Your privacy compliance

EARLEEN MOULTON

VP COMPLIANCE, BRIDGEFORCE FINANCIAL GROUP

Agenda

- What's the risk
- Where to find help, tools
- Working through it

Mandatory Compliance Regime

1. Appointment of Compliance Officer
2. Development, application and maintenance of up-to-date written policies and procedures.
3. Ongoing training program for staff
4. Regular review of policies and procedures (at least every 2 years) – “self assessment”

PIPEDA/privacy basics

- PIPEDA applies to the collection, use and disclosure of personal information in the course of commercial activities
- Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. 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
- PIPEDA doesn't apply to business contact information–including:
  - an employee's name, title, business address, telephone number, facsimile number or email addresses–which an organization collects, uses or discloses solely for the purpose of communicating with a person in relation to their employment, business or profession

Canada Life's privacy template

Please note that this sample compliance program constitutes an overview of the main requirements for compliance under Privacy legislation. It is provided to you for information and education purposes only and should not be construed as legal advice or a guarantee of compliance. The information is accurate to the best of our knowledge at the time of publication but keep in mind that rules and interpretation may change. Therefore, applicable laws and regulations have priority over the content of this document. For any particular or complex situation, it is advisable to seek the advice of a legal professional.

This document cannot, for any purposes, be reproduced or transmitted to any third party without the express authorization of the Market Conduct Compliance department of Great-West.

How to use this template:

- *Fields that are to be filled out are in blue*
- *Please make sure you follow the instructions in red*
- *Delete instructions (in red) before printing*

COMPLIANCE PROGRAM
FOR PRIVACY

as required UNDER PIPEDA (Personal information protection and electronic documents Act) or applicable provincial privacy legislation

OUTSIDE QUEBEC:

[NAME OF ADVISOR/CORPORATION]

IN QUEBEC:

[NAME OF ADVISOR/CORPORATION (FIRM)]

INDEPENDENT REPRESENTATIVE / FINANCIAL SERVICES FIRM

COMPLIANCE PROGRAM FOR PRIVACY
(Effective/revised DATE)

OUTSIDE QUEBEC:

[NAME OF ADVISOR/CORPORATION]

IN QUEBEC:

[NAME OF ADVISOR/CORPORATION (FIRM)]

INDEPENDENT REPRESENTATIVE / FINANCIAL SERVICES FIRM

Index

REVIEWS AND AMENDMENTS TO THE COMPLIANCE PROGRAM FOR PRIVACY

The present program was adopted on DATE.

The present program was revised and amended on DATE. Below is a summary of these amendments:

(Insert all documentation regarding privacy reviews or self-assessments, complaints or concerns which led to adjustments to policies and/or procedures)

(Adjust if no amendments were made further to the review. A review should be performed at least every two years.)

For corporations, modify document for independent representatives/sole proprietors

RESOLUTIONS OF THE BOARD OF DIRECTORS OF
[NAME OF THE FIRM] (The "Firm")
EFFECTIVE [DATE]

WHEREAS the Firm must adopt a compliance program in order to comply with PIPEDA (the "Act") and/or applicable provincial legislation, applicable to its operations;

WHEREAS the Firm must ensure that persons that it hires and/or who act on its behalf, whether or not they have a sales licence, comply with the same provisions;

WHEREAS in order to ensure compliance with the various applicable rules, the Firm wishes to adopt a compliance program and to appoint one or more persons to be responsible for the application of this program;

IT IS THEREFORE RESOLVED:

THAT the compliance program attached is hereby adopted by the Firm;

- **THAT** [name(s) of person(s) in charge of compliance] is/are appointed as compliance officer(s) with regard to the Act;

THAT as compliance officer(s) [Name(s) of those in charge of compliance] is/are responsible for:

- Implementation and monitoring of the compliance program;
- Establishing and periodically revising the Firm's policies and procedures;
- Initial and continuing training of representatives, employees and persons acting for and on behalf of the Firm;
- Immediately notifying the principal of the Firm of any known or presumed violation of the Firm's compliance program;

THAT the compliance officer(s) may obtain the assistance of another person to manage the Firm's compliance responsibilities provided that this person has the requisite experience and skills in respect of the compliance aspects that are entrusted to him or her, provided that the name of this person or these persons and his/her/their responsibilities are documented in the compliance program.

THAT [name of principal of the Firm] is authorized to sign documents and take any other measures required to give full effect to the resolutions herein.

The resolutions herein are adopted by the director(s) of the Firm as witnessed by his/her/their signature(s) below.

_____ _____

ACCEPTED BY THE COMPLIANCE OFFICER(S):

_____ _____

POLICIES & PROCEDURES FOR PRIVACY COMPLIANCE

(NAME OF ADVISOR/FIRM)

Effective (date)
Revised on: (date)

Understanding expectations and privacy best practices will help you determine which areas of your business are impacted by the need to protect personal information and for which you may require policies and procedures.

Step 1:

Review 'Privacy and your business' and all related privacy material from RepNet: Advisor support Compliance > Privacy, client file & record retention

Review privacy polices of the insurer(s) that you do business with

Step 2:

Determine what measures you/the firm needs to take in order to comply with PIPEDA or applicable provincial privacy legislation and privacy best practices.

Step 3:

Insert details of policies and procedures, modified to suit your business and adopt it as your policies and procedures.

Responsibility under the Act

The 10 principles that businesses must follow are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

A Guide for **Businesses** and **Organizations**

PRIVACY TOOLKIT

Canada's *Personal Information Protection and Electronic Documents Act*

Office of the
Privacy Commissioner
of Canada

How the tool kit's organized

1. BE ACCOUNTABLE

Your responsibilities

- Comply with all 10 of the principles of Schedule 1.
- Appoint an individual (or individuals) to be responsible for your organization's compliance.
- Protect all personal information held by your organization or transferred to a third party for processing.
- Develop and implement personal information policies and practices.

How to fulfill these responsibilities

Develop a privacy management program. As part of this program:

- Give your designated privacy official senior management support and the authority to intervene on privacy issues relating to any of your organization's operations.
- Communicate the name or title of this individual internally and externally (e.g. on websites and in publications).
- Analyze and document all personal information handling practices including

TIPS

Train your front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our organization's privacy policies?
- What is consent? When and how is it to be obtained?
- To whom should I refer complaints about privacy matters?
- What are the ongoing activities and new initiatives relating to the protection of personal information

2. IDENTIFY THE PURPOSE

Your organization must identify the reasons for collecting personal information before or at the time of collection.

Your responsibilities

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it.

3. OBTAIN VALID, INFORMED CONSENT

Consent is considered valid only if it is reasonable to expect that individuals to whom an organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.

Your responsibilities

- Specify what personal information you are collecting and why in a way that your customers and clients can clearly understand.
- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified.

Here's the 'how'

How to fulfill these responsibilities

- Obtain informed consent from the individual whose personal information is collected, used or disclosed.
- Explain how the information will be used and with whom it will be shared. This explanation should be clear, comprehensive, and easy to find. Retain proof that consent has been obtained.
- Never obtain consent by deceptive means.

4. LIMIT COLLECTION

Your responsibilities

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

How to fulfill these responsibilities

- Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Identify the kind of personal information you collect in your information-handling policies and practices.
- Ensure that staff members can explain why the information is needed.

5. LIMIT USE, DISCLOSURE AND RETENTION

Your responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

How to fulfill these responsibilities

- Document any new purpose for the use of personal information.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms.
- Dispose of information that does not have a specific purpose or no longer fulfills its intended purpose.
- Dispose of personal information in a way that prevents a privacy breach. Shredding paper files or deleting electronic records are ideal.
- Before disposing of electronic devices such as computers, photocopiers and cellphones, ensure that all personal information is fully deleted.

7. USE APPROPRIATE SAFEGUARDS

Your responsibilities

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

Note: PIPEDA does not specify particular security safeguards that must be used. Rather, the onus is on organizations to ensure that personal information is adequately protected.

How to fulfill these responsibilities

- Develop and implement a security policy to protect personal information.
- Use appropriate security safeguards to provide necessary protection:

  - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
  - technological tools (passwords, encryption, firewalls)
  - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, agreements)

10. PROVIDE RECOURSE

Your responsibilities

- Develop simple and easily accessible complaint procedures.
- Inform complainants of their avenues of recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Office of the Privacy Commissioner of Canada.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

Protect Your Business.

GETCYBERSAFE GUIDE FOR
SMALL AND MEDIUM BUSINESSES

Cyber crime and smaller businesses

- Small and medium-sized businesses (i.e., businesses with fewer than 500 employees) employed 10 million people in 2012, nearly 90% of all employees in Canada.[1]
- In 2012, 87% of Canadian businesses used the Internet, and 46% had a website.[2]
- The largest growth area for targeted cyber attacks in 2012 was businesses with fewer than 250 employees — 31% of all attacks targeted them.[3]
- Over a 12-month period in 2012, 69% of Canadian businesses surveyed reported some kind of cyber attack, costing them approximately $5.3 million, or about $15,000 per attack.[4]

Cyber security = protecting information

Confidentiality – any important information you have – such as employees, client, or financial records – should be kept confidential, only access by people (or systems) that you've given permission to do so.

Integrity: You need to make sure to maintain the integrity of this information and other assets (such as software) in order to keep everything complete, intact and uncorrupted.

Availability: You should maintain the availability of systems (such as networks), services, and information when required by the business or it's clients.

What’s covered

- Getting started
- Web security
- Email security
- Data security
- Remote access security
- Mobile device security
- Physical security

Web security

Quick tips from this section:

- Restricting the types of websites that employees are allowed to visit can help you exclude the sites that could compromise your network.
- Advise employees on what software is safe to install on their computers, and to seek permission when downloading new programs.
- When someone outside of your business requests any personal or business information, verify that they are a safe person to send the information to.

Email security

Develop email guidelines for employees that include the following:

- Always follow the company's password standard, including the use of a strong password for email whether the account is inside the business or hosted as webmail. This is important with webmail services, as they are more accessible for cyber criminals who will use compromised accounts for other criminal activities (such as emailing spam).
- Use the recommended security and privacy settings in the Web browser or email client software unless the person responsible for cyber security in the company tells you to change them. The security features built into those applications are there to protect the business. (In your business, it is possible that your employees set up their own email software. If that's the case, it is best that they follow the security recommendations of the browser or email client developer).

Data security

Quick tips from this section:

- Frequently back up your data to an external hard drive, server and/or online service — having multiple backups of your data is key in case of the failure of one of them.
- Download or purchase automatic backup software to ensure timed backups of your system(s).
- Store your physical backups (e.g., external hard drive) offsite in a safe place.
- Have emergency system boot DVDs or USB sticks prepared in case of a system crash.
- Properly label any sensitive information you have to ensure secure handling.
- When disposing of your data, thoroughly destroy it — shred all paper and CDs — so that no information could potentially be gathered and used to harm you.

Mobile device security

Quick tips from this section:

- Ensure that all of your mobile business devices (phones, tablets) have system access passwords and are locked when not in use.
- Properly safeguard data on mobile devices. Most mobile devices have security features and many smartphones and tablets can even run anti-malware software.
- Encrypt all of your sensitive data on portable storage devices.

- Use the safeguards available for your device. Most mobile peripherals have security features and even many smartphones and tablets can run anti-malware software.
- Label all of your portable storage devices with your business name and a contact number in case it is lost.
- Encrypt sensitive files on portable storage so that they cannot be copied or used by someone in case of loss, theft or illicit use. It may be more effective for you to encrypt the entire storage device (e.g., USB flash drive) so that all of the information placed on it is protected.

Helpful government sites

OPCC - Privacy tool kit:

https://www.priv.gc.ca/information/pub/guide_org_e.pdf

From Safety Canada - Canadian cyber incident response centre (CCIRC):

http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx

Questions?

SEE YOU IN MARCH!