CAOB
CAROL ANNE O'BRIEN
BARRISTER & SOLICITOR

OFFICE 416·640·7270 MOBILE 416·399·6270 EMAIL caob@caobrienlaw.com FAX 416·368·5655 WEB caobrienlaw.com
151 Yonge Street, Suite 1500 Toronto, ON M5C 2W7

September, 2018

Privacy Breach Notification Requirements

Coming Into Effect on November 1, 2018

Businesses that collect, use and disclose the personal information of Canadian residents will now have to disclose any privacy breaches that may cause harm.

The new notification requirements come into effect on November 1, 2018. In general, organizations must give notice to affected individuals and to the Office of the Privacy Commissioner of Canada (the "Commissioner") about privacy breaches involving a "real risk of significant harm".

Context for the Changes to PIPEDA

Privacy legislation in Canada can be enacted both federally and provincially. The federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[1] generally applies to organizations and the personal information they collect, use, and disclose in connection with their commercial activities. Separate legislation applies to personal information collected and used by federal undertakings and businesses and all levels of government. Separate legislation also applies to personal health information.

British Columbia, Alberta, and Quebec have enacted equivalent legislation governing the collection, use, and disclosure of personal information in the private sector. This provincial legislation displaces PIPEDA in those provinces only when the personal information is collected, used, or disclosed within that province. PIPEDA generally applies when organizations transfer personal information across provincial or international boundaries.

The *Digital Privacy Act* was enacted in 2015 to amend PIPEDA. To allow time for new regulations to be developed, the amendments relating to mandatory breach notifications

[1] PIPEDA is posted on the Justice Canada web site at: http://laws.justice.gc.ca/eng/acts/P-8.6/

were delayed in coming into force. The *Breach of Security Safeguards Regulations*[2] (the "Breach Regulations") come into effect on November 1, 2018, along with the new provisions of PIPEDA.

What is a Breach and a "Real Risk of Significant Harm"?

PIPEDA defines a "breach of security safeguards" as the "loss of, unauthorized access to or unauthorized disclosure" of personal information resulting from a breach of an organization's security safeguards, or from its failure to establish the safeguards required by PIPEDA.[3] Organizations will now be obliged to disclose breaches of security safeguards involving personal information under its control "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." "Significant harm" is broadly defined to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."[4] Factors to be considered in determining whether a breach creates a real risk of significant harm to an individual include:(a) the sensitivity of the personal information involved in the breach; (b) the probability that the personal information has been, is being or will be misused; and (c) any other prescribed factor.[5]

Where the organization determines that there is a "real risk of significant harm to an individual", the breach must be reported to the Commissioner and to affected individuals.[6] Reports to other organizations, including government institutions, will also be required, if the organization believes that the other organization may be able to reduce or mitigate the risk of harm to the affected individuals.[7] Notifications must be made "as soon as feasible after the organization determines that the breach has occurred."[8]

---

2 The Breach Regulations are posted on the Justice Canada web site at: http://laws.justice.gc.ca/eng/regulations/SOR-2018-64/.

3 PIPEDA's definition, s. 2(1).

4 PIPEDA, Division 1.1, s. 10.1(7).

5 PIPEDA, Division 1.1, s. 10.1 (8).

6 PIPEDA, Division 1.1, s. 10.1(1) and (2) for the Commissioner, and Division 1.1, s. 10.1(3) to (6) for affected individuals.

7 PIPEDA, Division 1.1, s. 10.2.

8 PIPEDA, Division 1.1, s. 10.1 (6).

Breach Regulations: Notification Requirements and Record Keeping

The Breach Regulations establish requirements for the content, form, and manner of the notifications, and requirements for records to be retained by the organization:[9]

Notifications to the Commissioner	Notifications to Affected Individuals
(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 that 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 that 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 that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of the Act; 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.	(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 that the information is known; (d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach; (e) a description of the steps that 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 that the affected individual can use to obtain further information about the breach.

Direct notification to affected individuals must be provided "in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances"[10]. This will be determined in the context of the relationship between the organization and the person, and the nature of the breach. Indirect notification (e.g. via the organization's website) may be appropriate in circumstances where:

---

[9] Breach Regulations, s. 2(1) for the report to the Commissioner and s. 3(1) for notifications to affected individuals.

[10] Breach Regulations, s. 4.

(a) direct notification would be likely to cause further harm to the affected individual;
(b) direct notification would be likely to cause undue hardship to the organization; or
(c) the organization does not have contact information for the affected individual.
Where used, indirect notification must be given by public communication or similar measure "that could reasonably be expected to reach the affected individuals."[11]

Organizations must maintain a record of every such breach for 24 months from the date that it determined a breach had occurred. Such records must be provided to the Commissioner on request to verify compliance with all requirements of PIPEDA.[12]

Preparing to Comply

Organizations that comply with the *General Data Protection Regulation* that now applies in Europe may already have established internal controls to ensure compliance with those breach notification requirements. These controls will likely be sufficient to comply with the new Canadian requirements. However, all organizations should review the new requirements of PIPEDA and make any necessary changes to procedures relating to the collection, use, and disclosure of personal information, so that as of November 1, 2018 they will quickly be able to complete the required notifications in the event of a breach. The Commissioner's Office provides guidance in "Key Steps for Organizations Responding to Privacy Breaches".[13]

Please address any questions about the new privacy breach notification requirements, or about other privacy or advertising and marketing issues, to Carol Anne O'Brien at caob@caobrienlaw.com, or (416) 640-7270.

Carol Anne O'Brien's law practice is focused on regulatory matters including communications law (broadcasting and telecommunications), competition law, advertising and marketing, Internet domain names and privacy.

---

11 Breach Regulations, s. 5 (1) for circumstances and (2) for form and manner.

12 Breach Regulations, s. 6.

13 The Home page of the OPC is at https://www.priv.gc.ca/en/ and the "Key Steps" Guidelines are at: https://www.priv.gc.ca/media/2086/gl_070801_02_e.pdf.