



Best Practices in Data Management

- A Guide for Marketers -



CANADIAN
MARKETING
ASSOCIATION
CANADIENNE
DU MARKETING

CMA|ACM

Prepared with support from the Office of the Privacy
Commissioner of Canada's Contributions Program

INTRODUCTION

As consumers' personal information has become an integral part of virtually all effective marketing programs, Canadian marketers have become adept at meeting both customer expectations and their own business needs while achieving compliance with the various regulatory guidelines that govern the use of personal information.

These regulatory guidelines include federal regulations under the Personal Information Protection and Electronic Documents Act, better known as PIPEDA, as well as provincial regulations in Quebec, Alberta, and British Columbia. These guidelines are equally appropriate for dealing with employee information.

Since these regulatory guidelines provide comparatively few specific instructions on how to carry out the intent of the regulations, preferring, instead, to provide broad directional statements, Canadian marketers have been free to implement the regulations according to the 10 Fair Information Principles established by the CSA that are integrated into Privacy Legislation across Canada. These 10 Principles include:

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

These Principles are reflected in PIPEDA and provincial legislation in Quebec, Alberta, and British Columbia. If organizations and marketers comply with these principles, they will be in compliance with PIPEDA.

Leading marketing organizations have generally been very successful in achieving a workable and sustainable balance between their commercial interests and the privacy interests of their customers. Based on the practices of some of the top companies in Canada, these guidelines provide best practices in four areas of data management: collecting, using, safeguarding, and sharing data.

A. COLLECTING INFORMATION

Organizations collect customer information at different touchpoints and through various channels. When it comes to collection of personal information, some best practices have been established within Canadian companies.

A1. Challenge your motives

Under Principle 2 – Identifying Purposes, it reads:

4.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

When collecting information, there is a tendency to collect more than what is needed “just in case” you need it at a later date. Unless you have clearly indicated how that information will be used, you should not collect it. You would be required to go back to the consumer and identify the new use for the information.

Scrutinize the need for each piece of information you collect. If you don’t need it, don’t collect it. Avoid incident.

A2. Updates cross over all databases

Under Principle 6 – Accuracy, it reads:

4.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

It is the responsibility of the organization to maintain up-to-date customer information as well as ensuring that changes to customer consent preferences are adhered to across the organization.

Regardless of whether information feeds into a single view of the customer or must be updated in several databases, this must be seamless to the customer.

Ramifications of not updating consent preferences across all databases could result in improper use of personal information and unwanted communications going to the customer.

A3. Provide a single view of the Customer

Companies are moving toward holding a single view of the customer. For some companies this is an easy task. For others, there are roadblocks and they are working to overcome the challenges of legacy systems and provisions set out by the CRTC and other regulators.

Companies that are dealing with industry regulations often have many divisions or affiliates with whom they can not share information. For these companies, opt-in campaigns have been introduced to reach out to customers and educate them on the benefits of a company being able to share information across divisions.

Companies that face the IT expenditure roadblock of legacy systems are promoting the need for change throughout their organizations and gaining buy-in from their various business units.

A4. Limit use of free form fields

Information is often collected by customer service representatives. Data is input into onscreen forms and is automatically saved in the database. By eliminating free form fields, often titled “Notes” or “Additional Information”, you are ensuring that customer service representatives will only collect the necessary information, limited by the form on their screen.

Free form fields invite the input of unauthorized information, like opinions about a customer or information about a specific complaint. It is not always possible to completely eliminate free form fields so it is imperative that staff be trained in privacy issues and are able to make informed decisions on the information captured in these fields. Information held in these fields is considered personal information that can not be used or disclosed without consent.

It is also important to remember that all information, including information in these free form fields must be disclosed to customers when asked as per Principle 9:

4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

B. CONSENT TO USE INFORMATION

Principle 3 – Consent states:

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Consent is defined as a customer's agreement for the future use of his or her personal information for marketing purposes, subject to the following industry definitions of types or degrees of consent:

Implied consent is used to communicate with one's own customers, such as sending out a magazine subscription renewal notice or a solicitation for a further donation.

Opt-out consent is used to grant permission for use of the customer's information to send future marketing offers or solicitations not directly related to the original transaction, as well as to grant permission for the transfer of the customer's personal (non-sensitive) information to a third party. (Example: a list rental of newspaper subscribers' names and addresses for marketing purposes).

Positive or opt-in consent is required for the transfer of information a reasonable person would consider sensitive, to a third party (Example: financial or health information, or certain video rentals or magazine subscriptions).

Best practices in gaining consent have been established:

B1. Provide examples

Privacy language and intended uses of information can be confusing to a customer. If they don't know exactly what you are intending to use their information for, there is a chance they will err on the side of caution and withdraw their consent. You will have lost your opportunity to contact them.

Customers need to see the specifics. For example, when listing the intended uses of their information, if you simply state that you will be using the information "To develop, enhance, market or provide products and services" warning bells may go off that they will be bombarded with advertising from your company. By further adding an example a customer has a better idea of what that means and is less concerned. So, instead say:

"To develop, enhance, market or provide products and services. For example, we look at how our customers use our products and services, so that we can understand how to improve them. From time to time, we may review and analyze your use of our products and services to help us provide better product recommendations and special offers that we think will interest you."

B2. Don't further irritate customers with the opt-out process

The Canadian Marketing Association (CMA) Privacy Code provides marketers with specific guidelines around opt-out consent. It must be easy for the customer to see, understand and execute. CMA further explains what this means for marketers:

Easy to see - the placement or timing of the opt-out opportunity must be obvious to the customer (including, for example, being 'Easy to hear,' by way of vocal style or loudness), and that the manner of its presentation (whether by size, colour, contrast, length of presentation or other characteristic) must be reasonable, and fairly balanced with the placement, timing and manner of presentation of any marketing offer which accompanies it. Marketers should not hide, minimize, obscure or distract customers from the opt-out opportunity.

Easy to understand - the language employed in the opt-out opportunity must be familiar to the customer and appropriate to his or her age and inferred educational attainment or general sophistication.

Easy to execute - the customer can accept and implement the opt-out opportunity in a minimum number of steps. Marketers must not require a customer who accepts an opt-out opportunity to respond within unreasonably restricted dates or times, to call frequently busy or unanswered telephone numbers, or to incur an unreasonable cost. CMA believes that customers incurring costs not exceeding the cost of a postage stamp are reasonable.

Provide sufficient information to allow a reasonable person to make an informed decision - marketers must provide customers considering an opt-out opportunity with a general indication of the purposes and subsequent uses of their information. For example the opt-out could include an explanation of the types of goods or services -or charitable need - being offered/solicited and the frequency of offers or solicitations. Members must still advise customers and obtain their consent prior to transferring personal information to any third party.

They say that "timing is everything". So, as one retailer pointed out, discussing consent on a busy Saturday afternoon while customers are lined up to make their purchases, is not an appropriate time.

To ensure that the process of opting out is not a new irritant for customers, think carefully about what makes sense for your business and your customers while keeping the principles of easy to see, use, and understand top of mind.

B3. Help customers understand benefits of consent

Looking at opt-out options, a simple “do not market” might be too vague. If you expanded the language to say, “By opting out of marketing, you will no longer receive x, y, and z”, you are informing the customer about what opportunities they will miss out on. This could be an annual catalogue, bonuses, or new service opportunities. Guaranteed, you will hear from customers who have not been extended the same opportunities as their friends and neighbors even if the reason is the fault of their decision to opt-out.

B4. Provide specific opt-outs

Although creating too many opt-outs is confusing to the customer and a logistics nightmare for the company, you need to create a balance. You do not want to miss out on legitimate opportunities to contact your customers and in many cases, they do not want a full “do not solicit” privacy block.

Allow your customers to opt-out of different channels, e.g. email solicitations. This will help to keep the lines of communication open with customers through their preferred channels so they do not miss out on opportunities.

For companies offering a broad range of products and/or services, allowing customers to opt-out of specific things they do not want leaves you open to market them the products or services they do want to hear about.

B5. Define what they can't opt-out of

For obvious reasons, a customer cannot opt-out of all uses of information and communications with a company they do business with. A company must be able to provide invoices, statements, or other critical materials in order to maintain a business relationship.

Some companies have taken this a step further by saying that their customers can not opt-out of being contacted for market research. They clearly state that understanding customer satisfaction, needs and preferences are imperative to successfully meet the needs of customers. The customer can simply decline to complete the survey when approached.

B6. Find out what triggered a decision to opt-out

Whenever possible, have a dedicated 1-800 number for dealing with privacy issues. What makes the 1-800 option more effective is it allows the customer service personnel to probe for specific reasons for wanting to opt-out and potentially resolve an issue for that customer or highlight a larger issue that affects several customers.

B7. Watch your wording

Do not fall into the “Do not solicit” trap. Although seemingly similar to “Do not market”, the term solicit is all encompassing and will thwart all opportunities to contact them, even for non-marketing related reasons.

B8. Individual versus household

Understanding your customer base and how it rolls up into households is critical in assuring that opt-outs are properly recognized. For each product and service offering you need to consider what is appropriate, treating as a household or an individual. It should be transparent to your customers.

Household

For example, suppose a lawn care company has both a husband and wife as separate records in their database. Subsequently, the husband has asked to no longer be contacted about lawn care. It is in the best interest of the company to assume that the opt-out applies to the household and should then indicate in the database that the wife should not be contacted about lawn care.

Individual

On the other hand, suppose a financial institution has accounts with both a husband and wife as two separate records in the database. If the husband asks not to be contacted for marketing purposes, this request cannot be carried over to the wife’s record unless she makes the same request.

B9. Permission based e-Marketing

When it comes to e-Marketing, Canadian marketers clearly recognize that opt-in consent maximizes their opportunities to interact successfully with consumers, while minimizing the chances of annoying or offending the customer. This is the coveted ‘win-win’ situation.

C. SAFEGUARDING INFORMATION

The Canadian Marketing Association's Principles for the Protection of Personal Information start from the foundation of recognizing that consumers' personal information is a unique and valuable asset. In addition, and unlike tangible assets, the consumer retains an interest in that asset, even though it's in the possession of the marketer.

Accordingly, the Principles mandate a multi-disciplinary approach to protecting such assets. This approach begins with limiting the collection and use of personal information to that required to complete the purpose for which it was originally collected, and retaining it only so long as it is required for that purpose.

Under Principle 7 – Safeguards, it reads:

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

To uphold this principle, top organizations have established some best practices, including.

C1. Information should be viewed on a “Need to Know” basis

Organizations have taken considerable care to ensure that access to the information they hold is strictly limited and granted only on a 'need-to-know' basis – sometimes to a very small group.

C2. Central data warehouse

Many organizations have data warehouses where data comes in from various databases and updated information, such as changes to consent status is then disseminated back to the individual databases. Those with data warehouse resources noted a variety of means of assuring the integrity of their customer files, notably requiring both substantial points of similarity in contact information, such as surname, first name and initial matches, and addresses, as well as activity 'timestamps' so you know when key information was last updated.

C3. Incident investigation

Regardless of how big or small, you are required by law to take every privacy complaint or internal notification of a breach seriously. Establish a formal incident investigation process to determine if it was “a one-off oops” or indicative of a systemic problem.

Under Principle 10 – Challenging Compliance, it reads:

4.10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

C4. Seek and you will find

Identify information security issues before someone else does.

Companies tend to focus on the big things but it is the small stuff that tends to slip through the cracks. As an exercise, think about all the places a customer's credit card information has been recorded over the years, including all forms (paper and online). Now, think about where that information is stored today. Is it in filing cabinets, on personal computers, in a central database? Who has access to those areas and subsequently, perhaps unknowingly has access to that sensitive information. Other questions you might ask is whether forms provided to contractors included the credit card information that they did not need. Based on your answers, can you with confidence say that your organization is doing everything possible to ensure the security of personal information?

Remember, one person does not have all the answers. It must be an organizational wide endeavor to seek out security breaches before a customer or competitor points them out to you.

D. SHARING INFORMATION WITH PARTNERS

Where personal information is to be disclosed to another party or used for some purpose not directly connected to the original purpose, the customer must be provided with an opportunity to opt-out of further marketing uses of their information.

When it comes to sharing information, Canadian companies have established some best practices, including:

D1. Develop standard outsourcing requirements

You are responsible for your customer's personal information when in the hands of a third-party. Whenever entering into a contract with a third party where it involves the transfer of customer's personal information, you must have a standard outsourcing requirements for privacy. These should be presented first in the RFP and then written into the contract.

Under Principle 1 – Accountability, it reads:

4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

D2. Use a third party methodology when working with partners

Leading Canadian marketers zealously protect the value represented by their lists. They have the utmost respect for their customers and endeavor to ensure that they maintain the confidence of their customers. They recognize that customer lists, for example, are a proxy for their customer relationships and are therefore extremely valuable assets.

To protect their assets they are very careful to ensure that any other marketer (or service provider) with whom they partner will represent their company well, but beyond that they have a duty to the customer to maintain the privacy of their information.

A number of companies have adopted what is termed a third-party methodology. Rather than disclose their customer base to their partners, information is shared with an independent third-party, often the group that is running the partner's campaign. That third-party is under contract to only use the list for the intended purpose and is not permitted to share the list with the partner company.

The only way a partner company will know if a customer was contacted with their offer is if the customer responds directly to the partner company.

D3. Share only the necessities

Strip out all information about your customers other than the essential information needed to perform a given task.

For example, a mailing house does not need customer phone numbers or email addresses.

D4. Seed the list

Regardless of the legal or contractual agreements you have with partners or other parties such as mailing houses, it is best to have checks in place. Seeding your list with your own address and a fictitious name will give you peace of mind that the lists you provide are only used for the purposes set out in the agreement. Be up front and honest by telling your partners that it is a standard practice of your organization to seed your lists to monitor partners' performance and ensure that partners are abiding by the terms of the list use agreement.

SUMMARY OF BEST PRACTICES

While the most important thing is to ensure your company is compliant with Privacy Laws in Canada, these Best Practices can help take your company to the next level.

A. Collecting Information

1. Challenge your motives
2. Updates cross over all databases
3. Provide a single view of the customer
4. Limit use of free form fields

B. Consent to Use Information

1. Provide examples
2. Don't further irritate customers with the opt-out process
3. Help customers understand benefits of consent
4. Provide specific opt-outs
5. Define what they can't opt-out of
6. Find out what triggered a decision to opt-out
7. Watch your wording
8. Individual versus household
9. Permission based e-Marketing

C. Safeguarding Information

1. Information should be viewed on a "Need to Know" basis
2. Central data warehouse
3. Incident investigation
4. Seek and you will find

D. Sharing Information with Partners

1. Develop standard outsourcing requirements
2. Use a third party methodology when working with partners
3. Share only the necessities
4. Seed the list