Disclaimer

Privacy Policy

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**
- **Payment card number**
- **Payment card expiry date**

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:

- **Customer service**
- **Marketing**
- **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:

Marketing

- Name
- Address

- Postal code
- Phone number
- Email address

Customer service

- Name
- Address
- Postal code
- Phone number
- Email address

To complete a sale/transaction

- Payment card number
- Payment card expiry date

Sharing of personal information with third parties

Sometimes, we also share your personal information with other companies, including:

- **None of the above**

We will also disclose your personal information if we are required by law to do so.

How do you get my consent?

When you provide us with personal information to complete a transaction, verify your credit card, place an order, arrange for a delivery or return a purchase, we assume you consent to our collecting it and using it for that specific reason only.

If we ask you for personal information for a secondary reason, like marketing, we will either ask you directly for your consent or provide you with an opportunity to say no. Saying no is called "opting out". By opting out, you can tell us not to collect the information and/or not to share it with other companies.

How do I opt out?

Describe exactly what a customer has to do to opt out. Give concrete examples. For e.g.:

When you fill out a warranty card, you provide us with information about your preferences and opinions. At the bottom of the card, there are boxes you can check off if you do not want that information to be used for marketing purposes or to be shared with other companies.

How do I get more information?

Our staff will be happy to answer any questions you may have about your personal information. If you would like more information about our policies, or you would like to see exactly what personal information we have about you in our records, or you wish to register a complaint, please contact:

Name/Title: Matt Strano CEO
Address: 2060 Fisher Drive
Phone: 705-740-2880
Email: strano@charlotteproducts.com

You can also contact the Privacy Commissioner of Canada for assistance between the hours of 8:30 a.m. to 4:30 p.m. est, at:

Toll-free: 1-800-282-1376
Phone: (819)994-5444
Fax: (819)994-5424
TTY:(819)994-6591

or by mail at:

30 Victoria Street
Gatineau, Quebec
K1A 1H3

or on the web at:

http://www.priv.gc.ca

You can also contact your Provincial or Territorial Privacy Commissioner's office for more information:

Provincial and territorial privacy laws and oversight

- **Alberta**
  Office of the Information and Privacy Commissioner of Alberta
- **British Columbia**
  Office of the Information and Privacy Commissioner for British Columbia
- **Manitoba**
  Manitoba Ombudsman
- **New Brunswick**
  Office of the Integrity Commissioner for New Brunswick
- **Newfoundland and Labrador**
  Office of the Information and Privacy Commissioner for Newfoundland and Labrador
- **Northwest Territories**
  Information and Privacy Commissioner of the Northwest Territories
- **Nova Scotia**
  Office of the Information and Privacy Commissioner Nova Scotia
- **Nunavut**
  Information and Privacy Commissioner of Nunavut
- **Ontario**
  Office of the Information and Privacy Commissioner of Ontario
- **Prince Edward Island**
  Office of the Information and Privacy Commissioner (Prince Edward Island)
- **Quebec**
  Commission d'accès à l'information du Québec
- **Saskatchewan**
  Saskatchewan Information and Privacy Commissioner

- **Yukon**
  Yukon Information and Privacy Commissioner

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	FINANCIAL INFORMATION	OPINIONS/INTERESTS
TO COMPLETE A SALE/TRANSACTION	Name Address Postal code Phone number Email address	• Payment card number • Payment card expiry date	
MARKETING	Name Phone number Email address	• Payment card number • Payment card expiry date	Customer satisfaction info Opinions about products and services
CUSTOMER SERVICE	Name Phone number Email address	• Payment card number • Payment card expiry date	Customer satisfaction info Opinions about products and services

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

You indicated that your organization does not collect any information without knowing why.

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.

- **Sales representative in the field**
- **Call centre/Telemarketer**
- **Marketing representative**
- **Other:**
    - **Director of Finance**

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:

- **Payment card number**
- **Payment card expiry date**

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 paper files:

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

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:

- **Payment card number**
- **Payment card expiry date**

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:

Marketing

- Name
- Address
- Postal code
- Phone number
- Email address

Customer service

- Name
- Address
- Postal code
- Phone number
- Email address

To complete a sale/transaction

- Payment card number
- Payment card expiry date

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

- **Payment card number**
- **Payment card expiry date**

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:

- **Call centre/Telemarketer**
- **Marketing representative**
- **Other:**
    - **Director of Finance**

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:

- **None of the above**

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
- require the third party to destroy the information once the contract is completed