THE MARKETER'S PIPEDA CHECKLIST 1 OF 3

Ensure Your E-Newsletter Campaign is PIPEDA-Compliant

Online privacy remains a key concern for your customers and an important point of differentiation.

Use this checklist – created by privacy experts in the fields of Internet Marketing, Privacy, Accounting and Law – to help ensure that your marketing campaigns and processes are compliant with the current PIPEDA legislation.

Before your E-newsletter Marketing Campaign

- Review your distribution list to ensure accuracy of recipients' contact information.
- Review your distribution list to ensure recipients have provided consent – either explicit or implicit (*See note on third parties).
- Collect permission, confirm contact information and document how consent was obtained.
- If you are using business email addresses, apply the relevant provincial rules for gathering consent.
- Confirm special age-related consent requirements and that materials are age appropriate.
- Identify the person(s) who require access to the databases storing the recipients' information – based on if they are going to collect, store, update, analyze and/or distribute the information.
- Establish a policy (i.e. timetable, guidelines and accountability) for updating or purging recipients' personal information. Communicate this policy to those employees who have access to personal information. Train thoseemployees responsible for implementing and monitoring privacy procedures.
- Identify a contact person who will deal directly with any recipient, prospect and supplier who inquires about the use of their personal information.
- Develop and make available a privacy policy outlining your firm's commitment and processes to protect recipients' personal information. For example, define how information gathered during the distribution of the newsletter will and won't be used.

During your E-Newsletter Marketing Campaign

- Use the e-newsletter to collect consent and update information.
- Clearly identify your organization and the purpose of each e-newsletter.
- Provide recipients the option of opting out of receiving the newsletter. Ensure opting out is easy to understand and easy to execute.
- Provide a link to your privacy policy from within the e-newsletter – e.g. on pages requesting personal information.
- Inform recipients whose emails wereobtained from a third-party why they are receiving the e-newsletter and when/ how consent was obtained.
- Gather consent again if you plan to use personal information in a different way than you had stated when originally gathering consent.

After your E-Newsletter Marketing Campaign

- Deposit any feedback from recipients that is attributable to a specific person into database(s) with restricted access.
- Clearly identify your organization and the purpose of each e-newsletter.
- Provide recipients the option of opting out of receiving the newsletter. Ensure opting out is easy to understand and easy to execute.

*Note on Third Parties: If you have used any third parties in collecting your list, review their commitments to ensure that they have safeguards to adequately protect the list and will not share information without your expressed consent.

For example, have service providers sign agreements that safeguard data to protect personal information from unauthorized access and audit their compliance with contractual obligations. Also, choose suppliers that have passed privacy and security audits.

This checklist has been created as a joint effort by:

Thindata 1-1 A TRANSCONTINENTAL COMPANY

NYMITY

Bennett Gold LLP CHARTERED ACCOUNTANTS

Lang Michener LLP

THE MARKETER'S PIPEDA CHECKLIST 2 OF 3

Ensure Your Online Contest (i.e. On Website and Email) is PIPEDA-Compliant

Online privacy remains a key concern for your customers and an important point of differentiation.

Use this checklist – created by privacy experts in the fields of Internet Marketing, Privacy, Accounting and Law – to help ensure that your marketing campaigns and processes are compliant with the current PIPEDA legislation.

Before your Online Marketing Contest

If the contest consists of an email component, follow the guidelines for E-Newsletters on Checklist #1.

- Review your distribution list to ensure accuracy of contestants' contact information.
- Identify the person(s) who require access to the database(s) storing the contestants' information – based on if they are going to collect, store, update, analyze and/or distribute the information.
- Review who has access to the database(s). Limit access to those who need access to the database(s).
- Establish a policy (i.e. timetable, guidelines and accountability) that clearly defines how information gathered during or after the contest will and won't be used. (*See note on third parties).
- Establish a policy for updating or purging contestants' personal information. Communicate this policy to those employees who have access to personal information. Train those employees responsible for implementing and monitoring privacy procedures.
- Identify a contact person who will deal directly with any contestant who inquires about the use of their personal information.

During your Online Marketing Contest

- Clearly define the terms of the contest. Make the terms available. Terms need to comply with The Competition Act and The Criminal Code.
- If contestants include children, consider including age-appropriate validation and comply with the Canadian Marketing Association's rules regarding advertising to children.
- Ensure "ballot" form is secure and encrypted.
- Provide a link to your privacy policy on the same page as the contest entry form.

After your Online Marketing Contest

- Deposit any feedback from contestants that is attributable to a specific person into database(s) with restricted access.
- Identify an individual responsible for monitoring the collection, use, storing, updating and distribution of contestants' personal information as set out in the firm's privacy policy. Establish a schedule for monitoring and documenting these procedures.
- Provide up-to-date training for those held accountable for maintaining privacy procedures.
- Establish, follow and monitor a timetable for purging contestants' personal information. This information should be kept long enough to deal with any complaints or audits.

*Note on Third Parties: If you have used any third parties in collecting your list, review their commitments to ensure that they have safeguards to adequately protect the list and will not share information without your expressed consent. For example, have service providers sign agreements that safeguard data to protect personal information from unauthorized access and audit their compliance with contractual obligations. Also, choose suppliers that have passed privacy and security audits.

This checklist has been created as a joint effort by:

Thindata 1-1 A TRANSCONTINENTAL COMPANY

NYMITY

Bennett Gold LLP CHARTERED ACCOUNTANTS

Lang Michener LLP

THE MARKETER'S PIPEDA CHECKLIST 3 OF 3

Ensure Your Online Event Registration (i.e. Webinar) is PIPEDA-Compliant

Online privacy remains a key concern for your customers and an important point of differentiation.

Use this checklist – created by privacy experts in the fields of Internet Marketing, Privacy, Accounting and Law – to help ensure that your marketing campaigns and processes are compliant with the current PIPEDA legislation.

Before your Online Marketing Event

Note: If online registration uses email, follow the guidelines for E-Newsletters on Checklist #1.

- ☐ Identify the person(s) who require access to the database(s) storing the registrants' information - based on if they are going to collect, store, update, analyze and/or distribute the information.
- ☐ Establish a timetable for regularly updating or purging registrants' personal information.
- ☐ Review who has access to the database(s). Limit access to those who require it.
- ☐ Establish a policy (i.e. timetable, guidelines and accountability) that clearly defines how information gathered during or after the event will and won't be used. (*See note on third parties).
- ☐ Establish a policy for updating or purging registrants' personal information. Communicate this policy to those employees who have access to personal information. Train those employees responsible for implementing and monitoring privacy procedures.
- ☐ Identify a contact person who will deal directly with any registrant who inquires about the use of their personal information.
- ☐ Develop and make available a privacy policy outlining your firm's commitment/ efforts to protect registrants' personal information.

During your Online Marketing Event's Registration

- ☐ Clearly explain how any information gathered during the event registration process will and won't be used. Also explain that information is collected, used and discarded in accordance with your privacy policy.
- ☐ Ensure registration and/or collection of credit card information is secure and encrypted.
- ☐ Provide a link to your privacy policy on the same page as the registration form.

After your Online Marketing Event

- ☐ If you are collecting credit card information, ensure that PCI security standards have been implemented.
- ☐ Identify an individual responsible for monitoring the collection, use, storing, updating and distribution of registrants' personal information as set out in the firm's privacy policy. Establish a schedule for monitoring and documenting these procedures.
- ☐ Provide on-going training for those held accountable for maintaining privacy procedures.
- ☐ Establish, follow and monitor a timetable for purging registrants' personal information. This information should be kept long enough to deal with any complaints or audits.
- ☐ Only use information for the purpose stated during the registration.

*Note on Third Parties: If you have used any third parties in collecting your list, review their commitments to ensure that they have safeguards to adequately protect the list and will not share information without your expressed consent. For example, have service providers sign agreements that safeguard data to protect personal information from unauthorized access and audit their compliance with contractual obligations. Also, choose suppliers that have passed privacy and security audits.

This checklist has been created as a joint effort by:

Thindata 1-1 A TRANSCONTINENTAL COMPANY

NYMITY

Bennett Gold LLP CHARTERED ACCOUNTANTS

Lang Michener LLP