Human Resources Legislative Update

Reminder: Mandatory Data Breach Notification in Force on November 1, 2018

Date: October 10, 2018

As we previously reported, as of November 1, 2018, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will require notification to affected individuals and the federal Office of the Privacy Commissioner (OPC) when a security incident involving personal information results in a "real risk of significant harm."

The supporting regulations published March 27, 2018 set out the requirements for:

- the content, form, and manner of the report required to be provided to the OPC by an organization in the event of a breach of security safeguards involving personal information if it is reasonable to believe that the breach creates a real risk of significant harm to an affected individual
- the content of the notification organizations are required to provide individuals affected by a breach of security safeguards
- record-keeping and the length of time (24 months) organizations must maintain a record of every breach of security safeguards

The federal Office of the Privacy Commissioner has published a consultation draft overview of information relating to the reporting of breach security safeguards, which at this point includes:

- additional guidance on interpreting and applying the "real risk of significant harm test" to determine whether an organization has a reporting obligation when its security safeguards are breached
- direction on the record-keeping obligations for all breaches of safeguards for personal information, even where the "real risk of significant harm" test does not warrant formal reporting
- clarification for the information that must be provided to affected individuals in the required notification, and guidance on whether notification can be done indirectly
- direction on circumstances in which third party organizations may need to be notified if doing so could "reduce the risk of harm that could result from the breach or mitigate the harm"
- notably, if more than one organization has control of the same information that was subject to a breach, a requirement that the organizations submit a report to the OPC (regardless of whether or not an organization was directly involved in the incident).

Organizations should measure their policies against these practice points and the new PIPEDA requirements. If you would like our assistance with this, please contact a member of our Information, Data Security and Privacy Practice Group