Goodmans LLP Update

Canadian Regulations Released About Breach Notification and Record-Keeping Requirements

Yesterday, the Canadian government published the *Breach of Security Safeguards Regulations* (the "Regulations"), which specify how organizations are to comply with the breach notification and record-keeping amendments that were made to Canada's federal privacy statute, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). The Regulations are aligned with similar requirements under Alberta's approach to breach notification and Europe's soon-to-be-implemented *General Data Protection Regulation* ("GDPR"), allowing for the continued free flow of personal information from the EU to Canadian organizations. Both the PIPEDA amendments and the Regulations will come into force on November 1, 2018, giving organizations, that have not yet done so, an opportunity to put in place systems to implement the new requirements.

See our April 5, 2018 Update, *Canada's Privacy Breach Notification Requirements Coming into Force*, for our summary of the relevant provisions of PIPEDA.

Breach Notification

Each organization will be required to report to the Privacy Commissioner of Canada any breach of security safeguards involving personal information under its control, if it is reasonable in the circumstances to believe the breach creates a *real risk of significant harm* to an individual. If this test is met, and unless otherwise prohibited by law, an organization will be required to notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control. Both the report to the Commissioner and notification to an individual must be made *as soon as feasible* after the organization determines that the breach has occurred.

The report to the Privacy Commissioner must be in writing and contain:

a. a description of the circumstances of the breach and, if known, the cause;
b. the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
c. a description of the personal information that is the subject of the breach to the extent the information is known;
d. the number of individuals affected by the breach or, if unknown, the approximate number;
e. a description of the steps the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
f. a description of the steps the organization has taken or intends to take to notify affected individuals of the breach; and
g. the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

Notably, an organization may submit the best information available at the time of reporting to the Privacy Commissioner and may submit follow-up notifications, if it becomes aware of new information.

The notification to an affected individual must contain:

a. a description of the circumstances of the breach;
b. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
c. a description of the personal information that is the subject of the breach to the extent the information is known;
d. a description of the steps the organization has taken to reduce the risk of harm that could result from the breach;
e. a description of the steps affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
f. contact information the affected individual can use to obtain further information about the breach.

The new regulation permits two approaches to sending such notification to affected individuals – direct and indirect. Direct notification can be done in person, by telephone, mail, email or "any other form of communication that a reasonable person would consider appropriate in the circumstances". This last form of direct notification allows for flexible forms of notification specific to the circumstances of a particular breach situation. Indirect notification (given by public communication or similar measure that could reasonably be expected to reach the affected individuals) is to be given where:

a. direct notification would be likely to cause further harm to the affected individual;
b. direct notification would be likely to cause undue hardship for the organization; or
c. the organization does not have contact information for the affected individual.

Record-Keeping

An organization will be required to keep and maintain – *for a minimum of 24 months after the day on which the organization determines the breach has occurred* – a record of every breach of security safeguards involving personal information under its control. The record-keeping obligation applies to *all* breaches, regardless of the risk of harm posed.

Such a record must contain information that enables the Privacy Commissioner to verify the organization's compliance with the breach notification requirements. In other words, the organization must keep sufficient records to show it is tracking personal information security incidents and properly evaluating the risk of harm to individuals. An organization must provide the Privacy Commission with access to, or a copy of, such records upon request.

For more information, please contact any member of our Privacy Law Group.

Key Contacts

Peter Ruby
pruby@goodmans.ca
416.597.4184

Monique McAlister
mmcalister@goodmans.ca
416.597.4255