

Tensions around the public cloud: ISO Standards and other Calming Measures

February 4, 2016

A way through the tensions

Tensions

- Should we be afraid of cloud?
- Does foreign cloud make a difference?

Calming measures

- Putting the abstraction of cloud in perspective
- Implementing the right safeguards
- Facing the fears
- Reaping the benefits

1. Should we be afraid of the cloud?



2. Does foreign cloud make a difference?



3. Putting the abstraction of cloud in perspective: Banking



4. Implementing the right safeguards

1. Cost benefit analysis

- Considering the organisation's IT resources, is its information safer on cloud?
- How important is scalability for the organization?
- How important is accessibility?
- How complex is information management?

Cost benefit analysis in a health care institution

Benefits

- Simplification of information management reduced IT staff costs
- Scalable infrastructure
- Tiered data storage
- Remote disaster recovery and business continuity
- Continuity of patient care
- Accessibility
- Comprehensive report generation
- Increased quality care

Risks

- Breaches through information sharing
- Data leakage in multi-tenancy clouds
- Loss of control through delocalization
- Of highly sensitive information

4. Implementing the right safeguards

2. Due diligence on,

- Organizational IT needs
- Sensitivity of personal information
- Privacy obligations
- Cloud provider
 - Record
 - Reliability
 - Undertakings
 - Financial viability

4. Implementing the right safeguards

3. A compliance framework – Jurisdiction:

- Applicable privacy law is the law of the cloud customer
BUT
- Laws of general application of the cloud provider continue to apply
 - The interesting case of *Microsoft v US 2015*
- The new General Data Protection Regulation will cover foreign processors such as cloud

4. Implementing the right safeguards

4. Compliance framework – Control:

The model of ISO 27018 *Code of practice for Personally Identifiable Information (PII) Protection in Public Clouds Acting as PII processors*

- Asserting cloud customer authority over data
- Requiring:
 - Data destruction or return upon request
 - Breach reports
 - Consultation on lawful access request
 - Disclosure of geolocation of servers
 - Breach notification
 - Audits

Facing the privacy fears

- Government surveillance
 - Ensuring cloud provider commitment to privacy
 - Requiring consultation on lawful requests
 - Avoiding clouds with data servers in State with “dubious records”
- Loss of technological control
 - Negotiating robust security clauses
 - Prohibiting independent use of data by cloud provider
 - Providing for compliance measures such as audits and reports
 - Favour ISO 27018 certified clouds

Reaping the privacy benefits

- More data security:
 - A reliable cloud, even abroad, is more secure than a fledgling local infrastructure
- More accountability for data protection:
 - Governance framework in contractual clauses
 - Appointment of a contact person
 - Transparency on security, measures and geo-localisation of servers
 - Independent compliance mechanisms

Thank you

大成 DENTONS

Dentons Canada LLP
99 Bank Street
Suite 1420
Ottawa, Ontario K1P 1H4
Canada

Dentons is the world's first polycentric global law firm. A top 20 firm on the Acritas 2015 Global Elite Brand Index, the Firm is committed to challenging the status quo in delivering consistent and uncompromising quality and value in new and inventive ways. Driven to provide clients a competitive edge, and connected to the communities where its clients want to do business, Dentons knows that understanding local cultures is crucial to successfully completing a deal, resolving a dispute or solving a business challenge. Now the world's largest law firm, Dentons' global team builds agile, tailored solutions to meet the local, national and global needs of private and public clients of any size in more than 125 locations serving 50-plus countries. www.dentons.com.

© 2015 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This document is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. We are providing information to you on the basis you agree to keep it confidential. If you give us confidential information but do not instruct or retain us, we may act for another client on any matter to which that confidential information may be relevant. Please see dentons.com for Legal Notices.