PRO-44: NEW ZEALAND PRIVACY ACT (2020)

PROGRAM SUMMARY

2021/01/28

Effective From 2021-01-19 00:00:00
Effective To N/A
Report Date 2021-01-28 08:56:21
Standards New Zealand Privacy Act 2020

Description

The Privacy Act 2020 came into force on 1 December 2020, replacing Privacy Act 1993.

The purpose of this Act is to promote and protect individual privacy by—
(a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognizing that other rights and interests may at times also need to be taken into account; and
(b) giving effect to internationally recognized privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

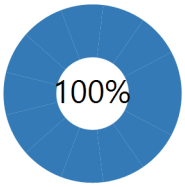
Scope

xMatters SaaS (Software as a Service) platform and services are in compliance to the New Zealand Privacy Act 2020.

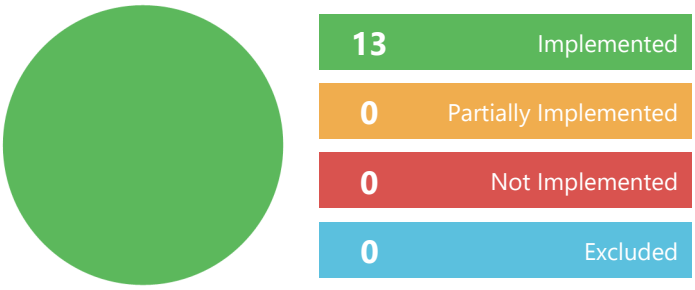
Notes

N/A

Overall Progress



Implementation Status



Total Controls/Policies

17

Number of Requirements

13

Requirements Per Standard

Requirement	Status	Owner
NEW ZEALAND PRIVACY ACT 2020		
Privacy Principles		
Principle 1	**Implemented**	Legal Counsel

Purpose for collection
Personal information shall not be collected by any agency unless:

The collection is for a lawful purpose.
It's necessary to collect the information for that purpose.

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

Notes

Client data collected by xMatters is for specified, explicit and legitimate purposes. The purpose for collection is service delivery and lawful basis is contract execution. All client provided data is used for service delivery as per contracted terms and agreements to facilitate emergency communications.

Principle 2	**Implemented**	Legal Counsel

Source of information
An agency should generally collect personal information directly from the person it is about. Because that won't always be possible, the agency can collect it from other people in certain situations. For instance, if:
The person concerned gives permission
Collecting it in another way would not prejudice the person's interests
Collecting the information from the person directly would undermine the purpose of collection
The agency is getting it from a publicly available source.

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

Notes
All client data in xMatters systems is inputted by the clients. xMatters informs its clients on how, when and what data is used to perform our services. All client provided data is used for service delivery as per contracted terms and agreements to facilitate emergency communications.

Principle 3 **Implemented** Legal Counsel

What to tell an individual
When an agency collects personal information, it must take reasonable steps to make sure that the person knows:

Why it's being collected
Who will receive it
Whether giving it is compulsory or voluntary
What will happen if they don't give you the information.

Sometimes there may be good reasons for not letting a person know the agency is collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

Satisfied By
- **Control:** C-80: Trust Portal
- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-72: Privacy Notice
- **Policy:** P-179: Sub-Processors List

Notes
The Client can, by the use of their xMatters Web Based User Interface (WebUI) delete, modify or add any records that will continue to support their Business and Use Case(s). xMatters provides contact and support information in contractual agreements and on it's public facing website (https://support.xmatters.com/hc/en-us)

Principle 4 **Implemented** Legal Counsel

Manner of collection
An agency may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. An agency should particularly care when collecting personal information from children and young people.

Satisfied By
- **Control:** Master Service Agreement (MSA)

Notes
All client data that is collected and provided to xMatters is for the sole purpose of service provision and contract execution.

Principle 5 **Implemented** Information Assurance Department

Storage and security
An agency must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

Satisfied By
- **Control:** GCP Physical security perimeter (A1111)
- **Control:** C-21: Access Control SaaS
- **Control:** C-32: Role Base Access Control (RBAC)
- **Control:** C-72: GCP dashboard
- **Policy:** P-23: Access Control Policy (A91)
- **Policy:** P-54: Internal Audit Process (SOP 92)
- **Policy:** P-75: Security at xMatters
- **Control:** C-80: Trust Portal

Notes

https://www.xmatters.com/trust/

https://www.xmatters.com/trust/security/assurance-process/

https://www.xmatters.com/trust/security/soc-2-type-ii/

https://www.xmatters.com/trust/security/iso-27001-certificate/

https://www.xmatters.com/trust/security/gcp-certifications/

Principle 6 **Implemented** Information Assurance Department

Access
An agency should know that people have a right to ask for access to their personal information. In most cases the agency has to promptly give them their information. Sometimes there may be good reasons to refuse access. For example, if releasing the information could:

Endanger someone's safety.
Create a significant likelihood of serious harassment.
Prevent the detection or investigation of a crime.
Breach someone else's privacy.

Satisfied By
- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-15: Subject Access Request (SARS)

Notes
Clients have 24x7 access to all data they input in xMatters systems. xMatters has also established processes and plans in place to manage data access requests.

Principle 7 **Implemented** Information Assurance Department

Correction
A person has a right to ask an agency or business to correct their information if they think it is wrong. Even if the agency don't agree that it needs correcting, the agency must take reasonable steps to attach a statement of correction to the information to show the person's view.

Notes
xMatters provides all clients with complete control over their own data. All clients have a Web Based User Interface (WebUI) access to xMatters SaaS for control and data entry, deletion and modification. xMatters has no control over the accuracy of client data inputted into the system.

Principle 8 **Implemented** Legal Counsel

Accuracy
Before using or disclosing personal information, an agency must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

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

Notes
xMatters provides all clients with complete control over their own data. All clients have a Web Based User Interface (WebUI) access to xMatters SaaS for control and data entry, deletion and modification. xMatters has no control over the accuracy of client data inputted into the system.

Principle 9 **Implemented** Legal Counsel

Retention
An agency that holds personal information must not keep that information for longer than is necessary for the purposes for which the information may be lawfully used.

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

Notes
Data is retained for the duration of the contract or unless indicated within the Master Service Agreement (MSA). Data destruction and sanitization is conducted in alignment with the National Institute of Standards and Technology (NIST) Special Publication 800 – 88: Guidelines for Media Sanitization. In the event of contract termination or deletion request, client data is purged within 60 days from both the primary and secondary data centers. In Google Cloud Storage, customer data is deleted through cryptographic erasure. This is an industry-standard technique that renders data unreadable by deleting the encryption keys needed to decrypt that data.

Principle 10 **Implemented** Legal Counsel

Use
An agency can generally only use personal information for the purpose it was collected. The agency may use it in ways that are directly related to the original purpose, or it may be used in another way if the person gives permission, or in other limited circumstances.

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

Notes
xMatters inc. does not 'share' or 'sell' any data. All client provided data is used for service delivery as per contracted terms and agreements to facilitate emergency communications. Client data collected by xMatters is for specified, explicit and legitimate purposes, which depends on client's Business and Use case.

Principle 11 **Implemented** Legal Counsel

Disclosure
An agency may only disclose personal information in limited circumstances. For example, if:

Disclosure is one of the purposes for which the information was received.
The person concerned authorised the disclosure.
The information will be used in an anonymous way.
Disclosure is necessary to avoid endangering someone's health or safety.
Disclosure is necessary to avoid a prejudice to the maintenance of the law.

Satisfied By
- **Control:** Data Processing Agreement (DPA)
- **Control:** C-29: Data Map
- **Policy:** P-179: Sub-Processors List

Notes
xMatters only discloses client data with authorized sub-processors and for the purposes of the service. An updated sub-processor list and a data mapping diagram can be shared with clients under NDA.

Principle 12 **Implemented** Legal Counsel

Cross-border disclosure
An agency can only send personal information to someone overseas if the information will be adequately protected. For example:

The receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
The information is going to a place with comparable privacy safeguards to New Zealand
The receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, an agency can only send personal information overseas if the individual concerned gives express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

Satisfied By
- **Policy:** P-77: Standard Contractual Clauses (SCC)
- **Control:** Data Processing Agreement (DPA)

Principle 13 **Implemented** Operations Department

Unique identifiers
An agency can only assign their own unique identifier to individuals where it is necessary for operational functions. Generally, the agency may not assign the same identifier as used by another organisation. If a unique identifier is assigned to people, the agency must make sure that the risk of misuse (such as identity theft) is minimised.

Notes
xMatters does not collect or generate any type of unique identifiers.