Human Resources Legislative Update

Federal Government Consults on PIPEDA Data Breach Regulations

Date: April 1, 2016

On March 4, 2016, the federal government posted Data Breach Notification and Reporting Regulations (Regulations) for public discussion.

Amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) enacted by the *Digital Privacy Act* (Bill S-4) will, upon proclamation, require private sector organizations to notify the public in circumstances where security safeguards involving their personal information have been breached, and the breach creates a real risk of significant harm. These PIPEDA amendments, which create a new Division 1.1 (Breaches of Security Safeguards) are not yet in force pending finalization of supporting regulations. However, when proclaimed, they will further require organizations to report these potentially harmful data breaches to the Privacy Commissioner of Canada.

The discussion paper seeks stakeholder input around a number of specific and key implementation issues, including:

- **Determination of "real risk of significant harm."** The assessment of risk and specifically, additional prescribed relevant factors or presumptions, if any.
- **Form and content of reports to the Privacy Commissioner.** The prescribed form and content of mandatory reports to the Privacy Commissioner, and whether the reports should contain assessments of the type, and likelihood of, harm that may occur.
- **Form, content and manner of notification to individuals.** Elaboration of additional criteria for the provision of "sufficient information" as well as permissible manners of direct and/or indirect notification to ensure conspicuous and effective communication to the individual.
- **Notification to other organizations.** Mandatory notification for prescribed organizations, if any, and under which circumstances.
- **Form, content and maintenance of data breach records.** Prescribed information to be included for the purposes of maintaining a data breach record, as well as a prescribed framework for retention.

The regulations will have a critical impact on federally-regulated employers and organizations that handle personal information in the course of commercial activity. Stakeholders and invited to provide input and views on the discussion paper by May 31, 2016.