What Businesses Need To Know About Their Legal Obligations When Outsourcing Data Processing To Third-Party Service Providers

Did you know that Canadian businesses have legal obligations under Canada's federal privacy law, the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), when they engage third-parties to process personal data?

By now, Canadian businesses should be aware of their mandatory data breach reporting obligations under *PIPEDA*. In short, those obligations require Canadian businesses to:

1. report to the Office of the Privacy Commissioner ("OPC") breaches of security safeguards involving personal information under the organization's **control** if it is reasonable in the circumstances to believe that the breach of the security safeguard creates a real risk of significant harm to an individual or individuals;
2. notify the affected individuals about those breaches; and
3. keep records of all breaches.

What you might not be aware of is that these data breach obligations apply to your business even if it is your third-party data processor who suffered the actual data breach. Additionally, if your business transfers personal data to a third-party for processing, your business is legally obligated to ensure appropriate contractual terms are place with that third-party to protect the personal data while in the possession of the third-party.

Do You Use Third-Party Data Processors?

If you have a business, it almost certainly engages third-party service providers to process its data. For example, if your business uses any cloud services, you have engaged a third-party to process your data. Cloud services include things like online data storage, webmail, social networking websites, online business productivity applications, and software-as-a-service offerings. Any time you collect personal information about an individual (e.g. your

customers or employees) and store that information in the cloud, you have engaged a third-party to process personal data thereby triggering legal obligations under *PIPEDA*.

It is important to keep in mind that third-party data processors are not limited just to cloud services providers. Processing does not necessarily require the application of a computer. For the purposes of *PIPEDA*, processing is better understood as a use of personal information by a third-party service provider where the third-party did not directly collect the personal information from the individual who is the subject of the personal information, but instead received the personal information from the organization (e.g. a business) that directly collected the personal information and obtained consent to use the personal information for the purposes that the third-party is now carrying out on behalf of the organization (i.e. the entity that originally collected the personal information). Consequently, a third-party data processor could be, for example, a third-party call centre you engage to contact your customers about important product information, a payroll company that provides your business with payroll services, or an insurance provider that provides group benefits to your employees.

Who Is Responsible In The Event of a Data Breach

It would be reasonable to assume that if your business transfers personal information to a third-party for processing, and that third-party suffers a data breach related to such personal information, the third-party would be legally obligated to comply with the mandatory data breach reporting obligations under *PIPEDA*; however, this is not the case. It is the outsourcing organization (i.e. the transferor of the data) – and not the third-party service provider – who is responsible for compliance with *PIPEDA*'s mandatory data breach reporting obligations. This is because the reporting obligation falls upon the organization in ***control*** of the personal information, and the OPC has taken the position that it is typically the outsourcing organization, and not the third-party service provider, who has ***control*** of the personal information. Consequently, if you engage a third-party service provider to processes personal information that you have collected and that third-party service provider suffers a data breach, you (the outsourcing organization) have the reporting, notification, and record keeping obligations and the corresponding liability under *PIPEDA* for failure comply with those obligations.

PIPEDA Compliant Contractual Terms

Since *PIPEDA* holds the *customer* (i.e. the outsourcing organization) of the third-party data processor liable for data breach reporting, it is crucial that contracts involving third-party data processing expressly address the customer's rights, and the third-party service provider's obligations, upon the occurrence of a data breach. Without data breach terms in your contracts, you might not even be notified by your third-party service provider that a data breach has occurred. This lack of notice would obviously undermine your ability to comply with *PIPEDA*'s data breach reporting, notification, and record keeping requirements. But to make matters worse, failing to have appropriate contractual arrangements with your third-party processors regarding data security and breaches is in and of itself a violation of *PIPEDA*'s accountability principle, which states:

> *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.*

Unfortunately, third-party service provider contracts often completely omit data security and breach terms. This should be of immediate concern to customers of those third-party service providers, since the omission of contractual terms regarding data security and breaches places the customer in contravention of *PIPEDA* (regardless of whether or not a breach has actually occurred) and exposes the customer to significant risk and uncertainty should their third-party service provider suffer a data breach.

So what contractual arrangements should be implemented? For one, outsourcing organizations should ensure that their third-party service providers are obligated to notify the outsourcing organization of data breaches within the time periods required by *PIPEDA*. The third-party processors should also be obligated to ensure the notice contains enough information to enable the outsourcing organization to comply with *PIPEDA*'s mandatory data breach reporting obligations. This means that, at the very least, the notice should contain information concerning:

1. Date and time of breach;
2. Duration of the breach;
3. How the breach was discovered;
4. When the breach was discovered;
5. Type of security safeguard breached or whether breach occurred due to lack of security safeguard;
6. The type of breach;
7. Whether there is evidence of criminal intent or a state sponsored attack;
8. Who may have had access to the personal information;
9. Steps taken to mitigate harms flowing the breach and prevent future breaches;
10. The types of information involved (e.g. financial information, health information, etc.);
11. The number of affected individuals;
12. The names and contact information of the affected individuals; and
13. Other information that would enable the outsourcing organization to determine if the breach creates a real risk of significant harm to an individual.

Outsourcing organization should also contractually obligate third-party processors to:

1. comply with all applicable privacy and data security laws to which they are subject;
2. limit their use of the personal data to specific purposes;
3. not disclose personal data to third parties, subject to certain exceptions;
4. protect personal data from unauthorized access or breach by implementing security safeguards and controls;
5. investigate data breaches and take actions directed by the outsourcing organization to contain the breach; and
6. cooperate with the outsourcing organization in connection with the

outsourcing organization’s reporting and notification obligations.

Although a good starting point, the above is not a complete statement of all contractual terms that should be included in agreements with third-party data processors and is of course a simplification of a complex topic. Deciding upon and drafting appropriate data security and breach contract terms requires an analysis of the totality of your circumstances by experienced legal counsel knowledgeable in privacy law.

by David R. McHugh
Segev LLP