WeirFoulds LLP

Privacy Breaches: New Mandatory Notification Requirements Under PIPEDA

November 1, 2018

By John Wilkinson,

As of November 1st, 2018 new mandatory breach notification and record-keeping requirements under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and the *Breach of Security Safeguards Regulations* came into force.

A privacy breach is the loss of, unauthorized access to, or unauthorized disclosure of, personal information. Breaches can happen when personal information is stolen, lost or mistakenly shared.

Organizations subject to PIPEDA will be required to:

- report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals
- notify affected individuals about those breaches
- notify any other organization that may be able to mitigate harm to affected individuals; and
- keep records of all breaches.

Deliberate failure to report a data breach, or deliberate failure to notify an individual as required will be separate offences subject to fines of up to $100,000. In the case of notification to individuals, it will be a separate offence for every individual left without notification of the breach. Deliberate failure to keep, or destroying, data breach records will also be an offence, subject to a fine of up to $100,000.

What kind of breach requires reporting?
Not all breaches which involve personal information under your control need to be reported, only those breaches in which it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to an individual. The number of persons affected by the breach is irrelevant – if there is a real risk of significant harm arising from the breach, then it must be reported. The record of the breach must be kept for 24 months after the day on which the breach occurred, whether there is a real risk of significant harm or not.

How do I determine what constitutes a real risk of significant harm?
Significant harm includes 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. To determine whether a real risk of significant harm is posed by the breach, one must conduct a risk assessment considering both the sensitivity of the information involved, and the probability that the information will be misused.

When and how must notice be given?

Organizations must report a breach to the Privacy Commissioner "as soon as feasible after the organization determines that [a breach of security safeguards] has occurred" using a PIPEDA breach report form.

WeirFoulds can assist with considering, and appropriate reporting regarding, any actual or possible privacy breach scenario. Please contact John Wilkinson or Ada Keon with any questions you may have.

For more information or inquiries:

John Wilkinson

Toronto
416.947.5010

Email:
jwilkinson@weirfoulds.com

John Wilkinson practises corporate and commercial law for universities, not-for-profit organizations, charities, self-regulatory bodies, owner-managed businesses, and associations (including industry associations and sport organizations).

Toronto

Email: