David Young Law
Compliance Bulletin

September 2017

Proposed Breach of Security Safeguards Regulations published

On September 2, 2017 the federal government published its proposed *Breach of Security Safeguards Regulations* under the new breach reporting provisions of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). The breach reporting provisions were enacted by the *Digital Privacy Act* but are not yet in force pending publication of the final regulations.

These mandatory provisions will require organizations to report to the Office of the Privacy Commissioner of Canada ("OPC") any breach of security safeguards involving personal information within their custody or control where such breach poses a "real risk of significant harm" to any individual whose information has been compromised. As well, they require that notification of the breach be given to such individuals. Furthermore, the provisions require organizations to maintain records of *all* breaches involving personal information within their custody or control.

The proposed regulations address three key requirements:

- information required to be included in a report to the OPC
- information required to be included in notifications to individuals
- certain specifics regarding the requirement to maintain records

Why are they important

In addition to a "heads-up" regarding the full scope of the breach reporting provisions, the release of the proposed regulations makes clear the expected timing of their coming into force. The proposed regulations have been published for a 30-day consultation, following which they will be finalized. Based on comments provided by Innovation, Science and Economic Development Canada ("ISED") in the *Regulatory Impact Analysis Statement* accompanying the proposed regulations, it can be expected that the breach reporting provisions will come into force next year - as early as May 1.

The significance of the imminent coming into force of the breach reporting provisions is that they will make mandatory practices and procedures for breach response that largely correspond with those currently being followed by many organizations. These practices correspond to voluntary guidance provided by the OPC and provincial privacy regulators. There now will be a clear statutory obligation to follow such practices; failure to comply with that obligation can result in penalties of up to $100,000 per offence and potentially a civil claim under PIPEDA's private right of action[1]. In addition to the specific

[1] PIPEDA, ss. 28, 14-17

requirements set out for reporting and notification of breaches, the regulations provide some guidance as to the nature of records required to be kept by organizations.

Reporting and notification requirements

Under the new breach reporting provisions, both the reporting requirement and the requirement to notify affected individuals only operate if it is reasonable to conclude that there is a "real risk of significant harm to an individual". To assist in making this determination, the PIPEDA provisions provide a non-exhaustive definition of "significant harm"[2] and identify factors relevant to determining whether there is a real risk of such harm to individuals[3]. The report to the OPC and notification of individuals must be made as soon as feasible after discovery of a breach.

The proposed regulations require that a report to the OPC must be in writing and must contain the following information[4]:

(i) the circumstances of the breach and, if known, the cause;
(ii) the day or period when the breach occurred;
(iii) the personal information subject of the breach;
(iv) an estimate of the number of individuals for whom there is a real risk of significant harm;
(v) the steps that the organization has taken to reduce the risk or mitigate the harm;
(vi) the steps that the organization is taking to notify affected individuals; and
(vii) contact information of a person at the organization with whom the OPC can communicate.

Notification of affected individuals must contain sufficient information to allow the individual to understand the significance of the breach and to take steps to reduce the risk of harm. The proposed regulations set out the minimum information that must be included, as follows:

(i) a description of the circumstances of the breach;
(ii) the day or period when the breach occurred;
(iii) the personal information subject of the breach;
(iv) the steps that the organization has taken to reduce the risk or mitigate the harm;
(v) the steps that the individual could take to reduce the risk or mitigate the harm;
(vi) a toll-free number or email address at the organization; and
(vii) information about the organization's complaint process and the individual's right to file a complaint with the OPC.

[2] S. 10.1(7)
[3] S. 10.1(8)
[4] While the OPC will receive and develop a file of all reported breaches, there will be no general public disclosure of such breaches. The procedure under the Alberta *Personal Information Protection Act*, which requires the Commissioner to make a determination as to whether notification of a breach is required, can be contrasted with the PIPEDA provision. The Alberta Commissioner publishes on her website a report of all breaches for which she has determined notification is required.

The proposed regulations stipulate that notification may be made by email or other secure means[5], postal mail, telephone or in person.

Indirect notification may be used if direct notification would cause further harm to the individual, the cost of direct notification would be prohibitive, or the organization does not have up to date contact information for the individual. Indirect notification may be given either by a conspicuous message posted on the organization's website for at least 90 days, or by an advertisement likely to reach the affected individuals[6].

Record-keeping requirements

The proposed regulations also provide certain guidance respecting PIPEDA's new requirement for organizations to retain records of all security breaches. An organization must maintain such records for a minimum of 24 months following the date on which it determined that a breach occurred. Such records must contain any information pertaining to a breach that enables the OPC to verify that the organization has complied with the mandatory reporting and notification requirements.

Neither the Act nor the proposed regulations contains a definition of a "breach of security safeguards" with the result that there is some lack of clarity as to incidents for which records must be kept. For example, is an intrusion or system failure that does not result in loss of data constitute such a breach? Furthermore, the stipulated requirements contain limited guidance as to the actual records to be kept[7].

Guidance from ISED and the OPC

In its *Regulatory Impact Analysis Statement*, ISED indicates that it will work with the OPC to develop guidance documents to assist organizations in regards to the record-keeping requirements. Guidance materials also will be developed in regard to additional factors to be considered when assessing the risks associated with a breach.

Forward-looking considerations

Publication of the federal government's proposed *Breach of Security Safeguards Regulations* provides important guidance to organizations in connection with the transition to PIPEDA's mandatory breach

[5] Email may be used if consented to by the recipient. It may be asked whether requiring "consent" for e-mail and other electronic communications notifying of an urgent matter such as a breach is appropriate. A more appropriate requirement might be along the lines of "if the individual is accustomed to receiving or would expect to receive such communications".

[6] In addition to notifying individuals, the organization is required to notify any other organization or any government institution of the breach if, by notifying, the organization believes that entity may be able to reduce the risk or mitigate the harm that could result; PIPEDA, s. 10.2(1).

[7] For reported breaches, the report to the OPC may be used as a record; however not clear is whether such report will suffice as the full record. Also not clear is whether, or to what extent, underlying data and internal investigation reports must be kept.

reporting provisions. There is a 30-day consultation period following which the regulations will be finalized and, following a further transition period of likely six to eight months, the breach reporting provisions and the regulations will come into force.

While some adjustments may be made to the proposed regulations following the consultation, it is unlikely that there will be major changes. Consequently, organizations can be informed by the proposed regulations as to key specifics of the reporting and notification requirements as well as the record-keeping requirement. Organizations should commence a review of their internal breach response policies and procedures and make required adjustments. They can be confident that the details set out in the proposed regulations will be reflected substantially in the final regulations.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.

© David Young Law 2017