PROPOSAL OUTLINE

PRIVACY IMPACT ASSESSMENT

1. Introduction

A great deal of confusion surrounds the application of the Personal Information and Electronic Documents Act (PIPEDA) and the various provincial privacy laws. Most likely, these laws will affect your organization and you will have to act by January 1, 2004. First and foremost, our proposal will address the applicability of the laws to your organization. The various legislation does not apply to some organizations, or applies to them in a very limited way. Not every organization is affected in the same fashion. For these reasons, it is our submission that consultants with legal knowledge and experience are best, as they will have the best ability to assess applicability and stay current with changes in law, regulations and decisions. Simply providing boilerplate-type precedent for organizations will not serve your organization well. Not all systems or contracts are applicable to all organizations.

Our proposal, therefore, begins with a management education forum, so that management may make a more informed choice as to what level of analysis is necessary for them. We are available to meet one-on-one with management to assess an organization's needs and tailor their assessments properly. (I attach two recent papers I have written and published for the non-profit community in particular, for general background).

General information provided in these first educational sessions includes:

(a) What is the legislation that applies to your organization?

(b) Is more legislation expected?

(c) What are the types of information that may be collected without an individual's consent?

(d) What is a "commercial activity"?

(e) How can our organization *maintain compliance*, once a privacy policy and procedures are adopted?

(f) Are there *business reasons* for adopting compliancy measures, policies and procedures, even if the laws do not immediately affect your organization?

(g) Who is the best choice for an in-house Chief Privacy Officer? (most organizations make the wrong choice, initially).

2. Inventory Personal Information Handling Practices

An inventory of an organization's privacy practices will be based upon the PIPEDA's Schedule 1 (the Canadian Standards Association's "Model Code for the Protection of Privacy").

Questions will be structured and asked to determine and track data flow within your organization:

(a) "Personal information" holdings will be identified – what personal information is collected? (Marketing lists, donor lists, alumni lists, e-mail, direct mail programs, contests, tele-fundraising lists, surveys, video-audio, warranties, application forms, website, employment applications)

(b) How is this information collected?

(c) Where is personal information collected?

(d) Why is it collected in the first place? (Sales, marketing, fundraising, advocacy)

(e) Is commercial information, as defined by the Act, involved?

(f) What forms of consent are involved?

(g) Does an organization have sensitive information on clients? Employees? Partners? Third parties? Purchasers? Vendors? Debtors?

(h) How is this information stored, safeguarded and disposed of?

(i) What protocols are in place to ensure continued protection when information is disclosed to outside (third) parties? Are adequate contractual terms imbedded in your agreements with these third parties?

(j) Information flow will have to be mapped, even if it moves only internally. However, if it moves externally, there are additional important considerations. Consider payroll outsourcers, benefits providers, cross-border flows.

(k) Why is personal health information different?

(l) Who in the organization has access to the personal information?

(m) Are firewalls, "Chinese Walls", other security measures, such as software encryption in place? Are they necessary in your case?

(n) Is the organization contemplating a merger, joint venture, business acquisition or other alliance of a strategic nature?

(o) Are there mechanisms in place to allow affected individuals' access to their own information and allow them an opportunity to correct it?

(p) Is your organization a non-profit or a business enterprise? Why does it matter?

(q) Bottom Line: What is your risk exposure?

3. Staff and Management Education

An essential role to be performed is the training and education of management and staff. A Chief Privacy Officer, once properly selected, has to be trained and be able to access information quickly. Everyone in the organization should understand the Privacy Policy.

So, principal issues to be dealt with include the following ones:

(a) What policies has the Organization established to deal with the collection, use, disclosure retention and disposal of personal information?

(b) How are the policies and procedures for managing personal information communicated to management and employees?

(c) What is your "Privacy Policy" and how is it to be made available to the public? (It must be).

(d) Who is the Chief Privacy Officer? How is his/her training completed and maintained?

(e) How is the effectiveness of control measures monitored? Reported?

(f) What mechanisms are in place to manage failures to apply privacy policy?

4. Special Considerations – Impact of PIPEDA on Transactions, Outsourcing

Unique considerations apply to organizations that are undergoing change. For example, new risks are created when organizations are buying or selling assets or shares. For organizations with significant databases, it is a potentially complex (and if not done properly, read, "costly") issue. A multitude of questions arise, including whether PIPEDA-compliant contractual protections and paperwork is complete, whether the transaction involved is cross-border, whether any assets purchased are future PIPEDA "time-bombs", and whether proper consents were acquired.

As this area is very specialized, we do not go into detail in this proposal document concerning the due diligence process involved. However, if a purchase or sale is in your organization's future, we will ensure that your organization is well prepared.

One element worth examining here, though, is a review of third party outsourcing arrangements. Most non-profits, charities, small and medium-sized businesses have such arrangements, be they with a printer, a payroll outsourcing company, providers of benefits (insurance companies, etc.) or other third party contractual arrangements. Legal responsibilities are attached to the use and disclosure of "personal information" with these entities. Adequate consents must be provided.

Contractual agreements governing these relationships should be reviewed by privacy consultants to ensure that organizations are not put at risk by a third party's failure to safeguard against unlawful use or disclosure.

Protective contractual additions would include the following ones:

(a) A right of the disclosing party to audit the third party for PIPEDA compliance;

(b) A requirement that personal information be destroyed by the recipient and proof of such destruction provided when there is no longer a need to use or retain the information;

(c) *Restrictions on the uses* to which personal information may be used and transferred to others;

(d) *Undertakings* to comply with PIPEDA to the same extent as the disclosing organization;

(e) *An Indemnity Agreement* in favour of the disclosing party for a breach of PIPEDA.

Other contractual terms would be possible, dependant upon the circumstances of each individual case. All audits are unique.

Further considerations that may escape review include the sale of redundant assets. Files, old computers containing old hard drives containing personal information of clients, donors and customers give rise to serious security concerns.

In sum, transactions and relations with third parties are not to be overlooked. They, too, will give rise to PIPEDA obligations that should be audited, implemented and protected.

5. Conclusion

It is our conclusion that professional advice is broadly needed, in both the non-profit and the for-profit sectors, to ensure compliance with PIPEDA and provincial privacy legislation. Inasmuch as the law is not brand new (it has been phased-in since 2001 for government entities and larger businesses), there is a body of caselaw that is available to analyze. Decisions have been rendered and a direction for the Office of the Privacy Commissioner is determinable. However, most small and medium-sized businesses, even including professionals (lawyers and accountants), and non-profit and charitable entities, which have not been following the laws, are *not prepared* for the law's effects. It is time for these organizations to act now, to meet this most complex of regulatory environments. A strategy for compliance is essential. An approach based upon analysis of systems, the law and an organization's education and culture is key to success. Of course, monitoring of compliance is required, too.

We will provide a strategic plan to protect your organization and add real value to it. We will provide the following services:

1. Determine where there are shortfalls between your systems of compliance and the legal requirements;

2. Educate your management first, so that they can make informed decisions about next steps;

3. Assist in the proper choice and then education of a Chief Privacy Officer for your organization;

4. Implement the change needed in your organization. All systems, forms, contracts and even future transactions will be made compliant with the laws;

5. Recommend software protections where needed, by providing access to providers of same;

6. Draft your Privacy Policy (in most cases, it is needed by January 1st);

7. Provide your Chief Privacy Officer with regular "Privacy Updates" to ensure on-going compliance. We will be available for on-going and future audits.

Legal compliance and competence is attractive to your business partners, competitors, donors, shareholders, clients and customers. Protecting your organization is not only wise legally; it is also a strategically wise business proposition.