

Getting Ready for PIPEDA

November 2003

PIPEDA (Personal Information Protection and Electronic Documents Act) is a federal law giving Canadians protection against the misuse of their personal information by any organization in Canada. This legislation was prompted in part by well-publicized leaks of medical files and customer information. Governments want to ensure that Canadians can have confidence that their personal information ("PI") is secure, as organizations become larger, and e-commerce expands.

Privacy legislation has been in place for several years at the federal level. As of January 1, 2004, the federal law will also be applied to provinces such as Ontario, which have not yet developed their own equivalent. This means that every business, professional office, club, church, association, or any other organization holding PI, and using or disclosing it in the course of activities which are commercial in nature, will come under PIPEDA. The legislation will only cover information which is clearly personal in nature, such as social insurance numbers, donations, religious or political affiliations, income levels, or credit, medical or employment histories. Whereas there is a common law duty to care for information relating to corporations or other business entities, this is not covered by PIPEDA.

It is important to prepare for the new PIPEDA era. We can't predict how the new rules will be applied in practice, but as Canadians become aware of their new rights under PIPEDA, they will expect organizations with access to their private data to comply with the

new standards. Businesses and other organizations should therefore be aware of the changing environment, alert to developments as they occur, and ready to meet these new requirements. The legislation provides for significant penalties for organizations which don't comply. These range from an audit by the Privacy Commissioner's office, which can publish its results, using its "power of embarrassment", to fines of up to \$100,000.

PIPEDA is organized around ten Privacy Principles:

1. **Accountability** - Organizations are accountable for all PI under their control.
2. **Identify purposes** - There must be a clear purpose for collecting PI, and people must be told why information is being collected.
3. **Consent** - PI can only be collected with an individual's consent.
4. **Collection** - PI must be limited to what is needed for the defined purpose.
5. **Use and retention** - An organization can't disclose PI for any reason outside the defined purpose, without consent, and can only keep PI as long as needed for the defined purpose.
6. **Accuracy** - All PI must be kept accurate, complete and up-to-date.
7. **Safeguards** - PI must be protected, with especially strong safeguards for unusually sensitive information.
8. **Openness** - Specific information about PI policies must be available upon request.

9. **Individual access** - Anyone can ask about the existence, use and disclosure of his or her PI, have a right to access it, and insist on amendment of inaccurate PI.
10. **Compliance** - Anyone is free to challenge the organization regarding its compliance with these Principles.

Every organization should therefore be evaluating what PI it currently has, and how it is managed. The amount and nature of PI will vary depending on the nature of the organization, with some businesses or not-for-profit organizations holding extensive data banks about their clientele, and others almost none.

Action Plan:

The following basic action plan will help to define commitments under PIPEDA:

1. Appoint a person (or committee) responsible for privacy issues.
2. Determine what PI is currently collected, why, where it is stored, how it is used, and when it is disposed of.
3. Consider weaknesses in the organization's current system.
4. Prepare appropriate new policies, in line with the ten Privacy Principles above.
5. Appoint a team to oversee implementation of the new policies.
6. Implement the new program.
7. Monitor progress, and report back to the other members of the organization.

Because this legislation goes into effect January 1, 2004, planning should begin now. Each organization will have to approach this in a way suitable to its particular needs. For example, a hotel regularly deals with individuals, and collects personal data from them. Beginning January 1, 2004, guest registration will specifically provide for the guest's instructions regarding collection and use of his or her PI. On the other hand, though a private club may also have substantial PI about its members, getting their consent for its use or retention may be impractical. Accordingly, the focus would be on obtaining consents from new members, and on retention, accuracy and safeguard issues related to PI currently on hand.

* * * * *

The web-site of the Canadian Institute of Chartered Accountants at www.cica.ca has excellent PIPEDA resource materials. Click on "Privacy" under "Areas of Interest", to access their Privacy packages. And please telephone us if you have any questions about how your organization should start thinking about PIPEDA. We have been developing approaches for dealing with PIPEDA, and can work with you and your legal and other advisors to design an appropriate program for your organization's needs. You can call Steve Van Dyck, our privacy co-ordinator, at (416) 449-9171 extension 221. ■

November 2003

For more information on these and other topics, please refer to our website www.pkfhill.com.



Disclaimer: The above is a general discussion of selected tax planning topics. This is not a substitute for professional advice. You should review these points of discussion with your professional advisor, who should be fully informed of your circumstances before you take, or refrain from taking, any significant action.