

## **Personal Information Protection and Electronic Documents Act**

### **Can I speak to your Privacy Officer? I would like to see a copy of my file!**

Does your receptionist know where to direct the call? Does your Privacy Officer know what to do with the caller? Do you have a Privacy Officer in your organization?

Welcome to the world of PIPEDA! If since January 1, 2004 you cannot answer “Yes” to each of the previous 3 questions, you should review your procedures.

One of the most significant pieces of legislation to affect all businesses in Canada came into force on January 1, 2004 with little or no fanfare. It was not supposed to happen this way. When in April 2000, the Federal Parliament adopted the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”), it was assumed that by January 1, 2004 most if not all provinces would have their own privacy legislation in place and would have made the public aware of its implementation. The provisions of PIPEDA were only to apply in the “unlikely” case where a province or two did not have its own privacy laws.

Good intentions. Wrong assumptions.

While the Ontario government came close at one point to introducing its own legislation, it decided to send the draft bill back for another round of consultations. To date, only a handful of provinces have either introduced or implemented privacy legislations<sup>1</sup> and Ontario is not one of them.

As a result, the provisions of PIPEDA, which were intended to apply only to federally-regulated companies and inter-provincial transactions, apply to all businesses operating in Ontario. PIPEDA regulates the collection, use and disclosure of personal information. Although an organization may not be disclosing personal information of its customers or others, it is likely to collect and use it.

### **What is Personal Information?**

Essentially, personal information means any information about, or relating to, an identifiable person. Section 2 of PIPEDA defines personal information as “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.”

---

<sup>1</sup> Quebec has a privacy law in place since 1993. British Columbia adopted the Personal Information Protection Act on October 6, 2003. It came into effect on January 1, 2004. Alberta also has a Personal Information Protection Act which came into effect on January 1, 2004.

The word “identifiable” is the key to the definition. It is what distinguishes personal information from other types of information. If you know who the information relates to, it constitutes personal information. Common types of personal information include the obvious such as : name, address, age, residential telephone numbers, personal e-mail addresses and birth date, just to mention a few. One component that may come as a surprise to many is that it also includes opinions, evaluations and comments relating to the individual or by the individual. It will, however, exclude employee information, for constitutional reasons. Furthermore, the name, title, business address and business phone number of an employee is not personal information and can be disclosed without the employee’s consent.

Business organizations who maintain files on persons who can be identified in the files are caught by the Act and must comply with it. From a practical standpoint, businesses that maintain files and records on their contacts, associates, suppliers or clients maintain personal records.

PIPEDA not only tells business organizations what they can and cannot do with the personal file of an individual. It also provides that the person about whom the file exists can have *access* to the file including all opinions, evaluations and comments relating to the individual or by the individual.

PIPEDA also applies to all files which already existed on January 1, 2004. Once someone requests access to the file, it is against the law to remove or destroy any document in the file.

### **What are your obligations under PIPEDA?**

PIPEDA essentially enacts as law the 10 principles developed by the Canadian Standards Association in 1996 concerning privacy. These 10 principles are as follows:

- Accountability;
- Identifying purpose;
- Consent;
- Limiting collection;
- Limiting use, disclosure and retention;
- Accuracy;
- Safeguards;
- Openness;
- Individual access;
- Challenging compliance.

If you have not already done so, the first order of business is to determine who in the organization will be designated as the “Privacy Officer”. This person will need the support of the senior management of your organization. This is also the first step in complying with the principle of Accountability, one of the guiding principles of this legislation. The name of the “Privacy Officer” should be communicated internally and externally such as on the organization’s website and in publications.

Once a Privacy Officer is identified and appointed, it will be his/her first priority to determine the needs and the level of preparation of the organization in order to comply with the legislation. In this respect, help is available. The Office of the Information and Privacy Commissioner of Ontario has a very useful tool available on its website. ([www.ipc.on.ca](http://www.ipc.on.ca)). The “Privacy Diagnostic Tool (PDT) Workbook” can be accessed through the “resources” section of the website. It enables organizations to establish where they are in terms of compliance and what needs to be done.

Completing the diagnostic tool is only one initial step. There is much more to do. One important point to remember is that there is NO “grandfathering” under PIPEDA. On January 1, 2004, the existing personal information became subject to PIPEDA. This means that any person on whom an organization keeps personal information must receive a privacy statement and their consent must be obtained for the ongoing use of the personal information within the confines of the privacy statement.

Other steps will include a review of all existing files and closed files and the discarding of information that is no longer required. This will allow your organization to comply with the requirement that personal information should be kept only as long as necessary to satisfy the purpose. Keep in mind, however, that an organization is required to keep personal information used to make a decision about a person for a reasonable time period in order to allow the person to obtain the information after the decision and pursue redress.

Another priority will also be developing the privacy statements that the organization will provide to people on whom it maintains a file. The privacy statement must inform the individual in a meaningful way of the purposes for the collection, use or disclosure of the personal data. Furthermore, it will also be necessary to obtain consent for the ongoing use or disclosure of the information. While consent must normally be obtained before the collection of the personal information, it is of course impossible in the case of existing information. In this case, the consent will be for the ongoing use or disclosure of the information. Consent can be explicit or implied. It must be explicit when dealing with financial, medical or other sensitive information.

Finally, it is recommended that organizations develop formats for acceptable content of notes and memos that will be kept in the files and will include opinions, evaluations or comments on individuals. This may prevent embarrassment if an individual requests access to the personal information kept on her/him by your organization.

Several businesses are likely to have personal information including opinions, evaluations and comments relating to their clients or suppliers. There are grounds on which access can be denied (such as the fact that the disclosure would reveal confidential commercial information). If, however, the person who is trying to obtain access disputes your decision to deny such access, the final decision will rest with the Federal Privacy Commissioner or the Federal Court.

### **Compliance and Penalties**

The Federal Privacy Commissioner is responsible for the enforcement of PIPEDA. Any person who has a complaint related to PIPEDA against a business organization can contact the Federal Privacy

Commissioner. The Commissioner will appoint an investigator who will handle the complaint. The investigator has wide ranging powers. Once the investigation is completed, the Commissioner will issue a report. The Commissioner has one (1) year from the date of complaint to issue a report. The Commissioner also has the right to make public any information relating to the personal information management practices of an organization. It is safe to assume that such public disclosure by the Commissioner will not consist of a catalogue of “best practices”.

Once the Commissioner’s report has been issued, a complainant may also apply to the Federal Court for a hearing. The Federal Court may order an organization to correct practices that do not comply with PIPEDA. The Federal Court may also order an organization to publish a notice of any action taken or proposed to correct its practices. Failure to comply with an order of the Federal Court is “Contempt of Court” and can lead to fines and to a jail term for the “directing mind” of the organization.

The Federal Court also has a right to award damages to a complainant, including awards for humiliation. PIPEDA does not provide for any ceiling for such damages. There are also fines of up to \$100,000.00 for taking disciplinary measures against an employee who is a “whistle blower” or refuses to contravene PIPEDA and for not retaining personal information for as long as necessary to allow someone to exhaust his or her recourse under PIPEDA.

## **Conclusion**

There is no doubt that PIPEDA changed the way businesses operate in Canada. The good news is that businesses in the European Union and in the province of Quebec have operated under similar (if not more stringent) statutes for years. Experience has shown that once the business processes are in place, complying with privacy requirements becomes a way of doing business. The challenge is to be ready and to manage the change.

## **DISCLAIMER**

**This document is intended to provide general information and should not be relied upon as legal advice. If you require legal advice we would be pleased to assist you.**

\*\*\*\*\*

**Jean Bédard, Q.C. is a member of the Bars of Quebec and Ontario and practices law in Kingston. He is a member of the Advocacy & Government Relations Committee of the National Privacy Law Section of the Canadian Bar Association. He has been involved in files related to privacy and data protection for more than 10 years.**