Data Protection Agreements



Outsourcing and sub-contracting often make good sense from a business perspective. However, when an organization transfers personal information ("PI") about customers, employees or other individuals to a third party, it remains responsible for protecting such PI and ensuring that it is handled in accordance with applicable privacy laws.

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") explicitly provides that: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization **shall** use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."[1] (emphasis added) Similar explicit or implicit requirements exist under substantially similar provincial legislation.

Therefore, before transferring any PI to a contractor or service provider, organizations should ensure that appropriate steps have been taken to protect such information. This can include reviewing the privacy policies and past practices of contractors or service providers, as well as requesting information about prior privacy complaints and data breaches. It should also include appropriate contractual protections, either in the form of a full data protection agreement or privacy provisions in the service agreement itself.

Although such contracts should be customized in every case, to reflect the relationship between the parties, the nature of the services, and the amount and sensitivity of PI involved, generally such agreements should address the following:

- Ownership of PI
- The amount, type and nature of PI that will be transferred between the parties
- The purposes for which PI can (and cannot) be collected, used and disclosed
- Confidentiality obligations
- Restrictions on access to PI
- Physical, technological and organizational safeguards required to protect PI
- Updating, correcting and deleting PI
- Auditing, inspection and/or monitoring rights
- Restrictions on sub-contracting, or provisions governing terms upon which sub-contracting is allowed
- Compliance with applicable privacy laws
- Notice requirements and obligation to co-operate in the event of an access request

- Requirements to disclose government access requests or other disclosure orders (where permitted by law)
- Breach notification requirements
- Procedure upon termination of contract/relationship (e.g., requirement to return or irrevocably destroy PI)
- Timelines for compliance with the above obligations
- Consequences of failure to comply with data protection obligations in contract and/or applicable privacy laws (e.g., indemnities)

This list is not intended to be all-inclusive. Depending upon the circumstances, additional terms may be required. For example, in some cases the organization may want to restrict cross-border transfers of information (or at least require consent to, or notice of, such transfers), and/or require segregation of PI from other information held by the service provider.

In addition, specific provincial laws should be taken into account. For example, Quebec legislation contains specific requirements related to placing technology-based documents in the custody of a service provider.

In an era of increasing focus on privacy and rising class actions for data breaches, organizations cannot afford to ignore the information handling practices of their service providers and sub-contractors. Given their continued responsibility for protecting PI, all organizations would be well-advised to review their contracts with third parties to ensure that such agreements contain appropriate provisions governing privacy and security.

Article by Lyndsay A. Wasser