

Getting the Deal Done: Negotiating and Contracting Privacy Protections in Cross-Border Outsourcing Transactions

Kristine Robidoux, QC

Partner

Gowling Lafleur Henderson LLP

Calgary, Alberta

GOWLINGS

The Power of Original Thought

gowlings.com

Montréal | Ottawa | Toronto | Hamilton | Waterloo Region | **Calgary** | Vancouver | Moscow | London

The Dilemma

- Vast amounts of information + rapidly evolving technologies + business efficiencies = private sector nirvana
- Vast amounts of information + rapidly evolving technologies + daunting jurisdictional challenges = headache for privacy commissioners
- Requirement to ensure a “comparable level of protection” (PIPEDA)
- Accountability of organizations for the breaches of its contractors (PIPA)

Jurisdiction

- What are the laws of the country to which the information could be subject once transferred?
- Can personal information be made available to the foreign government under a lawful order made in that jurisdiction?
- Different levels of knowledge or awareness of privacy obligations in different locations
- A tale of two jurisdictions: Texas and India

Definitions

“Applicable Laws”

- All Canadian, US, or other applicable federal, state and provincial laws, statutes, codes, ordinances, decrees or other governmental rules and regulations
- Published policies and directives issued by the Office of the Privacy Commissioner of Canada, judicial or arbitral or administrative or ministerial or departmental or regulatory judgments, orders, decisions, rulings or awards applicable to the performance of the services under the Master Agreement
- Where applicable, should include common industry standards of practice related to data security, including the Payment Card Industry Digital Security Standards (“**PCI-DSS**”) and all Merchant 1 Tier 1 Processor Compliance requirements

Definitions

“Confidential Information”

- information, data and/or material which gives a party some competitive business advantage?
- the disclosure of which could be detrimental to the interests of a party?
- is marked “Confidential,” “Restricted,” or “Proprietary Information”?
- is known by the parties to be considered confidential and proprietary?
- from all the relevant circumstances should reasonably be known to be confidential and proprietary?
- is not generally disclosed to the public?

Definitions

“Personal Information”

“any and all data and information provided by Company to DataCo, or by Company’s customers to DataCo, or otherwise made accessible to DataCo that identifies or is identifiable to a person, including without limitation, an employee, contractor, or customer of Company, including without limitation: (i) such person’s name, address, email address, telephone number, password, passport information, payment card data as defined in the PCI-DSS, other personal financial information, other travel or reservation information, personal preferences, demographic data, marketing data, credit data, or any other identification data; (ii) any information that reflects such person’s interactions with Company, including without limitation information concerning computer search paths, any profiles created or general usage data; and (iii) any data otherwise submitted by such person in the process of registering for or using a Company service.”

Definitions

“Personal Information”

-VS-

“information about an identifiable individual”

Physically and Logically Secure Environment

- Require that Personal Information be housed in a facility with physical security controls including alarm systems, fire suppression, access controls (including off-hour controls) which may include visitor access procedures, security guard force, and video surveillance
- Require that DataCo maintain data security controls for such facility in order to protect and secure the Company Personal Information, including logical access controls with user sign-on identification and authentication, data access controls (e.g., password protection of applications, data files and libraries), anti-virus software, restricted download to disk capability and provision for system backup

Confidentiality Safeguards

- Maintain and enforce security procedures that provide technical and organizational safeguards against destruction, loss, alteration or unauthorized disclosure or access, including:
 - Policies and procedures
 - Communication and training for employees and contractors (including written instructions and acceptable use agreements with users)
 - Defense against hackers
 - Periodic testing
 - Secure storage (no laptop or other portable storage medium unless protected by then-current industry standard security mechanisms)
 - Secure destruction or disposal

Transmission from DataCo

- Approved encryption mechanism
- Maintain active anti-virus tools
- Only use compatible, Company-approved network communication programs for interactions with the Company network

Audit and Monitoring

- Access monitoring
- Annual SAS 70 or equivalent assessment and certification
- Where applicable, annual certification by Qualified Security Assessor of PCI-DSS compliance
- The right (but not the obligation) to audit DataCo's conformity with the compliance requirements (either by Company or third party, at Company's expense)

Demand For Information by Authorities

- If DataCo is requested or required to disclose any Company Personal Information, whether by oral questions, interrogatories, requests for information or documents, subpoena or other legal processes, DataCo will:
 - (i) promptly provide Company with written notice of any such request or requirement prior to any disclosure so that Company may seek an appropriate protective order or other appropriate remedy, or may waive compliance with the nondisclosure provisions of this Data Protection Agreement; and
 - (ii) comply with any applicable protective order or equivalent.
- If such protective order or other remedy is not obtained by Company, or Company waives compliance with the nondisclosure provisions of the Data Protection Agreement, DataCo will disclose only that portion of the Company Personal Information as to which it has been advised by legal counsel that disclosure is legally required; and DataCo will obtain reliable assurances that confidential treatment will be accorded to the Company Personal Information that is disclosed in response to such requests or requirements.

Breach Notification

- DataCo to notify Company immediately of any suspected or actual security or confidentiality violations of which it becomes aware
- In such case DataCo agrees to immediately terminate access to Company Confidential Information and to the Company network

Privacy Claim/Access Request

- DataCo shall immediately notify Company if it receives any legal or regulatory action related to Personal Information and agrees to cooperate with Company in investigating and responding to any complaint or inquiry
- DataCo shall promptly assist Company in disclosing to an individual, the nature of the use and disclosure of any Personal Information obtained as well as the particular Personal Information held by Company and DataCo as it relates to such individual, as may be required under Applicable Privacy Laws

Subcontractors

- Ideally, a prohibition against engaging any subcontractors without the prior express consent of Company
 - in the alternative –
- DataCo represents, covenants and warrants that it will not engage any subcontractors in connection with the Master Agreement unless it has reviewed that subcontractor's Personal Information privacy and security measures as they relate to the specific services to be provided by the subcontractor and has ensured that these measures are comparable to and in any event no less stringent than the measures imposed by the terms of this Data Protection Agreement

Conclusion

- An organization's primary means of protecting personal information in an outsource deal is through the legal contract
- Retain specialized counsel and understand at the outset of the negotiation what are the "need-to-have" provisions versus the "nice-to-have" provisions
- Measure by measure comparison not required
- But must assess all of the risks that could jeopardize the integrity, security and confidentiality of personal information
- Must take all reasonable steps
- Be transparent with your constituents about your information handling practices

Thank you

**Kristine Robidoux, QC
Partner**

**Gowling Lafleur Henderson LLP
kristine.robidoux@gowlings.com
403.298.1817**