Standardising privacy and security for the cloud

Chris Mitchell
Royal Holloway, University of London
www.chrismitchell.net

Acknowledgements

- Like to thank organisers of event for inviting me to contribute.
- Must also thank John Phillips of Microsoft for his support and encouragement.

Agenda

- The need for standardisation
- Data protection obligations
- Context and structure of standard

Huge scope

- As has been widely discussed, cloud computing encompasses a very range variety of activities.
- Covering:
  - **deployment types**: public, community, hybrid and private cloud services;
  - **service types**: software, platform or infrastructure as a service.

Security and privacy

- Much has been said about security and privacy risks of cloud use.
- This is because cloud inevitably involves storage (and possibly processing) of data by a third party (the cloud provider).

Range of possible standards

- Various security aspects of cloud computing services can usefully be standardised.
- For example:
  - security requirements on cloud providers;
  - privacy requirements on cloud providers;
  - service interfaces;
  - security techniques specific to cloud.

Growing attention

- Cloud standards work is now being undertaken by both ITU-T and ISO/IEC JTC1.
- The ITU-T Focus Group on Cloud Computing has recently produced a general document (Cloud-O-064) providing key definitions and threat discussions, that is intended to provide a foundation for future standardisation.
- Two ballots on possible future cloud security standards are about to be circulated to ISO/IEC member bodies.

Focus of this talk

- In this talk I am focussing on standardisation of security obligations of **public cloud providers**.
- Specifically, the security requirements on such providers in order for the providers to meet **data protection obligations**.
- Requirements may soon be codified in a new ISO/IEC standard: **ISO/IEC 27018**.

Parallel work

- In parallel with the work I will describe, ISO/IEC member bodes are about to be balloted on a second possible cloud security standard.
- This will be a more general cloud security controls standard.

Agenda

- The need for standardisation
- Data protection obligations
- Context and structure of standard

Royal Holloway University of London

Information Security Group

Cloud data protection standard:

- Controls that are applicable to a **data processor**, not to a **data controller**
- Controls are therefore primarily or wholly information security controls and not privacy controls (so the ISO/IEC 27001 ISMS is appropriate as the management system)

Audited public cloud provider certification to achieve:

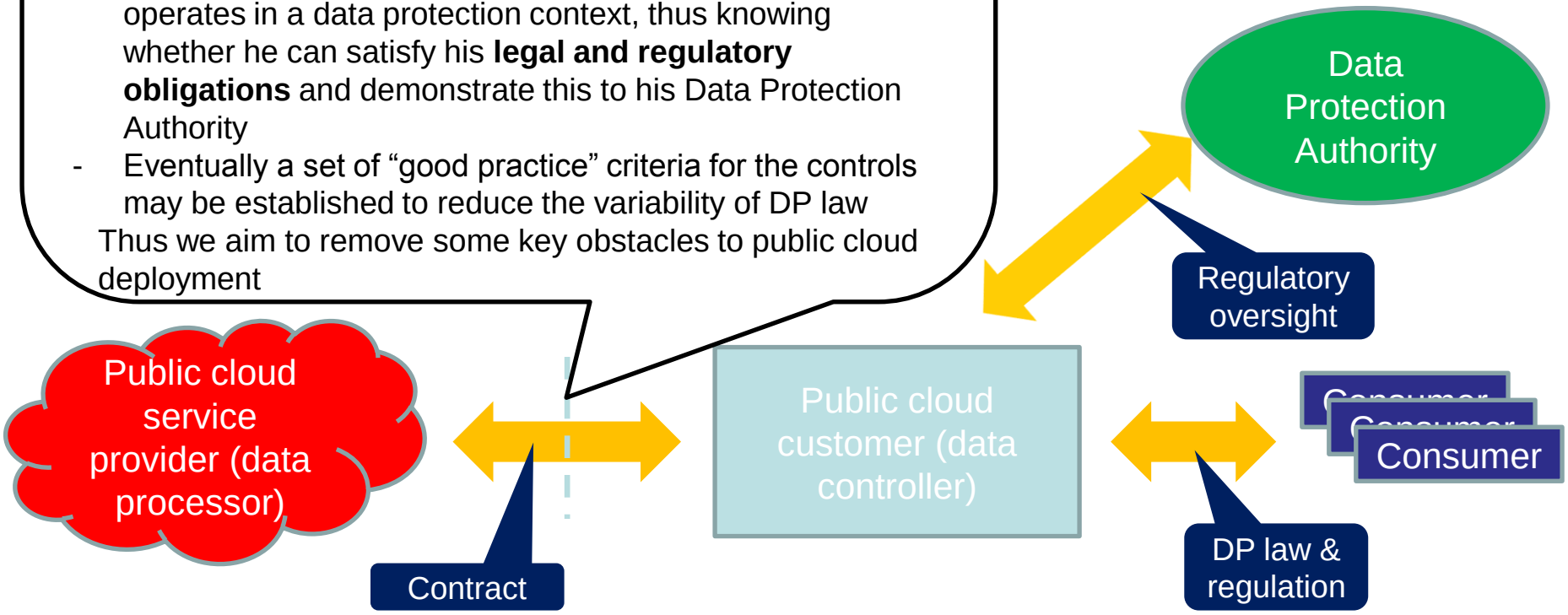
- Transparency in the **contract** relationship
- A **public cloud customer** can select a **public cloud service provider** knowing how the service provider operates in a data protection context, thus knowing whether he can satisfy his **legal and regulatory obligations** and demonstrate this to his Data Protection Authority
- Eventually a set of "good practice" criteria for the controls may be established to reduce the variability of DP law

Thus we aim to remove some key obstacles to public cloud deployment

The **Data Controller** 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.

The **Data Processor** is any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller.

Specifically these are EU data protection concepts, but may apply more widely in practice.



Data processors

- **Data Controller** (either alone or jointly) determines the purposes for which, and the manner in which, personal data are processed.
- **Data Processor** processes data on behalf of the Data Controller.
- Cloud service provider is typically the data processor – not the data controller.

Data protection obligations

- In every jurisdiction with data protection laws/regulations, public cloud providers must show potential data controllers that their service meets legal needs.
- That is, they must show their service respects the regulations with respect to the obligations of data processors.
- This is costly and time-consuming if done on a country-by-country basis.

Security and privacy

- Data protection is fundamentally a *privacy* issue.
- However, the issue of concern is primarily a *security* one, since we are dealing with data processors.
- That is, data processors must meet the necessary security requirements so that all data (including privacy-sensitive data) is handled appropriately.

Agenda

- The need for standardisation
- Data protection obligations
- Context and structure of standard

27000 series standards

- The ISO/IEC 27000 series of standards are concerned with information security management systems (ISMSs):
  - 27000: ISMSs – Overview and vocabulary;
  - 27001: ISMSs – Requirements;
  - 27002: Code of practice for information security controls.
  - … many more …

27001

- The first main standard in the series lists requirements for the establishment and operation of an ISMS.
- It covers high-level operational and staffing issues.

27002

- ISO/IEC 27002 is probably the most celebrated and widely used member of the 27000 family.
- It owes its origins to BS 7799 (a UK standard) which became ISO/IEC 17799 and was rebadged 27002.
- It provides a large catalogue of security controls, to be used when implementing an ISMS.

Sector-specific standards

- Within the 27000 family are sector-specific standards, i.e. standards which apply 27002 to specific application domains.
- For example, ISO/IEC 27011 is focussed on telecommunications.
- It provides an interpretation of ISO/IEC 27002 aimed specifically at this sector.
- It also provides additional security controls relevant to this sector.

ISO/IEC 27018 – status

- SC27 is committee of ISO/IEC JTC1 concerned with IT security standards – is responsible for maintaining 27000 series.
- SC27 is about to ballot its members (the national standards bodies) regarding a proposal to start developing a new sector-specific standard.
- This standard will focus on controls for providers of cloud services

ISO/IEC 27018 – title

- The proposed new standard has the working title:

Code of practice for data protection controls for public cloud computing services

ISO/IEC 27018 – content

- Objective is to collect and organise security categories and their controls from current data protection regulations.
- Help public cloud service providers to comply with their obligations and make this transparent to their customers.
- Customers can select cloud-based data processing services that allow them to meet their obligations.

ISO/IEC 27018 – structure

- The general structure will follow (new version of) ISO/IEC 27002, in which controls are listed under the following headings:
  - Security policy;
  - Organisation of information security;
  - Asset management;
  - Human resources security;
  - Physical and environmental security;
  - Supplier relationship management;
  - Communications and operations;
  - Management of application services on networks;
  - Access control;
  - Information systems acquisition, development and maintenance;
  - Information security incident management;
  - Business continuity management;
  - Compliance.

Contributions welcome!

- Necessary to get broadest possible consensus on proposed draft.
- Please contact me (me@chrismitchell.net) if you are interested in getting involved in reviewing and/or providing input.
- In UK, work coordinated by BSI IST/33.