

# New Privacy Legislation, What You Should Know

## Overview

Printers are often in possession of personal information as a third party or as the organization providing fulfillment services for a client. Some print companies that are diversifying are also in the business of collecting data for their clients.

Therefore, here is what you should know about the new Privacy Legislation.

On January 1<sup>st</sup>, the third portion of the Personal Information Protection and Electronic Documents Act (PIPEDA) came into effect. It regulates the collection, use and disclosure of personal information in commercial activities. Organizations covered by the Act must now obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

The federal government may exempt organizations and/or activities in provinces that have adopted substantially similar privacy legislation (Quebec being an example). The Act will also apply to all personal information in all inter-provincial and international transactions by all organizations subject to the Act in the course of their commercial activities.

Personal information includes any factual or subjective information, recorded or not, about an identifiable individuals. This includes information in any form, such as:

- Age, name ID numbers, income, ethnic origin, or blood type;
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

The activities not covered by the Act are limited to:

- The collection, use or disclosure of personal information by federal government organizations listed under the Privacy Act.
- Provincial or territorial government and their agents.
- An employee's name, title, business address or telephone number.
- An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list)
- An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes.

Private sector organizations must follow a code for the protection of personal information, which is included in the Act. The code was developed by business, consumers, academics, and government under the auspices of the Canadian Standards

Association. It lists 10 principles of fair information practices, which form ground rules for the collection, use and disclosure of personal information. These principles give individuals control over how their personal information is handled in the private sector. An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. The principles are:

**Accountability:** An organization must designate responsibility for ensuring the appropriate management of the personal information in its custody. The accountability principle also extends to any personal information transferred to third parties for processing.

**Identifying purposes:** An organization must identify why it collects personal information and how it will be used. It needs to communicate the purpose(s) to the individuals concerned.

**Consent:** An organization must obtain consent before collecting, using or disclosing an individual's personal information. You do not have to recollect the personal information in your possession; however, you must obtain consent for the continued use or disclosure of that information because the Act applies retroactively.

**Limiting collection:** An organization should not collect personal information indiscriminately and should limit collection to that which is necessary for the identified purpose(s). You are prohibited from collecting personal information through deception or misrepresentation.

**Limiting use, disclosure and retention:** Except with an individual's consent or as required by law, an organization should not use or disclose personal information except for the purpose(s) for which it was collected. However, you may keep the information for and long as necessary to satisfy an intended purpose or a legal requirement of retention.

**Accuracy:** An organization must ensure that the information is sufficiently accurate, complete and up-to-date for the purpose(s) for which it will be used, thereby minimizing the possibility that incorrect information could harm an individual.

**Safeguards:** An organization is required to provide adequate security for the personal information in its possession/control. Personal information – in any media format – must be protected against loss or theft and safeguarded from unauthorized access, disclosure, copying, use or modification.

**Openness:** Upon request, an organization is required to make available its policies and the name and contact information of the individual responsible for the organization's compliance with the Act.

**Individual access:** Upon a written request, an organization is required to provide an individual with access to his/her personal information, identify the uses to which the information was put and provide names of any third parties to whom the information was disclosed. Subject to a few exemptions, you must respond to a request with due diligence within 30 calendar days.

**Challenging compliance:** An organization must respond to complaints and take corrective action. Individuals may complain to your organizations or to the federal Privacy Commissioner. The Act's substantial enforcement provisions include audit rights, fines up to \$100,000, the possibility of personal liability, and unlimited punitive damages and damages for humiliation.