PIPEDA

Compliance report

Be Software International

Pty Ltd

Confidential

Report Issue Date: 06/10/2022
Testing Dates: 04/22/2022 to 06/07/2022
Assessor: Raul E Lopez

Scope

At the request of Be Software International Pty Ltd, the information security assessor performed a security assessment against the supporting services and assets of Be Software International Pty Ltd and the application to the The Personal Information Protection and Electronic Documents Act (PIPEDA) to electronic personal information that is created, received, used, or maintained.

The Personal Information Protection and Electronic Documents Act PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity.

The law defines a commercial activity as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

This document reports the results and conclusions of the security assessment engagement.

Objectives

The main purpose of this assessment is to validate the compliance of the 10 fair information principles to protect personal information, which are set out in Schedule 1 of PIPEDA.

The principles are:

Accountability
Identifying Purposes
Consent
Limiting Collection
Limiting Use, Disclosure, and Retention
Accuracy
Safeguards
Openness
Individual Access
Challenging Compliance

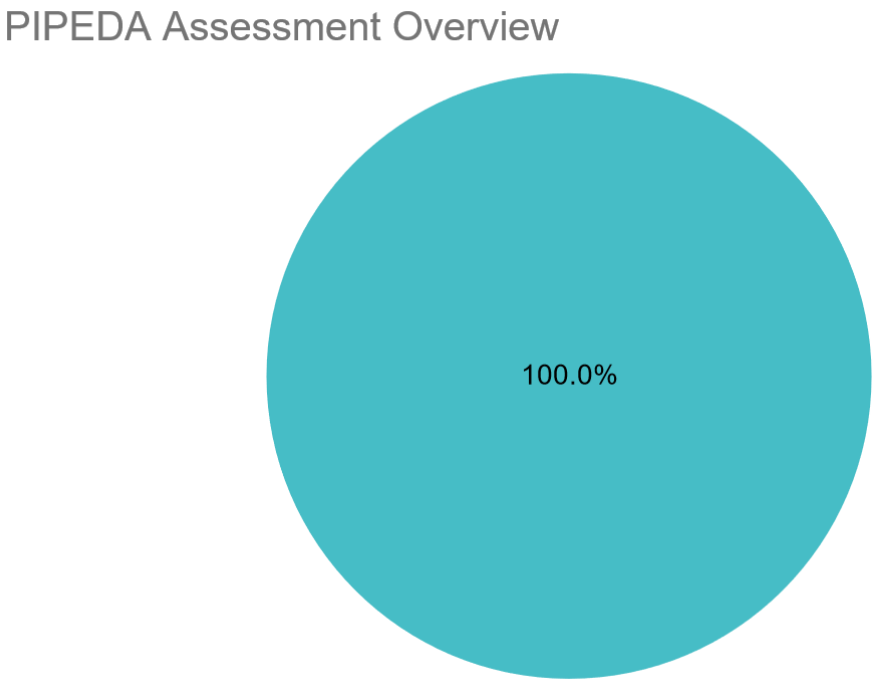
Assessment Resources

A set of interviews and sessions was performed in order to validate compliance and as part of the assessment it was presented and shared the following documentation

Asset inventory version 2.6 (2022)
Network Diagram version 1.0 (2022)
Dataflow register for personal health information version 2.0 (2021)
Penetration test latest reports (2022)
Third party and service providers list version 1.0 (2021)
Risk assessment version 2.6
Incident management procedure version 2.3 (2022)
Software change and development procedure version 1.2 (2022)
Access Control policies and procedures 3.2
Operational procedures 3.2
Information security standards version 3.1 (2022)
BCP/DRP Plan version 2.4

Executive Summary

Based on the control evaluation performed Be Software International Pty Ltd have provided evidence that support 100% of compliance based on the list of controls applicable based on the federal privacy law PIPEDA 10 fair information principles form the ground rules for the collection, use and disclosure of personal information, as well as for providing access to personal information, law enacted by the Parliament of Canada, Citation S.C. 2000, c.5 assented on 13 April 2000



Control summary	Count
Not Requested	0
Requested	0
Under review	0
Amendment to process required	0
Non Compliant	0
Compliant	92

Detailed Report

Based on the control evaluation performed Be Software International Pty Ltd have provided evidence that support 100% of compliance based on the list of controls applicable based on the federal privacy law PIPEDA 10 fair information principles form the ground rules for the collection, use and disclosure of personal information, as well as for providing access to personal information, law enacted by the Parliament of Canada, Citation S.C. 2000, c.5 assented on 13 April 2000

The detail of controls applicable to this assessment and the evaluation criteria of “Compliance” can be verified as follows:

Regulatory Source	**Regulatory Requirement**	**Assessment Question**	**In Scope**	**Current Status**
PIPEDA	Principle 1 - Accountability	You have reviewed your privacy policies and are satisfied that they are complete and easy to understand	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have clearly delineated who, within your organization, is responsible for privacy governance and management.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have privacy policies and practices that apply to the personal information of your employees as well as that of your customers.	No	N/A
PIPEDA	Principle 1 - Accountability	Your privacy framework clearly articulates that you will be responsible for all personal information you hold or control, including information which has been transferred to a third party for processing	Partial	Compliant
PIPEDA	Principle 1 - Accountability	You have appointed at least one person to be responsible for the organization’s overall compliance with PIPEDA.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have directed staff through policy, procedure or training to provide the name, address and phone number of the PIPEDA contact person to individuals when requested.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You use contractual agreements to ensure a comparable level of privacy protection is offered to personal information while it is in the custody of a third party for processing.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have verified that third parties have implemented the privacy controls stated in any contractual agreements.	Yes	Compliant

PIPEDA	Principle 1 - Accountability	You are accountable for the protection of personal information.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “identifying purpose” regarding personal information.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “consent” regarding personal information	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “limiting collection” of personal information.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “limiting use, disclosure and retention” of personal information.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “accuracy” regarding personal information	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “safeguards” with respect to personal information	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “openness” regarding personal information	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “individual access” regarding personal information.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	Your privacy framework addresses the principle of “challenging compliance” regarding personal information.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have communicated information related to personal information handling policies, procedures and practices to staff.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have trained staff regarding the protection of personal information by informing them of organizational privacy policies, procedures and best practices.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have the means in place to identify which of your staff should be trained in privacy, including new staff and refresher training of existing staff.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have developed documentation to explain your personal information protection policies and procedures to customers and the general public.	Yes	Compliant
PIPEDA	Principle 1 - Accountability	You have developed information to explain to your employees the policies and procedures which apply to their own personal information.	Yes	Compliant
PIPEDA	Principle 2 - Identifying Purposes	You identify why you are collecting personal information at or before the time of collection	Yes	Compliant

PIPEDA	Principle 2 - Identifying Purposes	You have documented your purpose(s) for collecting personal information.	Yes	Compliant
PIPEDA	Principle 2 - Identifying Purposes	You have notified clients and customers of new purposes for which you will use information if they weren't identified at the time information was collected	No	N/A
PIPEDA	Principle 2 - Identifying Purposes	You seek the consent of clients and customers before using information for any new purpose if required.	No	N/A
PIPEDA	Principle 2 - Identifying Purposes	You have notified clients and customers of the purposes before using or disclosing the information if notification at the time of collection was not practicable	No	N/A
PIPEDA	Principle 2 - Identifying Purposes	You have determined the amounts and types of personal information needed to fulfill your purpose(s).	No	N/A
PIPEDA	Principle 2 - Identifying Purposes	You have determined why you are collecting personal information and that the amount and types of personal information collected are reasonable in normal business circumstances.	No	N/A
PIPEDA	Principle 2 - Identifying Purposes	You have distinguished between essential information (required for primary business purposes) and non-essential information (voluntary information which facilitates use for secondary purposes).	No	N/A
PIPEDA	Principle 2 - Identifying Purposes	You have identified non-essential information as voluntary and have provided staff with information on how to proceed when clients and customers opt out of secondary uses.	No	N/A
PIPEDA	Principle 3 - Consent	You obtain customer consent for any collection, use or disclosure of personal information.	Yes	Compliant
PIPEDA	Principle 3 - Consent	If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under s.7 of PIPEDA.	Yes	Compliant
PIPEDA	Principle 3 - Consent	You make reasonable efforts to ensure that clients and customers are notified of the purposes for which personal information will be used or disclosed	Yes	Compliant
PIPEDA	Principle 3 - Consent	You do not require clients and customers to consent to the collection, use or disclosure of personal information beyond what is necessary to fulfill explicitly specified and limited purposes as a condition of supplying a product or service.	Yes	Compliant

PIPEDA	Principle 3 - Consent	You assess the purposes and limit the collection, use and disclosure of personal information when it is required as a condition for obtaining a product or service.	No	N/A
PIPEDA	Principle 3 - Consent	You obtain consent through lawful and fair means.	Yes	Compliant
PIPEDA	Principle 3 - Consent	You allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice	Yes	Compliant
PIPEDA	Principle 3 - Consent	You inform clients and customers of the implication of the withdrawal of consent.	Yes	Compliant
PIPEDA	Principle 3 - Consent	You consider the sensitivity and intended use of personal information, and the reasonable expectations of clients and customers in determining which form of consent (implied or expressed) you will accept for the collection, use and disclosure of personal information	No	N/A
PIPEDA	Principle 4 - Limiting Collection	You limit the amount and type of personal information you collect to what is necessary for the identified purpose.	No	N/A
PIPEDA	Principle 4 - Limiting Collection	You collect information only by fair and lawful means.	No	N/A
PIPEDA	Principle 4 - Limiting Collection	You have documented the specific types of information you collect along with the purposes for collection.	Yes	Compliant
PIPEDA	Principle 4 - Limiting Collection	You have documented when you collect information from sources other than the individual about whom it pertains.	Yes	Compliant
PIPEDA	Principle 4 - Limiting Collection	You distinguish between mandatory and optional collection of personal information.	Yes	Compliant
PIPEDA	Principle 4 - Limiting Collection	You limit your collection of the SIN to legally established purposes.	No	N/A
PIPEDA	Principle 5 - Limiting use, disclosure and retention	You do not use or disclose information for purposes beyond those for which it was collected, except with the consent of the individual or as required by law.	Yes	Compliant
PIPEDA	Principle 5 - Limiting use, disclosure and retention	You document new purposes conceived after the personal information is collected.	Yes	Compliant
PIPEDA	Principle 5 - Limiting use, disclosure and retention	You only retain personal information as long as necessary to allow for the fulfillment of identified purposes.	Yes	Compliant

PIPEDA	Principle 5 - Limiting use, disclosure and retention	You retain personal information used to make decisions about an individual long enough for the individual to request access to it	Yes	Compliant
PIPEDA	Principle 5 - Limiting use, disclosure and retention	Your privacy management framework governs the destruction of personal information, including the role of contractors performing such services	Yes	Compliant
PIPEDA	Principle 6 - Accuracy	You take reasonable measures to ensure that personal information is accurate, complete and up-to-date prior to using the information to make decisions.	No	N/A
PIPEDA	Principle 6 - Accuracy	You only update personal information if the process is necessary to fulfill the purposes for which the information was collected.	No	N/A
PIPEDA	Principle 6 - Accuracy	Your privacy management framework addresses the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.	No	N/A
PIPEDA	Principle 6 - Accuracy	Your privacy management framework specifies when updates are appropriate based on the defined purposes and uses of the information as well as the interests of the individual	No	N/A
PIPEDA	Principle 6 - Accuracy	You record when and where key information was collected, including dates of corrections or updates to such information.	No	N/A
PIPEDA	Principle 6 - Accuracy	You conduct periodic spot-checks, assessments or audits of information holdings and databases to ensure that key information is accurate, complete and up-to-date.	Yes	Complliant
PIPEDA	Principle 7 - Safeguards	You 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.	Yes	Compliant
PIPEDA	Principle 7 - Safeguards	You choose security safeguards that are commensurate with the sensitivity of the information and the means used to transmit it.	Yes	Compliant
PIPEDA	Principle 7 - Safeguards	You protect all personal information regardless of the format in which it is held	Yes	Compliant
PIPEDA	Principle 7 - Safeguards	You make your employees aware of the importance of maintaining the confidentiality of personal information.	Yes	Compliant
PIPEDA	Principle 7 - Safeguards	You have implemented processes to prevent unauthorized access to personal information during the disposal or destruction of information.	Yes	Compliant

PIPEDA	Principle 7 - Safeguards	You have implemented and adhere to your various information security policies and practices.	Yes	Compliant
PIPEDA	Principle 7 - Safeguards	You have established an information security breach policy and commit to investigating the root cause of such breaches.	Yes	Compliant
PIPEDA	Principle 7 - Safeguards	You have developed and implemented policies and practices including appropriate safeguards for all uses of personal information outside the office	Yes	Compliant
PIPEDA	Principle 8 - Openness	You make information regarding policies and procedures related to the management of personal information available to individuals	Yes	Compliant
PIPEDA	Principle 8 - Openness	You explain to customers why you collect, how you use and when you will disclose their personal information.	No	N/A
PIPEDA	Principle 8 - Openness	You make information available to clients and customers regarding who within the organization can address questions or complaints regarding the handling of personal information.	No	N/A
PIPEDA	Principle 8 - Openness	You make the name/title and address of the person accountable for the organization's privacy policies available on request	Yes	Compliant
PIPEDA	Principle 8 - Openness	You describe to your clients how they can obtain access to or correct their personal information	Yes	Compliant
PIPEDA	Principle 8 - Openness	You provide individuals with a description of what personal information you hold and what you disclose to other organizations	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You have adopted policies and procedures for responding to requests for personal information under PIPEDA	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You have advised staff of the need to direct requests for access to information to the staff member responsible for processing these requests.	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You inform individuals of the existence, use and disclosure of their personal information on receipt of a written request	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You provide individuals with access to personal information on receipt of a written request	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You limit refusal to provide access to information to exceptions described in Section 9 of PIPEDA	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You provide an account of the uses of information on request.	Yes	Compliant

PIPEDA	Principle 9 - Individual access	You provide an account of all third parties to whom information has been disclosed (or a listing of the types of third parties to whom such information is generally disclosed) on receipt of a request for such a list from an individual	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You assist those individuals who indicate they need help to complete a request for information	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You respond to a request for information at minimal or no cost to the individual	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You respond to a request for information in not more than 30 days unless you notify the requestor within that time period of your need to extend the time limit for response, indicate the extended time limit and inform the requester of his or her right to complain to the OPC.	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You rely on time limit extensions only in cases where responding within the original 30 days would unreasonably interfere with your activities, when additional time is needed to conduct consultations, or when additional time is needed to convert personal information to an alternative format	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You provide access to information in a format which is legible and will provide an explanation of abbreviations or codes on request from an individual	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You advise requestors of the reasons for refusal and recourse available to them when refusing to provide information.	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You allow individuals to challenge the accuracy of personal information and amend information when an individual demonstrates that information is inaccurate or incomplete.	Yes	Compliant
PIPEDA	Principle 9 - Individual access	You forward corrected personal information to third parties who would have received the original information	Yes	Compliant
PIPEDA	Principle 10 - Challenging Compliance	You enable individuals to address compliance challenges to the designated individual responsible for PIPEDA.	Yes	Compliant
PIPEDA	Principle 10 - Challenging Compliance	You have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.	Yes	Compliant

PIPEDA	Principle 10 - Challenging Compliance	You advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.	Yes	Compliant
PIPEDA	Principle 10 - Challenging Compliance	You investigate all complaints you receive about your personal information handling policies and practices.	Yes	Compliant
PIPEDA	Principle 10 - Challenging Compliance	You modify your actions if a complaint is substantiated, and take steps to minimize the likelihood that the issue will recur.	Yes	Compliant

Non applicable controls justification

Regulatory Source	**Regulatory Requirement**	**Assessment Question**	**In Scope**	**Current Status**	**Justification**
PIPEDA	Principle 1 - Accountability	You use contractual agreements to ensure a comparable level of privacy protection is offered to personal information while it is in the custody of a third party for processing.	No	N/A	Information is not transferred to a third party, processing is maintained solely on BSI
PIPEDA	Principle 2 - Identifying Purposes	You have notified clients and customers of new purposes for which you will use information if they weren't identified at the time information was collected	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 2 - Identifying Purposes	You seek the consent of clients and customers before using information for any new purpose if required.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 2 - Identifying Purposes	You have notified clients and customers of the purposes before using or disclosing the	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider

		information if notification at the time of collection was not practicable			
PIPEDA	Principle 2 - Identifying Purposes	You have determined the amounts and types of personal information needed to fulfill your purpose(s).	No	N/A	BSI is a service provider, all Personal Information flow will come from the clients
PIPEDA	Principle 2 - Identifying Purposes	You have determined why you are collecting personal information and that the amount and types of personal information collected are reasonable in normal business circumstances.	No	N/A	BSI is a service provider, all Personal Information flow will come from the clients
PIPEDA	Principle 2 - Identifying Purposes	You have distinguished between essential information (required for primary business purposes) and non-essential information (voluntary information which facilitates use for secondary purposes).	No	N/A	BSI is a service provider, all Personal Information flow will come from the clients
PIPEDA	Principle 2 - Identifying Purposes	You have identified non-essential information as voluntary and have provided staff with information on how to proceed when clients and customers opt out of secondary uses.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 3 - Consent	You assess the purposes and limit the collection, use and disclosure of personal information when it is required as a condition for obtaining a product or service.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider

PIPEDA	Principle 3 - Consent	You consider the sensitivity and intended use of personal information, and the reasonable expectations of clients and customers in determining which form of consent (implied or expressed) you will accept for the collection, use and disclosure of personal information	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 4 - Limiting Collection	You limit the amount and type of personal information you collect to what is necessary for the identified purpose.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 4 - Limiting Collection	You collect information only by fair and lawful means.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 4 - Limiting Collection	You limit your collection of the SIN to legally established purposes.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 6 - Accuracy	You take reasonable measures to ensure that personal information is accurate, complete and up-to-date prior to using the information to make decisions.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 6 - Accuracy	You only update personal information if the process is necessary to fulfill the purposes for which the information was collected.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 6 - Accuracy	Your privacy management framework addresses the accuracy, completeness and currency of personal	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider

		information which includes a process through which individuals can challenge the accuracy of information.			
PIPEDA	Principle 6 - Accuracy	Your privacy management framework specifies when updates are appropriate based on the defined purposes and uses of the information as well as the interests of the individual	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 6 - Accuracy	You record when and where key information was collected, including dates of corrections or updates to such information.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 8 - Openness	You explain to customers why you collect, how you use and when you will disclose their personal information.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider
PIPEDA	Principle 8 - Openness	You make information available to clients and customers regarding who within the organization can address questions or complaints regarding the handling of personal information.	No	N/A	3/1 - Information not intended to be used by BSI, it is a service provider

Compliance status

Based on a comprehensive assessment executed between April 2022 and June 2022 on Be Software International Pty Ltd technologies and assets used to transmit, process and store Personal Information (PI) and in order to validate the compliance of the 10 fair information principles to protect personal information, which are set out in Schedule 1 of The Personal Information Protection and Electronic Documents Act (PIPEDA) S.C. 2000, c. 5 it has been verified that:

Be Software International Pty provides appropriate protection of personal information that is collected, used or disclosed providing for the use of electronic means to communicate or record information or transactions as it is required by the Personal Information Protection and Electronic Documents Act of Canada

Raul E Lopez
CDP, LCSPC, CPTE, CySA+, Pentest+
Information Security Consultant
June 10, 2021

---------- END OF DOCUMENT ----------