LAPOINTE ROSENSTEIN MARCHAND MELANÇON
L.L.P. Attorneys

Newsletter

Commercial Law

May 2018

M^tre Marissa Carnevale

This newsletter was written in collaboration with Tania L. Pinheiro, student at law.

Privacy Law Update: New Rules for Data Breaches

On June 18, 2015, Canada's *Digital Privacy Act*[1] introduced several changes to the *Personal Information Protection and Electronic Documents Act*[2] (Canada) ("**PIPEDA**"), including the establishment of mandatory data breach record-keeping, reporting and notification requirements. These requirements and the formalities governing their application, as established under the *Breach of Security Safeguards Regulations*[3] ("**Regulations**"), will come into force on **November 1, 2018**.

As of that date, organizations that collect, use or disclose personal information of Canadian residents will be required to keep records of every breach of data security they suffer. A security breach is any situation where a *loss, unauthorized access or disclosure* of personal information occurs as a result of a breach of an organization's security safeguards or from a failure to establish those safeguards ("**Breach**").[4]

Where a Breach poses a "real risk of significant harm" to any individual, an organization will be required to report the Breach to the Privacy Commissioner of Canada ("**OPC**") and notify individuals whose personal information was affected by the Breach (the "**Affected Individuals**"), as well as other organizations that may be able to reduce the risk or mitigate the harm caused by the Breach.

Record-Keeping Requirements

The Regulations establish a mandatory retention period, requiring organizations to keep and maintain a record of *every* Breach involving personal information under their control, irrespective of whether they reach the "real risk of significant harm" threshold. Breach records must be kept for a minimum of **24 months** after the day of the Breach, as determined by the organization having suffered the Breach, and must include sufficient information to demonstrate that the organization is tracking data security incidents. The OPC must also be able to verify compliance as needed and Breach records must be provided to the OPC upon request.[5]

Reports and Notices

Under the new rules, organizations will be required to report to the OPC and notify Affected Individuals of any Breach involving personal information under the organization's control where the organization reasonably believes that the Breach creates a "real risk of significant harm" to an individual.[6] Where this occurs, organizations will also be required to notify any other organization or government institution if it believes they may be able to reduce the risk of harm or mitigate the harm that could result from the Breach.[7]

"Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record, as well as damage or loss of property.[8] In determining whether a Breach creates a "real risk of significant harm", organizations must consider various factors, including the sensitivity of the personal information involved in the Breach and the probability that the personal information has been or is being misused.[9]

The Regulations prescribe various details as to the information that must be included in data breach reports furnished to the OPC and in notices to Affected Individuals,[10] as well as the form and manner in which such reports and notices must be provided. In all cases, mandatory Breach reports and related notices must be sent as soon as feasible after an organization determines

that a Breach has occurred.[11] It is also possible for organizations to submit new information with respect to a Breach to the OPC upon discovery, even following an initial report.[12]

With respect to Affected Individuals, Breach notices must contain sufficient information to allow the person to understand the significance of the Breach and to take steps to reduce the risk of harm.[13] The Regulations encourage direct notification, either in person, by telephone, mail, email or any other reasonable form of communication.[14] However, indirect notification – i.e., by public communication or another similar method, such as an advertisement[15] – is also allowed when direct notification would be likely to cause further harm to the Affected Individuals or undue hardship for the organization, including in cases where it does not have contact information for the Affected Individuals.[16]

Provincial Legislation

In Quebec, the *Act respecting the protection of personal information in the private sector*[17] regulates the collection, use and disclosure of personal information. Therefore, the new data breach rules do not apply to an organization collecting, using or disclosing personal information in Quebec, unless the organization does it in connection with the operation of a federal work, undertaking or business, or if the organization discloses the information outside the province in exchange for consideration.[18]

Conclusion

Although the Regulations align closely with what is currently recommended in guidance issued by the OPC for voluntary data breach reporting,[19] organizations should ensure that they are ready to comply with these new mandatory data breach requirements by **no later than November 1, 2018**.

In order to properly comply with the requirements, organizations should consider implementing written policies regarding breach procedures, and ensure that systems are in place allowing for internal monitoring, tracking, record-keeping and reporting of all data breaches. Organizations should also work to develop written policies and systems allowing the conduct of risk assessments and the determination of when a "real risk of significant harm" has occurred for purposes of mandatory reporting and notification.

Organizations that fail to comply with these new rules could face fines ranging from $10,000 to $100,000, depending on the nature of the offence.

It is accordingly very important for businesses to promptly seek guidance in order to assess the legal risks to which they may be exposed as a result of the shifting legislative framework, and to verify their data security programs for compliance with the new rules.

1. RSC 2015, c 32.
2. RSC 2000, c 5.
3. Canada Gazette, Part 1, Vol. 151, No 35 – September 2, 2017.
4. *Supra note 2*, art 2(1).
5. *Ibid*, art 10.3(2).
6. *Ibid*, art 10.1(1) and 10.1(3).
7. *Ibid*, art 10.2(1).
8. *Ibid,* art 10.1(7).
9. *Ibid*, art 10.1(8).
10. *Supra* note 3, art 2(1) and 3.
11. *Supra note 2*, art 10.1(6) and 10.2(2).
12. *Supra* note 3, art 2(2).
13. *Supra note 2*, art 10.1(4).
14. *Supra note 2*, art 10.1(5); *Supra* note 3, art 4.
15. *Supra* note 3, art 5(2).
16. *Supra note 2*, art 10.1(5); *Supra* note 3, art 5(1).
17. CQLR, c. P-39.1.
18. *Supra note 2,* art 30(1).
19. "Regulatory Impact Analysis Statement", Data breach report to the Commissioner section.

For more information, please contact:

Marissa Carnevale
514 925-6324
marissa.carnevale@lrmm.com