PRIVACY PLAN FOR SMALL BUSINESSES

My Privacy Plan

www.priv.gc.ca
Toll-free: 1-800-282-1376

INTRODUCTION

Congratulations! You've just completed the first step to building better privacy protection into your business. Information about your customers - their names, addresses, purchasing history, product preferences - is a valuable business asset. But unlike other assets, there are strings attached. Your customers retain an interest in what you do with their personal information. Mishandling it exposes your business to risks. It can damage your reputation in the community, lead to legal liability and fines, and destroy the trust that is the cornerstone of good relationships with your customers. Building privacy protections into your business will limit these risks and protect your investment in a valuable business asset - your customer information.

The following report will provide you with an action plan and recommendations on how to ensure your organization is secure when it comes to privacy matters.

*Privacy laws vary from province to province. For more information please contact the Provincial or Territorial Privacy Commissioners Office in your area or refer to the case studies available on the provincial websites.

ACTION PLAN

You're now ready to put your privacy plan into action. The following sections will help you do this.

Review of Your Answers
The Review of Your Answers summarizes what information you collect, who in your business collects it, who uses it, and what they use it for. This document gives you a bird's-eye view of your information practices, and will help you manage training needs and ongoing security issues.

Consent Practices
The summary of your Consent Practices clarifies when you can assume a customer is consenting to the collection, use and disclosure of information, and when you need to provide an opt-out or get express consent.

Security Plan
The Security Plan sets out what you can do right now to improve the ways in which you safeguard your customers' information. It also identifies the sensitive information you collect, so you can make sure it's given the highest level of protection.

Third Parties List
The Third Parties List identifies those companies you share personal information with, so you can review the privacy practices of these firms to make sure they meet the same standards that you apply in your business.

Privacy Brochure
The Privacy Brochure helps you get the right information to your customers, so your privacy practices are open and transparent.

Training Plan
Last but not least, the Training Plan identifies the employees who need to be trained in how to obtain consent, and how to answer customer questions about your privacy practices.

Before we review the answers you provided in the quiz, below is a quick review of the different types of information.

Contact Information includes:

- Name
- Address
- Postal code
- Phone number
- E-mail address

Customer Demographics includes:

- Date of Birth/Age
- Gender
- Household Income

Financial Information includes:

- Payment card number
- Payment card expiry date
- Banking information
- Credit records

Purchase Information includes

- Purchase history
- Product/service preferences

Opinions / Interests include:

- Customer satisfaction information
- Opinions about products and services
- Interests and hobbies

Other Information includes:

- Social Insurance Numbers
- Health/medical information
- Drivers license number
- Video or audio security tapes
- Other

REVIEW YOUR ANSWERS

WHO'S ON POINT?

It is important that someone in your organization be responsible for implementing your privacy plan. In your organization, you indicated that individual is:

Name/Title: Design By Dorthy (BDA) Dorthy Roi
Address: 3103 Van Horne Rd
Phone: 250-752-0777
Email: Admin@designbydorthy.ca

INFORMATION YOUR ORGANIZATION COLLECTS:

The following table shows the information you selected when filling out the privacy tool.

TYPE OF INFORMATION	WHAT YOU COLLECT	WHO COLLECTS IT	FOR WHAT REASON	WHO USES IT	STORED BY	SHARED WITH

Contact Information	Name Address Postal Code Phone Number Email Address	Website or IT support	To complete a sale/transaction Contests/Surveys Orders	Website or IT support Myself	Electronic File	
Other Information	Video or audio security tapes	Security		Security	Electronic File	

CONSENT PRACTICES

Consent is voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where the consent may reasonably be inferred from the action or inaction of the individual.

EXPRESS CONSENT

You indicated that you collect the following information that is either sensitive or potentially sensitive.

- **Video or audio security tapes**

When collecting sensitive or potentially sensitive information, you should always make sure you get express consent from your customer. In other words, you must ask the customer directly if they consent to you collecting the information and/or disclosing the information to another company. For example, if you collect financial information for a credit check, have the customer sign an application form that states that you will disclose the information to a credit reporting agency and that the customer consents to this.

Express consent should be used whenever possible and in all cases when the personal information is considered sensitive.

IMPLIED CONSENT

You collect the following information to complete a sale or other transaction, verify a customer's credit, place a special order for a customer, arrange for a delivery, or process a return:

- **Video or audio security tapes**

So long as the information collected is necessary to complete one of the actions listed above, you can assume the customer has consented when he or she provides you with the information. (This is called "implied consent".)

Remember:

- You can't refuse to complete a transaction if the customer refuses to consent to the collection of information that isn't necessary to complete the transaction.
- If you decide later to use this information for another purpose, you have to go back and get the customer's consent.

OPT-OUT CONSENT

You collect the following information for secondary purposes, such as marketing, administering a customer loyalty program, or customer relationship management:

- **Video or audio security tapes**

In these circumstances, you have to give the customer an opportunity to tell you they don't want you to use their information for that purpose. This is called an "opt-out".

Opt-outs must be clear, easy to understand and easy for the customer to do. You can have an opt-out box on a paper-based or web application form, for example, that tells customers that if they don't want to receive promotional material in the mail, just check here. You may want to let the customer know what they'll be missing - special deals and new product information, for example - but don't minimize, hide or obscure the opt-out. And don't make it complicated, like requiring the customer to call a special phone number between certain hours. The point is to let the customer decide.

SECURITY PLAN

EMPLOYEE ACCESS TO CUSTOMER INFORMATION

The following table outlines which employees no longer need to see certain types of personal information in the following categories. Review this table with each group of employees and identify the information that they should no longer be collecting in each category.

EMPLOYEE	CONTACT INFORMATION	OTHER INFORMATION
CASHIER		
IN-STORE SALES REPRESENTATIVE		
SALES REPRESENTATIVE IN THE FIELD		
IN-STORE CUSTOMER SERVICE REPRESENTATIVE		
WEBSITE OR IT SUPPORT	X	
SECURITY		X
CALL CENTRE/TELEMARKETER		
MARKETING REPRESENTATIVE		
OTHER:		

Limit access to this information to those employees who have a need to know. According to your responses in the quiz some employees currently have access to information that they do not need to see. With your employees, review what information they should be collecting and how it should be used. Employees should only have access to information that is absolutely necessary to process transactions as part of their job requirements.

STORAGE OF PERSONAL INFORMATION: PAPER FILES

You indicated your organization does not keep any information in paper files.
In the future, if you do plan to store personal information in paper files, it is extremely important to take all measure possible in order to safely store your customer's personal information. You should protect those files by moving them to:

- **A locked cabinet**

- **A restricted area**
- **An area with an alarm system**

STORAGE OF PERSONAL INFORMATION: ELECTRONIC FILES

The following includes the types of information you may store in electronic files:

- **Name**
- **Address**
- **Postal Code**
- **Phone Number**
- **Email Address**
- **Video or audio security tapes**

It is extremely important to take all measures possible in order to safely store your customer's personal information. Try the following methods to protect those files by using:

- **Computer passwords**
- **Firewalls**
- **Encrypted data files**
- **Encrypted personal information that is sent or received over the Internet (by email or through web forms, for eg.)**
- **Electronic audit trails that identify who has access information**
- **Keeping backup files in a locked cabinet**

Be especially careful with laptops, USB keys and electronic wireless devices. These types of devices can potentially store a large quantity of your customer's personal information. All of these devices should be password protected and have the strongest form of protection possible.

COLLECTION OF SENSITIVE INFORMATION

You indicated that you collect the following information that is either sensitive or potentially sensitive:

- **Video or audio security tapes**

Because of the nature of this information, consider using more than one method to ensure that it is kept confidential.

Finally, go through your old files and destroy any personal information that you no longer need in order to fulfill the purpose that you collected it for.

THIRD PARTIES LIST

You share personal information with the following third party suppliers or agents:

- **With No Other Parties**

You'll have to review the privacy practices of these firms to make sure they meet the same standards that you apply to your business. You should also talk to your lawyer about adding special clauses to any contracts that involve you sharing information with a third party to:

- require the third party to protect your customer information
- give you the power to audit the third party to make sure they're complying with fair information practices
- make sure the third party only uses the information for the purposes set out in the contract
- require the third party to pass on to you any requests from customers to see their customer records

CREATING A PRIVACY BROCHURE FOR YOUR CUSTOMERS

A good privacy statement tells your customers:

- what personal information you collect
- how you use that personal information
- when you assume an individual has consented and when you ask for consent
- when and how an individual can opt out of collection
- who to talk to in your organization if they have questions or complaints

A good privacy statement also makes it much easier to provide your staff with the information they need to answer any customer questions about your privacy practices.

The following is a sample Privacy Statement that you can use to help create your own brochure. Once you've done so, make sure you have copies of the brochure prominently displayed at the cash and customer service desk. Also be sure to post it on your web site.

Sample Privacy Statement

We collect personal information from our customers in the regular course of doing business. This brochure answers some of your most frequently asked questions, and lets you know exactly how we're protecting the information you entrust to us.

What personal information do you collect about me?

We collect the following information about you:

- **Name**
- **Address**
- **Postal Code**
- **Phone Number**
- **Email Address**
- **Video or audio security tapes**

When you visit our web site, we also collect:

- information about your computer, including your IP address, the type of operating system and browser you use, and your computer's location
- what pages you visit on our site and what links you click on
- what other sites you've visited recently

How do you use this information?

The main reasons we collect personal information from you are:

- **Contests/Surveys**
- **Orders**
- **To complete a sale/transaction**

If it's a necessary part of any of these transactions, we may disclose your information to another company. For example, when you apply for credit, we pass on your personal information to a credit reporting agency so we can complete a credit check. We also pass on your name and address to a courier company to complete a delivery.

Use of Personal Information for Secondary Reasons

We also may use your personal information for other, secondary reasons, including:

To complete a sale/transaction

- Name
- Address
- Postal Code
- Phone Number
- Email Address

Contests/Surveys

- Name
- Address
- Postal Code
- Phone Number
- Email Address

Orders

- Name
- Address
- Postal Code
- Phone Number
- Email Address

Sharing of Personal Information with Third Parties

We do not share your personal information with any third parties.

British Columbia
Office of the Information and Privacy Commissioner for British Columbia
P.O. Box 9038, Stn. Prov. Govt.
756 Fort Street, 3rd Floor
Victoria, British Columbia V8V 1X4
Phone: (250) 387-5629
Toll-free: 1 (800) 663-7867 (free within B.C.)
Email: info@oipc.bc.ca
Web Site: http://www.oipc.bc.ca/

TRAINING

Training is absolutely essential if your privacy plan is going to be successful. Your front-line staff are the face of your business. If they can't tell customers why they're being asked for personal information or how they can opt out, it may affect whether or not that customer decides to do business with your organization in the future.

One of the easiest and cheapest ways you can make your business privacy-compliant is to make arrangements immediately to stop collecting information that is not required to run your business. The following table shows the information you said your organization no longer needs to collect in order to perform a certain action.

PURPOSE	CONTACT INFORMATION	OTHER INFORMATION
To complete a sale/transaction	Email Address	Video or audio security tapes
Marketing		
Customer service		
To administer a loyalty program		
Credit verification		
Customer relationship management		

Contests/Surveys	Address Postal Code	Video or audio security tapes
Delivery services		
Warranties		
Returns		
Orders		Video or audio security tapes
Application forms		
Complaints		
Because our computer software asks for it		
Because it may be useful in the future		
Because it is required by law		

It is important to limit your collection to only information that is necessary. In the quiz you indicated that you do not need to collect certain types of personal information for certain purposes. If you do not need to collect information for a certain purpose, then you should limit your collection of information to what is required and necessary. Remember, limiting the collection of personal information to what is required and necessary can reduce the amount of personal information you need to store and your costs to store and safeguard that information.

EMPLOYEE ACCESS TO PERSONAL INFORMATION

All employees should be informed for what purposes they collect, use or disclose customers' personal information and should know when to get consent to use that information for different purposes. Some employees may be questioned about the organization's privacy policies by customers. Prepare your staff to deal with these inquiries and complaints so your customers will be at ease knowing their information is well protected.

You have indicated that some employees do not need to see certain types of information. The following table outlines which employees no longer need to see certain types of personal information in the following categories. Review this table with each group of employees and identify the information that they should no longer be collecting in each category.

EMPLOYEE	CONTACT INFORMATION	OTHER INFORMATION
CASHIER		
IN-STORE SALES REPRESENTATIVE		
SALES REPRESENTATIVE IN THE FIELD		
IN-STORE CUSTOMER SERVICE REPRESENTATIVE		

WEBSITE OR IT SUPPORT	X	
SECURITY		X
CALL CENTRE/TELEMARKETER		
MARKETING REPRESENTATIVE		
OTHER:		

Limit access to this information to those employees who have a need to know. According to your responses in the quiz some employees currently have access to information that they do not need to see. With your employees, review what information they should be collecting and how it is used. Employees should only have access to information that is absolutely necessary to process transactions as part of their job requirements.

Your Privacy Information brochure will help you bring your staff up to speed. Make sure they are familiar with the contents, so they can answer customer inquiries and know what's expected of them.

Also be sure to tell staff that they should contact the individual designated to oversee compliance with privacy if they have any questions or concerns.

Good privacy protection is a group effort. Make sure you train all new staff members so everyone on your team will handle personal information properly.

RECOMMENDATIONS:

HOW MUCH PERSONAL INFORMATION SHOULD YOU COLLECT?

With new information technologies, there's a temptation to collect personal information just in case it could be useful in the future. But under privacy laws, you have to tell your customers why you're collecting the information and then stick to that purpose. If you want to use the information for another purpose, you have to go back to the customer and get his or her permission.

Once you do collect the information, you are also required by law to keep it up-to-date, accurate and secure and to provide customers with access to it on request.

In other words, there are hidden costs and obligations involved when you collect personal information. One of the easiest and cheapest ways you can make your business privacy-compliant is to collect only what you actually need.

Another quick and easy privacy win is to make sure any software or paper forms you use don't have any free-form fields - things like "Notes" or "Additional Information". That cuts down on the possibility that your staff will collect unnecessary personal information.

When you're deciding what to collect, remember that you're obligated to make sure you're only collecting information for purposes that a "reasonable person would consider appropriate in the circumstances". In Quebec, the requirement is that the information has to be "necessary for the object of the file".

So the next step is to review the information you collect and follow the **3 Rs** - make sure it's **Reasonable, Relevant** to your purpose, and **Really Needed** for your business. If not, don't collect it.

HOW TO PROTECT THE PERSONAL INFORMATION YOU COLLECT?

Now that you've limited the personal information you collect to what's **Reasonable, Relevant** and **Really Needed**, the next step is to make sure you keep that information safe and secure.

Under the law, you are required to use security safeguards to protect the personal information you have from things like unauthorized persons getting access to it for copying, modifying or destroying it. Federal laws also talk about protecting it from loss or theft, and Quebec laws call for safety measures that will ensure the information is kept confidential.

Keeping information secure doesn't have to be high-tech. The best protection is to limit who gets access to it on a "need-to-know" basis only. Here's a summary of who uses the personal information you collect in your business.

- **Website or IT support**
- **Security**
- **Other: Myself**

Next, think about how sensitive the information you collect is. Generally speaking, the more sensitive it is, the better your security arrangements should be. Information about a person's health or financial situation is always considered sensitive and must be protected with higher safeguards.

You've indicated that you collect the following sensitive or potentially sensitive information:

- **Video or audio security tapes**

This information needs to be well protected from prying eyes, so consider using multiple methods to protect it. For example, consider purchasing cash registers that truncate ("x" out) payment or credit card numbers on customer receipts to protect the information from identity thieves.

It is also important to remember that other information may be sensitive, depending on the context. For example, the fact a person subscribes to a magazine for cancer survivors may be sensitive in some circumstances. Customer relationship management databases and lists may also be sensitive because they are a lucrative target for identity thieves who want access to the information so they can impersonate your customers.

Next, think about where you keep your personal information. Security can be as simple as locking a filing cabinet or restricting who has access to an office.

You indicated that you keep the following information in electronic files:

- **Name**
- **Address**
- **Postal Code**
- **Phone Number**
- **Email Address**
- **Video or audio security tapes**

Finally, think about what you do with old files. As a general rule of thumb, you should only keep personal information for as long as you need to fulfill the purpose that you collected it for. After that, you should destroy it.

But take care. Canadian organizations have ended up in the news when their old files ended up in boxes on the beach or on the back of real estate pamphlets circulated in Toronto. Invest in a shredder for smaller jobs, and use a magnet to destroy any electronic files that may be stored on old equipment. If you're contracting out, make sure you use a reputable firm that will completely destroy your files.

EXPLAIN WHY AND ASK FOR PERMISSION

The best way to manage your privacy risks is to let your customers know why you're collecting the information and ask them for their permission.

There are times when it's obvious your customer knows why you're collecting the information and consents to it. For example, when a customer hands the cashier a payment card, he or she knows your business will record the card number and pass it onto the bank so you'll be paid. The customer's consent to the use of the card number for the limited purpose of payment can be implied from the circumstances.

You indicated that you collect the following information to complete a sale or transaction, verify a customer's credit, place a special order for a customer, arrange for a delivery, or process a return:

- **Video or audio security tapes**

So long as this information is necessary to complete one of the transactions listed above, you can assume your customer has consented to the collection and use of his or her personal information for that purpose. (This is called "implied consent.") But remember, if you decide later to use this information for another purpose, you have to go back and get the customer's consent.

You have indicated that you collect the following information for the following secondary purposes:

To complete a sale/transaction

- Name
- Address
- Postal Code
- Phone Number
- Email Address

Contests/Surveys

- Name
- Address
- Postal Code
- Phone Number
- Email Address

Orders

- Name
- Address
- Postal Code
- Phone Number
- Email Address

In these situations - when you're using personal information for a purpose other than the original sale or transaction - you can't assume the customer will consent to it being using for something else, like marketing or customer relationship management. In these circumstances, you have to give the customer an opportunity to tell you they don't want you to use their information for that purpose. This is called an "opt-out".

Opt-outs must be clear, easy to understand and easy for the customer to do. You can have an opt-out box on a paper-based or web application form, for example, that tells customers that they don't want to receive promotional material in the mail, just check here. You may want to let the customer know what

they'll be missing - special deals and new product information, for example - but don't minimize, hide or obscure the opt-out. And don't make it complicated, like requiring the customer to write a letter to a specific address within a specific time frame. The point is to let the customer decide.

You have indicated that you collect the following information that is either sensitive or potentially sensitive:

- **Video or audio security tapes**

With sensitive information like this, you should always make sure you get express consent from your customer. Especially if you're sharing the information with a third party, like a credit reporting agency, you must ask the customer directly if they consent to you disclosing the information. You can do this, for example, by having them sign an application form that states what you will do with the information and that they consent to it.

But remember that you can't refuse a sale if the customer refuses to consent to the collection of information that isn't necessary and legitimately needed to complete the transaction. This is called "tied consent" and it is against the law.

Lastly, under federal law, your customers have a right to withdraw their consent at any time, so long as they give you reasonable notice. The exception is where customers have signed a contract that restricts their right to withdraw their consent.

HOW TO RESPOND TO INQUIRIES AND COMPLAINTS

Responding fairly and quickly to customer concerns is one of the fastest ways to privacy compliance. The single most important thing you can do is to make sure your frontline staff knows exactly what personal information your organization collects and why you collect it, so they can answer customers' questions.

Here are the people in your organization who collect information from customers:

- **Website or IT support**
- **Security**

If a customer wants more information about your privacy practices, make sure your frontline staff has copies of a brochure that tells customers:

- what personal information you collect
- how you use it
- what other organizations you share it with and why
- who in your organization they can contact if they want to see their own records, or have questions or complaints
- how to contact the Privacy Commissioner's office for more information or assistance

Also be sure to post a copy of your privacy policy brochure on your web site.

Designing an effective brochure isn't that difficult, once you know what information the customer needs. To make it easier, we'll give you a sample brochure at the end of this training session.

THIRD PARTY SUPPLIERS OR AGENTS

Sometimes sharing customers' personal information is just a regular part of doing business, like when a store passes on a customer's address to a courier to deliver a product. Other retailers may decide to share that information - with the customer's consent - with partners or marketers.

It's important to remember that your responsibility doesn't end when the information leaves your hands. Whenever you share personal information with a third party, it's up to you to make sure it's going to be protected.

Your organization shares personal information with the following third parties:

- **With No Other Parties**

You'll have to review the privacy practices of these firms to make sure they meet the same standards that you apply to your business. You should also talk to your lawyer about adding special clauses to any contracts that involve you sharing personal information with a third party to:

- require the third party to protect your customer information
- give you the power to audit the third party to make sure they're complying with fair information practices
- make sure the third party only uses the information for the purposes set out in the contract
- require the third party to pass on to you any requests from customers to see their customer records
- require the third party to destroy the information once the contract is completed