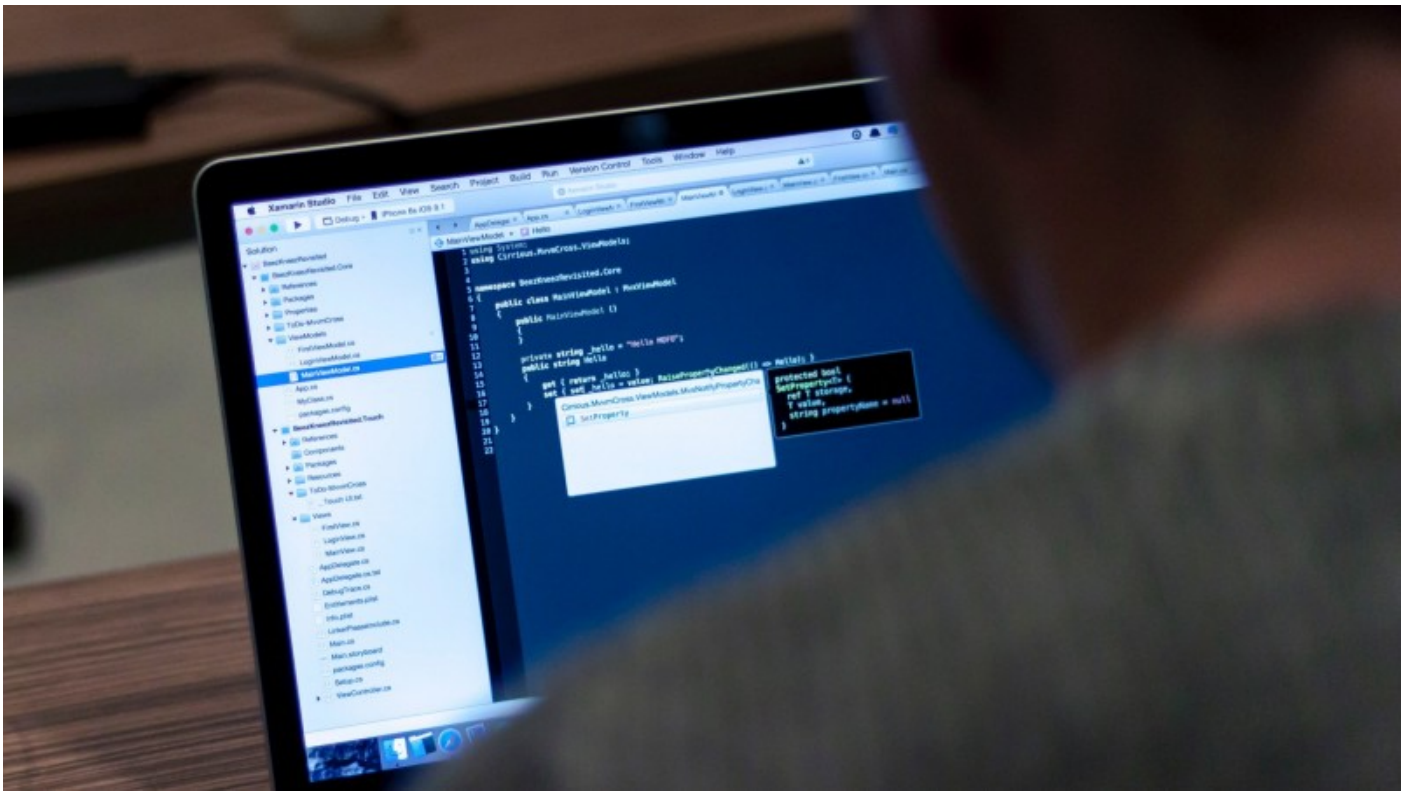
CLYDE&CO

INSIGHT

SEPTEMBER 8, 2017

Data breaches in Canada: New reporting rules released

At last, the federal government has released proposed regulations dealing with breach reporting, notification and recordkeeping for private sector data breaches. As things stand today, and setting aside sector specific statutes, only in Alberta are companies legally required to report on these events.



Non-compliant organizations will face fines ranging from $10,000 to $100,000

For a bit of background, Canada's Personal Information and Electronic Documents Act (PIPEDA) establishes a framework for the private sector's collection and use of individuals' personal information across Canada. PIPEDA does not apply to organizations whose operations take place entirely within provinces that have put in place

privacy legislation that is deemed “substantially similar” to PIPEDA. Québec, Alberta and British Columbia have such privacy laws in place.

Canada now in line with modern regulations

The changes are long overdue. It has been more than two years since PIPEDA was amended to require that organizations keep a record of every breach, and notify affected individuals as well as Canada’s privacy regulator, where there could reasonably be a risk of “significant harm.” “Significant harm” contemplates a range of scenarios, from humiliation and reputational damage loss to property and financial losses.

The government drafted those requirements, however, in large and broad terms. They cannot practically come into force until regulations are in place to prescribe a proper format for breach notifications. The proposed new rules do just that, and bring Canada in line with other regimes around the world in the context of increasing regulation, including the EU’s General Data Protection Regulation (GDPR) which is set to come into force in May 2018.

And once they are in place, non-compliant organizations will face fines ranging from $10,000 to $100,000, depending on the nature of the offence.

Detailed regulations mandatory to respect

Briefly, Ottawa’s proposed regulations detail the following:

- A list of information that must be included in a data breach report sent to Canada's Privacy Commissioner;
- A list of information to be notified to individuals who could potentially suffer from such breaches;
- The manner by which direct notification can be made to individuals (by email, letter, telephone or in person);
- The manner by which indirect notification can be made to individuals (a conspicuous message on the organization's website for a period of 90 days or by other advertising means likely to reach the affected individuals);
- The circumstances in which indirect notification is to be given (namely when direct notification would cause additional harm, or would be prohibitive to the organization; or when the organization is missing the proper contact information);
- The mandatory record-keeping period following the data breach (24 months of the day at which the organization has cognizance of the breach).

Those requirements address what an organization must do when a breach must be notified. Unfortunately, they bring no additional clarity to where the threshold for notification lies and what, in fact, poses a “reasonable risk” of significant harm to an individual.

This is certainly a clear reminder that organizations need to continue to work actively to prepare for mandatory breach requirements soon to be in force. This will be a challenge, given what is perceived by some as a certain vagueness when it comes to the actual application of these new rules.

Contact us to know more about data beach & insurance coverage →

ent

t of Canada – jurisdictions without

10 JULY, 2017

The Genetic Non-Discrimination Act – too little too late

the Canada-Europe trade deal will

11 APRIL, 2017

Data breaches and cyber attacks: How ready is your organisation?

2015

ι Privacy Update - December 2015

18 MARCH, 2015

Data Breach, Class Actions and Certification: Québec Turns Off the Tap…

Authors

Nathalie David
Partner

Samuel Robichon
Associate

More by the authors

- The Genetic Non-Discrimination Act – too little too late
- CETA : How the Canada-Europe trade deal will affect insurers
- Supreme Court of Canada – The solicitor-client privilege not far from absolute
- Canadian class actions on data breach: the good corporate citizen and…
- Quebec: Mandatory liability coverage can be annulled on the basis of…

Categories

Sectors

Cyber | Insurance & Reinsurance

Services

Commercial | Data Breach, Response & Recovery | Data Protection & Privacy | Data Security | E-commerce | HR Data Management | Insurance | Regulatory & Investigations | Technology

Locations

Montréal | The Americas | Toronto

Type

Français | Corporate Insurance Newsletter | Corporate Insurance Regulatory Update | Legal developments

Tags

canada | data breach | gpdr | personal informations | pipeda | privacy