Information
and Privacy
Commissioner/
Ontario

Privacy and Boards of Directors:

What You Don't Know *Can* Hurt You

Ann Cavoukian, Ph.D.
Commissioner
November 2003

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Professor Richard LeBlanc of the Schulich School of Business, York University, and Debra Grant of the IPC in preparing this report.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

This publication is also available on the IPC Web site.

Table of Contents

Introduction

Today, corporate directors are faced with a wide array of responsibilities arising from their board membership. For example, directors have a fiduciary duty to act in the best interests of the corporation and a duty to maintain the standard of care. The statutory standard for the amount of care, diligence and skill required of directors is derived from the common law and codified in the *Canadian Business Corporations Act*. As a general rule, directors are required to "exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances."

Increasingly, privacy is becoming one of the key issues on which directors must focus in order to execute their compliance and managerial oversight as well as mitigate risk. Privacy is often defined as the right of individuals to control the collection, use and disclosure of their own personal information (i.e., information that relates to an identifiable individual). Organizations can help to protect the individual's right to privacy by implementing what are commonly referred to as fair information practices.

New information technology, the globalization of the economy, the interconnectivity of businesses, and web-based delivery of products and services are posing new challenges to the protection of personal information. These challenges are reflected in a number of well-publicized privacy breaches. In one incident, a pharmaceutical company inadvertently disclosed the e-mail addresses of over 600 patients by sending a message to every individual registered to receive reminders about taking Prozac.

In another incident, a data management company failed to implement adequate security safeguards to prevent the theft of a hard drive containing the personal information of hundreds of thousands of Canadians. In California, a hacker was able to break into a state personnel database, gaining access to the names, Social Security numbers and payroll information of state employees ranging from office workers to judges. In Florida, personal health information was used inappropriately when free unsolicited samples of Prozac were mailed to patients using another brand of antidepressant.

Since incidents such as these can have serious consequences for both the individuals whose privacy is breached and the organization that is responsible for the breach, questions have been raised about the liability risks of directors in protecting the personal information collected, used and disclosed by their organizations.

By 2004, virtually all Canadian organizations will be required to comply with either federal or provincial privacy legislation. But, impending legislation and the potential risk of harm from privacy breaches are not the only factors compelling directors to pay closer attention

to privacy issues. Research has shown that consumers are becoming increasingly concerned, better informed and more demanding with regards to the protection of their personal information. Surveys have shown that consumers will alter their purchasing behaviour if they no longer trust an organization to manage their personal information appropriately.

On some occasions, consumer backlash has forced companies to abandon plans to implement new products and services that were seen to be privacy invasive. This could happen after substantial investments have been made in the development and promotion of a product or service. Thus, it is becoming increasingly clear that the cost of mismanaging privacy can have ramifications that go far beyond legal liability.

A lack of attention to privacy can have a number of adverse consequences for which directors may be held accountable. The degree of risk will vary from one organization to the next, depending on the nature of the business and the amount of personal information that is collected, used and disclosed. The potential consequences for which a director could be liable include:

- violations of privacy laws,
- damage to the organization's reputation and brand,
- physical, psychological and economic harm to customers whose personal information is used or disclosed inappropriately,
- financial losses associated with deterioration in the quality and integrity of personal information due to customer mistrust,
- loss of market share or a drop in stock prices following a "privacy hit" resulting in negative publicity or the failure or delay in the implementation of a new product or service due to privacy concerns.

Careful attention to privacy issues may not only help directors and their organizations to avoid these risks, but may also have a number of positive effects. The potential benefits of implementing sound privacy policies and practices include:

- a more positive organizational image and a significant edge over the competition,
- business development through expansion into jurisdictions requiring clear privacy standards,
- enhanced data quality and integrity, fostering better customer service and more strategic business decision making,

- enhanced customer trust and loyalty, and
- savings in terms of time and money.

To enhance awareness of the need to protect privacy among boards, the Information and Privacy Commissioner/Ontario (the IPC) has prepared this paper for dissemination to directors. The purpose of this paper is to raise awareness of privacy not only as a compliance issue but also as a business issue. In doing so, we hope to promote the understanding that oversight of an organization's privacy compliance policies and procedures is an integral and necessary component of effective board service.

The remainder of the paper is divided into four sections. The first section describes basic fair information practices – the foundation for privacy. The second section describes the potential risks that directors and officers take when they fail to pay close enough attention to privacy in their organizations. The third section describes some of the potential benefits that can be reaped through the implementation of sound privacy policies and practices. The final section sets out recommendations for what directors should do to promote privacy compliance in their organizations. The paper concludes with a list of questions directors should ask senior management about the privacy policies and practices in their organizations to ensure privacy compliance.

What are Fair Information Practices?

Fair information practices are a set of common standards that balance an individual's right to privacy with the organization's legitimate need to collect, use and disclose personal information. In Canada, fair information practices are set out in the *Canadian Standards Association Model Code for the Protection of Personal Information* (the *CSA Code*). The *CSA Code* is incorporated into federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*. As of January 1, 2004, all private sector organizations in Canada that collect, use or disclose personal information during the course of commercial activity will be subject to the federal legislation, except in jurisdictions that have substantially similar provincial legislation. The province of Quebec has had private sector privacy legislation in place since 1994. The province of British Columbia has passed legislation that will come into effect January 1, 2004. The province of Alberta plans to enact legislation before the federal legislation takes effect at the provincial level in 2004.

The *CSA Code* consists of ten principles. First, it requires the designation of at least one individual who is accountable for the organization's compliance with the other nine principles (**Accountability**). The organization must specify the purposes for which it collects personal information, at or before the time when the information is collected (**Identifying Purposes**). The consent of the individual must be obtained for the collection, use or disclosure of personal information, except where it is not appropriate to obtain consent (**Consent**). The collection of personal information must be limited to that which is necessary to fulfill the specified purposes (**Limiting Collection**). Personal information must not be used or disclosed for purposes other than those for which it was collected, unless the individual consents or as required by law (**Limiting Use, Disclosure, and Retention**). Personal information must be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used (**Accuracy**). The organization must implement security safeguards that are appropriate for the level of sensitivity of the personal information (**Safeguards**). The organization must make readily available specific information about its policies and practices relating to the management of personal information (**Openness**). Individuals have a right to access and request correction of their own personal information (**Individual Access**). Finally, individuals must be able to challenge an organization's compliance with the privacy principles (**Challenging Compliance**).

Directors would be proactive in satisfying their duties by assessing whether senior management has successfully implemented these practices in their organizations. A list of questions based on these principles that a director might ask is presented at the end of this document. It should be noted that the limitations placed on the collection, use and disclosure of personal information will, in many cases, require modification to existing information management practices.

What are the Potential Risks of Failing to Address Privacy?

1. Organizations that do not implement fair information practices risk violating privacy laws

As of January 1, 2004, virtually all Canadian organizations will be covered by either federal or provincial privacy legislation. The privacy rules will apply to all officers and directors of organizations covered by the legislation. Under the federal legislation, the Privacy Commissioner may initiate an investigation following a complaint or audit an organization's information management practices. The Commissioner also has the authority to publicize information about the information management practices of an organization. In addition, a complainant or the Commissioner may apply to the Federal Court for a hearing after which the court may order an organization to correct its practices; publish a notice of any action or proposed action to correct its practices; and award damages to a complainant, including damages for humiliation. The legislation puts no limit on the monetary damages that may be awarded to a complainant.

Regardless of whether a complaint turns out to be well founded or not, it would be prudent for directors to take reasonable steps to ensure that their organizations comply with the requirements of the legislation and to avoid privacy complaints that may lead to negative publicity, damage to the organization's reputation and brand, and the payment of monetary damages to a complainant.

2. A privacy breach could be damaging to you and your organization's reputation and business relationships

A significant privacy breach could lead to unwanted publicity and additional scrutiny of you and your organization. Even in cases where media attention can be avoided, a formal complaint to the Privacy Commissioner could result in adverse information about your organization becoming public. This could lead to further unwanted scrutiny by both privacy and consumer advocates.

Directors have a duty to act with the minimum standard of care that a reasonably prudent person would exercise in similar circumstances. Directors can look to the federal privacy legislation for guidance on the standard of care that organizations should adhere to in protecting personal information. Companies and their directors may be sued for negligence if they have failed to conform to the required standard of care in their actions or inactions. Since adverse publicity arising from privacy breaches could have an impact on stock prices, shareholders may question whether the directors of an organization have conformed to the

standard of care in acting or failing to act. In cases where directors were seen to fail to comply with the required standard – and it could be argued that the actual damages from their action or inaction were foreseeable – this could lead to shareholder-initiated lawsuits.

The interconnectivity of businesses adds an additional layer of risk. Where businesses are working collaboratively on partnering and joint initiatives, privacy should be a major consideration. Businesses that have made a commitment to privacy protection will not want to expose themselves to risk through associations or partnerships with organizations that fail to conform to the required standard of care in protecting personal information.

Directors will want to ensure that privacy is a key consideration when their organizations enter into partnership arrangements, or when contractual arrangements are made with companies for the provision of specific services (e.g., information technology). An organization cannot avoid their privacy obligations by outsourcing to third parties, and may be held liable if agents and service providers fail to comply with privacy legislation. Conversely, to avoid lawsuits initiated by business partners, directors should ensure that their organizations take reasonable steps to meet the minimum requirements for privacy protection set out in all contractual agreements with third parties and in privacy legislation.

In addition, to help minimize the damage following a privacy breach, directors should ensure that their organizations have a privacy crisis management protocol in place. The protocol should ensure that, following a privacy breach, appropriate steps are taken to minimize the damage to you and your organization's reputation and business relationships and to prevent similar breaches in the future. As part of the protocol, directors should be kept informed about all privacy breaches.

3. A privacy breach could result in serious harm to your customers

Directors need not only be concerned about the potential threat of lawsuits initiated by shareholders and business partners following a privacy incident. A privacy breach could also potentially expose you, your organization and your business partners to lawsuits initiated by customers who are the victims of a privacy breach.

Class-action lawsuits stemming from privacy breaches have emerged as a new litigation trend. In many situations, companies that have inadvertently used or disclosed the personal information of individuals without their consent have subsequently been sued. For example, in the year 2001 alone, US-based companies involved in litigation were forced to pay in excess of $60 million in settlements or judgements. In the majority of cases, judgements arose out of a failure to comply with a stated privacy policy.

Individuals may suffer a range of harms from the unauthorized or inappropriate collection, use and disclosure of their personal information. One of the more widespread harms is the unwanted intrusion into our lives from junk mail, spam and telemarketing. But, individuals can also be exposed to more serious risks including physical, psychological and economic harm. Unauthorized disclosures of seemingly innocuous personal information, such as address and telephone number, can expose some individuals, including children, to the risk of physical harm from stalkers, abusive partners, or sexual predators.

Individuals can be humiliated or stigmatized through the disclosure of personal information relating to medical or psychiatric conditions, alcohol or drug addiction, or financial status. Unauthorized disclosures of certain types of personal information to some third parties can lead to a loss of opportunities in terms of employment, insurance, housing, and other benefits and services. Furthermore, if an organization does not take appropriate steps to guard against it, personal information that is inaccurate, incomplete or out-of-date could be used to make administrative decisions that adversely affect individuals. For example, inaccurate financial information could be used to deny an individual access to credit.

Identity theft is another growing risk that needs to be addressed. If your organization fails to implement adequate privacy and security safeguards, this may open the door to identity thieves who attempt to gain access to enough personal information to assume the identity of another person, usually for the purpose of committing crimes in that person's name. Identity thieves may go on spending sprees, take over bank accounts, open new accounts, divert financial mail, rent apartments, and apply for loans, credit cards, utilities and social benefits – all at the expense of their victims! Victims of identity thieves are often left without any credit, their reputations in ruins and may even be arrested for the crimes of the persons who impersonated them. With a poor credit rating, a victim may be denied a job, a loan, or rental housing. Average financial losses for a typical victim have been estimated to be as high as $36,000.

The Solicitor General reports that identity theft is one of the fastest growing crimes in Canada. In 2002, the PhoneBusters National Call Centre received 7,629 identity theft complaints from Canadians, with total losses in excess of $8.5 million. Canadian credit bureaus report receiving from 1,400 to 1,800 identity theft complaints each month.

Even where there is no criminal intent, it could be argued that liability for financial and other losses may be attracted, if you and your organization do not take reasonable steps to mitigate this known threat. At a minimum, these steps should include the implementation of security measures that are appropriate to the level of sensitivity of the personal information being protected. Also, in the event that there is a privacy breach, your privacy crisis management protocol should require notification of individuals whose privacy has been breached so that they may take appropriate steps to protect themselves from harmful consequences, such as identity theft.

Thus, from a risk management perspective, it is very important that directors be aware of whether their organization is being proactive in taking steps to prevent breaches from occurring – well before they arise – and to minimize the damage caused by any breaches that do occur, in spite of your organization's best efforts at prevention.

4. A lack of attention to privacy could lead to customer mistrust and deterioration in the overall quality of your organization's information assets

In today's information economy, the quality and integrity of information is critical to the success of most businesses. Accurate, complete and up-to-date information is required to provide products and services designed to meet the needs of individuals and to make informed business decisions. Organizations rely on the integrity and quality of their information. A loss of data integrity and quality will have a direct impact on your organization's ability to make sound business decisions and to provide your customers with the types of products and services that they need. Without accurate data, an organization will have no way of knowing who its customers are and how they behave. This could result in financial losses for which directors may be held accountable.

Research shows that almost all companies admit that inaccurate customer data is costing them money in terms of ineffective marketing strategies and damage to their brand and reputation. In spite of this, a large proportion of organizations do not have policies and procedures to enhance the accuracy of their customer data.

Fair information practices require that personal information be as accurate, complete and up-to-date as necessary for the purpose for which it is to be used. Adhering to this accuracy principle can have a direct impact on the quality and integrity of your information assets. In addition, implementing fair information practices can have an indirect benefit by influencing your customers' attitudes and behaviour. If customers do not feel that an organization can be trusted to handle their personal information properly, they may do a number of things: they may avoid providing complete information, withhold consent for the use and disclosure of their personal information, or worse – provide misleading or inaccurate information.

For example, research has shown that the vast majority of Internet users are concerned that the personal information they provide online will be used in an unauthorized way. As a result of this lack of trust, users rarely provide accurate personal information online. About 70 percent of users report that they will typically abandon a website that requests personal information and about 40 percent report having entered false information to gain access to a site.

In short, the implementation of fair information practices can help you and your organization to enhance customer trust and avoid the financial losses associated with a lack of data quality and integrity.

5. A lack of attention to privacy could result in a loss of market share and a drop in stock prices

There are a number of other ways in which a lack of attention to privacy may affect your organization's profits and stock prices. Customers who lack trust in an organization may decide to take their business to a competitor with stronger privacy practices. Mistrust and a corresponding loss of business could be the result of a failure to implement a privacy policy, the implementation of an ineffective privacy policy, specific breaches of your customers' privacy, or privacy-related incidents that attract adverse publicity.

Business could also be lost if an organization attempts to introduce a product or service without carefully considering its impact on privacy. For example, public outrage forced two companies to abandon the roll out of a product that would have provided the personal information of 120 million American consumers on a compact disk. In the first few months following the announcement of this product, there were over 30,000 consumer inquiries and complaints. Other companies have been forced to abandon plans to embed their products with radio frequency identification devises (RFIDs) when an influential consumer group called for a consumer boycott over privacy issues inherent in what it referred to as a "smart shelf" spy system.

Delays in the roll out of a product or service to permit privacy issues to be addressed after the fact can also be costly. For example, in one incident, a manufacturer of computer chips was forced to redesign its latest computer chip when the plan to embed a unique identification number prompted two prominent privacy groups to call for a consumer boycott of all of the manufacturer's products. Delays such as these could leave the door open for a competitor to capture greater market share. In addition, it is often far more expensive to retrofit a product or service to enhance privacy than to build in privacy protections up-front, at the design stage.

Directors who ensure that privacy is part of their organization's culture can minimize the risk of financial losses resulting from a loss of business due to customer mistrust, cancellation or delays in the roll out of new products or services that are seen as impinging on privacy rights, and retrofitting products or services in accordance with privacy legislation and customer expectations.

What is the Business Case for Sound Privacy Practices?

1. Sound privacy practices will give your organization a more positive image and a significant edge over the competition

In today's highly competitive marketplace, most businesses rely heavily on brand image to differentiate their product or service from those of their competitors. Considerable resources are invested in advertising, communication, and general branding of a product or service. Negative publicity about one or more privacy breaches or poor privacy practices in general can do irreparable damage to a business's hard-earned brand image. The implementation of sound privacy policies and practices can be thought of as a kind of insurance for an organization's investment in its brand and image.

Privacy has become a business imperative emerging from the public's increased awareness of the value of their personal information. Where there are gaps in the privacy practices of competitors, privacy-sensitive consumers will choose to do business with those organizations that can demonstrate a clearer commitment to privacy and security. Thus, sound privacy practices will protect and enhance your organization's image and brand, as well as its bottom line.

2. Adherence to fair information practices can facilitate business development through expansion into other jurisdictions with privacy laws

Directors should be aware that privacy is a global issue. The original impetus for privacy legislation in Canada was the introduction of the European Union (EU) Directive on Data Protection, which prohibits the flow of personal information to countries where there are inadequate levels of privacy protection. To ensure the unimpeded free exchange of personal information across international borders, many countries have introduced privacy laws, or are in process of doing so.

In an interconnected and global business environment, weak privacy and security safeguards can impose a non-economic trade barrier to organizations that want to conduct business in jurisdictions with higher privacy standards. Awareness of international standards will help directors determine whether their organization's business practices will permit expansion into international markets.

3. Sound privacy policies and practices will allow you to customize your products and services to meet customer needs and will enhance strategic decisions

Directors should understand that customer information, lawfully collected by your organization, is a valuable asset – one that can be a useful tool in building relationships with customers. An organization's best source of information is its customers themselves. As noted previously, the integrity and quality of the personal information that your organization collects from its customers will depend on the extent to which your customers trust your information management practices. If your customers are confident that your organization will use their personal information properly, they will be more likely to share personal information that is accurate, complete and up-to-date. This will allow your organization to provide products and services that are tailored to your customers' preferences and to make sound business decisions based on the knowledge of who your customers are and how they behave.

In today's highly volatile and competitive marketplace, consumers are demanding more tailored offers for products and services, more convenience and better customer service. The Canadian Marketing Association estimated that, in the year 2000, direct marketing generated more than $51 billion in the sale of goods and services. To meet the challenges of today's business environment, organizations must know their customers intimately. Openness and transparency in information management practices and sound privacy policies provide a foundation upon which relationships with customers can be built and sustained.

4. Sound privacy policies and practices will enhance customer loyalty

As consumers are beginning to demonstrate a growing recognition of the value of their personal information and the importance of its security, the need for organizations to address privacy has become more pressing. Surveys consistently show that consumers will change their purchasing behaviour if they no longer trust an organization to manage their personal information. Whether the lack of trust stems from a publicized privacy breach or an individual's personal experience with your organization, the damage to your bottom line may be irreparable.

Frederick Reichheld in his book, *Loyalty Rules!*, has shown that an increase in customer retention rates of 5 percent increases profits by from 25 to 95 percent. This is largely due to the low cost of retaining existing customers in comparison to the high cost of acquiring new customers through advertising and special promotions. Sound privacy policies and practices are one component of a good customer retention strategy.

5. A proactive approach to privacy will save you time and money

There are many ways in which a proactive approach to privacy can save you and your organization time and money. For example, you could save time and money by avoiding the following:

- law suits initiated by customers, shareholders and business partners,
- inquiries and complaints from your customers,
- an investigation or audit by the Privacy Commissioner,
- inefficiencies resulting from poor information management practices and the retention of inaccurate, incomplete or outdated information,
- failure of a new product or service that is seen as impinging on privacy rights,
- delays in the rollout of a new product or service in order to address privacy concerns, and
- retrofitting of a product or service to address privacy concerns after it has been designed and implemented.

It is clear that the investment that your organization makes in preventing privacy breaches today could save you time and money spent on damage control for years to come.

What Should Directors Do?

1. Education is key – directors should ensure that they receive appropriate training in privacy and that there is some privacy expertise on their board

Directors should ensure that their knowledge about best privacy practices is current and up-to-date. Depending on the needs of the organization and those of the board, there are a variety of approaches that can be taken for educating directors. For example, the board could invite privacy experts to speak at one or more of their meetings; organize a privacy workshop for directors and senior officers of their organizations, or attend one of the many privacy workshops organized by third parties.

In addition, where it is feasible, boards should establish a committee whose terms of reference include privacy. The membership of this committee should develop a degree of expertise in privacy and should be familiar with the nature and scope of the personal information collected by the organization. In order to ensure that the interests of management do not overshadow the need for sound privacy practices, it is vital that outside directors are represented on this committee. Ideally, an outside director should chair the committee, as this will help to enhance its independence from management.

2. Directors should ensure that at least one senior manager has been designated to be accountable for the organization's privacy compliance

Accountability is a key fair information practice. Organizations can demonstrate accountability through the appointment of a member of senior management whose responsibilities include privacy or whose primary responsibility is privacy. In many organizations, this individual is known as the Chief Privacy Officer (CPO).

The CPO (or its equivalent) is the organization's resident privacy expert. He or she must be given the authority to oversee the design, implementation, monitoring and reporting on the organization's privacy policies and to ensure that the company's privacy compliance system and control measures comply with existing legislation. This individual should be responsible for ensuring the harmonization of privacy practices on an enterprise-wide basis. Depending upon the size and the scope of the business, the role of the CPO will vary. However, regardless of the size of the organization, the CPO has a crucial role to play – this individual must be knowledgeable about all aspects of the business.

Directors should ensure that the person appointed to carry out the functions of the CPO maintains a certain degree of separation from other senior managers of the organization. Independence will facilitate oversight of the organization's privacy policies and practices.

3. Directors should ensure that privacy compliance is a part of senior management performance evaluation and compensation

The designation of one or more individuals to oversee privacy compliance is not sufficient to ensure that privacy is being appropriately addressed throughout the organization. Before privacy policies and procedure can be effective, all senior managers have to make a commitment to privacy protection. Privacy compliance should be one of the criteria upon which senior managers are evaluated and compensated.

4. Directors should ask senior managers to undertake periodic privacy self-assessments and privacy audits and to report to the board on these activities on a regular basis

A good way to ensure ongoing privacy compliance is through regular self-assessments and privacy audits. A useful self-assessment tool is the Privacy Impact Assessment (PIA). The PIA is a systematic assessment tool designed to assess the impact of an application of new information technology or the introduction of new products and services. The PIA allows privacy issues to be identified and addressed throughout the design and implementation of a new technology, product or service. All innovations or modifications to existing information systems or products and services should undergo a PIA. Since the PIA can serve as an early warning system and risk assessment tool, directors should ensure that they receive and review all PIA reports.

Privacy audits are another useful tool that can be conducted by the CPO (or its equivalent) or by external privacy consultants. From an oversight perspective, it is preferable for the audit to be conducted by someone who is independent from the organization. The purpose of the audit is to ensure that the organization is in compliance with its own privacy policy and with existing legislation. The goal of the audit should be to promote education and awareness and to find practical solutions to everyday privacy issues. Audits should be conducted at regularly scheduled intervals, such as annually. As is the case with PIA reports, directors should ensure that they receive and review reports on all privacy audits.

5. Directors should ensure that they ask senior management the right questions about privacy practices in their organization

Keeping in mind the interests of shareholders and other stakeholders, including the company's employees and customers, directors have a responsibility to ensure the appropriate level of managerial oversight of privacy.

The duty of care that directors owe to their organizations entails that directors must ask the right questions of management – questions that will give management the opportunity to demonstrate compliance with both legislation and best privacy practices and generate "bottom line" advantages that result from implementing sound privacy policies. Below is a list of questions that directors may wish to ask to ensure privacy compliance.

Questions Directors Should Ask to Ensure Privacy Compliance

1. Has your organization designated at least one individual to be responsible for privacy?

2. Does your organization collect personal information? If so, would any of this information be considered to be sensitive?

3. Is the purpose for the collection of personal information explained to customers, at the time it is collected?

4. Is personal information collected only for purposes that are appropriate in the circumstances?

5. Is the personal information that is collected, used or disclosed by your organization limited to that which is necessary to achieve the specified purpose?

6. Have all necessary consents been obtained for the collection, use or disclosure of personal information?

7. Is the form of consent appropriate for the level of sensitivity of the information and consistent with the reasonable expectations of the individual?

8. Have controls been implemented to ensure that personal information is as accurate, complete and up-to-date as necessary for the purpose for which it is to be used?

9. Are the security safeguards to protect personal information appropriate for the level of sensitivity of the information?

10. Are the information management practices of the organization transparent? Does the organization make available to customers information about its policies and practices relating to the handling of personal information?

11. Do customers have the right to access and correct their own personal information?

12. Is there a mechanism through which customers can make an inquiry or complain about the organization's personal information management practices?

13. Has an organizational privacy policy been implemented? Is the privacy policy available to the public?

14. Has an employee privacy policy been implemented?

15. Has a privacy crisis management protocol been implemented to deal with privacy breaches? In the event of a privacy breach, do you communicate information to individuals whose privacy has been breached so that they may take appropriate steps to protect themselves from harmful consequences, such as identity theft?

16. Are all employees aware of the organization's privacy policy? Is privacy training, tailored to roles and responsibilities, mandatory for all employees?

17. Are privacy requirements built into contractual agreements with business partners and service suppliers and agents?

18. Are privacy requirements built into all employment contracts? Do these contracts include consequences for breaching the organization's privacy policy?

19. Does your organization conduct a privacy impact assessment prior to implementing new technologies, programs, products or services that could impact on privacy?

20. Does your organization have a compliance program that includes regular privacy self-assessments and privacy audits to ensure compliance with your privacy policy and privacy legislation?