosed and not overridden by the data subject's fundamental rights and freedoms.

Greater restrictions for sensitive personal data

---

EU Compliance Requirements (cont.)

Data subjects must be informed of:

- the identity of the data controller,
- what personal data is being processed,
- the purpose for which the data is processed, and
- the identity of the recipients of the information.

At any time, data subjects can request to have access to their information. They must be provided with the information without undue delay.

Data Controllers may have additional obligations:

- To appoint a Data Protection Officer
- To notify, or secure approval of, the Data Protection Authority
EU Compliance Requirements (cont.)

- Personal data must
  - be obtained and processed only for specified, legitimate and lawful purposes,
  - be adequate, relevant, and not excessive in relation to the purpose for which it is obtained and processed (the minimum information necessary to support the process must be used),
  - be kept accurate and up-to-date,
  - be kept secure and no longer than necessary
- Must have written contracts with any third party processor with sufficient guarantees as to the technical and organizational means that will be used to protect the data
- Transfers to third countries (outside of EEA) that do not provide adequate levels of protection are in principle prohibited
- A limited set of alternative ways to achieve adequate protection are recognized

![World Map showing data protection laws and regulations in different countries.](image)
Specific Issues for MNCs

- No “Group Privilege”
- Compliance Hotlines
- Monitoring – email, internet use, video cameras, GPS, biometrics, etc.
- Internal investigations
- Forensic imaging, access to emails
- Satisfaction surveys

Privacy Developments and Trends

Additional countries adopting DP laws (e.g. EU style law in Uruguay)
Additional enforcement powers (e.g., UK DPA gains power to impose fines up to £500,000) and activity (e.g., Google executives in Italy)
Lisbon Treaty establishes data privacy as fundamental human right in EU
Massachusetts/Nevada Protection laws
- Requires encryption if personal data (defined as name in combination with Social Security number, driver’s license number or financial information such as bank account or credit card number) are sent over public or wireless network or put on portable media
EU interest in breach notification laws
Focus on issues surrounding new technologies, cloud computing, behavioral tracking, etc.
Compliance Program Structure

Privacy Program - Organization

Chief Privacy Officer - Part of Compliance Organization
Chief Privacy Counsel
Data Protection Officials
Data Privacy Steering Council

Data Privacy Team
Consists of representatives from the Compliance organization, Law, HR, IT Security and one or more Data Protection Officials

Data Privacy Network

The Data Privacy Network members are an HR and Legal representative for each country in which the Company does business, plus the Data Protection Officials for those countries for which a DPO has been named
## Privacy Program - Documentary

### Legal Framework
- **Data Processing Frame Agreement (DPFA)**
  - contract signed by all legal entities
  - includes the EU model clauses for allowing data transfer outside the EU
- Controller to Controller to Processor
- System Annexes for each application

### Participation Agreements
- **Participation Agreement and Safe Harbor Certification (US)**
  - Americas
- **Participation Agreements**
  - EMEA
  - APAC

### Global Privacy Policy - Internal and Public

## Privacy Program – Example for Introduction of New HR System

### Data Privacy Team: System Annex
- based on EU Directive Principles
- (takes about 3 months to write)

### Regional Data Privacy Network:
- Local approvals (mostly in Europe)
- (can take up to 6 months to obtain)

1. The System Annex is written by the Data Privacy Team and the HR Business Owner at the time of Business Requirements.
2. It describes: Who (what function in the company) has access to What (what employee personal data) and Why (what is the objective, the justification)

### Notifying or getting approval from:
- ✓ The Data Privacy Supervisory Authorities and/or
- ✓ The Works Councils

---

Go Live
Global Outsourcing - Overview

Introduction

• Having a strong data privacy program is an important practice when outsourcing is considered.

• For a global business, jurisdictional and international boundaries create complex privacy issues, especially in global outsourcing.

• Any decision to outsource must be made carefully with consideration given to privacy issues/laws.
Global Outsourcing

- Outsourcing is the delegation of a non-core operation, function, process and/or task to an external entity that specializes in the specific area outsourced.
- Requires a party to entrust important business operations, functions, processes and/or tasks to a third party
- One of the important trends of the 21st century

Global Outsourcing - Types

- Tasking – 3rd party takes over some tasks (software development, web design...)
- Selective Outsourcing – specific parts of an area are awarded to a 3rd party to meet skill set requirements (IT application support...)
- Transitional Outsourcing – Exchange of technology transfer
- Comprehensive Outsourcing – transfer of an entire division, function or process to a 3rd party (long term with transfer of assets/resources)
- Transformational Outsourcing – combination of business consulting and outsourcing for reorganization to “best in class” (3rd party implements or transfers back)
- Business Process Outsourcing – An entire business process is transferred to a 3rd party (purchasing, HR management, payroll management, IT)
- Knowledge Process Outsourcing – transfer of more complex and labor-intensive tasks (special skills and accurate knowledge of a particular area required – market research, business research, legal services, IP services, medical services)
Global Outsourcing - Benefits

- Provides a party the ability to concentrate and invest more on core competencies
- Compensates for lack of expertise or qualified staff
- Permits higher and better performance
- Allows for optimal scalability
- Promotes cost effectiveness, reductions and efficiencies
- Overhead/administrative costs can be clearly calculated
- Provides job opportunities for non-core employees in a business that specializes in the areas of expertise
- Provides for faster response to change
- Reduces need for investments (software, hardware, new technology)
- Increases productivity
Global Outsourcing and Privacy

Represents Complex Global Issues for Privacy
Business Risks - Privacy
Breaches/Personal Data Loss

- Reputational Damage
- Legal Liability, Including Criminal Liability for Individuals and Corporations
- Charges of Deceptive Business Practices
- Customer or Employee Distrust
- Denial of consent by individuals to have personal info used for business purposes
- Loss of revenue or disruption of business operations

Global Outsourcing and Privacy

- Outsourcing increases the complexity of dealing with privacy issues
- The complexity is increased significantly when the third party is in a different country or the services will be provided from a different country and the third party will have access to personal data
- Part of a party’s privacy responsibilities may be outsourced with a business process but the accountability cannot be outsourced
- Consideration should be given to the privacy laws of the country and the third party’s ability to comply
- A strong internal privacy program is essential to the successful selection, contracting and implementation of a global outsourcing project.
Global Outsourcing - Privacy Risks

- Loss of control over personal data
- Greater risk of security breaches
- Ability to comply with own polices and applicable laws may be in jeopardy

Strong Privacy Program For Outsourcing - Example
Strong Privacy Program – Example – Third Party Processors

Third Party Risk Compliance Assessment
- Data Security Questionnaire
- System Connection Requirements

Privacy and Data Protection (Security) Agreements
- Data Protection (Security) and Connection, Contractual Clauses for other Privacy Issues
- Privacy and Data Protection - Model Clauses
  - EMEA
- Privacy and Data Protection - Per Regulatory Requirements
  - APAC

Strong Privacy Program – Assessment of Third Party

- Prescreening and Scoping Process/RFP/RFQ/RFI
  - Determine data to be collected, processed transferred
  - Request for information on privacy program (Controller and Processor) and any breaches/non-compliance
  - Provide a Data Security Questionnaire for information security
  - Compare current status with required state
  - Perform risk analysis to determine need for mitigation/remediation or alternate source
  - Determine if third party has process for DPA approvals
Strong Privacy Program – Assessment of Third Party

- Contract Negotiations
  - Include agreed upon standards in contract
  - Require third party support of regulatory filings (DPA)
  - Negotiate for audit rights on security and privacy compliance
  - Establish responsibilities for DPA approvals and process/forms/format and who will be responsible for costs

- Implementation
  - Establish a data privacy team (both parties) to determine privacy requirements
  - Ensure regulatory approvals are obtained, as required
  - Begin filing process as soon as possible
  - Conduct periodic audits on privacy program during term
EU Directive

Principle 8 of Directive:

Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Meeting EU Privacy Requirements – Inadequate Protection

Three means of developing a strong internal privacy program that meets EU Directive requirements for non-adequate countries

• Model Clauses
• Safe Harbor Certification
• Binding Corporate Rules
The European Commission has published Model Contractual Clauses

- Use ensures compliance with Principle 8
- Approval only extends to use of the model contractual clauses as they stand (no modifications only additional contractual language added to them that doesn't contradict them in any way)
- Designed to facilitate transfers of personal data from the EEA to all third countries (providing sufficient safeguards for the protection of the privacy of individuals)
- **Two sets of model clauses**
  - one governs controller-to-controller transfers
  - the other, controller-to-processor transfers (new version effective May 15).
  - no clauses for processor-to-processor transfers

Both data importer and exporter have to warrant and undertake that they have complied with data protection standards which meet the requirements of the Data Protection Directive in respect of the data, accept liability to data subjects for breach of those standards, with cross indemnities to ensure that the one responsible for the actual breach meets the cost of the breach.

- The data importer (based outside the EEA) has the most onerous task - must also agree to limit processing to the specification in the contract.
- The data importer must adopt appropriate levels of security, identify all staff who require training in data protection matters, and notify the data exporter of those laws which allow the authorities in the importer's country to access the exporter's personal data.
- The contract also provides for other termination requirements and deals with jurisdictional matters.
- The Mandatory Data Protection Principles are annexed to the standard contractual clauses.
Meeting EU Privacy Requirements – Inadequate Protection

SAFE HARBOR

• US considered a country that does not meet the “adequacy” standards
• Safe Harbor designed to bridge differences
• Streamlined means for US companies to comply with Directive (Developed by US Dept. of Commerce and European Commission)

Safe Harbor

Set of 7 privacy Principles
• Notice – inform individuals
• Choice – Offer the opportunity to opt out
• Onward Transfer – For transfer to third party, Notice and Choice applied, contractual terms with third party
• Security – Reasonable precautions must be taken to protect data
• Data Integrity – Personal information must be relevant for the purpose
• Access – Individuals must have access to their personal information
• Enforcement – Mechanisms for assuring compliance with the Principles
Safe Harbor

Certification

• Certification is entirely voluntary
• Must agree to comply with the Principles
• May join a self-regulatory privacy program
• Entity may develop its own self-regulatory privacy policies
• Failure to comply with self-regulation is actionable under Section 5 of the FTC Act (prohibiting unfair and deceptive acts)

Meeting EU Privacy Requirements – Inadequate Protection

BINDING CORPORATE RULES

• Developed by the EU Article 29 Working Party for use by a multinational organization or group of companies as a mechanism of transferring personal data throughout the organization.
• Intended as an alternative to model contracts and Safe Harbor and are aimed at providing a compliance solution to multinational organizations.
• Need to be approved by every European data protection authority in whose jurisdiction a member of the group will rely on them
• The approval process has been simplified as an application is made to one national "lead" data protection supervisory authority in Europe and that authority liaises with all other authorities to seek approval.
• Large multinational organizations are starting to look at binding corporate rules as an alternative to Safe Harbor and contracts, primarily because it does offer a global solution.
The Essential Role of a Strong Privacy Program in Global Outsourcing

- To provide the standards for the third party provider relationship
- To initiate the third party risk and compliance assessment
- To establish the processes and practices to be followed in the selection, contracting and implementation stages of the global outsourcing project
- To ensure continued compliance with internal privacy policies
- To ensure privacy issues are addressed in a timely manner
- To ensure compliance/continuing compliance with the applicable privacy and data protection laws
- To ensure protection and management of personal information by the third party
- To support the shifting of compliance and liabilities to the service provider
- To force the service provider to incorporate data privacy in their business processes
- To focuses all parties on processes and safeguards that reduce the likelihood of lost or misused data and non-compliance with applicable laws.
Conclusion

- Global Outsourcing increases the complexity in dealing with privacy issues and legal requirements
- Outsourcing a business process may allow outsourcing of privacy responsibilities but not privacy accountabilities
- The success of a global outsourcing deal can depend on the strength of the internal privacy program
- A strong privacy program will play an essential role in the successful implementation of a global outsourcing project

QUESTIONS AND ANSWERS ?????