Digital Privacy Act Creates New Safeguards for Personal Information

Provided by Cornerstone Insurance Brokers Ltd.

- Individuals can give consent only if they understand the nature, purpose and consequences of the collection, use or disclosure of their personal information.
- Organizations must report data breaches that pose a real risk of significant harm.
- An organization must maintain a record of every security breach involving personal information.
- Violating these new requirements could result in a fine of up to $100,000.

On June 18, 2015, the Digital Privacy Act (DPA), also known as Bill S-4, received Royal Assent and became law. The DPA was enacted to create higher consent prerequisites and impose notification and record-keeping requirements for organizations that collect, use or disclose personal information in commercial activities.

The Digital Privacy Act was enacted to create higher consent prerequisites and impose notification and record-keeping requirements for organizations that collect, use or disclose personal information in commercial activities.

All new measures introduced by the DPA are currently in force, except for the data breach notification and record-keeping requirements, which will come into force once the government implements regulations.

Background

Prior to the DPA, the Personal Information Protection and Electronic Documents Act (PIPEDA) regulated the collection, use and disclosure of personal information in commercial activities. PIPEDA applies to federal works, undertakings and businesses, and to private-sector organizations that collect, use or disclose personal information in the course of their commercial activities. PIPEDA is the controlling law in provinces that have not implemented personal privacy laws substantially similar to federal laws.

Under PIPEDA, an organization must first obtain an individual's consent before collecting, using or disclosing any personal information about that individual. Organizations are required to identify and document the purposes for which they seek to collect personal information, at or before the time of collection.

The DPA makes several important changes to PIPEDA. These changes include amending consent requirements, introducing mandatory breach notification and record-keeping requirements and adding significant fines for noncompliance.

Heightened Consent Requirement

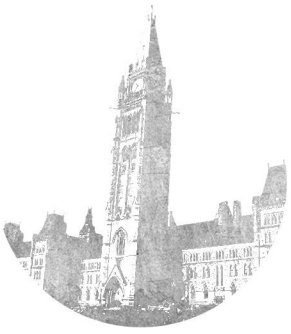
Prior to the DPA, an organization could obtain consent through a one-size-fits-all form, provided that the consent was informed and the purpose of collecting the personal information was clearly stated. The new consent rules will require organizations to determine whether individuals understand what they are reading and agreeing to.

Under the DPA, an individual's consent is valid only if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of his or her personal information. In essence, an individual must understand why he or she is giving consent and how his or her personal information will be used. Organizations will be held responsible for this obligation.

New Exemptions to Consent Requirements

The DPA also creates a number of exemptions to the consent requirements. Going forward, an organization will **not** be required to obtain consent in order to do the following:

- Use personal information contained in a witness statement that is necessary to assess, process or settle an insurance claim;
- Use personal information produced by an employee in the course of his or her employment, business or profession;
- Disclose personal information to a government institution if the disclosing organization has reason to believe the information relates to a violation of federal, provincial or foreign laws;
- Disclose personal information to the government, next of kin or an authorized representative, where there is reason to believe that an individual has been, is or may be the victim of financial abuse;
- Disclose personal information to the government upon request for the purpose of communicating with the next of kin or an authorized representative of an injured, ill or deceased individual, where the government has identified its lawful authority;
- Disclose personal information to the government, next of kin or an authorized representative which is necessary to identify an individual who is injured, ill or deceased;
- Disclose personal information to another organization to detect or supress fraud, or to prevent fraud that is likely to occur; or
- Use or disclose necessary personal information in association with a prospective business transaction, as long as the information is safeguarded and the information is returned or destroyed if the transaction does not proceed.



Mandatory Breach Reporting

The DPA imposes reporting requirements for every organization that suffers a data breach, if the data breach creates "a real risk of significant harm" to the personal information of one or more individuals. If such a breach takes place, the affected organization must do the following, as soon as feasible:

- Report the incident to the Office of the Privacy Commissioner of Canada;
- Notify affected individuals of the breach and provide them with information on steps they may take to minimize the harm caused by the breach; and
- Inform other organizations and government entities of the breach if it believes that doing so could reduce risks or mitigate harm.

Notices must contain enough information to help affected individuals fully understand the extent of harm caused by the breach. Additionally, notices must be conspicuous and provided directly to affected individuals. However, in limited circumstances, indirect notices may be permitted.

"Significant harm" is defined broadly to include, among other things, bodily harm, humiliation, damage to reputation or relationships, loss of employment or business or professional opportunities, financial loss, identity theft, negative effects on credit records, and damage to or loss of property.

The existence of "a real risk of significant harm" is determined by reference to the sensitivity of the personal information involved in the breach, the probability that the personal information will be misused and additional factors that may be prescribed by the forthcoming regulations.

Record-keeping Requirements

The DPA holds organizations accountable for the personal information placed in their custody. Therefore, the DPA requires all organizations to maintain records of **every** security breach involving personal information,

regardless of whether the breach gives rise to a real risk of significant harm.

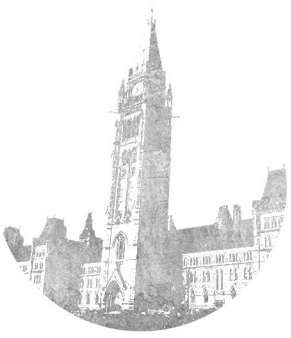
Organizations must preserve this information and provide it to the Privacy Commissioner of Canada upon request.

Penalties
The DPA creates liability for organizations that knowingly violate the new breach notification or record-keeping requirements.

An organization that knowingly fails to report or record a breach or that hinders the Commissioner's efforts to investigate a complaint or perform an audit may face fines of up to **$10,000** for summary offences and **$100,000** for indictable offences.

Implications for Employers
In light of the heightened consent requirements, it is imperative that all organizations that rely on consent immediately review their consent forms, Web privacy statements and other privacy terms to determine whether changes should be made to ensure consent is valid. Consent reviews should be performed on both employee and customer consent.

Mandatory breach notifications will present new costs, risks and challenges for organizations, both large and small. Organizations that handle personal information in the course of their commercial activities should ensure that they have internal safeguards, policies and procedures in place to adequately detect, escalate and respond to privacy incidents.



Organizations should also implement or review policies and procedures to help them maintain accurate records of security breaches that involve personal information. These policies and procedures should also establish a process the organization can follow to determine whether each recorded security breach constitutes a real risk of significant harm to any compromised personal information.