INSIGHTS

November 2018

The changing landscape of privacy legislation and how it impacts your plan

By Domenic Barbiero

With the major data breaches in the news recently, privacy has become a hot topic. From a plan sponsor's standpoint, it's important to know your members' personal information is protected. Data privacy and security has become a key issue where the collection, use, disclosure and storage of personal information is involved. And that includes the administration of pension and benefits plans, where data-sharing can involve many third parties acting as plan agents.

The requirement to comply with pension, benefit and income tax legislation is a primary responsibility for pension and benefits plans, but the issue of data privacy should also be a high priority. Plan administration involves collecting and using highly sensitive personal information, such as health information, spousal status, marriage breakdown information and union membership.

Domenic Barbiero, FCIA, FSA

Mr. Barbiero, a principal at Eckler, has been advising pension plans for over 15 years and specializes in working with multi-employer plans.

All views expressed are the author's own and do not necessarily reflect the official position of any agency, organization, employer or company.

Canada's current privacy laws

Data protection laws set out rules for organizations who use or store personal data, and give rights to those whose data has been collected. In Canada, the most recognized private-sector privacy law is the Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Private-sector privacy legislation exists at the provincial level in Alberta, British Columbia and Quebec. Health privacy legislation also exists in Ontario, New Brunswick, Newfoundland & Labrador and Nova Scotia.

While the principles are generally consistent, with the current patchwork of privacy laws, it can be challenging for plans to know which laws apply to them and what they need to do to comply. And in May 2018, a new standard was implemented by the European Union (EU): the General Data Protection Regulations (GDPR), thought to be the world's strictest data protection regime. One of the most remarkable aspects of the GDPR is that they have global reach and may apply to pension and benefits plans operating in Canada.

PIPEDA and the GDPR: what's the difference?

All organizations that offer goods or services to EU residents or monitor their behaviour will need to comply with the GDPR, regardless of where those organizations are based. However, practical application of the GDPR to Canadian pension and benefits plans is still unclear. Even if it does apply, where do these cases of limited exposure land in the EU supervisory authorities' queue for monitoring compliance? A plan member complaint may attract attention and move the issue up the priority list for further investigation. Therefore, a starting point for addressing the GDPR is determining the plan's exposure by identifying how many EU residents are in the plan membership. For example, a pension plan may have retired members or other former members entitled to benefits who have moved to the EU after working in Canada.

Non-compliance with any of the privacy laws noted earlier can result in a fine, depending on the nature of the violation. The maximum administrative fine under the GDPR is the greater of €20 million or 4% of the organization's total global revenue – compared with PIPEDA, where the maximum fine, in certain cases, is $100,000.

As previously noted, the GDPR may be considered stricter than Canada's current privacy laws in several key areas – for example, consent and portability. Under PIPEDA, an individual's consent is a necessary condition for the collection, use and disclosure of personal information (subject to limited exceptions). However, consent can be explicit or implied. Under the GDPR, there is no concept of implied consent; it must be explicit.

One way this impacts pension and benefits plans is the forms (whether paper or electronic) used to collect members' personal information. Does the mechanism for submitting personal information satisfy the requirement for explicit consent?

Data portability is a requirement under the GDPR, but not under PIPEDA. Under the GDPR, the right to data portability gives individuals control over their personal information, meaning they have the right to request and receive their personal data in a structured, commonly used, machine-readable format. Systems may have to be upgraded to meet these requests in an efficient manner.

Continued...

Whether or not the GDPR apply to your plan, their introduction may be part of a trend toward stricter privacy laws worldwide. For example, effective November 1, 2018, there are new breach notification requirements under PIPEDA more in line with the stricter requirements under the GDPR. Each plan should review its own unique circumstances to determine the best course of action. Whether plan administrators choose to implement changes immediately to be fully compliant with the GDPR or set a course of action to reach compliance over time, compliance with more stringent privacy laws seems inevitable – and costly to ignore.

Eckler
CONSULTANTS + ACTUARIES

Connect with us:

Halifax
902-492-2822

Montreal
514-395-1188

Quebec City
418-780-1366

Toronto
416-429-3330

Winnipeg
204-988-1586

Vancouver
604-682-1381

Barbados
246-228-0865

Jamaica
876-908-1203

eckler.ca