PROTECTION OF PRIVACY AMENDMENT ACT (DATA BREACH NOTIFICATION)

NOTE:

This is drafted as an amending bill that would add a Part on data breach notification to the jurisdiction's privacy protection statute or statutes. For example, in Ontario, the draft Part, with appropriate modifications, might be added to Ontario's Freedom of Information and Protection of Privacy Act, Municipal Freedom of Information and Protection of Privacy Act and Personal Health Information Protection Act, 2004. For ease of reference, the draft Part is numbered Part X and begins at section 100.

It is assumed that Acts to which the draft Part might be added already include a definition of "personal information" or a similar term or terms (for example, "personal health information") for privacy protection purposes. Therefore, the draft Part uses the term "personal information" without defining it further.

It is also assumed that Acts to which the draft Part might be added provide for a body or an official (such as a privacy commissioner or ombudsman) with significant responsibility for ensuring that the privacy protection provisions of the Act are respected. The term "privacy authority" is used in the draft Part as a proxy for the body or official on whom such responsibility is imposed in each jurisdiction. The draft Part does not define "privacy authority" on the assumption that an equivalent term is defined or otherwise described in the parent Act.

It is also assumed that an Act (or a portion of an Act) to which the draft Part might be added specifies the holders of personal information to which the Act (or portion of the Act) applies. In some cases, application will be limited to organizations with a public sector character. In other cases, application will be broader. The draft Part defines the generic term "organization" broadly, but in each jurisdiction the term and its meaning will vary, depending on the terminology and scope of the parent Act.

Finally, it is assumed that the parent Act imposes on a holder of personal information the duty to protect it.

1. **The Act is amended by adding the following Part:**

PART X
DATA BREACH NOTIFICATION

Definitions

100. In this Part,

"harm" includes bodily harm, humiliation, damage to reputation, damage to a relationship, loss of an employment, business or professional opportunity, a negative effect on the credit record, damage to or loss of property, financial loss and identity theft; ("préjudice")

"organization" means a corporation, partnership, association, trade union or other entity and an individual acting in a professional, commercial or public capacity but not in a personal capacity; ("organisation")

Comment: The enacting jurisdiction will choose the term that suits its own statute.

"prescribed" means prescribed by the regulations made under this Act. ("prescrit")

Breach of privacy

101. For the purposes of this Part, a breach of privacy occurs with respect to personal information if,

(a) the information is accessed and the access is not authorized under this Act;

(b) the information is disclosed and the disclosure is not authorized under this Act; or

(c) the information is lost and the loss may result in the information being accessed or disclosed without authority under this Act.

Organization to report to privacy authority

102. (1) An organization that knows or has reason to believe that a breach of privacy has occurred with respect to personal information under its control shall report the breach of privacy to the privacy authority in accordance with this section if the breach is material.

Material breach of privacy — factors

(2) The factors that are relevant to determining whether a breach of privacy with respect to personal information under the control of an organization is material include,

(a) the sensitivity of the personal information;

(b) the number of individuals whose personal information was involved;

(c) the likelihood of harm to the individuals whose personal information was involved; and

(d) an assessment by the organization that the cause of the breach is a systemic problem.

Time of report

(3) The report required by subsection (1) must be made as soon as reasonably possible after the organization knows or has reason to believe that the breach of privacy occurred and determines that the breach is material.

Content of report

(4) The report required by subsection (1) must describe the steps taken by the organization to comply with section 103 and must contain such other information as may be prescribed.

Manner, etc., of making report

(5) The report required by subsection (1) must be made in the prescribed form and the prescribed manner.

Organization to notify individual

103. (1) An organization that knows or has reason to believe that a breach of privacy has occurred with respect to an individual's personal information under the organization's control shall notify the individual of the breach of privacy in accordance with this section if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual.

Real risk of significant harm — factors

(2) The factors that are relevant to determining whether a breach of privacy with respect to an individual's personal information creates a real risk of significant harm to the individual include,

(a) the sensitivity of the personal information; and

(b) the probability that the personal information has been, is being or will be misused.

Time of notice

(3) The notice required by subsection (1) must be given as soon as reasonably possible after the organization knows or has reason to believe that the breach of privacy occurred and determines that the breach of privacy creates a real risk of significant harm to the individual.

Content of notice

(4) The notice required by subsection (1) must contain,

(a) sufficient information to allow the individual to,

(i) understand the significance to him or her of the breach of privacy, and

(ii) take steps, if any are possible, to reduce the risk of, or mitigate, any harm to him or her that could result from the breach of privacy; and

(b) such other information as may be prescribed.

Manner, etc., of giving notice

(5) The notice required by subsection (1),

(a) must be prominently stated;

(b) must be given to the individual directly, subject to subsection (6); and

(c) must be given in the prescribed form and the prescribed manner.

Exception

(6) If circumstances in which it is not feasible for the notice to be given to the individual directly are prescribed, the notice must, in those circumstances, be given to the individual indirectly.

Comment: The regulations should be drafted to give organizations the clearest possible direction on when indirect notice of the privacy breach will be sufficient.

Organization to notify others

104. An organization that notifies an individual of a breach of privacy under section 103 shall, at the same time, also notify a government institution, a part of a government institution or another organization of the breach of privacy if,

(a) the government institution, the part of the government institution or the other organization may be able to reduce the risk of, or mitigate, any harm to the individual that could result from the breach of privacy; or

(b) a prescribed condition is satisfied.

Direction from privacy authority to organization

105. (1) If a privacy authority receives a report under section 102 about a breach of privacy with respect to personal information under the control of an organization and determines that the breach of privacy creates a real risk of significant harm to one or more individuals to whom the information relates, the privacy authority may direct the organization to *[recommend that the organization]*,

(a) take steps specified by the privacy authority relating to notifying those individuals about the breach of privacy, if the privacy authority is of the opinion that the steps taken by the organization to comply with section 103 were not sufficient;

(b)take steps specified by the privacy authority to limit the consequences of the breach of privacy; and

(c) take steps specified by the privacy authority to prevent the occurrence of further breaches of privacy with respect to personal information under the organization's control, including, without limitation, implementing or increasing security safeguards within the organization.

Comment: If a privacy authority in any jurisdiction does not have the power to issue directions, this section would provide for it to make a recommendation only. In that situation, subsection (2) would be removed or altered.

Organization to comply and report

(2) An organization to which a direction has been given by the privacy authority under subsection (1) shall take the steps specified in the direction within the times specified in the direction and shall give the privacy

authority reports about the organization's compliance with the direction within the times specified in the direction.

Disclosure by privacy authority

106. If a privacy authority receives a report under section 102 about a breach of privacy with respect to personal information under the control of an organization and determines that the breach of privacy creates a real risk of significant harm to one or more individuals to whom the information relates, the privacy authority may, despite section X *[insert the section of the Act that prohibits disclosure by the privacy authority]*,

(a) disclose the breach of privacy to the individuals in the manner that the privacy authority considers appropriate, if the privacy authority has given the organization a direction under clause 105 (1) (a) and the organization has not taken the steps specified in the direction within the times specified in the direction; and

(b) disclose the breach of privacy to the public in the manner that the privacy authority considers appropriate, if the privacy authority is of the opinion that the disclosure is in the public interest.

Comment: The power of the privacy authority to disclose that a breach has occurred an important safeguard for the interests of the individuals affected. If any provision of the parent Act puts in doubt the right of the privacy authority to make such a disclosure, then that provision should be overridden. In the absence of a prohibition, this section goes without saying and is probably unnecessary in implementing legislation.

If a privacy authority in any jurisdiction does not have the power to issue directions, the wording and operation of clause (a) will need reconsideration, though the power to disclose may still be exercised as stated.

Offences

107. (1) An organization that contravenes section 102, 103 or 104 or subsection 105 (2) is guilty of an offence.

Employees and agents

(2) In a prosecution of an organization for an offence under this section, any act or omission of an employee or agent of the organization acting in the course of employment or agency shall be deemed to be the act or omission of the organization, whether or not the employee or agent has been identified or has been prosecuted for the offence.

Individuals directing management of organization's affairs

(3) If an organization that commits an offence under this section is not an individual, each of the individuals who were directing the management of the affairs of the organization at the time the organization committed the offence is also guilty of the offence if he or she failed to take reasonable care to prevent the organization from committing the offence, whether or not the organization has been prosecuted for the offence.

Defence

(4) No individual or entity shall be convicted of an offence under this section if he, she or it establishes that he, she or it acted reasonably in the circumstances that gave rise to the offence.

Penalty

(5) Any individual who is guilty of an offence under this section is liable, on conviction, to a fine of not more than $100,000 and any entity that is guilty of an offence under this section is liable, on conviction, to a fine of not more than $500,000.

Limitation period

(6) A prosecution for an offence under this section shall not be commenced more than two years after the date on which the offence was, or is alleged to have been, committed.

Comment: The enacting jurisdiction has a choice: it can choose a specific limitation period and take steps to avoid a conflict with any other legislation providing a different limitation period; or it can choose to have the same limitation period apply to this offence as to other offences under the parent statute, in which case this provision may not be necessary.

Regulations

108. (1) The Lieutenant Governor in Council may make regulations,

(a) governing the content of the report required by subsection 102 (1);

(b) governing the content of the notice required by subsection 103 (1);

(c) prescribing anything that is referred to in this Part as prescribed or that is required or permitted by this Part to be done in accordance with, or as provided in, the regulations and for which a specific power is not otherwise provided in this Part.

Content of notice

(2) A regulation under clause (1) (b) may require that the notice describe,

(a) the scope of the personal information involved;

(b) the type of personal information involved;

(c) the nature and circumstances of the breach of privacy;

(d) the steps, if any, that the organization has taken to limit the consequences of the breach of privacy;

(e) the steps, if any, that the organization has taken to prevent the occurrence of further breaches of privacy with respect to personal information under its control;

(f) the plans, if any, that the organization has made to take steps of the kind described in clauses (d) and (e); and

(g) the steps, if any, that individuals who receive a notice might take to reduce the risk of, or mitigate, any harm to them that could result from the breach of privacy.