MANDATORY DATA BREACH NOTIFICATION IN CANADA QUICK GUIDE

In June 2015, the Digital Privacy Act was passed into law. This act made a number of important changes to the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, including new language relating to what constitutes valid consent when collecting personal information and a new provision allowing the Privacy Commissioner to enter into compliance agreements with organizations to ensure that they comply with PIPEDA. Most of these changes were implemented straight away. However, the sections of the act relating to mandatory breach notification and record-keeping do not come into force until 1st November 2018. With the deadline fast approaching, organizations should be aware of what is required of them in order to ensure that they are in compliance with these changes.

WHAT IT IS

Simply put, the amendments coming into force on the 1st November now make it mandatory for applicable organizations in Canada to notify in cases where a privacy breach creates "a real risk of significant harm to the individual," and to maintain a record of every privacy breach that the organization suffers.

WHO IT WILL APPLY TO

The changes will apply to all those organizations with pre-existing obligations under PIPEDA. This means that any commercial (for profit) organization that uses, collects or discloses personal information in the course of their business activities will have to comply. PIPEDA does not generally apply to not-for-profit organizations or those commercial organizations operating in regions (Alberta, British Columbia & Quebec) where provincial laws have been deemed substantially similar to PIPEDA, unless the personal information that they hold crosses provincial or national borders.

WHAT IT WILL REQUIRE ORGANISATIONS TO DO

The Digital Privacy Act will require applicable organizations to notify affected individuals and the Commissioner of privacy breaches that are likely to cause a "real risk of significant harm to the individual." "Significant harm" is deemed to include, amongst other things, humiliation, damage to reputation or relationships and identity theft. Deciding on what constitutes "a real risk" requires reflection on the sensitivity of the information in question, the likelihood of misuse and any other prescribed factor.

In those cases where a privacy breach creates a real risk of significant harm, organizations must give notice "as soon as feasible" after the breach has been discovered. Notification can be given "in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances." The information a notification needs to contain differs between those that are sent to the Commissioner and those that are sent to affected individuals, but the content requirements common to both include:

- A description around the circumstances of the breach, including the day on which, or the period during which, the breach occurred;
- A description of the personal information affected by the breach;
- A description of the steps the organization has taken to reduce the risk of harm that could arise from the breach;
- Contact information to allow either the Commissioner or an affected individual to find out more about the breach.

CONCLUSION

The introduction of these notification and record-keeping requirements marks a significant change to the legislative environment in Canada, and those organizations affected will have to make sure that they are aware of their obligations under act, because failure to comply can result in fines of up to **$100,000** per offence.

That said, although this is an important change, it is important to note that dealing with a data breach isn't the only cyber risk that businesses face. Canadian organizations have had to deal with cyber risks for some time now, and there has already been a large number of cyber insurance claims in Canada for issues like cyber crime and system business interruption. The Digital Privacy Act adds to these exposures, but it certainly doesn't replace them. It also doesn't mean that those entities that are not subject to PIPEDA are free from cyber risk.

And while these changes will increase the privacy risk for organizations in Canada, it is unlikely that this will result in a US-style privacy landscape anytime soon. US legislation, regulatory appetite and litigation culture are still very different when compared to Canada.

USEFUL LINKS

- Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/
- Government of Canada: http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html
- Fasken: https://www.fasken.com/en/knowledgehub/2018/04/important-new-rules-for-mandatory-privacy-breach-notification