Contracting with a Cloud Service Provider

DATA PROTECTION WORKSHOP – NJERI OLWENY, MICROSOFT

Overview

Cloud computing offers great opportunities for organizations, including schools, hospitals and businesses in various industries.

These opportunities raise some important privacy issues, as a result of third party service providers having access to data, particularly in sectors such as healthcare, financial services and education.

What limits should be placed on Cloud Service Provider ("CSP") use of this data?

What is required under national and local laws?

Recent surveys highlight that "data mining" of data for advertising or marketing purposes is a key concern among data subjects

Policy-makers, administrators of various institutions and organizations, CIOs should ensure that IT service providers protect data subject privacy and refrain from commercial uses of their data.

Scary invasion of privacy

Privacy - Data Protection Basics

Key players in the processing of personal data

Data Subject	Data Controller	Data Processor
The individual who is the subject of the PII	Determines the purposes and means in which any PII is processed Legally responsible for compliance in most cases May require audit or similar rights from a processor	Processes PII only on the Data Controller's instructions Not a third party Must implement appropriate technical and security organizational measures (TOMs)
The employee or customer of the cloud	Customer	Microsoft

What to consider before selecting a Cloud Service Provider

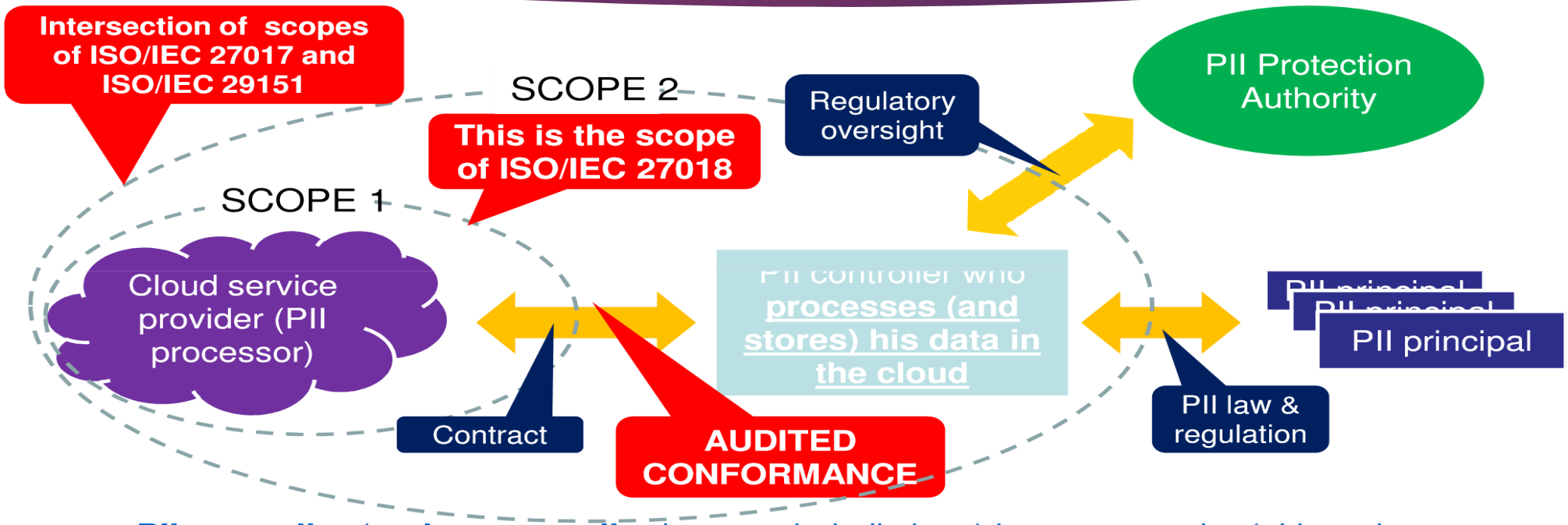
Know your cloud service provider

- Research provider's track record on privacy and security
- Understand provider's business model and assess whether your data is likely to be used or mined for a secondary purpose

Place clear contractual restrictions. Include contract clauses that:

- Allow provider to use customer data only to operate the service
- Prohibit use of customer data for advertising and marketing purposes
- Require provider to maintain appropriate administrative, physical and technical safeguards
- Require provider to comply with applicable privacy laws

Frameworks impacting Cloud Services



- **PII controller** (or **data controller** in some jurisdictions) is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- **PII processor** (or **data processor** in some jurisdictions) is any person (other than an employee of the PII controller) who processes data on behalf of the PII controller.

Questions to Ask Cloud Service Providers

- How will you use our data which we store in or transmit across the cloud services you are operating?
- Is our data segregated and stored separately from the data related to your consumer cloud offerings?
- Will you agree to contractual provisions that restrict your use of our data to only uses necessary to operate the contracted services, including provisions that specifically prohibit mining or use of our data for any purposes related to marketing or advertising?
- Identify baselines requirements such as Data Protection Legal Provisions or ISO Certifications that can be a measure for whether a cloud service provider has implemented rigorous security and data protections.

School practice and policy

A recent US University study shows that schools are challenged to deal with cloud services.

- "Cloud services are poorly understood, non-transparent, and weakly governed: only 25% of school districts inform parents of cloud services, 20% of districts fail to have policies for the use of online services, and a many districts have rampant gaps in their contract documentation, including missing privacy policies."
- "Districts are often passive parties to cloud service contracts that are drafted by vendors and not subject to any negotiations. These agreements must more directly address privacy obligations."
- The study recommends better contracting by schools, to prohibit sales, advertising and marketing uses of student and teacher data by cloud vendors.

Privacy protections in cloud contracts

Place clear restrictions in contracts on cloud service provider use of data.

Since the CSP will have access to, and will be storing, the customer's sensitive information, the agreement should contain specific language

(i) regarding the provider's obligations to maintain the confidentiality of such information;

(ii) placing appropriate limitations on the provider's use of such customer information (i.e., confirming that the provider has no right to use such information except in connection with its performance under the cloud computing agreement, including specifically exclude the provider from any mining of such data.

(iii) Requiring the cloud service provider to be transparent about their practices and internal policies, including compliance with local laws and meeting globally recognized standards – certifications such as ISO 27001, 270017, 27018; compliance audits by independent third parties.

Microsoft's commitment to data stewardship

- Our position, as we state on our Trust Center, is: "Your data belongs to you. Microsoft does not scan emails and documents to create advertisement products"
- We back that statement up with contractual provisions that limit how we can use or store data.
- Microsoft will only use customer data for the purpose of fulfilling its duties under the Agreement, which includes providing the Cloud Services in Office 365 or Azure for Customer's and its End Users' benefit.
- The Office 365 or Azure Services will not use Customer Data for any advertising or other commercial purpose of Microsoft or any third party.
- "Microsoft firmly believes advertising and marketing uses of personal data should not be permitted by service providers. Further, contracts with institutions such as schools should state these concepts in clear and unambiguous terms."