OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

Personal Information Protection Act ("PIPA")

Privacy-Proofing Your Retail Business

Tips for Protecting Customers' Personal Information[1]

More than ever before, retailers have to be prepared to deal with customers who ask questions about the type and amount of personal information retailers collect, what they intend to do with it, and how they will protect it from misuse.

Customers have a right to limit what happens to their personal information—who gets it and what they do with it. Many customers are keen on exercising that right, and private sector personal information protection laws now give them the means to do so.

The first step in privacy-proofing your retail operation is to know which personal information protection law is applicable. Provincially regulated retailers in Alberta, British Columbia and Quebec have to comply with the law in force in their province—Alberta and BC each have a *Personal Information Protection Act* (both came into effect in 2004); the Quebec law is entitled *An Act Respecting the Protection of Personal Information in the Private Sector*.

The federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to retailers in provinces other than Alberta, BC and Quebec and to inter-provincial personal information transfers.[2]

[1] This article is the product of a co-operative effort by the Retail Council of Canada, the offices of the Information and Privacy Commissioners for Alberta and British Columbia, and the Access and Privacy Branch of Service Alberta. The Office of the Privacy Commissioner of Canada has reviewed and provided their comments on this article and the product contributors are grateful for their support.

[2] PIPEDA also applies to the federally-regulated private sector, including banks, airlines, railways and telecommunications.

All of these laws are substantially similar to one another, and all are based on ten privacy principles enshrined in the Canadian Standards Association's Model Code for the Protection of Personal Information (see box).

Fair Information Practices—The 10 Privacy Principles

1. *Accountability*. Organizations are accountable for the protection of personal information under their control.
2. *Identifying purposes.* The purposes for the collection of personal information must be identified prior to or during the collection.
3. *Consent*. Organizations may collect, use and disclose personal information only with the knowledge and consent of the individual (with limited exceptions specified in personal information protection laws).
4. *Limited collection*. The collection of personal information is limited to what is necessary for the identified purposes and must be collected by fair and lawful means.
5. *Limiting use, disclosure and retention*. Personal information must be used and disclosed only for the purpose(s) intended, except where consent of the individual is obtained or as required by law. It can be retained only for the period of time required to fulfill the intended purpose(s).
6. *Accuracy*. Personal information must be complete, accurate and current.
7. *Safeguards*. An organization in control of personal information must ensure the information is protected by adequate safeguards.
8. *Openness*. An organization's privacy policies and practices must be readily available to individuals upon request.
9. *Individual access*. An individual has the right to access his/her personal information, subject to legislated exceptions, and has the right to seek correction.
10. *Challenging compliance*. Organizations must provide the means for an individual to challenge the organization's compliance with these privacy principles.

Canada's private sector personal information protection laws set the rules for the collection, use and disclosure of personal information. The questions and answers below illustrate how those laws apply to situations commonly faced by small to medium-sized retailers in their customer transactions.

COLLECTION

1. **What exactly is personal information?**

   Personal information is information about an identifiable individual. It includes information such as the name, address, phone number, e-mail address, credit card information, driver's license number and purchase and return records of an individual customer.

2. **What personal information can my business collect from customers?**

   Limit the information you collect to what is needed to complete the purchase of the product or service you are selling. Limiting the amount and type of information collected lessens the risk of improperly using or disclosing personal information, reduces costs associated with collecting, storing and retaining unnecessary information, and reduces the likelihood of customer complaints.

3. **What if we want to verify a customer's identity to protect against fraud?**

   If a customer pays cash, you have no need to ask for proof of identity. If a customer offers payment by other means, you may ask to see other identification, but may not record it (in writing or on the computer), unless the information is clearly needed for the product or service you're providing. For example, you may record driver's license information if the customer is renting or test-driving a vehicle. If required for the transaction, or for fraud prevention purposes, you may record that you have viewed or verified a customer's identification. You can only retain this personal information for as long as is reasonably required for your legal or business purpose.

4. **We have a generous returns policy that allows customers to bring items back for a refund. What protection can we take against returns from people who have obtained goods without paying for them? Simply collecting the receipt doesn't always protect us against the risk of repeated fraud by employees and others**.

You can require a customer to provide proof of identity, provided you explain the reason for the requirement. You can also record information about the transaction, including the customer's name, address and phone number and that the customer's identity was viewed or verified. You cannot, however, retain that personal information indefinitely or photocopy a proof of identity.

5. When can we ask a customer for a social insurance number ("SIN")?

No business is legally authorized to require a customer's SIN for purposes other than income reporting. If you reasonably need to conduct a credit check—e.g., if the customer has arranged to pay over time rather than paying the full amount immediately—a credit report can be produced by providing the customer's full name and date of birth. Providing a SIN should be optional to the customer for purposes such as credit checks and should not be used to verify customer identity at the point of sale.

6. Can we ask customers for their phone numbers or postal codes?

Yes, as long as you explain how the information will be used or disclosed. You can't require a customer to provide this information as a condition of sale if it isn't essential to make the sale. Staff should know what dummy number they can enter into a mandatory field if the customer refuses consent.

NOTICE AND CONSENT

7. Can we record a customer's personal information to speed up their future purchases or later notify them of attractive offers?

Yes, as long as you clearly explain why you're collecting the information and exactly how it will be used, and permit customers to decline this service. You cannot tell customers you're collecting their personal information to "track purchases" and then use it to market products to them. And if you're going to sell your customer list to other businesses, you must make it very clear to customers that you plan to do so and obtain their consent first. Bottom line:

you cannot ask for the information for one purpose and then use it for another.

8. Does this mean we always have to explain to customers why we're collecting their personal information and how we're planning to use it or disclose it to other organizations, and then get their consent to do so?

Yes, unless the purpose for collection, use or disclosure would be obvious to a "reasonable" person and the customer voluntarily provides the information for that purpose.

9. If we hold a draw for a weekend getaway to a ski resort, and we ask customers to put their names, addresses and phone numbers on a form to be eligible for the pick, isn't it obvious we're planning to use that information for marketing purposes?

It might seem obvious to some customers but not to others. Be transparent and clear about how you're going to use the information. In the case of a draw, you could do so by including an explanatory note on the form so customers will know.

10. Do we have to get customers' consent in writing?

Whether you need to acquire customers' written consent depends on your intended purposes for collection, use or disclosure of their personal information. The consent form you provide should explain all the uses and disclosures of the customers' personal information. Consent in writing and opt-in consent better protect you if consent is challenged by a customer; however, it may not always be practical to obtain written consent.

In most situations, consent can be obtained at the time the personal information is collected from the customer. Verbal consent for the use and disclosure of personal information is fine if you're dealing with a customer face-to-face, as long as the sensitivity of the personal information and the intended use or disclosure do not make verbal consent inappropriate in the circumstances. You can also give customers the choice of opting out of consent—e.g., by marking a check-off box on your on-line form if they don't agree to the use or disclosure of their information for certain purposes (such as being informed of special offers). This

form of obtaining consent is appropriate as long as the purposes are clearly explained and are reasonable having regard for the sensitivity of the personal information.

11. Can a customer withdraw consent that was previously given?

A customer can withdraw or change his or her consent by giving your business reasonable notice, as long as doing so does not break a legal duty or contract between the customer and your business. You must let the customer know what the consequences of withdrawing or changing consent will be. For example, if cancelling consent means that your business can no longer honour an extended warranty, you must inform the customer of this consequence. There should be reasonable terms and conditions on customers' consent. For example, the customer may say that your business can use the personal information to supply one specific product to the customer but cannot use it in the future to market new related products.

12. If we offer discounts to customers who join our rewards program, is it reasonable to track their purchases and notify them of special offers such as gifts and coupons?

Yes, as long as you clearly explain your intention to do so when they register for their program. Under personal information protection laws, businesses cannot make a customer's consent to collect, use or disclose personal information a condition of supplying a customer with a product or service if the business asks the customer to consent to something that is beyond what is needed to supply that product or service.

ACCESS AND CORRECTION

13. What if the customer asks to see our privacy policy and talk to our privacy officer? We try to do what's right, but as a small business we don't even have a policy or a privacy officer to administer it.

No matter how small your business, you are legally obliged to develop policies and practices to meet your responsibilities under the personal information protection law that applies to you. You also have to designate an employee to be responsible for ensuring your business complies with the law, and if a customer asks who

that is, you must provide the employee's position name or title and contact information.

14. What is a privacy policy and how do we develop one?

A privacy policy is critical to building trust with your customers and mitigating privacy risk. It's an effective way to explain how your business will put personal information protection laws into effect with respect to personal information that is collected, used, and disclosed by your business. The websites of the Office of the Information and Privacy Commissioner for British Columbia (oipc.bc.ca) and Service Alberta (pipa.gov.ab.ca) provide model privacy policies you can use as a template. Privacy policies can only be effective if all employees understand them and are committed to following them. The best way of making sure that happens is for management to emphasize, not only to customers but to staff as well, that protection of personal information is a company priority and to ensure that staff understand and follow the privacy policy in everyday transactions with customers.

15. What if a customer asks for a copy of all of his or her personal information in our records? Isn't it ours once we have it?

No. Under personal information protection laws, individuals have a right to access personal information about themselves, and if that person asks for the information, you must promptly provide access to it. (You may charge a *reasonable* fee in Alberta.) Under PIPEDA and in BC businesses may charge a *minimal* fee. In some cases, you may refuse access to some records or parts of records. For example, personal information protection laws require businesses to sever information about people other than the applicant.

16. What if a customer wants us to correct his or her personal information?

A business must make a reasonable effort to ensure that a customer's personal information in its custody is accurate and complete.

SAFEGUARDS AND RETENTION

17. What security measures do we need to protect customers' personal information?

You must protect all personal information in your custody or under your control by making reasonable security arrangements to prevent unauthorized access, collection, use, copying, modification or disposal or similar risks. That generally means keeping records under lock and key and ensuring that access is available only to staff with a need to know. Credit card slips and the like should be stored out of reach of the public, not beside the till. Information on your computers should be password-protected with adequate safeguards against hackers (such as firewalls, virus protection software and encrypted hard drives).

18. What responsibility do we have for the privacy practices of organizations to which we disclose customers' personal information?

In BC, you only have responsibility for personal information that is directly under your custody or control. However, it's a good business practice to try to ensure that businesses with which you share customer personal information (e.g., credit-granting agencies) have the same high standards you do in complying with personal information protection laws. In Alberta, if there is a contractual or agency relationship between you and the other business with which you share customer personal information, you are accountable for the other business's privacy obligations as well as your own. This should be addressed in the contract or agreement between you and the other business. Although PIPEDA does not contain any specific provisions with respect to data that is moved across a provincial or national border, it requires that any outsourced personal information is handled according to the standards set in the law.

19. We've had the occasional customer complain that our receipts show the credit card number in full. Should we change our practice?

While credit card information is personal information, you don't contravene personal information protection laws simply by giving a

customer their own information. However, customers who worry about fraud and identity theft may feel they have to shred receipts that show their full credit card number. That's a nuisance for them, and they may decide to take their future business elsewhere. You do need to have rigorous procedures in place to protect credit card receipts that contain all the information needed to misuse a credit card — name, credit card number and expiry date. You're responsible for keeping merchant copies of the receipts safe, and it may also be in your best interest to get a machine that obscures credit card numbers on customer copies.[3]

20. How long should we keep personal information after collecting it?

Records containing personal information should be destroyed when there is no longer a legal or business purpose for keeping them. PIPEDA requires businesses to develop guidelines for retention. In BC, if you have used customer personal information to make a decision that directly affects the customer, you have to keep it for at least a year after making the decision so the customer has a reasonable opportunity to access it.

21. How should we dispose of records containing personal information?

Whether your records assigned for disposal consist of paper or electronic records, disks, hard drives, or surveillance tapes, you have a responsibility to ensure that your practices and measures to properly dispose of personal information in your custody meet the safeguard obligations under personal information protection laws. For example, you may hire a paper disposal company to securely shred your records and receive confirmation that shredding was completed. As for the disposal of disks and diskettes you must ensure a complete wipe or destruction of personal information. Any hardware components must have all data removed; where this is not possible, the hardware must be disposed of in accordance with your safeguard policies and procedures.

[3] The technology capable of masking or truncating numbers on receipts does exist, but many businesses have not yet converted to it. Industry advises us that masking the information of the cardholder on all equipment used to electronically process credit card payments should be in place in 2007.

22. What should we do if customers' personal information is improperly used or disclosed?

Depending on the risk of unauthorized access and use, you should contact the information and privacy office that enforces the law that applies to you (Alberta, British Columbia, Quebec, or the federal law) and find out what steps you need to take. Remember, it is important to minimize any harm to your customers.

Resources for Further Information

Organization	Website	Toll-free Phone
Retail Council of Canada	www.retailcouncil.org	(888) 373 - 8245 or (in Edmonton) (888) 481 – 2993 (in Vancouver) (888) 246 - 7705
Office of the Information and Privacy Commissioner of Alberta	www.oipc.ab.ca	(888) 878-4044
Government of Alberta-Service Alberta-Access and Privacy Branch	www.pipa.gov.ab.ca	310-0000; enter (780) 644-7472
Office of the Information and Privacy Commissioner for British Columbia	www.oipc.bc.ca	(800) 663-7867 or (in Vancouver) (604) 660-2421 Local Access: (250-387-5629)
Office of the Privacy Commissioner of Canada	www.privcom.gc.ca	(800) 282-1376
Information and Privacy Commissioner/Ontario	www.ipc.on.ca	(800) 387-0073
Commission d'acces a l'information	www.cai.gouv.qc.ca	(888) 528-7741

This document was prepared to help organizations implement the *Personal Information Protection Act* ("PIPA"). The document is an administrative tool intended to assist in understanding PIPA. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of PIPA, please read PIPA in its entirety. This document is not binding on the Information and Privacy Commissioner of British Columbia.

FOR MORE INFORMATION CONTACT:

Office of the Information & Privacy Commissioner for BC
P.O. Box 9038, Stn Prov Govt
Victoria, BC V8W 9A4
info@oipc.bc.ca

March 2007