BLG PUBLICATION

Borden Ladner Gervais

Impact of the New Mandatory Breach Notification Requirements under PIPEDA on Pension Plan Administration

Thursday, October 18, 2018

New mandatory breach notification and record keeping requirements in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will come into force on November 1, 2018. Where PIPEDA applies, these new requirements will have significant implications for the administration of pension plans since plan administration necessarily involves the collection, use and disclosure of the personal information of plan beneficiaries.

Applicability of PIPEDA

PIPEDA is the federal privacy legislation that applies to the collection, use, disclosure, maintenance and destruction of personal information by federal undertakings (*e.g.*, banks), in the course of both employment relationships and commercial activities. It also applies to the collection, use, disclosure, maintenance and destruction of personal information by other private sector organizations in provinces that do not have their own private sector privacy legislation (*e.g.*, Ontario) in the course of commercial activities (*e.g.* plan administration), although not to employee personal information collected, used, disclosed, maintained or destroyed by the private sector organization acting as employer in relation to the pension plan.

New Mandatory Breach Notification Requirements

Under the new breach notification requirements, the organization which is "in control" of personal information is required to report a breach of security safeguards involving personal information where it is reasonable to believe that the breach creates a "real risk of significant harm to individual(s)". A breach of security safeguards refers to the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of the security safeguards required under PIPEDA or the failure to have in place such safeguards. "Significant harm" is very broadly defined to include humiliation, loss of employment, professional or business opportunities. The reporting obligation arises where it is reasonable to believe that a breach creates a real risk of significant harm. PIPEDA sets out the factors the organization needs to consider in determining whether there is such a risk.

The notification requirements involve a number of steps and compliance will be aided by establishing policies and procedures. Notification is required to be given to the Privacy Commissioner of Canada (Commissioner), affected individuals, and any other organization or government institution if it is believed that notifying such organization or institution may reduce the risk of harm or mitigate the harm resulting from the breach. PIPEDA sets out the minimum required content for notification, when and how notification needs to be given. The required content differs to certain extent, depending on whether notification is to the Commissioner or affected individuals.

Record Keeping Requirement

Organizations that are subject to the new mandatory breach notification requirements are also required to keep and maintain a record of every breach of security safeguards. The

record must contain sufficient information to enable the Commissioner to verify the organization's compliance with the notification requirements and be retained for 24 months after the date on which the organization determines that the breach has occurred.

Required Actions for Pension Plan Administrators

The new requirements come into force in less than a month. Where PIPEDA applies, pension plan administrators should take appropriate steps to ensure that they will be in a position to comply with the new requirements. Here are some of the recommended actions:

- If plan administration has been outsourced in whole or in part, determine who is "in control" of personal information.
- Review outsourcing agreements to determine whether they need to be amended to make it clear whether the service provider or the plan administrator (or both) is subject to the new notification and record keeping obligations. If the plan administrator is the organization that is subject to the new requirements, whether it needs any contractual covenant from the service provider to provide information to enable the administrator to comply with the requirements.
- Ensure that policies and procedures are in place to aid compliance, (*e.g.* providing direction on who employees are to contact if they become aware of a breach, how breaches are to be investigated, who is responsible for determining whether notification is required and whether any changes should be made to avoid similar breaches).
- Review the guidelines issued by the Commissioner to clarify the new requirements (currently in draft, but likely finalized in the near future).

If you have any questions about the new requirements, please contact Bonnie Freedman of our Privacy and Data Protection Group or any member of our Pensions and Benefits Group.

AUTHORS

Bonnie Freedman
T 416.367.6239
BoFreedman@blg.com

Sonia T. Mak
T 416.367.6171
SMak@blg.com

Borden Ladner Gervais

BLG OFFICES

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T +1.403.232.9500
F +1.403.266.1395

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T +1.514.954.2555
F +1.514.879.9015

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T +1.613.237.5160
F +1.613.230.8842

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415