Human Resources Legislative Update

PIPEDA Breach of Security Safeguards Regulations Published

Date: April 19, 2018

Beginning November 1, 2018, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will require private sector organizations to provide notice 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, Breach of Security Safeguards Regulations, have now been published. Among other things, the Regulations set out the requirements for:

- the content, form and manner of the report required to be given to the OPC by an organization in the event of a breach of security safeguards involving personal information under its control where it is reasonable to believe that the breach creates a real risk of significant harm to an individual
- the content of the notification required to be given by organizations to individuals affected by a breach of security safeguards (this is in addition to the notification requirements set out in section 10.1(4) of PIPEDA, which states that the notification must contain “sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm”)
- the manner of direct notification required to be given by organizations to affected individuals, or, where applicable in specified circumstances, the manner of indirect notification
- record-keeping and the length of time (24 months) organizations must maintain a record of every breach of security safeguards after the day on which the organization confirms a breach has occurred (note that this would include breaches that do not pose a real risk of significant harm).