ISO/IEC 27018: Outsourcing personal data processing to the cloud

Chris Mitchell (editor)
Information Security Group, Royal Holloway, University of London
www.chrismitchell.net

Overview

- When personal data is processed in the cloud:
  - you outsource the processing, but
  - you keep the data protection legal obligations.
- How do you find a cloud service provider who will meet your legal obligations?
- An auditable standard for cloud service providers who process personal data would help – auditor can check and issue a compliance certificate.
- Audited compliance to this standard could be written into the cloud contract.
- **ISO/IEC 27018** is being developed as such a standard, to solve a key problem for the cloud industry.

The problem

- PII controllers wish to use cloud service providers (acting as PII processors) to process their personally identifiable information (PII).
- Developing this cloud industry opportunity needs customer and regulatory authority confidence in PII processing in the cloud, to be developed speedily.

Royal Holloway University of London
Information Security Group

The solution

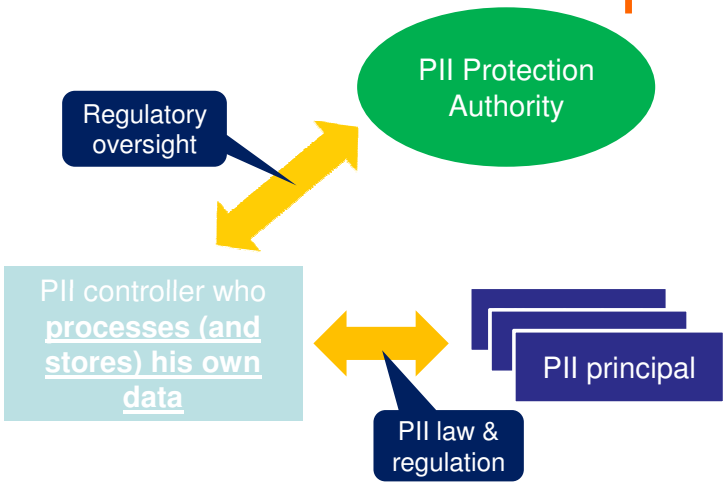
- Must create a system for cloud PII processor governance, and for showing this with certification, which:
  - integrates with processes already used by today's cloud infrastructure, based on existing PII processing obligations (to encourage rapid and wide adoption);
  - can be developed in future releases to move towards improved cloud privacy as cloud infrastructure & privacy requirements develop.

ISO/IEC 27018

- ISO/IEC 27018 (*Code of practice for PII protection in public clouds acting as PII processors*):
  - implements privacy principles of ISO/IEC 29100 (the *privacy framework*) as applied to a PII processor (but not as applying only to a PII controller).
  - is a key element to start the cloud industry moving down the path of privacy conformance.

Protection of PII: basic relationships

- **Personally identifiable information** (PII) is any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.
- **PII principal** (or **data subject** in some jurisdictions) is a person to whom the PII relates



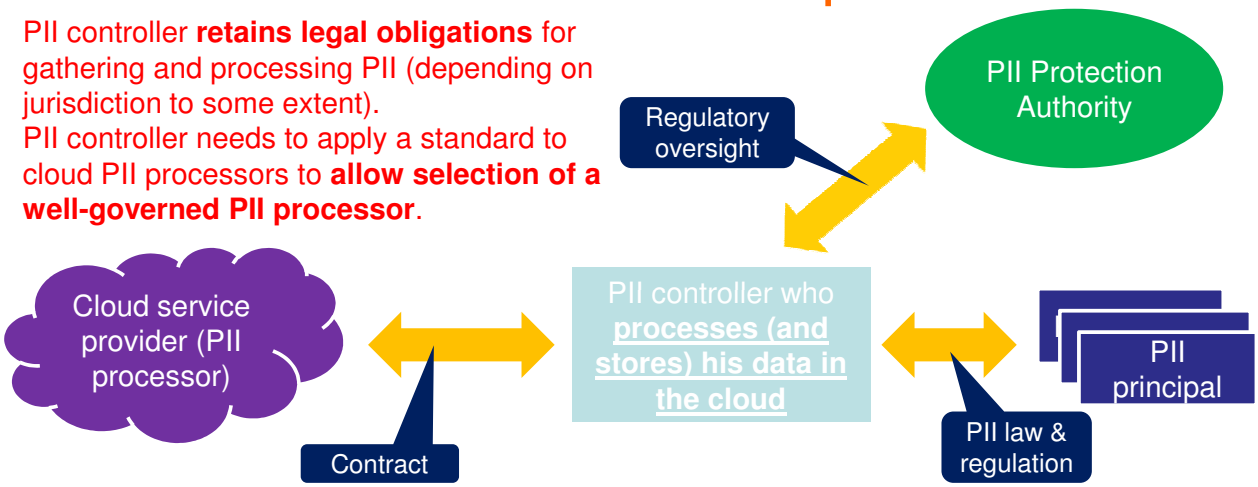
- **PII controller** (or **data controller** in some jurisdictions) is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Royal Holloway University of London

Information Security Group

Protection of PII: relationships in the cloud

- PII controller **retains legal obligations** for gathering and processing PII (depending on jurisdiction to some extent).
- PII controller needs to apply a standard to cloud PII processors to **allow selection of a well-governed PII processor**.

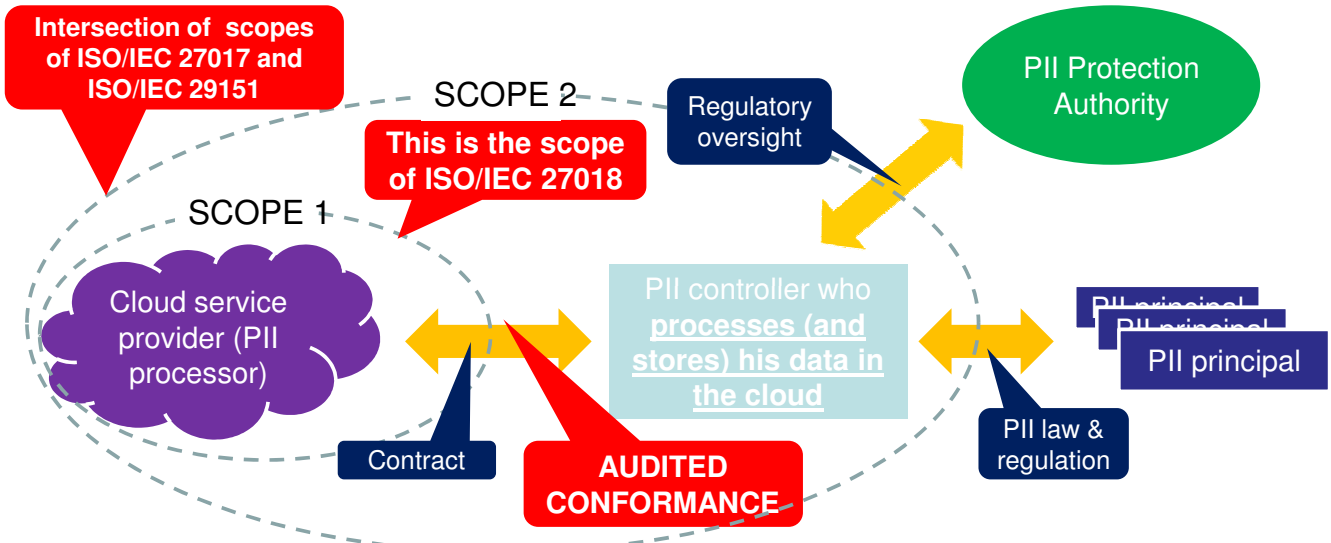


- **PII controller** (or **data controller** in some jurisdictions) is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- **PII processor** (or **data processor** in some jurisdictions)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

Royal Holloway University of London

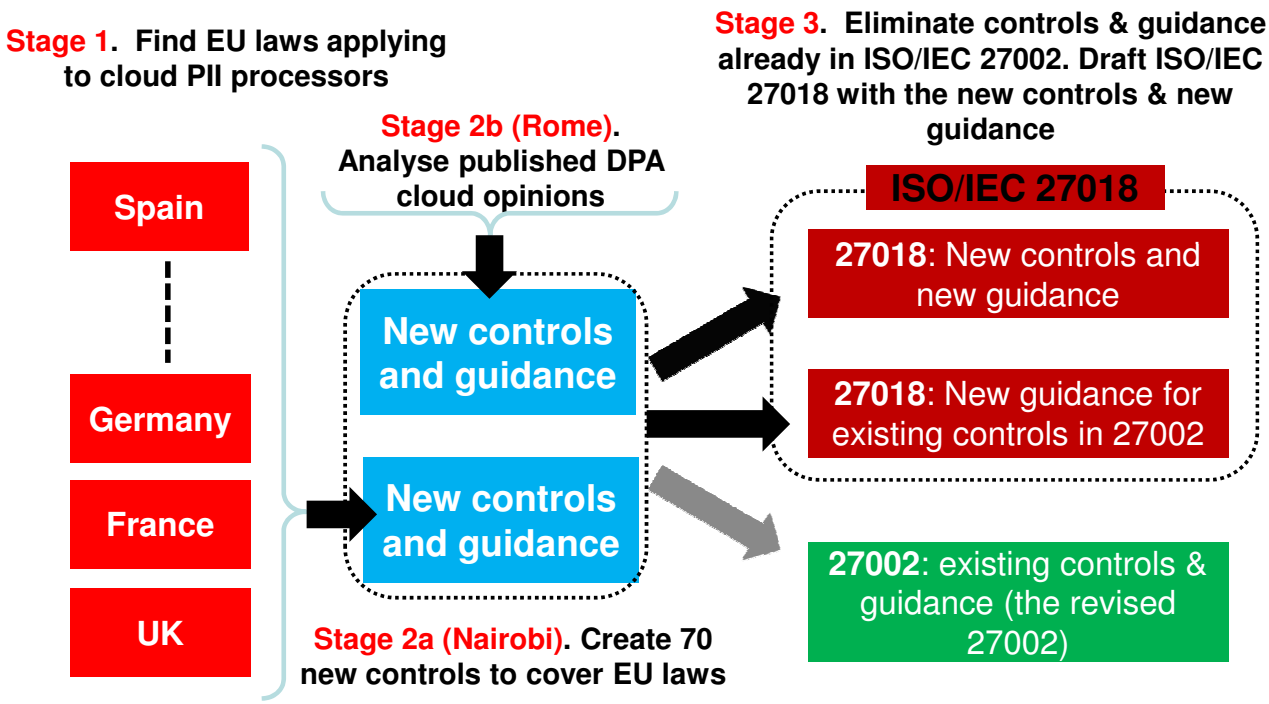
Information Security Group

Protection of PII: the scope of ISO/IEC 27018



- **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.

Origins of ISO/IEC 27018 PII protection controls



Royal Holloway University of London
Information Security Group

The 27018 approach

- Cloud provider market already knows, invests in, and extensively implements, audited certification to ISO/IEC 27001 (*information security management system requirements*), using information security controls catalogue in ISO/IEC 27002.
- So it is advantageous to base cloud provider PII protection certification on ISO/IEC 27001, by extending ISO/IEC 27002 controls in ISO/IEC 27018, structured as a sector-specific standard to cover PII protection for cloud PII processor.

Rationale for approach

- Provides a practical base to start creating confidence that cloud industry deals properly with the PII they process.
- This approach:
  - likely to be attractive to existing cloud providers and scales well;
  - likely to be economically viable for developing incremental accreditation & certification; and
  - can be continuously improved once in place.

Who is developing 27018?

- ISO/IEC 27018 is being developed within ISO/IEC JTC1/SC 27, concerned with *Security techniques*.
- Within SC 27, work being performed within Working Group 5 (WG 5), concerned with *Privacy and identity management*.

Where are we?

- New work item ballot for ISO/IEC 27018 successfully concluded on 16 Feb 2012, and preliminary working draft discussed at Stockholm meeting of SC 27 in May 2012.
- 1st Working Draft (WD) circulated in June 2012, and discussed at the Italy meeting of SC 27 in October 2012.
- 2nd WD circulated in December 2012, and was discussed at the France meeting of SC 27 in April 2013.
- 1st CD circulated in June 2013 – to be discussed in the Korea meeting of SC27 in October 2013.

Further information

- To participate in the development of ISO/IEC 27018 please consider joining the work on SC 27/WG 5, via your national standards body.
- As editor I am always happy to provide information and answer questions – please contact me at me@chrismitchell.net.