THE DARK CLOUD: DATA PROTECTION IN THE ERA OF CLOUD COMPUTING

Gillian Carter & Karen Reyes, Payments Canada

November 21, 2018

AGENDA

1. Introduction
2. Challenges of Cloud Computing
3. Cross-Border Data Protection Laws
4. CLOUD Act
5. GDPR
6. Takeaways for Managing Business Risk

What is Cloud Computing?

- Delivery of on-demand computing services or resources over a network on a pay-per-use basis

- Cloud-based applications run on distant computers (i.e. “cloud” platforms) that are owned and operated by others and that connect to users’ computers via the Internet

Cloud Models

SERVICE MODELS

- Software as a Service (SaaS)
  - end-user applications
- Platform as a Service (PaaS)
  - cloud platform service and management
- Infrastructure as a Services (IaaS)
  - databases
  - storage or backup
  - disaster recovery

DELIVERY MODELS

- Private
  - exclusive use, dedicated environment, customized for specific business requirements, most secure
- Public
  - multi-user platform, infrastructure available to the public
- Hybrid
  - use of private cloud foundation combined with public cloud services
  - preferred model

Benefits of the Cloud Model

- Cost effective and metered service - pay-per-use model; zero infrastructure or hardware costs for computing resources e.g. servers, networks, storage, data centres

- Access to innovative technologies - access to cutting edge business applications; develop applications for faster market availability

- Operational flexibility - innovative services available on demand; immunity from data loss

- Elastic resources and scalability - can scale to usage needs; infrastructure can support dynamic workloads

Challenges of Cloud Computing

- Data Governance
  - Ownership
  - Collection, storage, retention, transfer
  - Privacy and Security

- Third party vendors

- Statutory and regulatory requirements (PIPEDA; OSFI Guidelines)
  - Cross-border legislation (e.g. GDPR; US Cloud Act)

Cloud Computing Due Diligence

- Architecture – underlying technologies, type of cloud, meta data
- Ownership – who owns the data, where are data centres
- Retention – effectiveness, impact of multiple locations for storage
- Breach response and coordination – include in contracts

Cross-Border Data Protection Laws

- CLOUD Act
- GDPR
- California Consumer Privacy Act

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Canadian legislation that came into force April 13, 2000

- Applies primarily to the **collection, use, disclosure, and retention** of personal information in the course of commercial activity

Clarifying Lawful Overseas Use of Data (CLOUD) Act

- US legislation that came into force March 23, 2018
- application to US-based electronic communication and remote-computing service providers
- US government can compel service providers to disclose data stored on servers outside the US
- empowers foreign governments through executive agreements

Microsoft Ireland Case

- Illegal drug trafficking case
- US government sought disclosure of server in Dublin, Ireland
- Microsoft, U.S. based company, refused to disclose data stored outside US

EU’s General Data Protection Regulation (GDPR)

- EU legislation that came into force May 25, 2018
- To protect individuals in relation to processing of personal data; applies to both public and private sectors
- Most comprehensive privacy legislation to date
- Extends beyond EU borders

When does the GDPR apply?

(1) Processing of Personal Data

AND

(2) (a) Establishment within the EU; OR

(b) Outside the EU, if

- offering goods or services to data subjects in the EU, OR
- monitoring behaviour in the EU

Important Concepts under the GDPR

- **Personal Data**: any information related to an identified or identifiable natural person (“**data subject**”) e.g. business contact information, IP address

- **Processing:** any operation performed on personal data, whether automated or not e.g. collection, recording, storage

- **Controller**: determines the purpose and means of processing of personal data

- **Processor**: processes personal data on behalf of the controller

- **Data subject in the EU:** any human physically located in the EU

Weltimmo case

- **Establishment:** extends to “any real and effective activity — even a minimal one — exercised through stable arrangements
  - e.g. presence of a single representative may be enough

- **Intent is key** to determine **if** offering goods and services to data subjects or monitoring behaviour in EU e.g. use of EU language, currency, domain name

Legitimate Processing of Personal Data

Processing of Personal Data is lawful when:

- Consent obtained/given;
- Performance of a contract;
- Performance of task in the public interest;
- Compliance with legal obligations
- Protect vital interests of data subject or another individual;
- Legitimate interests pursued by controller or third party

Takeaways for Managing Business Risk

1. Examine existing data practices – compliance programs
   - specific purposes, minimal amount, retention as long as necessary
   - security controls (pseudonymization vs. anonymization)
   - processes to enable withdrawal of consent
   - data breach response plan
   - applicability of foreign data protection laws

2. Conduct rigorous vendor due diligence
   - internal due diligence (be selective)
   - rigorous third-party assessment (collection, management, use)
   - architecture and vulnerability testing

Takeaways (continued)

3. Identify key contractual issues
   - contracting parties and implications (jurisdiction, dispute resolution)
   - liability, indemnities
   - obligations for notification if processing
   - term and termination
   - service levels
   - regulatory requirements (OSFI Guidelines)

4. Inform and engage business partners/experts

QUESTIONS?

Contact Details

Gillian Carter
Legal Counsel, Payments Canada
gcarter@payments.ca

Karen Reyes
Legal Counsel, Payments Canada
kreyes@payments.ca

Thank You!

payments.ca