PIPEDA Compliance Policy

PIPEDA Compliance Policy

Note: This document has been updated to be compliant with changes to the Personal Information Protection and Electronic Documents Act (PIPEDA) that come into effect on November 1, 2018.

Intent

The Personal Information Protection and Electronic Documents Act (PIPEDA) establishes rules to govern the collection, use, and disclosure of personal information in a manner that recognizes the right to privacy of individual's personal information and the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PBC Communications Inc is committed to protecting and respecting the personal information of its customers, employees, business partners, and all other entities it interacts with in accordance with PIPEDA. This policy will provide guidelines to ensure that PBC Communications Inc remains compliant with PIPEDA requirements.

Definitions

Breach of security safeguards: The loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.

Personal information: Information about an identifiable individual. Security

safeguards: Security safeguards include the following:

- Physical measures: for example, locking filing cabinets and restricting access to offices;
- Organizational measures: for example, security clearances and limiting access on a "need-to-know" basis; and Technological measures: for
- example, the use of passwords and encryption.

Significant harm: Includes bodily harm; humiliation; damage to reputation or relationships; loss of employment, business, or professional opportunities; financial loss; identity theft; negative effects on a credit record; and damage to or loss of property.

All definitions sourced from PIPEDA. Guidelines

Compliance

PBC Communications Inc has implemented these guidelines to ensure continuing compliance with PIPEDA requirements. The personal information of PBC Communications Inc employees, customers, clients, business partners, and so on will be managed to meet the following PIPEDA requirements:

- All personal information in PBC Communications Inc possession or custody must be protected appropriately. Individuals must be
- informed as to why personal information is being collected.
- Consent must be obtained for the collection and use of information.
- The consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose, and consequences of the collection, use, or disclosure of the personal information.
- Personal information may only be collected without consent if:
  - The collection is clearly in the interests of the individual and consent cannot be obtained in a timely way; The personal
  - information was produced by the individual in the course of their employment, business, or profession, and the collection is consistent with the purposes for which the information was provided; The collection is made for the
  - purpose of making a disclosure; or
  - Any other reason as defined in PIPEDA section 7(1).
- Individuals have the right to withdraw their consent.
- Personal information collected is only collected, used, or disclosed for purposes that a reasonable person would consider appropriate in the circumstances.
- Personal information is used only for the purposes for which it was collected, except with the consent of the individual or as required by law.
- Personal information is retained only for the period of time that it is reasonably required.
- Personal information is destroyed that is no longer required using a safe, secure, and effective manner (for example, shredding).
- All personal information collected is accurate.
- Individuals are allowed access to their personal information, and to make corrections as appropriate. Appropriate
- security and safeguards are employed for the protection of personal information.
- Access to personal information is limited to authorized personnel who have a legitimate need to access the information. Consent must
- generally be obtained before the release of personal information to any third party.
- Consent to disclose personal information to a third party is not required if:
  - PBC Communications Inc has reasonable grounds to believe that the information could be useful in the investigation of a contravention of the laws of Canada, a province or territory, or a foreign jurisdiction, and the

information is used for the purpose of investigating that contravention;
    - It is used for the purpose of acting in respect to an emergency that threatens the life, health, or security of an individual;
    - The information was produced by the individual in the course of their employment, business, or profession, and the use is consistent with the purposes for which the information was produced; or
    - Any other circumstances as defined in PIPEDA section 7(2) are met.
- The forms of information being collected must be identified and communicated to the individual, as well as the rationale for the collection of these forms of information.
- Individuals must be notified and consent must be obtained before using personal information for any reason other than those provided at the time of collection.

In addition to the above requirements, PBC Communications Inc will designate a representative to hold accountability for the organization's compliance with PIPEDA. The representative will hold responsibility for the management of the personal information policies and procedures of PBC Communications Inc.

- The representative shall be the CEO.

The PIPEDA representative shall be responsible for:

- Developing and implementing policies and practices under PIPEDA, including:
    - Procedures that address the collection, use, retention, destruction, and management of personal information; Procedures for
    - protecting personal information in all formats;
    - Procedures for complaints and inquiries; and Staff
    - training on PIPEDA obligations.
- Using privacy agreements and contracts to ensure the protection of personal information where the information must be provided to a third party.
- Reviewing policies, practices, and procedures annually or as needed, making appropriate revisions.

Breaches of Security Safeguards Reporting

Breaches

If PBC Communications Inc becomes aware of a breach of our security safeguards that compromises the privacy of the personal information retained by the company, the following action shall be taken:

- The CEO is responsible for coordinating the response to the breach and ensuring that all reasonable action is taken to address the breach.
- The CEO will notify the privacy commissioner of Canada of the breach in the prescribed form and manner as soon as feasible once PBC Communications Inc has determined that a breach has occurred. PBC Communications Inc will also submit any new information that the company becomes aware of after having made the report.
- The CEO will notify any affected individuals of the breach in the prescribed form and manner as soon as feasible
- PBC Communications Inc will comply to the greatest extent possible and in a timely manner with any requests, orders, or other instructions from the Office of the Privacy Commissioner of Canada in order to respond to and address the security breach.
- PBC Communications Inc will maintain records of every breach of security safeguards, and will provide the privacy commissioner of Canada with access to or a copy of a record of a breach at the request of the commissioner.

As per the Breach of Security Safeguards Regulations, the report submitted to the privacy commissioner will contain: A description of the circumstances of the breach and if known the cause;

- The date on which or the period during which the breach occurred or if neither is known the approximate period;
- A description of the personal information that is the subject of the breach to the extent that the information is known; The number of
- individuals affected by the breach or if unknown the approximate number;
- A description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
- A description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of PIPEDA; and
- The name and contact information of a person who can answer the commissioner's questions about the breach on behalf of the organization.

Notifying Affected Individuals

Determining Whether a Real Risk of Significant Harm Exists

PBC Communications Inc will assess the following factors when determining whether a security breach constitutes a real risk of significant harm to an individual or individuals:

- The sensitivity of the personal information involved in the breach;
- The probability that the personal information has been, is being, or will be misused; and

- Any other prescribed factor.

Notifications

The CEO is responsible for ensuring that all individuals for whom the breach creates a real risk of significant harm are notified at the earliest available opportunity, subject to any legal restrictions, in a form of communication that a reasonable person would consider appropriate in the circumstances. As per the regulation, notifications shall contain sufficient information to allow the individual to understand the significance to them of the breach, including:

- A description of the circumstances of the breach;
- The date on which or period during which the breach occurred or if neither is known the approximate period;
- A description of the personal information that is the subject of the breach to the extent that the information
- is known; A description of the steps that the organization has taken to reduce the risk of harm that could
- result from the breach; A description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm;
- Contact information that the affected individual can use to obtain further information about the
- breach; and Any other prescribed information.

The notice shall be conspicuous and given directly or indirectly to the individual in the prescribed form and manner as legislatively required as the situation dictates.

In addition to the individuals affected by the breach, PBC Communications Inc may notify other parties of the breach or disclose personal information relating to the breach, subject to the following guidelines:

- PBC Communications Inc will notify other organizations, government institutions, or parts of government institutions if PBC Communications Inc believes that doing so can reduce or mitigate the harm from the breach.
- PBC Communications Inc may disclose personal information without the knowledge or consent of the individual if:
- The disclosure is made to the other organization, the government institution, or the part of a government institution that was notified under the breach; and
- The disclosure is made solely for the purpose of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.