PRO-39: PIPEDA PRINCIPLES (REV 2)

PROGRAM SUMMARY

2020/10/15

Effective From 2020-10-07 16:00:00
Effective To 2021-10-07 16:00:00
Report Date 2020-10-15 07:41:50
Standards PIPEDA Principles

Description

This document describes the xMatters Privacy Program in compliance with PIPEDA requirements. These practices are crafted in alignment to the Privacy requirements of ISO 27001:2013 and other Privacy Regulations that are relevant to xMatters business and clients.

xMatters design and implementation of Privacy will be conducted by reviewing and incorporating the privacy laws and regulations from the regions that xMatters operates in. As well using a risk-based approach to determine the requirements of information security and organizational policies, processes and procedures to protect privacy related information. In regard to privacy data and systems that store and process personal information, industry best and accepted practices will be used to provide protection.

Scope

xMatters SaaS platform and services in compliance to the Australian Privacy principles.

Notes

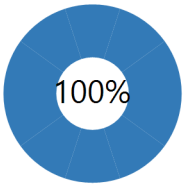
PIPEDA's 10 fair information principles form the ground rules for the collection, use and disclosure of personal information, as well as for providing access to personal information. They give individuals control over how their personal information is handled in the private sector.

In addition to these principles, PIPEDA states that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances.

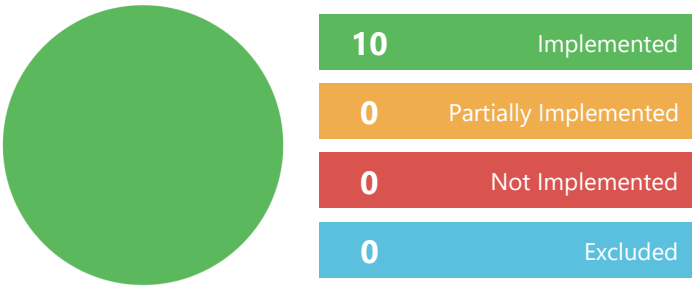
The OPC has determined that the following purposes would generally be considered inappropriate by a reasonable person (i.e., no-go zones):

- collecting, using or disclosing personal information in ways that are otherwise unlawful;
- profiling or categorizing individuals in a way that leads to unfair, unethical or discriminatory treatment contrary to human rights law;
- collecting, using or disclosing personal information for purposes that may cause significant harm to someone;
- publishing personal information with the intent of charging people for its removal;
- requiring passwords to social media accounts for the purpose of employee screening; and
- conducting surveillance on an individual using their own device's audio or video functions.

Overall Progress



Implementation Status



Total Controls/Policies

16

Number of Requirements

10

Requirements Per Standard

Requirement	Status	Date	Owner
PIPEDA PRINCIPLES			
Data Privacy			
Principle 1	Implemented		Information Assurance Department

Accountability
An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Satisfied By
- **Policy:** P-2: ISMS Manual
- **Control:** Steering Committee
- **Control:** ISMS Roles and Responsibilities

Notes

xMatters Data Protection Officer (DPO) is the owner of and accountable for xMatters compliance with fair information principles. xMatters DPO (coordinating with Information Assurance team and Legal Counsel) also oversees privacy governance including policy, dispute resolution, education, communications activities and compliance.

Principle 2	Implemented		Information Assurance Department

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.

Satisfied By
- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-72: Privacy Notice

Notes

xMatters only collects its clients' personal information for the purposes outlined on the Privacy Policy and Data Processing Agreement. If a new purpose for using your Personal Information develops, it will be identified in specific documentation.

Principle 3	Implemented		Information Assurance Department

Consent
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Satisfied By
- **Policy:** P-72: Privacy Notice
- **Policy:** P-66: Data Retention and Destruction Policy
- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-15: Subject Access Request (SARS)

Notes

All data in xMatters SaaS platform is provided by the client themselves depending on their business and use case. When clients start using our SaaS platform, xMatters obtains their consent to collect, use or disclose their PII. All users can manage their preferences in information directly on xMatters platform. xMatters has a Subject Access Process in place for any users that might want access to their information at any time and/or withdraw access to that information. This process is owned by xMatters Information Assurance Team.

Principle 4 **Implemented** Information Assurance Department

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.

Satisfied By
- **Policy:** P-21: Privacy Code of Practice
- **Policy:** P-72: Privacy Notice
- **Control:** Data Processing Agreement (DPA)

Notes

xMatters only collects Personal Information for the purposes set out in the agreements, policies and/or notices. All data in xMatters SaaS platform is provided by the client themselves depending on their business and use case. https://www.xmatters.com/trust/privacy/privacy-notice/

Principle 5 **Implemented** Information Assurance Department

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.

Satisfied By
- **Policy:** P-72: Privacy Notice
- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-66: Data Retention and Destruction Policy

Notes

xMatters will share clients' personal information with third parties only in the ways that are described in this privacy statement. xMatters do not sell personal information to third parties.

xMatters may provide users' personal information to companies that provide services to assist with service delivery such as submitting promotional email communications and emergency alerts to the users on the behalf of xMatters. These companies are assessed at regular intervals and are authorized to use this personal information only as necessary to provide these services to us. Transfers to subsequent third parties are covered by the provisions in this policy regarding notice and choice and the service agreements with xMatters clients.

Principle 6 **Implemented** Information Assurance Department

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.

Satisfied By
- **Policy:** P-15: Subject Access Request (SARS)

Notes

All data in xMatters SaaS is provided by the clients themselves and they have full access and control over the accuracy of that information. However, xMatters is committed to maintaining the accuracy of the client's PII and ensuring that it is complete and up-to-date. If our clients discover inaccuracies in xMatters records, they have all control over their information via the SaaS portal. xMatters also maintains a documented process too support customers on having access to their information.

Principle 10 **Implemented** Information Assurance Department

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.

Satisfied By
- **Policy:** P-15: Subject Access Request (SARS)

Notes
All privacy specific and other concerns can be sent to privacy@xmatters.com (as per the SAR process). xMatters can also be contacted using the contact form here: https://www.xmatters.com/company/contact-us/

Data Security

Principle 7 **Implemented** Information Assurance Department

Safeguards
Personal information must be protected by appropriate security relative to the sensitivity of the information.

Satisfied By
- **Control:** TRUSTe/TrustARC certified
- **Control:** Virtual Private Networking (VPN)
- **Control:** Endpoint Protection
- **Control:** C-17: Firewall rules audits
- **Control:** C-29: Data Map
- **Control:** C-40: Endpoint Security - Duplicate of C-55 Antivirus protection
- **Control:** C-55: Antivirus protection
- **Policy:** P-46: Cryptographic and Key Management Policy (A101)
- **Policy:** P-75: Security at xMatters

Notes

xMatters uses physical, electronic and procedural safeguards to protect against unauthorized use, access, modification, destruction, disclosure, loss or theft of PII in our custody or control. xMatters publishes detail information on our security controls and features here: https://www.xmatters.com/trust/security/

Principle 8 **Implemented** Information Assurance Department

Openness
An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Satisfied By
- **Policy:** P-21: Privacy Code of Practice
- **Policy:** P-72: Privacy Notice

Notes
xMatters privacy Notice and other privacy related information can be accessed here: https://www.xmatters.com/trust/privacy/

Principle 9 **Implemented** Information Assurance Department

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.

Satisfied By

- **Policy:** P-66: Data Retention and Destruction Policy
- **Policy:** P-15: Subject Access Request (SARS)

Notes

xMatters has Subject Access Request (SARS) process, owned by the Information Assurance team, which provides detailed roadmap and details for client data access requests.