WHITE PAPER

CYBERSCOUT® SOLUTIONS

CANADIAN DATA BREACH NOTIFICATION REQUIREMENTS

CYBERSCOUT®

1

CALL OUT

INTRODUCTION

The importance of breach notification in data protection law is a widely recognized concept worldwide. Appropriate technical and organizational measures to ensure the security of personal information are central to the principle of accountability. Canada has taken a significant step towards harmonizing its data breach notification requirements with Europe's General Data Protection Regulation, known as GDPR.

PIPEDA, Canada's privacy law for private sector organizations, places responsibility on an organization for protecting personal information under its control. The Digital Privacy Act ("the Act") amended PIPEDA to add mandatory breach reporting obligations, which will come into force on November 1, 2018. The Office of the Privacy Commissioner enforces PIPEDA by overseeing compliance with its obligations.

The mandatory breach requirements set out clear rules for companies to inform affected individuals when there is a breach and a real risk of significant harm. They also set out an obligation to report such breaches to the privacy commissioner, maintain records of all breaches experienced by the organization and to provide such records to the privacy commissioner upon request.

WHEN IS THE NOTICE REQUIREMENT TRIGGERED?

The notice requirement is triggered when there is a breach of security safeguards or a failure to establish those safeguards.

A breach of security safeguard is defined as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards." There is no specific time frame set for breach notification. When the organization determines that a breach is posing a real risk of significant harm, it must notify affected individuals and file a report with the commissioner as soon as feasible.

WHAT IS REAL RISK OF SIGNIFICANT HARM?

PIPEDA requires organizations to conduct a situational analysis to determine if there is a real risk of significant harm.

Section 10.1(8) sets forth factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual. This includes:

2

CALL OUT

a. the sensitivity of the personal information involved in the breach;
b. the probability that the personal information has been, is being or will be misused; and
c. any other prescribed factor.

NOTICE AND REPORT TO THE OFFICE OF THE PRIVACY COMMISSIONER

When an organization concludes that a breach of security safeguards poses a real risk of significant harm, the regulation requires that the organization report the breach to the privacy commissioner. This ensures that the commissioner receives consistent and comparable information about data breaches that pose a risk of significant harm.

The regulation lists the categories of information that must be contained in a report to the commissioner but does not preclude additional information from being provided by the organization. The organization must submit the best information available at the time of reporting. It also may provide updates to the report later, when the information becomes available.

A report of the breach must be made 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 breached 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 each affected individual resulting 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 each affected individual 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.

The breach report may be made in a secure manner to maintain the confidentiality of the information.

3

CALL OUT

NOTIFICATION TO INDIVIDUALS

The objective of the regulation is to ensure that data breach notifications contains sufficient information to enable individuals to understand the significance and potential impact of the breach. The regulation requires organizations to notify individuals of any breach involving their personal information that poses a real risk of significant harm. Organizations must notify consumers “as soon as feasible after an organization determines that a breach has occurred.”

The notification 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 breached to the extent that 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 the affected individual could take to reduce the risk of harm from the breach or to mitigate that harm
f. Contact information that the affected individual can use to obtain further information about the breach.

NOTIFICATION TO BE DIRECT OR INDIRECT COMMUNICATION

The regulation allows for the use of any form of communication for direct notification that a reasonable person would consider appropriate in the circumstances, including mail, email, telephone and in-person communication.

The regulation lists specific circumstances where indirect notification to affected individuals is permitted in place of direct notification:

a. When direct notification may cause further harm to the affected individual;
b. When the organization does not have contact information for the organization; or
c. When providing direct notification to all individuals within the required time frame would result in undue hardship for the organization.

Public announcements, such as advertisements, can be considered as appropriate for indirect notifications. Indirect notification can be by any means of public communication.

4

CALL OUT

NOTIFICATION TO OTHER ORGANIZATIONS

Organization must notify other organizations that may be able to mitigate harm to affected individuals. Other organizations may include law enforcement agencies, insurance companies, professional or other regulatory bodies, credit card companies, financial institutions or credit reporting agencies, and union or other employee bargaining units.

In Alberta, it is the provincial privacy commissioner who determines whether notification to other organizations is required and which organizations to notify.

RECORD KEEPING REQUIREMENTS

Organizations that become aware of a breach of security safeguards must keep and maintain a record of the breach, regardless of the conclusion of their situational analysis into whether the breach poses a "real risk of significant harm." The records must be maintained for 24 months after the day the organization determines that the breach has occurred. This ensures 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

EFFECTS ON PROVINCIAL DATA BREACH REQUIREMENTS

The federal government may exempt from PIPEDA organizations in provinces that have adopted substantially similar privacy legislation. Quebec, British Columbia and Alberta have adopted private sector legislation deemed substantially like PIPEDA. To be deemed "substantially similar," provincial legislation must have all the 10 principles of PIPEDA. This regulation closely aligns with the mandatory breach reporting in Alberta.

Even in those provinces that have adopted legislation that is substantially like federal privacy legislation, PIPEDA continues to apply to:

a. All interprovincial and international transactions by all organizations subject to the Act, and
b. to federally regulated organizations.

PENALTIES

Any organization that knowingly fails to report or maintain records of a breach as required by PIPEDA will be subject to fines of up to CA$100,000.

5

CALL OUT

EFFECTS ON STAKEHOLDERS

This regulation will give businesses an opportunity to adjust their information systems, practices and procedures and train their employees before this Act comes into force. Consumers will have assurance that they will be informed when there is a risk of significant harm. Where appropriate, the commissioner will investigate complaints, conduct audits and report annually to Parliament on PIPEDA. This regulation will increase the protection of Canadian's personal information and help them mitigate the harm. It will further harmonize the data breach reporting requirements for organization operating in multiple jurisdictions. ■