Breach of Security Safeguards Regulations: SOR/2018-64

Canada Gazette, Part II: Volume 152, Number 8

Registration

March 27, 2018

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

P.C. 2018-368 March 26, 2018

Her Excellency the Governor General in Council, on the recommendation of the Minister of Industry, pursuant to subsection 26(1) [a] of the *Personal Information Protection and Electronic Documents Act* [b], makes the annexed *Breach of Security Safeguards Regulations*.

Breach of Security Safeguards Regulations

Interpretation

Definition of *Act*

1 In these Regulations, ***Act*** means the *Personal Information Protection and Electronic Documents Act.*

Report to Commissioner

Report — content, form and manner

2 (1) A report of a breach of security safeguards referred to in subsection 10.1(2) of the Act must be in writing and must contain

(a) a description of the circumstances of the breach and, if known, the cause;

(b) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;

(c) a description of the personal information that is the subject of the breach to the extent that the information is known;

(d) the number of individuals affected by the breach or, if unknown, the approximate number;

(e) a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;

(f) a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of the Act; and

(g) the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

New information

(2) An organization may submit to the Commissioner any new information referred to in subsection (1) that the organization becomes aware of after having made the report.

Means of communication

(3) The report may be sent to the Commissioner by any secure means of communication.

Notification to Affected Individual

Contents of notification

3 A notification provided by an organization, in accordance with subsection 10.1(3) of the Act, to an affected individual with respect to a breach of security safeguards must contain

(a) a description of the circumstances of the breach;

(b) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;

(c) a description of the personal information that is the subject of the breach to the extent that the information is known;

(d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;

(e) a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

(f) contact information that the affected individual can use to obtain further information about the breach.

Direct notification — form and manner

4 For the purposes of subsection 10.1(5) of the Act, direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.

Indirect notification — circumstances

5 (1) For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by an organization in any of the following circumstances:

(a) direct notification would be likely to cause further harm to the affected individual;

(b) direct notification would be likely to cause undue hardship for the organization; or

(c) the organization does not have contact information for the affected individual.

Indirect notification — form and manner

(2) For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.

Record-keeping

Record-keeping requirements

6 (1) For the purposes of subsection 10.3(1) of the Act, an organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred.

Compliance

(2) The record referred to in subsection 10.3(1) of the Act must contain any information that enables the Commissioner to verify compliance with subsections 10.1(1) and (3) of the Act.

Coming into Force

S.C. 2015, c. 32

7 These Regulations come into force on the day on which section 10 of the *Digital Privacy Act* comes into force, but if they are registered after that day, they come into force on the day on which they are registered.

REGULATORY IMPACT ANALYSIS STATEMENT

(*This statement is not part of the Regulations.*)

Issues

On June 18, 2015, the *Digital Privacy Act* (also known as Bill S-4) amended Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA or the Act), in a number of areas. A key change was the establishment of mandatory data breach reporting requirements.

These new provisions are set out in Division 1.1 of PIPEDA, but are not yet in force. The Regulations will provide further details pertaining to certain statutory requirements and will prescribe the process for the coming-into-force of the Regulations.

Background

Legislative framework

PIPEDA applies to the collection, use or disclosure of personal information by every organization in the course of a commercial activity. A commercial activity is defined as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or fundraising lists.

The federal government may exempt from PIPEDA organizations and/or activities in provinces that have adopted substantially similar privacy legislation. To date, Quebec, British Columbia and Alberta have adopted private sector legislation deemed substantially similar to PIPEDA. Further, Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia have adopted substantially similar legislation with respect to personal health information.

Even in those provinces that have adopted legislation that is substantially similar to the federal privacy legislation, PIPEDA continues to apply to (i) all interprovincial and international transactions by all organizations subject to the Act, and (ii) to federally regulated organizations — “federal works, undertakings or businesses” — such as banks, and telecommunications and transportation companies, in the course of their commercial activities.

The purpose of PIPEDA is to facilitate growth in the digital economy by ensuring that Canadians have trust and confidence in how organizations handle their personal information. The Act employs a principles-based approach that balances the privacy rights of individuals with the legitimate needs of businesses to use or exchange information.

Mandatory data breach reporting under PIPEDA

With the implementation of Division 1.1 of PIPEDA, organizations that experience a data breach — referred to in the Act as a “breach of security safeguards” — will have certain obligations, as follows:

- The organization must determine if the breach poses a “real risk of significant harm” to any individual whose information was involved in the breach (“affected individuals”) by conducting a risk assessment. The assessment of risk must consider the sensitivity of the information involved, and the probability that the information will be misused;
- When the organization considers that a breach is posing a real risk of significant harm, it must notify affected individuals and report to the Privacy Commissioner of Canada (the Commissioner) as soon as feasible;
- The organization must notify any other organization that may be able to mitigate harm to affected individuals; and
- The organization must maintain a record of any data breach that the organization becomes aware of and provide it to the Commissioner upon request.

Paragraph 26(1)(c) of PIPEDA provides the Governor in Council with the authority to make any regulations that are required under the Act. The objective of this regulatory proposal is to provide greater certainty and specificity with respect to certain elements of the Act's data breach reporting requirements under Division 1.1.

Objectives

The objectives of the Regulations are the following:

1. Ensure that all Canadians receive consistent information about data breaches that pose a risk of significant harm to them.
2. Ensure that data breach notifications contain sufficient information to enable individuals to understand the significance and potential impact of the breach.
3. Ensure that the Commissioner receives consistent and comparable information about data breaches that pose a risk of significant harm.
4. Ensure that the Commissioner is able to provide effective oversight and verify that organizations are complying with the requirements to notify affected individuals of a data breach and to report the breach to the Commissioner.

Description

With regard to the statutory requirements for data breach reporting under Division 1.1 of PIPEDA, the Regulations will

- specify the minimum requirements for providing a *data breach report to the Commissioner*;
- specify the minimum requirements for *notifying affected individuals of a data breach*; and
- confirm the scope and retention period for *data breach record-keeping*.

Recognizing the vast range of organizations that are subject to PIPEDA, the Regulations are designed to provide maximum flexibility for organizations to fulfill their statutory obligations in a manner that is compatible with their particular circumstances.

Data breach report to the Commissioner

The Regulations list the categories of information that must be contained in a report to the Commissioner, but do not preclude additional information from being provided by the organization, should it wish to further the Commissioner's understanding of the incident.

The Regulations align closely with what is currently recommended in guidance by the Office of the Privacy Commissioner of Canada (OPC) for voluntary data breach reporting, and with what is required for mandatory breach reporting in Alberta [1] and the European Union (EU). [2]

The Regulations allow for data breach reports to be submitted with the best information available to the organization at the time of reporting. This allows an organization to report a breach within an appropriate time frame, even when all information is not yet available. In these cases, organizations may provide updates to the report at a later date if further pertinent information becomes available.

The Regulations provide that breach reports may be provided to the OPC in a secure manner, in

recognition of the confidential nature of the information, and to protect the information accordingly.

Notifying affected individuals of a data breach

The Regulations list the categories of information that must be contained in a notification to affected individuals. However, organizations are not precluded from including additional information or designing the notice to suit the intended audience.

This approach provides certainty to organizations as to what is required as a minimum to comply with the statutory requirements for notification. At the same time, it provides flexibility on the format, design and means of notification, enabling organizations to conduct notifications in line with established practices and expectations of their stakeholders.

The Regulations provide examples of commonly used forms of communication that are appropriate means of direct notification to individuals, in addition to providing for the use of any other means that would be considered reasonable under the circumstances.

The Regulations list specific circumstances where indirect notification to affected individuals is permitted in place of direct notification. Specifically, the Regulations establish that this is appropriate where direct notification may cause further harm to the affected individual; where the organization does not have contact information for the organization; or where providing direct notification to all individuals within the required time frame would result in undue hardship for the organization.

With respect to the permitted format of indirect notification, the Regulations also confirm that public announcements, such as advertisements, can be considered as appropriate for indirect notifications.

Data breach record-keeping

The Regulations will affirm that the purpose of data breach record-keeping is to facilitate oversight of organizations' breach reporting and notification obligations by the Commissioner. This in turn will encourage better data security practices by the organizations.

To this end, the Regulations will require organizations to maintain sufficient information in a data breach record to demonstrate that they are tracking data security incidents that result in a breach of personal information for the purpose of determining whether they pose a risk of harm to individuals.

The Regulations allow for a broad interpretation of what information would constitute a "record" for the purpose of PIPEDA. This approach provides protection for any material that is provided to the Commissioner in response to a request for data breach records under the *Access to Information Act* (ATIA). By not enumerating what constitutes a record in the Regulations, the ATIA exemption implemented by the *Digital Privacy Act* may be extended to any material that is considered a record for the purpose of Division 1.1 of the Act.

The Regulations specify that organizations must maintain a data breach record for a minimum period of time; specifically 24 months from the date that the breach has been confirmed by the organization. This time frame is intended to be a minimum requirement, providing for the retention of data breach records for longer than two years if an organization's other obligations, practices or requirements so dictate.

The OPC recommended that records be kept for five years, however, this is considered overly burdensome for regulated organizations given that the record-keeping requirement pertains to all breaches, regardless of the risk of harm posed.

Coming into force

To facilitate compliance with the new data breach reporting regime under PIPEDA, the Regulations provide for implementation at the same time as the related statutory requirements under Division 1.1 of PIPEDA, namely November 1, 2018.

"One-for-One" Rule

The "One-for-One" Rule does not apply, as the Regulations are not expected to directly increase the administrative burden on businesses.

Costs to regulated organizations resulting from this regulatory proposal are considered to be nominal given that the administrative burden for record-keeping arises from the statutory obligations imposed by the *Digital Privacy Act*. The Regulations simply provide further specification on those obligations. With respect to reporting requirements, the Regulations reflect existing best practices established by the voluntary reporting initiative of the OPC and under equivalent legislation in certain provinces.

Small business lens

The small business lens does not apply, because the estimated nationwide cost impact of the Regulations is less than $1 million per year.

Consultation

During Parliament's review of the *Digital Privacy Act*, many stakeholders representing businesses, consumers and the legal community presented their views on the proposed regime for data breach reporting. The majority generally supported the proposed approach, which indicated that the Regulations would provide further details on statutory requirements for data breach reporting, notification to individuals, and record-keeping.

Subsequent to the royal assent of the *Digital Privacy Act*, stakeholders were specifically consulted on the proposed use of the Regulations. Innovation, Science and Economic Development Canada (ISED) published a comprehensive discussion paper that posed a series of specific questions and invited stakeholders to provide their views on how the Government should exercise its regulatory authority. The discussion paper was posted on the Government's consultation portal (www.consultingcanadians.gc.ca (http://www.consultingcanadians.gc.ca)) and was distributed directly to specific stakeholder groups. ISED also held bilateral and multilateral meetings and teleconferences with interested stakeholders to allow them to express their views on the proposed Regulations.

On September 2, 2017, a draft regulatory proposal, titled *Breach of Security Safeguards Regulations*, was published by ISED in the *Canada Gazette*, Part I for a 30-day consultation period. This draft of the Regulations can be consulted at the following link: www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.html (http://www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.html). ISED

received approximately 20 written submissions from business associations, civil societies, academics, experts in the fields of privacy law and data security, as well as the OPC. The submitted comments were carefully examined and considered when reviewing the final Regulations.

In general, respondents provided constructive proposals for fine-tuning the wording of the draft regulations to provide greater clarity and certainty on the extent of organizations' obligations. In some cases, however, respondents called for changes to the Regulations that would exceed the regulation-making authority provided by the *Digital Privacy Act*, or would alter statutory provisions which have been passed by Parliament; in particular, to limit the data breach record-keeping requirements to significant or "material" breaches.

Report to Commissioner

Several respondents raised concerns that the proposed regulatory text did not explicitly recognize that organizations may not necessarily have all of the information required for a report to the Commissioner as soon as feasible after the organization determines the breach has occurred. Organizations that have experienced a breach indicate that it often takes weeks or months to fully investigate the incident and that initial theories about the time frame, cause or scope of the breach are often proven incorrect.

In recognition of the complexity and evolving nature of breach investigations, and that additional information may come to light after an organization has fulfilled its obligation to report to the Commissioner, the Regulations provide that organizations may report certain information to the extent that it is available at the time of reporting and that an organization may update the report at a later date.

Some respondents pointed to the use of different terms pertaining to a breach; in particular, that the terms "breach of security safeguards" and "breach that creates a real risk of significant harm" are used throughout section 2 of the Regulations and that it is not clear if they are to be distinguished from one another. The final Regulations clarify that all of the information required in a report to the Commissioner should pertain specifically to a breach that poses a real risk of significant harm to individuals. In a situation where a breach impacts individuals differently (poses a real risk of significant harm to some, but little or no risk to others), the information reported need only pertain to the former. However, this does not preclude the organization from including information about the circumstances of the breach as a whole, should it be helpful to the Commissioner's understanding of the incident.

Some respondents raised concerns about the security of information contained in a report during transmission to the OPC and called for the Regulations to expressly permit organizations to provide information in password protected or encrypted formats. In recognition of the sensitive and confidential nature of information contained in a breach report, the Regulations expressly permit organizations to submit a breach report to the OPC via a secure means. The Regulations remain silent on what means are considered "secure" to provide flexibility to organizations in the absence of further direction from the OPC.

Content of Notification

The majority of business respondents strongly opposed the proposed requirement to include details in a notification to individuals about the organization's internal complaint process or the individual's right to file a complaint with the OPC. These respondents stated that it is unclear how such a requirement would facilitate the stated objective of the Regulations; to ensure that consumers receive consistent

information about the breach. Some also cautioned that it runs counter to well-established privacy management practices that encourage individuals to resolve privacy complaints directly with the organization prior to submitting a complaint to the Commissioner. The Regulations have been amended to remove this requirement.

In line with the changes made to the provision pertaining to the reporting requirements, the information to be included in the notification to affected individuals would also be information that is to the best knowledge of the organization at the time of reporting.

Means of notification

With regards to direct notification to individuals, respondents raised concerns that the wording of the draft Regulations was not technology neutral and did not necessarily allow for the use of new forms of communication that, among certain stakeholder groups, may be preferred, such as for the example in-app notifications, and text messaging. The final Regulations employ language that will allow for the use of any form of communication for direct notification that a reasonable person would consider appropriate in the circumstances, including for example, mail, email, telephone and in-person communication.

In a similar vein, several respondents raised concerns that the draft Regulations limited indirect notification to individuals to the use of a “conspicuous message” or an “advertisement.” This wording was seen to be too prescriptive given the rapid evolution of communication technologies. The final Regulations provide for indirect notification by any means of public communication.

Indirect notification

Several respondents highlighted that the use of the term “prohibitive” or the use of a “cost prohibitive” concept at paragraph 5(1)(b) of the Regulations are unclear. Therefore, clarification was brought to the threshold for determining whether indirect notification is justified and now includes the broader notion of “undue hardship.” This legal concept replaces the concept of “cost prohibitive” to grant organizations the latitude needed to account for broader factors and unique characteristics of the organizations in determining whether indirectly notifying individuals is justified.

Record-Keeping

Many respondents took the opportunity to reiterate concerns about the burden imposed by a requirement to keep a record of all data breaches, and called for limiting requirement to “material” or significant breaches. However, with the passage of the record-keeping provisions in the *Digital Privacy Act*, it was the intent of Parliament to allow the Commissioner to verify that organizations are tracking all breaches for the purpose of determining whether a breach triggers the requirement to notify individuals.

Several respondents also called for the Regulations to clarify that the extent of information required in a data breach record should not exceed that of a breach report to the Commissioner. As noted in the Regulatory Impact Analysis Statement published with the draft Regulations on September 2, 2017, the Regulations purposefully do not prescribe the content of a record in order to provide organizations with flexibility in how tracking is implemented.

Comments on the draft Regulations submitted by the OPC reiterated the need for breach reports and breach records to include details on the risk assessment conducted by an organization, stating that this information is key to shared learning and understanding of the extent and nature of breaches in Canada. However, with the passage of the *Digital Privacy Act*, it was the intent of Parliament that regulated organizations bear the responsibility for conducting risk assessments pertaining to breaches that they experience, given that they are best positioned to understand the circumstances at hand. It was also Parliament's intent to grant organizations with flexibility in the manner in which they conduct their analysis. Imposing an obligation to provide the Commissioner with details of a risk assessment for each and every breach experienced by organizations subject to PIPEDA would be unnecessarily burdensome for regulated organizations, and is not required to achieve the overriding objective of notification, which is to provide individuals with information they need to mitigate harm resulting from the breach.

Stakeholders have noted that the commencement of the retention period tied to record-keeping should be more precisely defined. One respondent indicated that the requirement to keep records 24 months after the date that the organization determines the breach to have occurred could be misinterpreted as the date that the breach occurred. To align with and conform to the wording in subsection 10.1(2) of PIPEDA, the Regulations clarify and provide that the retention period commences once the organization has concluded that a breach has occurred.

Coming into force

Most organizations that provided comments on the need for a transition period between publication of the final Regulations and their coming into force called for a lag period of between 12 and 18 months after the Regulations are final. Respondents indicated that some lag time is required to implement policies, procedures and information systems that are necessary for compliance with their new obligations under the Act. By contrast, the Privacy Commissioner and several other respondents representing privacy and consumer advocacy groups have asked for immediate implementation, stating that organizations have been aware of the statutory requirements since their passage in 2015 and should be well prepared. Given the lengthy period of consultations on the Regulations and the frequency of data breaches involving the information of Canadians, the Regulations provide for a coming-into-force date of November 1, 2018. This provides some transition period for organizations, while implementing these important protections for individuals by the end of 2018.

Aside from comments pertaining directly to the verbiage and meaning of the draft Regulations, stakeholders also took the opportunity to flag the EU's privacy legislation, titled the *General Data Protection Regulation* (GDPR), which comes into force in May 2018. Many respondents cited the need to align the Regulations more closely with those of the breach reporting requirements of the GDPR given that many Canadian organizations must comply with both Canadian and European law. The final Regulations were drafted with a view to harmonizing the requirements to the extent possible.

Rationale

Stakeholder Impacts

Businesses

All organizations subject to PIPEDA will be impacted by the Regulations. However, many will have already implemented data breach reporting practices that align with the proposal given that it reflects existing best practices established by the OPC and legislative requirements in Alberta.

For those organizations that do not have established processes and procedures for tracking data breaches and reporting accordingly, the Regulations will provide for a delayed coming into force date after the publication of the final Regulations.

Consumers

The Canadian marketplace will see a positive impact of as a result of the Regulations. Consumers will have the assurance that when they are affected by a data breach posing a risk of significant harm, they will receive information in an appropriate manner, regardless of where the breach occurred.

Office of the Privacy Commissioner of Canada

The responsibility for overseeing compliance with PIPEDA rests with the Commissioner. As part of its oversight of data breach reporting requirements under the Act, the OPC will receive reports on data breaches posing a real risk of significant harm, request data breach records of organizations, at its own discretion, and provide advice and guidance to organizations as to how to comply with their breach reporting obligations under the Act. Where appropriate, the Commissioner will investigate complaints pertaining to suspected contraventions of data breach reporting requirements, and conduct audits of organizational practices in this regard.

As part of its annual report to Parliament on PIPEDA, the OPC may provide information on the extent and nature of reported data breaches in an aggregate and anonymized manner.

Benefits and costs

Social benefits

The Regulations will contribute positively to the privacy and security of individuals. Mandatory breach reporting allows individuals who are affected by a breach to take immediate action to protect themselves against further compromise that may lead to fraud, identity theft, humiliation, loss of employment or other forms of significant harm.

The Regulations will help mitigate harm to individuals who are affected by a data breach, and will increase the protection of Canadians' personal information in general by encouraging better data security practices.

The costs to consumers stemming from data breaches are significant and far-reaching. Beyond financial costs, the potential for humiliation and loss of opportunity resulting from breaches of personal information also exists, and has been recognized by the courts in Canada.

Mandatory data breach notification under PIPEDA provides an increased level of protection for Canadians and other consumers in the Canadian marketplace by allowing them to take steps to protect themselves from potential harm resulting from that breach.

The Regulations will enhance this protection in a number of ways. By ensuring that all breach notifications contain a core set of information and are provided in an appropriate manner, the Regulations will result in more effective notifications by increasing the probability that affected individuals will receive information and understand its significance.

A minimum standard for notification also assures Canadians that they can expect a similar approach to notification by all organizations.

Economic benefits

The Regulations will serve to codify existing best practices for data breach reporting and create certainty across the marketplace about how organizations notify individuals affected by a breach. They will also harmonize Canada's regime for data breach reporting with those of other jurisdictions, reducing the burden of reporting for organizations operating in multiple jurisdictions.

Prescribing the content of notifications to individuals and reports to the Commissioner will align the federal private sector regime for mandatory breach reporting with equivalent provincial legislation, and those of Canada's major trading partners. In particular, the EU's GDPR, which comes into force in May 2018, includes mandatory data breach reporting and requires organizations to include similar information in reports to authorities and to individuals. EU companies will also be required to keep a record of all data breaches for the purpose of demonstrating due diligence with regard to their reporting obligations.

This alignment is important to Canada–EU trade. PIPEDA is currently deemed to provide an essentially equivalent level of privacy protection to the EU, which allows for the free flow of personal information from the EU to Canadian organizations.

It is also an important factor in mitigating compliance costs for organizations that operate in multiple jurisdictions. Many organizations subject to PIPEDA are also required to comply with provincial or international laws and, in the case of a data breach, may be required to notify individuals in various jurisdictions. To the extent that the Regulations align, data breach reporting under PIPEDA with requirements in other jurisdictions, this will reduce the burden of notification for many organizations in Canada.

Public security benefits

The Regulations are expected to contribute positively to the security of individuals and the cyber security readiness of Canadian businesses. The regulatory proposal implements statutory requirements to report data breaches, which has been established as an important element of Canada's cyber security policy.

A requirement to maintain records of all breaches for a two-year period will incentivize organizations to track and analyze the impact of all data security incidents.

The Regulations will also ensure that breach reports to the Commissioner are provided in a consistent way such that incidents can be compared and aggregated to provide a repository of information on data security incidents in Canada. Importantly, the prescribed content of the report to the Commissioner includes information pertaining to the general nature of the breach. In doing so, an efficient repository may be created, enabling the OPC to acquire a general understanding of the nature and extent of breaches occurring in Canada.

Consistency in reporting will also allow for metrics to be developed for evidence-based policy-making. Currently, there is little data available about the extent and nature of data breaches across the Canadian marketplace, outside of Alberta and the health sector in certain provinces.

Costs

The costs to businesses directly resulting from the Regulations are expected to be nominal, given that the bulk of the compliance and administrative burden arises from the statutory obligations imposed by the *Digital Privacy Act*.

The Regulations reflect in large part existing best practices that have been established under the voluntary reporting initiative of the OPC and under equivalent legislation in certain provinces. Given that these practices have been in place for several years, it is expected that many regulated organizations will have already incorporated them to some degree into their own policies and procedures.

It is anticipated that the flexible approach taken in the Regulations will serve to mitigate the costs of complying with the statutory requirements for notifying individuals. The Regulations allow for organizations to notify individuals indirectly where directly contacting each affected individual may prove unreasonably costly. In these cases, the Regulations allow notification to take place via communication channels that are much more cost effective and efficient, greatly reducing the burden of notification. This may be particularly important for small to medium-sized organizations that may experience a data breach involving a very large number of customers.

The Regulations also allow for organizations to craft notifications in a way that is appropriate for the circumstances and the audience. Though a core set of information is required to be included in notifications to individuals, the Regulations are silent on their format and design.

Implementation, enforcement and service standards

The Regulations will come into effect at the same time as the statutory requirements pertaining to data breach reporting under Division 1.1 of PIPEDA on November 1, 2018. This will give regulated organizations some time to adjust their policies and procedures accordingly and to ensure that systems are in place to track and record all breaches of security safeguards that they experience.

Enforcement of the Regulations will reflect the existing compliance regime under PIPEDA, whereby the Commissioner is responsible for providing oversight and investigating complaints. In its 2016 –2017 Annual Report to Parliament, the OPC indicated that the development of guidance material for organizations with respect to their new obligations for data breach reporting is a priority. In the meantime, existing guidance material published by the OPC for voluntary reporting of data breaches will assist organizations in complying with their new obligations.

New offences and fines for willful and deliberate contravention of the statutory requirements for data breach reporting, notification to individuals and record keeping were imposed by the *Digital Privacy Act*. In line with other offences under PIPEDA, courts are authorized to impose these fines and to order non-compliant organizations to change practices.

ISED will evaluate the need for amendments to the Regulations on an ongoing basis. Parliamentary reviews of PIPEDA, which are to be conducted every five years after implementation of the Act, will provide an opportunity for examining the need for amendments to statutory provisions, including regulation-making authority under PIPEDA pertaining to data breach reporting.

Contact

Charles Taillefer
Director
Privacy and Data Protection Directorate
Marketplace Framework Policy Branch
Strategy and Innovation Policy Sector
Innovation, Science and Economic Development Canada
Telephone:
343-291-1774

Email:
charles.taillefer@canada.ca (mailto:charles.taillefer@canada.ca)

Footnotes

a S.C. 2015, c. 32, s. 21

b S.C. 2000, c. 5

1 Alberta *Personal Information Protection Act.*

2 European Union *General Data Protection Regulation* (coming into force in 2018).

Government of Canada activities and initiatives

#YourBudget2018 – Advancement

(https://www.budget.gc.ca/2018/docs/themes/advancement-advancement-en.html?utm_source=CanCa&utm_medium=Activities_e&utm_content=Advancement&utm_campaign=CAbdgt18)
Advancing our shared values

#YourBudget2018 – Reconciliation

(https://www.budget.gc.ca/2018/docs/themes/reconciliation-reconciliation-en.html?utm_source=CanCa&utm_medium=%20Activities_e&utm_content=Reconciliation&utm_campaign=CAbdgt18)
Advancing reconciliation with Indigenous Peoples

#YourBudget2018 – Progress

(https://www.budget.gc.ca/2018/docs/themes/progress-progres-en.html?utm_source=CanCa&utm_medium=Activities_e&utm_content=Progress&utm_campaign=CAbdgt18)
Supporting Canada's researchers to build a more innovative economy