Operationalising PIPEDA

A Practical Guide for Business Leaders

TRUE NORTH

• PSR

Table of Contents

1.0 What is PIPEDA?..... 2
2.0 Data Privacy Controls..... 2
2.1 Chief Privacy Officer (CPO) Responsibilities:..... 2
2.2 Privacy Program Management:..... 3
2.3 Data Privacy Governance:..... 3
2.4 Data Classification & Handling:..... 3
2.5 Data Protection Impact Assessment (DPIA):..... 4
2.6 Data Loss Prevention (DLP):..... 4
2.7 Mobile Device Management (MDM):..... 4
2.8 Administrative Processes and Technologies:..... 5
2.9 Data Privacy in Governance:..... 5
3.0 Information Security Controls..... 6
3.1 Chief Information Security Officer (CISO) Responsibilities:..... 6
3.2 Security-Focused Conceptual Framework:..... 6
3.3. Governance, Risk & Compliance (GRC) Function:..... 6
3.4 Identity & Access Management (IaAM):..... 7
3.5 IT Asset Management (ITAM):..... 7
3.6 Third-Party Management (TPM):..... 7
3.7 Secure Engineering & Architecture:..... 7
3.8 Compliance Management:..... 8
4.0 Definitions..... 8
5.0 Control Descriptions and Questions Guidance..... 11

1.0 What is PIPEDA?

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian law designed to protect the personal information of Canadian consumers. Like many data privacy regulations, can seem complex, but at its core, it's simply about ensuring that personal information is handled with care and respect.

PIPEDA compliance is essential for any company that deals with personal data, or, in PIPEDA-speak, *Personal Information (PI)*. It ensures that businesses implement robust policies to protect personal information and maintain customers' trust. Compliance with PIPEDA demonstrates a company's commitment to data privacy best practices.

If this is your first time hearing about PIPEDA, you might want to start by downloading our "PIPEDA Project Guide," available on the same page where you found this document. It provides a comprehensive overview to get you up to speed.

Please feel free to use this document as a high-level description of the operational controls – practical steps your company needs to take – to align with PIPEDA requirements. Implementing these controls is crucial for ensuring compliance and safeguarding personal information effectively.

2.0 Data Privacy Controls

2.1 Chief Privacy Officer (CPO) Responsibilities:

The Chief Privacy Officer (CPO) analyses the organisation's business strategy to develop and publish guidance on the data privacy program. This role ensures that statutory, regulatory, and contractual data privacy obligations are properly identified and implemented, thereby protecting personal information.

Recommended Controls:

1. The CPO analyses the organisation's business strategy to develop and publish authoritative guidance on the organisation's data privacy program.
2. The CPO ensures that applicable statutory, regulatory, and contractual data privacy obligations are properly identified and implemented.
3. The CPO publishes a clear set of "data privacy principles" based on leading data privacy practices.[1]

[1] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#principles

2.2 Privacy Program Management:

Privacy program management involves running a comprehensive privacy program led by a CPO and supported by a project management office (PMO). This ensures that data privacy principles [1] are incorporated into all projects and programs. The purpose is to protect personal information across the company systematically.

Recommended Controls:

1. A Privacy program, run by a CPO, is established to ensure the proper handling and security of personal information.
2. A project management office (PMO) has established project management controls to ensure that both cybersecurity and data privacy principles are identified and implemented within projects.

2.3 Data Privacy Governance:

Data privacy governance includes establishing an internal steering committee to provide executive oversight and ensuring data/process owners and third-party service providers (i.e., vendors, and contractors) adhere to data protection requirements. The purpose is to maintain high standards of data privacy and accountability throughout the organisation.

Recommended Controls:

1. The company has established an internal steering committee that provides executive oversight of the cybersecurity and data privacy program.
2. Data/process owners operationalise data privacy controls into the business processes they control.
3. Counsel, in cooperation with the CPO and CISO, ensures that all third-party contracts include data protection requirements, including flow-down requirements to subcontractors.

2.4 Data Classification & Handling:

Data classification and handling controls involve categorising data, setting protection requirements, and maintaining data flow diagrams and network diagrams. The purpose is to ensure that data is appropriately protected based on its classification.

Recommended Controls:

1. Data classification procedures and associated audit controls have been established to identify categories of data and specific protection requirements.
2. The company's data retention processes protect archived data in accordance with statutory, regulatory, and contractual obligations.

3. Data/process owners create and maintain *Data Flow Diagrams (DFDs)* and *Network Diagrams*.

2.5 Data Protection Impact Assessment (DPIA):

A *Data Protection Impact Assessment (DPIA)* evaluates the impact of data processing activities to help ensure the protection of sensitive/regulated data and implement necessary cybersecurity and data privacy controls.

Recommended Controls:

1. The company ensures the protection of sensitive/regulated data processed, stored, or transmitted on internal or external systems.
2. Pertinent Human Resources (HR) and Information Technology (IT) documents have established formal "rules of behaviour" for handling sensitive/regulated data.

2.6 Data Loss Prevention (DLP):

Data Loss Prevention (DLP) involves using content filtering capabilities to block unauthorised file transfers. The purpose is to prevent data leaks and ensure data security. The business value of implementing such technical measures is to protect the company from data breaches and maintain the confidentiality of sensitive information.

Recommended Controls:

1. The company has implemented and actively manages DLP capabilities to block system users from performing unauthorised file transfers through unapproved third-party service providers (e.g., Box, Dropbox, Google Drive).

2.7 Mobile Device Management (MDM):

Mobile Device Management (MDM) software restricts and protects data on mobile devices (e.g., smartphones). In other words, MDM software secures data accessed or stored on mobile devices used within the organisation.

Recommended Controls:

1. The company has implemented MDM software to restrict and protect data residing on users’ mobile devices.

2.8 Administrative Processes and Technologies:

Administrative processes and technologies include applying data classification labels to company documentation, documenting information locations, and governing data transfers and disclosures. The purpose is to ensure adequate cybersecurity and data privacy controls by applying appropriate levels of security to data across the organisation.

Recommended Controls:

1. The company has established data classification categories and has classified all company documentation to ensure adequate control of those documents.
2. The company has identified and documented the location of its information.[2]
3. Restrict and govern the transfer of data to third countries or international organisations.
4. Limit the disclosure of data to authorised parties.[3]
5. Prohibit unapproved third parties from storing, processing, or transmitting data.[4]

2.9 Data Privacy in Governance:

Data privacy in governance controls ensures that statutory, regulatory, and contractual compliance requirements are identified, documented, and tested regularly. The purpose is to maintain a consistent approach to data privacy controls across the organisation.

Recommended Controls:

1. Statutory, regulatory, and contractual compliance requirements are identified and documented.
2. The company's Governance, Risk & Compliance (GRC) function exercises oversight concerning organisational cybersecurity and data privacy controls.
3. Internal policies and standards address all in-scope cybersecurity and data privacy obligations.

[2] The restriction of such transfers depends on adequate vendor risk management (section 3.6), contract terms governing applicable relationships (section 2.3), and identity and access management (section 3.4)
[3] refer to footnote-2
[4] refer to footnote-2

3.0 Information Security Controls

3.1 Chief Information Security Officer (CISO) Responsibilities:

The Chief Information Security Officer (CISO) analyses the business strategy to provide prioritised guidance for cybersecurity practices. The purpose of assigning a dedicated CISO is to ensure a specific person is responsible and accountable for developing a security-focused framework for operations and has an adequate level of expertise and authority to implement that change across the organisation.

Recommended Controls:

1. The CISO analyses the organisation's business strategy to determine and execute prioritised guidance for cybersecurity-related data privacy practices.
2. The CISO has developed a security-focused conceptual framework for operations.

3.2 Security-Focused Conceptual Framework:

A Security-focused conceptual framework documents managerial, operational, and technical measures to apply defence-in-depth techniques. The purpose is to enhance the organisation's security architecture. Implementing such a framework establishes a structured approach to managing cybersecurity risks, which improves the organisation's overall security resilience.

Recommended Controls:

1. The company has documented all necessary managerial, operational, and technical measures (e.g., policies, procedures, guidelines, technical controls) to apply defence-in-depth techniques.

3.3. Governance, Risk & Compliance (GRC) Function:

The governance, risk & compliance (GRC) function provides oversight for the implementation of statutory, regulatory, and contractual cybersecurity controls. The purpose is to ensure consistent application and compliance with security standards.

Recommended Controls:

1. A company GRC function (team) provides governance oversight for the implementation of statutory, regulatory, and contractual cybersecurity controls.
2. The GRC team conducts regular and ongoing assessments to validate the efficacy of the privacy and security controls program and provides status reports to company stakeholders.

3.4 Identity & Access Management (IaAM):

Identity and access management (IaAM) controls implement "principle of least privilege" (PoLP) practices for managing user, group, and system accounts. The purpose of IaAM controls is to ensure that information access is restricted to authorised individuals.

Recommended Controls:

1. The company has implemented identification and access management (IDaAM) controls for "least privileges" practices.

3.5 IT Asset Management (ITAM):

IT Asset Management (ITAM) categorises *Assets* and applies security controls based on the data those Assets store, transmit, and process. The purpose of ITAM controls is to protect organisational assets and the data they handle.

Recommended Controls:

1. The company categorises Assets according to the data those Assets store, transmit, and process, applying appropriate technology controls.

3.6 Third-Party Management (TPM):

Third-party management (TPM) involves safeguarding the company from supply chain threats (vendor-related risks) through procurement contracts and layered defences. The purpose is to manage risks carried or otherwise borne by third-party service providers.

Recommended Controls:

1. The company ensures that procurement contracts and layered defences safeguard the company and its clients from supply chain threats.
2. The GRC function has implemented and maintains a third-party risk management (vendor risk management) program.
3. The company has established processes to evaluate and manage risks associated with third-party risk through regularly scheduled (e.g., annual) vendor reviews.
4. The company ensures compliance with established contract agreements through regular monitoring and auditing.

3.7 Secure Engineering & Architecture:

Secure engineering & architecture practices involve implementing a "layered defence" (defence in depth) network architecture and governing system changes through a Change Advisory Board (CAB). The purpose is to ensure systems are designed and operated securely.

Recommended Controls:

1. The company's IT and cybersecurity teams have established and implemented a "layered defence" network architecture.
2. Changes to systems, applications, and services are governed by a Change Advisory Board (CAB) and associated administrative controls to ensure organisational stability, reliability, and resiliency.
3. A formal Change Management (CM) program documents and controls changes; the controls are regularly audited to validate control adherence.

3.8 Compliance Management:

Compliance management processes and controls have been established to ensure that statutory, regulatory, and contractual obligations are documented and tested regularly. The purpose of compliance management is to maintain and regularly validate the company's compliant security posture.

Recommended Controls:

1. Statutory, regulatory, and contractual compliance requirements are documented and tested.
2. The GRC team ensures data/process owners manage applicable controls.
3. Cybersecurity and data privacy controls are centrally managed through a combination of administrative, physical, and technical controls.

4.0 Definitions

Asset: Any resource owned or controlled by the company that can be used to produce positive economic value for the company. In this context, Assets most notably include applications, databases; IT equipment, and infrastructure.

Change Advisory Board (CAB): A group of stakeholders that support the assessment, prioritisation, and approval of changes to IT systems.

Change Management (CM): A systematic approach to dealing with changes in an organisation, ensuring changes are thoroughly and smoothly implemented, and that the lasting benefits of change are achieved.

Chief Information Security Officer (CISO): A senior executive responsible for overseeing and implementing the information security program to protect the organisation's information assets.

Chief Privacy Officer (CPO): A senior-level executive responsible for managing an organisation's data privacy policies and ensuring compliance with privacy laws and regulations.

Cybersecurity Supply Chain Risk Management: The process of identifying, assessing, and mitigating risks associated with the supply chain for information technology systems.

Data Classification: The process of organizing data into categories for its most effective and efficient use and protection.

Data Flow Diagram (DFD): A graphical representation of the flow of data within a system, showing how data is processed, where it comes from, where it goes, and how it is stored.

Data Loss Prevention (DLP): A set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorised users.

Data Privacy Principles: Fundamental guidelines and practices designed to protect personal information from unauthorised access, use, or disclosure.

Data Protection Impact Assessment (DPIA): A process to help identify and minimise the data protection risks of a project, ensuring compliance with data protection laws.

Defense-in-Depth: A layered approach to security, employing multiple security measures to protect information and systems.

Governance, Risk & Compliance (GRC): A structured approach to aligning IT with business objectives, while managing risk and meeting compliance requirements.

Identity & Access Management (IAM): Policies, processes, and technologies used to manage digital identities and regulate user access to critical information within an organisation.

IT Asset Management (ITAM): A set of business practices that join financial, contractual, and inventory functions to support lifecycle management and strategic decision-making for IT environments.

Mobile Device Management (MDM): Software that enables IT administrators to secure, monitor, manage, and support mobile devices deployed across an organisation.

Network Diagram: A visual representation of a computer network, illustrating the connections and relationships between network components, such as devices, routers, and servers.

Personal Information (PI): Information about an identifiable individual. This includes any factual or subjective information, recorded or not, about an identifiable individual. Examples include age, name, identification (ID) numbers, income, ethnic origin, opinions, evaluations, comments, social status, or disciplinary actions. Personal Information does not include the name, title, business address, or telephone number of an employee of an organisation.

Principle of Least Privilege (PoLP): A security concept that dictates users and systems should have the minimum level of access—or permissions—necessary to perform their tasks, reducing the risk of accidental or malicious misuse of access rights.

Project Management Office (PMO): A centralised management structure that standardises project-related governance processes and facilitates the sharing of resources, methodologies, tools, and techniques.

Sensitive Data: Data that is protected under laws and regulations due to its sensitive nature, such as personal, financial, or health information.

Shared Responsibility Matrix: A document that outlines the division of responsibilities between parties, such as between the company and its third-party service providers.

Steering Committee: A group of high-level stakeholders who provide direction, oversight, and support for a specific project or initiative.

Third-Party Management (TPM): The process of overseeing and managing the activities, risks, and performance of external service providers.

Validated Architecture Design Review: A process used to evaluate design criteria for secure practices and ensure systems are designed, built, and operated securely.

5.0 Control Descriptions and Questions Guidance

PIPEDA Reference No.	Control Description	Control Question
Principle 1 Principle 8	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	Does the company facilitate the implementation and operation of data privacy controls?
Principle 10	Mechanisms exist to utilise technical controls to correct Personal Information (PI) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	Does the company utilise technical controls to correct PI that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified?
Principle 10	Mechanisms exist to establish and implement a process for: ▪ Data subjects to have inaccurate PI maintained by the company corrected or amended; and ▪ Disseminating corrections or amendments of PD to other authorised users of the PD.	Does the company establish and implement a process for: ▪ Data subjects to have inaccurate PI maintained by the company corrected or amended; and ▪ Disseminating corrections or amendments of PD to other authorised users of the PD?
Principle 2	Mechanisms exist to: ▪ Make data privacy notice(s) available to individuals upon first interacting with the company and subsequently as necessary; ▪ Ensure that data privacy notices are clear and easy to understand, expressing information about PI processing in plain language that meets all legal obligations; ▪ Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; ▪ Content of the privacy notice is periodically reviewed and updates made as necessary; and ▪ Retain prior versions of the privacy notice, in accordance with data retention requirements.	Does the organisation: ▪ Make data privacy notice(s) available to individuals upon first interacting with the company and subsequently as necessary; ▪ Ensures that data privacy notices are clear and easy to understand, expressing information about PI processing in plain language that meets all legal obligations; ▪ Defines the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; ▪ Content of the privacy notice is periodically reviewed and updates made as necessary; and ▪ Prior versions of the privacy notice are retained in accordance with data retention requirements?
Principle 6	Mechanisms exist to confirm the accuracy and relevance of PI throughout the information lifecycle.	Does the company confirm the accuracy and relevance of PI throughout the information lifecycle?

Principle 7	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	Does the company facilitate the implementation of cybersecurity & data protection governance controls?
Principle 7	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	Does the company facilitate the identification and implementation of relevant statutory, regulatory and contractual controls?
Principle 7	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organisation's executive leadership.	Does the company provide a cybersecurity & data protection controls oversight function that reports to the organisation's executive leadership?
Principle 7	Mechanisms exist to facilitate the implementation of data protection controls.	Does the company facilitate the implementation of data protection controls?
Principle 7	Mechanisms exist to facilitate the implementation of industry-recognised cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	Does the company facilitate the implementation of industry-recognised cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services?
Principle 7	Mechanisms exist to develop an enterprise architecture aligned with industry-recognised leading practices, with consideration for cybersecurity and data privacy principles that address risk to organisational operations, assets, individuals, and other Companies.	Does the company develop an enterprise architecture aligned with industry-recognised leading practices, including consideration for cybersecurity and data privacy principles, and that addresses risk to organisational operations, assets, individuals, and other Companies?
Principle 7	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Does the company implement security functions as a layered structure, minimizing interactions between design layers and avoiding any dependence by lower layers on the functionality or correctness of higher layers?
Principle 8 Principle 9	Mechanisms exist to enable data subjects to access their PI maintained in organisational record systems.	Does the company give data subjects channels to access their PI maintained in organisational record systems?
Sec 11	Mechanisms exist to provide an organisation-defined process for data subjects to appeal an adverse decision and have incorrect information amended.	Does the company provide an organisation-defined process for data subjects to appeal an adverse decision and have incorrect information amended?

Sec 20	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	Does the company identify and document the location of information and the specific system components on which the information resides?
Sec 20	Automated mechanisms exist to identify by data classification type to ensure adequate cybersecurity & data privacy controls are in place to protect organisational information and individual data privacy.	Does the company use automated mechanisms to identify by data classification type to ensure adequate cybersecurity & data privacy controls are in place to protect organisational information and individual data privacy?
Sec 20	Mechanisms exist to restrict and govern the unintentional transfer of sensitive and/or regulated data to third countries or international Companies.	Does the company restrict and govern the unintended transfer of sensitive and/or regulated data to third countries or international Companies?
Sec 20	Mechanisms exist to distribute processing and storage across multiple physical locations.	Does the company distribute processing and storage across multiple physical locations?
Sec 20	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	Does the company restrict the location of information processing/storage based on business requirements?
Sec 20 Sec 23	Mechanisms exist to disclose PI to third parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	Does the company disclose PI to third parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject?
Sec 20 Sec 23	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	Does the company include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers?
Sec 5 Principle 2	Mechanisms exist to identify and document the purpose(s) for which PI is collected, used, maintained and shared in its data privacy notices.	Does the company identify and document the purpose(s) for which PI is collected, used, maintained and shared in its data privacy notices?
Sec 5 Principle 4	Mechanisms exist to collect PI only for the purposes identified in the data privacy notice and include protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	Does the company collect PI only for the purposes identified in the data privacy notice and include protections against collecting PD from minors without appropriate parental or legal guardian consent?

Sec 5 Principle 4	Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of PI, either generally or in support of a specific program or system need.	Does the company determine and document the legal authority that permits the collection, use, maintenance and sharing of PI, either generally or in support of a specific program or system need?
Sec 6	Mechanisms exist to appoint a Data Protection Officer (DPO): ▪ Based on the basis of professional qualities; and ▪ To be involved in all issues related to the protection of PI.	Does the company appoint a Data Protection Officer (DPO): ▪ Based on the basis of professional qualities; and ▪ To be involved in all issues related to the protection of PI?
Sec 6 Sec 7 Principle 3	Mechanisms exist to authorise the processing of their PI prior to its collection which: ▪ Employ plain language and provide examples to illustrate the potential data privacy risks of the authorisation; and ▪ Provides a means for users to decline the authorisation.	Does the company authorise the processing of their PI prior to its collection that: ▪ Uses plain language and provides examples to illustrate the potential data privacy risks of the authorisation; and ▪ Provides a means for users to decline the authorisation?
Sec 6 Sec 7 Principle 3	Mechanisms exist to present authorisations to process PI in conjunction with the data action, when: ▪ The original circumstances under which an individual gave consent have changed; or ▪ A significant amount of time has passed since an individual gave consent.	Does the company present authorisations to process PI in conjunction with the data action, when: ▪ The original circumstances under which an individual gave consent have changed, or ▪ A significant amount of time has passed since an individual gave consent.
Sec 7 Sec 8 Principle 5 Principle 6	Mechanisms exist to: ▪ Retain PI, including metadata, for an organisation-defined time period to fulfil the purpose(s) identified in the notice or as required by law; ▪ Dispose of, destroys, erases, and/or anonymises the PD, regardless of the method of storage; and ▪ Use organisation-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	Does the organisation: ▪ Retain PI, including metadata, for an organisation-defined time period to fulfil the purpose(s) identified in the notice or as required by law; ▪ Dispose of, destroys, erases, and/or anonymises the PD, regardless of the method of storage; and ▪ Use organisation-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).