

Data Privacy Policy



Article 1. Governing Texts

Data protection law in Canada is comprised of a complex set of federal and provincial statutes. These laws include federal and provincial data protection statutes of general application, as well as sector-specific statutes, such as health privacy laws, and related laws such as anti-spam and consumer protection laws. There is a large and growing body of regulator and court findings and guidance at the provincial and federal levels.

The relevant data protection statutes are:

- Federal: Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA');
- Alberta: Personal Information Protection Act, SA 2003 c P-6.5 ('AB PIPA'); and
- In addition, Canadian anti-spam law, Canada's Anti-Spam Legislation, SC 2010 c 23 ('CASL'), relates to electronic marketing activities.

CASL prohibits companies from:

- “sending users commercial electronic messages without consent, including email, social media and text messages.
- altering the transmission data in an electronic message so the message is sent to a different destination without express consent
- installing software on your electronic devices without consent (including, in some cases, updates and upgrades, even if you were the one who installed the original software)
- using false or misleading representations to promote products or services online
- collecting personal information by accessing a computer system or electronic device illegally
- harvesting addresses (collecting and/or using email or other electronic addresses without permission)”¹

Article 2. Data protection principles

The Organization is committed to processing data in accordance with its responsibilities under PIPEDA and AB PIPA.

¹ <https://fightspam-combattrelepourriel.ised-isde.canada.ca/site/canada-anti-spam-legislation/en/understand-canadas-anti-spam-legislation/understand-canadas-anti-spam-legislation-sub/understanding-canadas-anti-spam-legislation>

PIPEDA requires that personal data shall be in accordance with the following ten principles:

- a. **“Accountability** - PIPEDA and provincial laws hold organisations accountable for information under their control and require the appointment of an individual or individuals who are responsible for the organisation's compliance with the law.
- b. **Identifying purposes** -The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
- c. **Consent** - The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
- d. **Limiting collection** - The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
- e. **Limiting use, disclosure, and retention** - Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
- f. **Accuracy** - Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
- g. **Safeguards** - Organisations are required to use security safeguards in order to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification.
- h. **Openness** - An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
- i. **Individual access** - Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- j. **Challenging compliance** - An individual shall be able to challenge an organization’s compliance with the above principles. Their challenge should be addressed to the person accountable for the organization’s compliance with PIPEDA, usually their Chief Privacy Officer.”² *At Besa Global, the Communications and Project Officer is accountable for the organization’s compliance with PIPEDA.*

² https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Article 3. Types of Data Collected

Personal Data

“Personal information” is any information about an individual that could lead to identification of the individual. In some jurisdictions, personal information is described as “personally identifiable information” or as “personal data”. In this policy, all such information is identified as “personal information”.

Personal information includes information such as the age, ethnic origin, opinions, evaluations, and comments of identifiable individuals.

Applicable privacy laws and regulations exclude certain information from the scope of personal information. Any such excluded information is excluded from the term “personal information” under this privacy policy, but only as provided by applicable law for purposes of the applicable jurisdiction. For example, under PIPEDA, an individual’s business contact information may be excluded in certain circumstances, and certain publicly available information, such as telephone directory listings, may also not be considered to be personal information.

Exclusions include:

- “Information that is not about an individual, because the connection with a person is too weak or far-removed (for example, a postal code on its own which covers a wide area with many homes)
- Information about an organization such as a business.
- Information that has been rendered anonymous, as long as it is not possible to link that data back to an identifiable person
- Certain information about public servants such as their name, position and title
- A person’s business contact information that an organization collects, uses or discloses for the sole purpose of communicating with that person in relation to their employment, business or profession.
- Government information³

³ https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Article 4. Collection of Information

Information you provide directly to us

For certain activities, such as when you register for our mailing list, or contact us directly, we may collect some or all of the following types of information:

- Contact information, such as your full name, email address, phone number, and organizational and nation affiliation(s); and
- Any other information you provide to us.
- We may combine such information with other public information.

Information we see automatically

We may collect certain information automatically when you use our website, such as your device and advertising identifiers, browser type, operating system, Internet service provider nationality, the date and time of your visit, information about the links you click, the pages you view, the general manner in which you navigate the website, and other standard server log information.

Article 5. Use of Information

We generally use the information we collect online to:

- Send you informational materials;
- Analyze the use of website and user data to understand and improve the website;
- Customize the content you see when you use the website;
- For any other purposes disclosed to you at the time we collect your information or pursuant to your consent.

Article 6. International Users

For residents in the European Union (EU)

Without limitation to the other provisions of this Privacy Policy, if you are a resident of the EU, you have the following additional rights under applicable law in relation to our processing of your personal information under the GDPR:

- The right to request the erasure of your personal information, particularly where the continued processing of the information is no longer necessary;
- The right to object to the processing of your personal information, particularly where there are no longer sufficient legitimate grounds continue processing the information;
- The right to restrict processing, data portability and the right to appeal any automated decision making or profiling; and
- The right to complain to a Data Protection Regulator about our processing of your personal information;

It is important to note that the rights set out above are not unconditional and the specific circumstances of the processing being undertaken will determine if these rights may be exercised.

If you are a resident of the EU, our legal basis for collecting and using the personal information described in this privacy policy will depend on the personal information concerned and the specific context in which we collect it.

Article 7. Revision

Besa Global Inc. reserves the right to change this Policy from time to time. Proposed changes will normally be developed by those responsible for this Policy with appropriate stakeholders.

Policy Name (Reference No.)	Data Privacy Policy (BGIP03)
Approval Date	20 March 2023
Effective Date	20 March 2023
Version	1.0
Approved By	Cheyenne Scharbatke-Church, Executive Director
Responsibility of Review	Executive Director
Frequency of Review	Every 2 years
Last Updated	17 March 2023
Related Policies and Guidelines	Data Protection Policy Data Protection Guideline