Data Protection and Privacy Rights – An IT Industry Perspective

National Seminar on Privacy Rights and Data Protection in Cyber Space, Bangalore

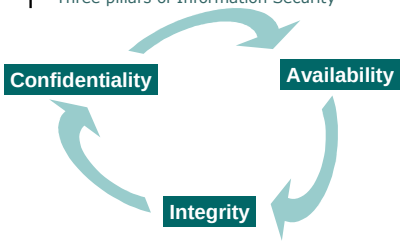
17th Oct, 2008

Author: Rajneesh Sharma
BCP and IS Manager – Hewlett Packard

Background

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation"

Three pillars of Information Security



Data Privacy

- Special category of data
- Involvement of Personal / Personally Identifiable Information (PII)
- Driven through applicable Data Privacy laws

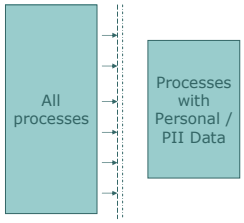
* PII: Any information that can be traced to a particular individual. Usually a set of identifiable information is identified through an identification block of data, such as a name, mailing address, phone number, social security number, or e-mail address.

Information Security vs. Data Privacy

1) Data Privacy is related only to personal or personally identifiable information, whereas, Information Security deals with any key information (such as product information, marketing information) related to an organization.

2) Data Privacy requirements are legal requirements and wherever applicable they are driven through applicable data privacy laws. Information Security requirements are driven through well known industry standards such as ISO 27001 (earlier BS7799).

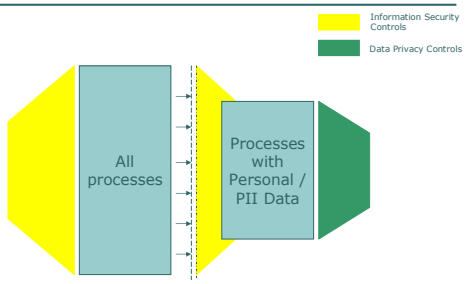
Process Segregation



- Invoice processing
- Application development

- Payroll processing
- Credit card data processing

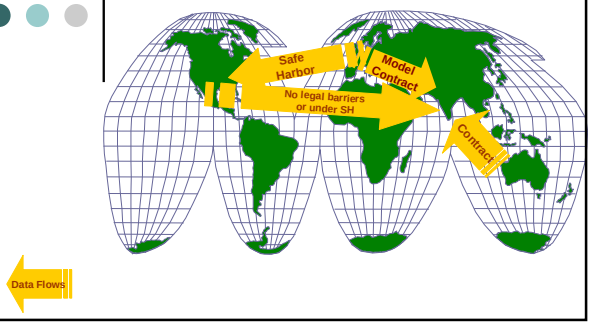
Level of protection



- Physical access controls
- Password controls
- Anti-virus

- Masking credit card numbers

Current landscape of privacy laws



Adequate vs. Inadequate destinations

Adequate Country
A country that meets the adequacy standards outlined in EU data protection directives (Key requirement being the availability of a comprehensive data privacy law). The only countries recognized as adequate as of July 2005 are Argentina, Canada, Switzerland, Guernsey, and the Isle of Man. The US is considered adequate for data transfer only under the limitations of the Safe Harbor agreement.

India is considered to be "Inadequate" country

Need for a Data Privacy law in India

Some Points..

- Organizations are currently not aware of their responsibilities / liabilities while dealing with the personal data. E.g. Liabilities of data collectors, data processors and intermediaries.
- Ad-hoc / inconsistent measures taken by the organizations.
- Efforts limited to cover the current data privacy requirements of the organization. Holistic approach is missing.
- Indian IT / Other organization do not to get the benefits of operating in an environment which is considered to be 'safe' from the data privacy point of view.

Key Privacy Principles

Principles	Key Requirements
Fair and lawfully processing	•Consent from the data subject •Part of a contract involving data subject •Legal obligation
Processed for limited purposes.	•The collection of personal information should be limited to information that is relevant to the purposes of collection. •Data shall not be used beyond the scope of notice without consent
Adequate, relevant and not excessive	•Data should be collected for specified purposes and used accordingly. •Data Processor to get permission for secondary purpose
Accurate	•Data has to be kept accurate and up to date •Data Subject may ask Data Controller to notify third parties who have previously processed the incorrect data to make these corrections.
Data not to be kept longer than necessary	•Data have to be kept for a prescribed period of time as specified in a statute •PII needs to be protected against loss. •Data have to be disposed after a prescribed period of time. •Disposal of media and equipment has to be done in a secure manner.

Key Privacy Principles contd.

Principles	Key Requirements
Processing in accordance with the data subject's rights	•Data subjects must be given the ability to determine if the entity stores data about them, to access data stored about them and to correct data stored about them
Security	•Technical and organizational measures to protect against destruction, unauthorized loss, unauthorized alteration, unauthorized disclosure or access •If further subcontracting by Data Processor is involved this needs to be addressed in an outsourcing contract between Data Controller and Data Processor.
Not transferred to other countries without adequate protection	•Personal information shall not be transferred to a third country unless consent has been received. However a number of alternatives apply. (such as Model Contract between Data Exporter and Data Importer)

Compliance to Privacy requirements

- Type of data
- Countries involved
- Call recording

- Model Contract
- Security of data
- Data retention timelines

- Adherence to contract
- Background checks
- Schedule for safe data disposal

Key Benefits

- Increased Customer confidence
- Competitive advantage
- Personal data specific to data subjects if sent out to other countries, would required to safeguarded appropriately
- Uniform understanding about the responsibilities / liabilities