

CANADA PRIVACY PROGRAM FRAMEWORK

Last updated: September 21, 2023

OUR VISION

Our vision of privacy is simple: it is about promoting a culture of privacy in all areas of the organization. Our aim is for all our employees and collaborators to protect personal information as if it was their own and incorporate sound judgment into the performance of their daily tasks.

OUR APPROACH

1. Developing products and building processes that respect privacy

JTI-Macdonald Corp. ("JTI", "we", "us", "our") considers privacy by design to be the foundation of everything we do to protect personal information. We take a proactive approach and choose to design products, including websites, and processes that respect individuals' choices.

2. Provide our employees with a clear, easy-to-operate framework

We want our privacy policies and practices to reflect the day-to-day tasks of our employees, and to be easily identifiable and achievable. We recognize that a large part of the success of our privacy program is in our employees. We strive to provide them with the opportunity to tell us where we can improve our privacy practices.

3. Be transparent with our customers, partners and employees

Transparency is one of our most important values when it comes to protecting personal information. We aim to foster the trust of our customers, partners and employees by avoiding unpleasant surprises and by clearly describing our personal information management practices. We make every effort to obtain clear and unambiguous consent. We are always available to answer privacy-related questions.

4. Act in accordance with our responsibility and accountability

We take our accountability for the way we (or our suppliers and agents) collect, use, communicate and store the personal information of our customers, partners and employees in a serious way. We ensure sound management of data throughout its life cycle, making sure that personal information is properly inventoried and classified according to its sensitivity. We maintain a holistic view of our privacy risks and cooperate fully with regulatory authorities or agents where necessary.

OUR PRIVACY PROGRAM

Guiding principles

Our privacy program is based on the following guiding principles:

1. Responsibility

We take responsibility for personal information in our possession and control, including that held by our suppliers.

2. Determining the purpose of collection

We identify the purposes for which we collect personal information before collecting them.

3. Consent

We inform individuals of the collection of their personal information and obtain their consent to use or disclose it, unless applicable exceptions under the law apply.

4. Limitation of collection

We only collect personal information that is necessary for the purposes identified to the individual.

5. Restrictions on use, disclosure and storage

We limit the use and disclosure of personal information to purposes to which the individual has consented or to purposes consistent with those purposes, unless otherwise permitted by law. We retain information only as long as necessary to fulfill the identified purposes, subject to the rules set out in our retention schedule (where available) and applicable legal requirements.

6. Accuracy

We strive to ensure that the personal information we hold is up-to-date, accurate and complete for as long as it is used, as far as is reasonably possible.

7. Safety measures

We take appropriate security measures to protect the personal information we collect, use, disclose, retain or destroy. Such measures will be reasonable considering the sensitivity of the information, the purpose for which it is to be used, its quantity, distribution and medium.

8. Transparency

We make our policies and procedures concerning the management of personal information available to our employees. We also make information on our personal information management practices available to the public.

9. Access to personal information

We inform any person who so requests of the existence of personal information concerning them, of the use made of it and of the fact that it has been communicated to third parties. It allows any person to consult or obtain a copy of his or her personal information and to have it rectified, where applicable, subject to applicable exceptions provided under the laws.

10. Possibility of lodging a complaint about non-compliance with the principles

An individual shall be able to address a challenge concerning our compliance with its personal information policies and practices or on these principles. We will respond promptly to any complaints regarding personal information management.

OUR CONTROL FRAMEWORK

Data classification and personal information mapping

We maintain and update a classification and mapping of the data we collect, use and communicate, in order to be able to know in detail the type, quantity and sensitivity of the personal information it holds.

Governance policies and practices

We implement personal information management policies and practices to embody our privacy culture and demonstrate compliance with applicable laws. These policies and practices are an essential part of our privacy program. They enable our employees to understand their obligations and how to meet them.

These policies and practices cover various aspect including:

Roles and responsibilities

We have a chain of accountability in all our privacy-related policies and practices.

Our policies and practices describe the responsibilities of the Privacy Officer and other members of our staff.

Our employees are required to familiarize themselves with and to comply with all privacy and information security guidelines.

Managing privacy rights and handling complaints

We respect individuals' privacy rights, including the right to access and rectify personal information. To this end, we have established a process to respond promptly and transparently to such requests.

Upon receipt of privacy-related requests/complaints, our Privacy Officer will acknowledge receipt promptly, usually within 2 business days. Our Privacy Officer will analyze all requests and complaints fairly, and will provide a clear, unambiguous response within 30 business days.

Retention and destruction of personal information

We ensure that personal information whose retention periods have expired is destroyed or anonymized, if applicable.

We retain personal information used to make a decision about an individual long enough to allow the individual to exercise his or her right to make a request for access or rectification after the decision has been made.

Confidentiality incident management

To be able to deal with privacy incidents within a reasonable timeframe and to reduce the risk of serious harm to individuals, our Privacy Officer has implemented a process for the assessment and management of privacy incidents.

We prioritize depersonalization and anonymization techniques, thereby reducing the risk of confidentiality incidents and protecting individuals' right to privacy by masking certain information in order to make it difficult or technically impossible to identify an individual.

Security measures

We strive to ensure the protection of personal information under our control against loss, theft, destruction, consultation, communication, reproduction, use and unauthorized modification, through the use of appropriate security measures. Appropriate measures may be administrative, technical or physical, and vary according to the sensitivity, purpose, use and distribution of the personal information, as well as the medium used. In particular, we have a comprehensive global information security program.

Privacy risk assessment tools

We conduct privacy impact assessment in appropriate circumstances, such as when acquiring, developing, or overhauling an information system or electronic service delivery system that involves the collection, use, release, keeping, or destruction of personal information.

Our Privacy Officer is consulted at all times on situations that may require a privacy impact assessment.

Management of third-party service providers and agents

We developed a due diligence process when entering into or updating a contract with a third-party supplier or partner, to assess the third party's compliance with applicable privacy laws.

The process follows due diligence at the supplier selection stage and a privacy impact assessment (where appropriate) when a supplier is selected.

Training and awareness-raising

We have established internal training program on subject matters relating to the protection of personal information, such as the management of confidentiality incidents and the processing of requests for access to information.

Training and awareness-raising cover our legal and regulatory requirements, as well as all our internal guidance relating to privacy and certain aspects of information security.

CONTINUOUS ASSESSMENT AND REVISION

Our privacy program is subject to ongoing evaluation and annual review by our Privacy Officer to ensure its relevance, effectiveness and compliance, particularly considering legislative changes and/or changes in our operations.

QUESTIONS OR COMMENTS

If you have any questions or comments about this document, our handling of personal information or your rights, please contact our Privacy Officer at privacy.canada@jti.com.