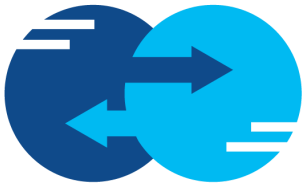

Trackon Canada Private Ltd

Canadian Privacy Policy

Version Number: 1.0

Last Updated: July 2022

Next Update: January 2023

Senior Officer Approval for Program: Jaspreet Singh, Director

Document Classification: Confidential

Table of Contents

1 Policy Statement

1.1 Our Commitment

Trackon Canada Private Ltd (Trackon) is committed to the protection of personal information (PI) in its possession and adheres to prescribed and best practices to ensure appropriate methods are followed in the collection, use, security and access to information collected from customers and potential customers. To that end, it is the responsibility of every employee (including contract and part time employees) to comply with this program and with Personal Information Protection and Electronic Documents Act (PIPEDA), legislation related to PIPEDA and applicable provincial and/or territorial privacy laws as required.

Personal information (PI) is defined as information about an identifiable individual such as name, date of birth. This also includes non-personal information that we link to personal information.

Our procedures for implementing this policy are described in separate documents.

There are also separate training materials for staff, which include quizzes designed to test the effectiveness of training.

Note that legislative requirements for other jurisdictions in which Trackon operates is dealt with in documents specific to those jurisdictions. The set of documents described in this section is specific to Trackon's Canadian operations, customers and staff.

In addition, we assure our customers that we uphold their privacy with the utmost respect. Below is our Privacy Policy to our customers:
"At Trackon, we respect your privacy and take pride in protecting your personal information. Our Privacy Policy is designed to meet or exceed the requirement of Canadian privacy laws and we are constantly reviewing our practices and procedures as well as considering feedback from our consumers.

From time to time, we may make changes to this Privacy Policy to comply with applicable law or because of changes to our Privacy practices.

The below demonstrates our commitment to you.

Consent: Unless permitted or required by law, we will not collect use or share personal information without first obtaining your consent. We will obtain

consent when we want to use personal information for a new purpose or for a purpose other than that which was stated at the time of collection.

You may withdraw your consent for certain purposes. For example, if you choose not to receive marketing or information related to our products services or promotions.

Collection: We collect your personal information in a variety of ways such as during the course of onboarding and servicing, We may also collection personal information through our marketing activities. The following are examples of personal information that we collect:

- Customer name and contact information, including mailing address, telephone numbers, fax number and/or email address;
- Additional information for identity matching and credit check purposes.
- Payment-related information, such as banking information; and
- Such other information we may collect with your consent or as permitted or required by law.

Purpose: We identify the purpose for which personal information will be used at or before the time the information is collected. We collect personal information for the provision of severing.

How We Share: We may share personal information for the purposes described at the time we obtain consent. This may include sharing of your personal information with third parties.

How We Protect

We strive to maintain appropriate physical and technical safeguards to ensure no loss miss use an authorized access or modification of your personal information on file. All records are kept electronically and securely.

Inquires

Trackon has appointed a Privacy Officer to oversee compliance with this Privacy Policy and applicable privacy laws. Any questions related to the Policy or the handling of personal information by Trackon can be addressed to the Privacy Officer who may be contacted at:

Attention: Privacy Officer
Rishi Dubey, Privacy Compliance Officer,
Trackon Canada Private Ltd
4440 5th St. NW
Edmonton, AB, Canada T6T 0Z9
rk@paypenny.io
416-323-3112

If you are not satisfied with Trackon's response to a privacy-related matter, you may contact the Office of the Privacy Commissioner of Canada at 1-800-282-1376 or at www.privcom.gc.ca."

2 Regulatory Background

2.1 Privacy and Related Legislation

The Personal Information Protection and Electronic Documents Act (PIPEDA) sets out the requirements that Trackon must use to collect, use or disclose personal information in the course of its commercial activities, including information about employees[1]. In addition, some provinces have privacy laws and have additional requirements that must be followed.

Additional legislation, that has privacy related components, that set out other requirements that Trackon must comply with is Canada's Anti-Spam legislation (CASL). The requirements in these pieces of legislation guide the way we can electronically market to potential customers and how we communicate with our existing customers.

2.2 The Regulators

The Office of the Privacy Commissioner of Canada (OPC), also referred to as the Privacy commissioner, oversees compliance with PIPEDA. Their mission is to protect and promote the privacy rights of individuals which is done by:

- Investigating complaints;
- Conducting audits and pursuing court action under federal privacy law;
- Publicly reporting on the personal information handling practices of public and private sector organizations;
- Supporting, undertaking and publishing research into privacy issues; and
- Promoting public awareness and understanding of privacy issues.

The OPC is also tasked with investigating violations related to CASL, in particular,

- The harvesting of electronic addresses, in which email list are compiled through the use of computer programs to automatically mine the Internet for email addresses; and,
- The collection of personal information through illicit access to other computer systems (i.e. through spyware).

[1] https://www.priv.gc.ca/en/privacy-topics/privacy-at-work/

Each province and territory in Canada has a commissioner or ombudsman responsible for overseeing provincial and territorial privacy legislation. In most cases, these individuals or bodies defer to the OPC.

The Canadian Radio-television and Telecommunications Commission (CRTC) has been tasked with overseeing compliance with CASL. They are responsible for investigating the sending of unsolicited commercial electronic messages, unsolicited telecommunications and the installation of software without consent.

2.3 Regulator Audits

The OPC conducts audits to ensure companies are sufficiently managing personal information in its possession. These audits may look at the physical and security controls in place, what policies and procedures exist, and how the organization manages privacy issues. Through these reviews, the OPC can identify areas for improvement which may result in public disclosure or compliance agreements.

The OPC has the power to receive, initiate, investigate and attempt to resolve complaints about any aspect of Trackon' s compliance with PIPEDA provisions.

The CRTC has the power to receive, initiate, investigate and attempt to resolve complaints about any aspect of Trackon's compliance with CASL provisions under which they can leave decisions, notices and orders in respect to non-compliance.

3 Roles and Responsibilities

Everyone has a responsibility to ensure that our privacy compliance program runs smoothly.

- **Senior Management**:
  - Ensure occurrences of non-compliance with this policy, associated procedures and applicable governing legislation are appropriately addressed;
  - Approve the Privacy Officer's appointment;
  - Approve a CASL point person; and
  - Reviewing and approving amendments to this policy, as required but at least annually.

- **Privacy Officer**:
  - Developing and maintaining this policy, which includes regularly reviewing and updating and maintaining a record of all updates;

- Ensuring effective procedures and controls are in place in order to meet privacy obligations under law.
- Ensuring that all employees and other relevant parties received appropriate privacy and privacy related training;
- Reporting the Senior Management and the Board of Directors (if applicable) on the status of the privacy program, including any issues of non-compliance with governing legislation;
- Maintaining records in accordance with privacy legislation;

- Corresponding with the OPC and other regulators as required;
- Conduct Privacy Impact Assessments as required; and
- Developing breach and incident management response protocols, initiating them when necessary;

- **All Employees**:
  - Complying with the requirements set out in the Privacy program;
  - Reporting privacy concerns to the Privacy Officer; and
  - Complete privacy and privacy related (i.e. CASL) training as required.

4 Privacy Compliance Program Requirements

As a company subject to PIPEDA Trackon is required to comply with the 10 privacy principles. Trackon is responsible for the protection of personal information and the safeguarding of it, extending to third parties Trackon may deal with. Trackon is required to obtain an individual's consent when collecting, using or disclosing the individual's personal information and the purpose for which we are collecting, using or disclosing must be disclosed when obtaining that consent.

4.1 Principle 1 – Accountability

Trackon is responsible for the personal information it holds and must designate a Privacy Officer that is accountable for compliance with the following principles.

Under the "Accountability" principle Trackon must:

- Designate a Privacy Officer to be accountable for Trackon's compliance with the 10 principles set out below;
- Make the identity of the Privacy Officer known;
- Protect all personal information in Trackon 's possession, including information that has been transferred to a third party;
- Use contractual or other means to ensure protection of personal information which has been passed to a third party;
- Develop and implement procedures to uphold the 10 principles;

- Establish procedures for receiving and responding to complaints and inquiries – including information access request; and
- Train staff and ensure dissemination of Trackon's procedures related to privacy.

4.2 Principle 2 - Identifying Purposes

The purposes for which personal information is collected must be identified at or before the time it is collected.

Under the "Identifying Purposes" principle Trackon must:

- Identify why personal information is being collected at the time of or before collection;
- Disclose the purposes for collecting personal information; and
- Notify customers, before using personal information for any purpose not identified at the time of collection.

4.3 Principle 3 – Consent

The consent of an individual is required for the collection, use or disclosure of personal information.

Under the "Consent" principle, Trackon must:

- Obtain the individual's consent for any collection, use, or disclosure of personal information ensuring that the individual understands;
- Advise of the purposes for which personal information will be used for or disclosed ensuring the individual can reasonably understand what their personal information will be used for;
- Obtain consent before using personal information for other purpose not identified at the time of collection;
- Never require an individual to consent, as a condition of supplying a product or service, beyond what is necessary to fulfill on the product or service;
- Consider the reasonable expectations of the individual in obtaining consent;
- Never obtain consent through deception;
- Consider the sensitivity of the personal information when determining how you will obtain consent; and
- Allow the individual to withdraw consent at any time and inform of any consequences of withdrawing consent.

4.4 Principle 4 – Limiting Collection

The collection of personal information is limited to that which is necessary for the purposes identified by Trackon.

Under the “Limiting Collection” principle Trackon must:

- Limit its collection of personal information (type and amount) to what is necessary for identified purposes;
- Never collect personal information indiscriminately;
- Collect personal information without misleading; and
- Document the types of information we will collect.

4.5 Principle 5 – limiting use, Disclosure, And Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required under law. Personal information shall be retained only as long as necessary.

Under the “Limiting Use, Disclosure, and Retention” principle Trackon must:

- Never use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law;
- Retain personal information only as long as necessary;
- Develop procedures regarding the disposal of personal information.
- Assess risks of destroying personal information on or off-site.
- Destroy, erase, or anonymize personal information that is no longer needed;
- Develop and implement procedures regarding the retention of personal information; and
- Include minimum and maximum retention periods in the procedures.

4.6 Principle 6 – Accuracy

Personal information should be accurate and up-to-date for the purposes for which it is to be used.

Under the “Accuracy” principle, principle Trackon must:

- Ensure that personal information is as accurate and up-to-date;
- Update personal information if necessary to fulfill the purposes for which the information was collected; and
- Ensure that information is sufficiently accurate and up-to-date to ensure fair decisioning of an individual.

4.7 Principle 7 – Safeguards

Personal information must be safeguarded appropriately based on the sensitivity of the information.

Under the “Safeguards” principle, Trackon must:

- Protect personal information by security safeguards appropriate to the sensitivity of the information;
- Institute security safeguards that will protect personal information against loss, theft, unauthorized access, copying, modification, etc.;
- Protect personal information regardless of the format in which it is held;
- Ensure staff is aware of the importance of maintaining the confidentiality of personal information;
- Use care to prevent unauthorized access when destroying or disposing of personal information; and
- Include physical controls such as locked filing cabinets and restricted access to offices use of passwords and encryption.

4.8 Principle 8 – Openness

Trackon must make available to individuals specific information about its policies and practices relating to the management of personal information.

Under the "Openness" principle, Trackon must:

- Be open about practices relating to the management of personal information;
- Make specific information regarding the management of personal information readily to your clients and customers;
- Include the name or title, and address, of the person who is accountable for the Privacy program and where complaints or inquiries can be sent; and
- Describe how to gain access to personal information it holds.

4.9 Principle 9 – Individual Access

Upon written request, Trackon must inform individuals of the existence, use, and disclosure of their personal information and must give access to that information. Individuals can challenge the accuracy and completeness of the information.

Under the "Individual Access" principle Trackon must:

- On written request, inform individuals of the existence, use, and disclosure of their personal information, and give access to that information, except as specified in Section 9 of PIPEDA such as in doing so would likely reveal personal information about a third party;
- Allow individuals to challenge the accuracy of their personal information;
- Upon receiving a request in writing inform individuals (via an acknowledgment letter) if we hold personal information about them;

- Allow access to the information, providing details of how Trackon has used or will use it including if the information has been passed to third parties.
- Respond to the access request within 30 days after receiving the request. Note the acknowledgment letter does not constitute a response.
- Where more than 30 days is required, we must send the individual a notice within 30 days, advising of the new time limit and the reasons for the extension, and inform them they have the right to complain to the OPC;
- Provide requested information in a format that is easy to understandable;
- Respond to access request with no cost to the individual;
- If you refuse an access request, inform the individual in writing, along with the reasons and inform them they have the right to complain to the OPC;
- Keep records for access request for as long as necessary;
- When an individual proves there is inaccuracy of personal information, we must amend the information as required;
- When a challenge is not resolved, a record of the details of the unresolved challenge should be kept;

4.10 Principle 10 – Challenging Compliance

An individual is able to challenge compliance with the above principles to Trackon's Privacy Officer.

Under the "Challenging Compliance" principle, Trackon must:

- Trackon must have in place procedures for receiving and responding to complaints regarding the handling of personal information;
- Establish complaint procedures that are easily accessible and easy to use;
- Inform complainants that there are complaint procedures;
- Investigate all complaints; and
- Take appropriate action if a complaint is found to be justified, such as correcting the issue and amending procedures as necessary.

5 Privacy Impact Assessments[2]

A Privacy Impact Assessments (PIA) is a tool that helps ensure privacy is a core consideration to our business on an ongoing basis and when a new project or a

[2] In Canadian legislation and related guidance, PIAs may also be described as self-assessments. While this is a best practice for medium and large organizations, Trackon has chosen to conduct such assessments on an ad-hoc basis.

significant change in Trackon's business model is being planned and implemented.

PIAs are meant to describe and document what personal information will be involved and what privacy controls are needed to be in place to ensure compliance and how we have improved our own privacy systems and practices over time.

The 10 privacy principles, described above, guide how a PIA is conducted. Trackon must look at the design effectiveness, implementation, and operating effectiveness of privacy controls/processes.

A sample PIA form is included as an appendix to this document. This form has been developed based on OPC guidance[3], however, the Privacy Officer may make modifications to the form on an as-needed basis.

The PIA form should be completed in conjunction with the Privacy Officer as it related to new projects or significant change in Trackon's business model. Any staff managing initiatives involving personal information must notify the Privacy Officer that a PIA is required, and work with the Privacy Officer to complete the PIA. In order to avoid delays, sufficient time must be allotted in project plans to allow for the completion of a PIA, as well as any risk mitigation implications deemed necessary. These must be completed prior to the "go live" date of new projects and/or processes.

Staff that are uncertain as to whether or not a project or process change under their management has a privacy or PI related component that requires the completion of a PIA should contact the Privacy Officer.

6 Breach Response Plan (Mandatory Breach Notification)

In the event Trackon suspects or has a breach of security safeguards, which is the loss of, unauthorized access to, or disclosure of, personal information under our control and if it is reasonable to believe the breach creates a real risk of significant harm, the breach must be reported to the Privacy Commissioner, regardless of how the potential breach was detected..

The following are the steps we must take when we believe there is such a breach.

- Determine if there is a "real risk of significant harm" (RROSH);
- Report the breach;
- Notification; and
- Record keeping.

[3] https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/

6.1 Determine if there is a "Real Risk of Significant Harm"

To determine if the breach poses a RROSH to any individual whose personal information was involved in the breach we must conduct a risk assessment. The following factors are some of the considerations that we must include in assessing the risks taken from OPC guidance[4]:

- Sensitivity of the personal information involved i.e. How sensitive is the information? Was the personal information adequately encrypted, anonymized or otherwise not easily accessible?
- Probability of Misuse. i.e. What happened and how likely is it that someone would be harmed by the breach? Who actually accessed or could have accessed the personal information? How long has the personal information been exposed?
- The cause and extent of the breach i.e. Is there a risk of ongoing breaches or further exposure of the information – is it a systemic issue? Has the personal information been recovered?
- The individuals affected by the breach i.e. How many individuals' personal information was involved? Who is affected by the breach: employees, customers, etc.?

6.2 Reporting the Breach

We must notify the privacy commissioner, of any breach of security safeguards involving personal information under its control if it is reasonable to believe the

breach creates a real risk of significant harm as determined in the step above. The report should contain the following:

- A description of the circumstances of the breach and, if known, the cause;
- The day or the period in which the breach occurred;
- A description of the personal information that was involved in the breach;
- an estimate of the number of individuals impacted – where the breach creates a real risk of significant harm;
- The steps that the organization has taken to reduce the risk of harm to the impacted individuals;
- The steps that the organization has taken or will take to notify impacted individuals; and

[4] https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_6

- The name and contact information of a person who can answer, on behalf of the organization, the Privacy Commissioner's questions about the breach.

The OPC has published a reporting form the should be used for reporting breaches which can be accessed here:
https://www.priv.gc.ca/media/4844/pipeda_pb_form_e.pdf

6.3 Notification

We must notify affected individuals if it is determined that there is a RROSH. How the notification will take place depends on serval factors such as if contact information of the impacted individuals is known, cost, and if the method chosen to deliver such a notification will cause further harm.

Issuing notification that contains:

- A description of the circumstances of the breach;
- The day or period during which the breach occurred;
- A description of the personal information that was involved in the breach;
- the steps that the organization has taken to reduce the risk of harm to the impacted individuals;
- The steps that the impacted individuals could take to reduce the risk of harm resulting from the breach;
- A toll-free number or email address that the impacted individuals can use to obtain further information about the breach; and
- Information about the organization's internal complaint process and about the individual's right, under PIPEDA and that they can make a complaint with the privacy commissioner.

We must also notify other organizations or government institution if we believe they may be able to reduce the risk of harm to the impacted individuals. (i.e. law enforcement agencies). If this is the case, consent of individuals is not required for such disclosures.

6.4 Record Keeping

Organizations are required to keep and maintain records of all breaches of security safeguards, including those that do not meet the harm threshold for reporting and notification. These records must be provided to the privacy commissioner upon request. Records must be maintained for 24 months from the day that the organization determined that the breach occurred, and that they contain sufficient information to enable the privacy commissioner to verify compliance with the breach reporting obligations.

7 Privacy Management Program

A comprehensive privacy management program provides an effective way for Trackon to foster a strong privacy culture throughout the organization and ensure compliance with legislation. While we have discussed many aspects of what is needed in such a program in the sections above, the following are the fundamental elements Trackon ensures are in place and operate effectively.

- Senior management support in order to foster a privacy respectful culture.
- The Privacy Officer is involved in business decision-making process. The Privacy Officer monitors compliance and ensures program controls are assessed regularly.
- The Privacy Office supports the ability of staff to monitor compliance and fosters a culture of privacy.
- Reporting mechanisms are in place and are reflected in our program controls.
- We can identify the personal information we have in our possession, what that information is used for, and the sensitivity of the personal information.
- We have procedures in place related to the following:
    - Collection, use and disclosure of personal information, which include requirements for consent and notification
    - Access to and correction of personal information
    - Retention and disposal of personal information
    - Responsible use of information and information technology, including physical and technological security controls
- We have ways to challenging compliance in place:
    - Risk assessment tools
    - Training
    - Breach and incident management response protocols
    - Service Provider management
    - External communication

8 Complaints

Trackon must have in place a complaint process to allow customers to submit complaints. Trackon should respond to and resolve complaints timely. This process

is in addition to processes for withdrawing of consent. Trackon must respond as quickly as possible within 30 days.

The Privacy Officer is responsible for ensuring appropriate measures are taken when a complaint is found to be justified. These measures will include:

- written response to the complainant within 30 days;
- revision of the challenged personal information;
- revision to policies and procedures, if required; and

- review of any complaint that requires disciplinary action.

Details of all complaint, as well as all steps of investigation and resolve the compliant, will be logged into a compliant tracking spreadsheet.

Complaints are directed to:

Rishi Dubey, Privacy Compliance Officer,
Trackon Canada Private Ltd
4440 5th St. NW
Edmonton, AB, Canada T6T 0Z9
rk@paypenny.io
416-323-3112

9 Law Enforcement Requests

There may be exceptional times when Trackon is required to disclose personal information, without an individual's consent, in order to comply with a subpoena, warrant, court order or other law enforcement request. Similarly, Trackon may disclose personal information without consent to a government institution or an investigative body for a purpose such as national security, national defence or the deterrence of terrorism, law enforcement, or in relation to a suspected money-laundering offence.[5]

If Trackon receives a request from law enforcement the Privacy Officer must be notified immediately.

A request has to be in writing: In order to understand the request, the Compliance Officer will request a subpoena, Court Order or other evidence, if it has not been provided. This documentation protects the company and Compliance Officer in the request for information and the release of information under Canadian privacy law.

The person requesting information should be identified and the date of the request should be recorded. The request should be analyzed and clarification should be

sought from the law enforcement officer if necessary before any information is disclosed. Exemptions under PIPEDA should also be consulted[6].

---

5 https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/

6 https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/

Once the supporting evidence of received and information request is understood, Trackon will comply with the information request in a format reasonable to the request such as having the individual review records in the office or providing paper copies of information. Trackon will retain copies of any and all information disclosed during this process for a minimum of five years.

It is possible that the individual concerned may request access to information related to this disclosure. If this happens, Trackon must notify the institution to which the information was disclosed. The institution has 30 days to respond.

Trackon may not respond to the individual's access request before either hearing back from the institution or until 30 days has passed since Trackon notified it; whichever occurs first.

If the institution objects to the release of the information to the individual based on permissible grounds, Trackon must withhold it. Trackon may not reveal that we communicated with the institution, or that it objected to the disclosure.

10 CASL Compliance Program

CASL is Canada's anti-spam law that applies to all electronic messages (i.e. email, texts) and governs how Trackon communicates related to its commercial activity. Trackon is responsible for ensuring all commercial electronic messages (CEMs) comply with the requirements of CASL. Trackon is required to obtain an individual's express consent before sending messages, manage unsubscribe request and ensure CEMs clearly identify who is sending the message. In addition, the CRTC has outline CASL compliance program requirements that Trackon must adhere to.

10.1 Senior management involvement

Trackon must identify a point person who is responsible and accountable for compliance with the Rules and/or CASL. Trackon has chosen their Lee Ernest Fox as this person.

10.2 Risk assessment

The Privacy Officer is to conduct a risk assessment to determine which business activities are at risk for possible violations under CASL. Where there is a risk, procedures are put into place to mitigate.

10.3 Requirements for CEM

In order to ensure any commercial electronic messages, such as emails promoting a Trackon's services that we send, we must comply with the following requirements:

- Obtaining consent;

- Including required information; and
- Including an appropriate unsubscribe mechanism.

CEMs can include messages that have another primary purpose (for example a Christmas card) but also include messaging promoting a product or service.

10.3.1.1 Obtaining Consent

To send a CEM, Trackon needs express consent, either orally or in writing. Written consent can be electronic. Consent must be obtained prior to sending any communication, excluding ones that are exempt under regulations. Express consent cannot be obtained via a CEM, unless you already have implied consent. Trackon ensures express consent requires a positive or explicit indication of consent. A record of what type of information or content a customer has agreed to receive (i.e. e-newsletters, sales info, product promotions, etc.) must be retained.

10.3.1.2 Information to be included in CEMs

Each CEM must identify the sender of the message and, if applicable, the person(s) on whose behalf the message is sent. Trackon must ensure that each CEM contains the full mailing address of the person sending the message or, if different, the mailing address of the person on whose behalf the message is sent. Additionally, a URL, email address, or phone number, where the sender can be contacted should be included. This information must be valid for at least 60 days after the message has been sent. This information should also to be included in a request for consent. The subject line of the CEM must accurately describe the contents of the message.

10.3.1.3 Unsubscribe mechanism for CEMs

Each CEM must contain an unsubscribe mechanism. Trackon must ensure that each CEM contains an unsubscribe mechanism that is clearly and prominently located and easy for the consumer to use. Trackon must honour all unsubscribe requests within 10 days following receipt of the request.

10.4 Requirements Related to Installation of Computer Programs

Trackon is required to obtain consent before the installation of a computer program, including installation of digital platforms, that will do one or more of the following:

- collect personal information stored on the computer;
- interfere with the user's control of the computer system; and
- change or interfere with settings, preferences, or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system.

The consent must obtain an acknowledgement from the person from whom consent is being sought that he or she understands and agrees that the program performs the specified functions. Consent may be obtained via an empty toggle box, separate from a license agreement and other requests for consent.

10.5 Additional Compliance

In addition to this Policy Trackon may also implement the following:

- Procedures for compliance with CASL;
- CASL Training;
- An auditing and monitoring program;
- Procedures for dealing with third to ensure that they comply with CASL;
- Record keeping requirements especially with respect to consent; and
- A means to allow employees to provide feedback to the Privacy Officer in relation to CASL.

10.6 Record keeping

Trackon must ensure records related to obtaining consent and managing unsubscribe are kept. Records may be kept in hard copy or electronic form and may help in investigating and responding to consumer complaints or establish a due diligence defense in the event of complaints to the Commission against the business.

10.7 Training program

Trackon should implement CASL training. Training should contain what is required under legislation and the penalties for not meeting those requirements. For training to be effective, links should be made to TRACKON's procedures and include examples that staff may face in their daily activities.

The training should be adapted and re-administered when there are changes to the business or changes in regulation.

10.8 Auditing and monitoring

Trackon must have in place auditing and monitoring mechanisms to help prevent and detect CASL compliance issues. Trackon must ensure that audits are conducted regularly (with or without external help).

The results of all such monitoring activities should be recorded, maintained, and communicated to senior management. Any finding or recommendations should be addressed in a timely fashion.

10.9 Corrective action

Trackon takes corrective actions, or providing refresher training, as appropriate, to address non-compliance with CASL requirements. A record of the contravention and the actions taken should be kept.

11 Appendix: Definitions & Acronyms

Breach: A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information.

Canadian Radio-television and Telecommunications Commission (CRTC): An independent public authority in charge of regulating and supervising Canadian broadcasting and telecommunications.

Commercial electronic message (CEM): any electronic message that contains a marketing message, (i.e. an email that tells customers about a promotion). CEMs must be sent to an electronic address this includes test messages.

Office of the Privacy Commissioner of Canada (OPC): Body that governs the personal information handling. Their mission is to protect and promote the privacy rights of individuals.

Personal Information Protection and Electronic Documents Act (PIPEDA): Federal privacy law for private-sector organizations. It sets out the requirements of how businesses must handle personal information they hold.

Real Risk of Significant Harm (RROSH): A risk assessment that takes into account the sensitivity of the information and the probability that it will be misused factor when there is a privacy breach.

Telemarketing: refers to the use of telecommunications facilities to make unsolicited telephone calls to consumers for the purpose of selling or promoting of a product or service. This includes calls made for donations.

Telemarketer: any person or organization who makes telemarketing calls on their own behalf or for someone else.

12 Appendix: Sample Privacy Impact Assessment (PIA) Form

Requirement	Assessment			Controls in Place	Actions
	Met	Not Met	Partially Met		
Principle 1					
We have reviewed our privacy policies and are satisfied that they are complete and easy to understand and staff has been trained on them.					
We have clearly designated a person responsible for privacy governance and management.					
Our privacy framework outlines that we are responsible for all personal information we hold, including information which has been transferred to a third party for processing.					
Principle 2					
Purpose for collecting personal information is identified at or before the time of collection.					
We have documented the purpose for collecting personal information.					
We have notified customers of new purposes for which We will use information if this wasn't identified at the time information was collected?					
Principle 3					
We obtain consent of customers before using information for any new purpose if required.					
We obtain customer consent for any collection, use or disclosure of personal information.					
We make reasonable efforts to ensure customers are notified of the purposes for which personal information will be used or disclosed.					
We obtain consent through lawful and fair means.					

Requirement	Assessment			Controls in Place	Actions
	Met	Not Met	Partially Met		
We allow our customers to withdraw consent at any time and inform of the implication of the withdrawal of consent.					
Principle 4					
We limit the amount and type of personal information We collect to what is necessary for the identified purpose.					
We limit collection of the SIN or mark it as an optional field.					
Principle 5					
We only retain personal information as long as necessary to allow for the fulfillment of identified purposes.					
Our privacy framework governs the destruction of personal information and includes a minimum and maximum retention period is outlined.					
Principle 6					
We take reasonable measures to ensure that personal information is accurate, complete and up-to-date prior to using the information to make decisions.					
We only update personal information if the process is necessary to fulfill the purposes for which the information was collected.					
Our privacy framework addresses the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.					
Principle 7					
We have adopted physical, technical and administrative safeguards to protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification – includes need to know access.					
We choose security safeguards that are commensurate with the sensitivity of the information and the means used to transmit it.					
We protect all personal information regardless of the format in which it is held.					
We make employees aware of the importance of maintaining the confidentiality of personal					

Requirement	Assessment			Controls in Place	Actions
	Met	Not Met	Partially Met		
information and the importance of security our policy.					
We have implemented processes to prevent unauthorized access to personal information during the disposal or destruction of information.					
Principle 8					
We make information regarding policies and procedures related to the management of personal information available to individuals.					
We explain to customers why We collect, how We use and when We will disclosure their personal information.					
We make information available to our customers regarding who within the organization can address questions or complaints regarding the handling of personal information.					
We make the name/title and address of the personal accountable for the organization's privacy policies available on request.					
We describe to our customers how they can obtain access to or correct their personal information.					
Principle 9					
We provide individuals with a description of what personal information We hold and what We disclose to other organizations.					
We inform individuals of the existence, use and disclosure of their personal information on receipt of a written request.					
We provide individuals with access to personal information on receipt of a written request.					
We respond to a request for information at minimal or no cost to the individual.					
We assist those individuals who indicate they need help to complete a request for information.					
Principle 10					
We enable individuals to address compliance challenges to the designated individual responsible for PIPEDA.					

Requirement	Assessment			Controls in Place	Actions
	Met	Not Met	Partially Met		
We have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.					
We advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.					
We investigate all complaints We receive about your personal information handling policies and practices.					