PRO-36: NEW ZEALAND PRIVACY ACT

PROGRAM SUMMARY

2020/06/01

Effective From 2020-05-29 00:00:00
Effective To N/A
Report Date 2020-06-01 12:05:31
Standards New Zealand Privacy Act

Description

The New Zealand Privacy Act 1993 was created to combat concerns about technological advances and their potential to be used to access private information, when this risk had been far less under manual data systems.

The Act contains 12 Information Privacy Principles which govern the handling of private information by agencies. An 'agency' is widely defined as any person or body of persons, whether public or private, and whether corporate or unincorporated, with specified exceptions. There are also numerous exceptions to the Information Privacy Principles, which can be found both within the principles and in other places within the Act. The Privacy Act recognises that privacy is not an absolute concept and that there are other factors which need to be weighed. The Privacy Commissioner must always have regard to factors such as human rights, social interests, and international obligations and guidelines. The Privacy Commissioner is able to make authorisations regarding the use of private information which would normally be contrary to the Act if he or she is satisfied that the public interest or benefit outweighs the interference with privacy.

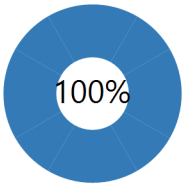
Scope

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

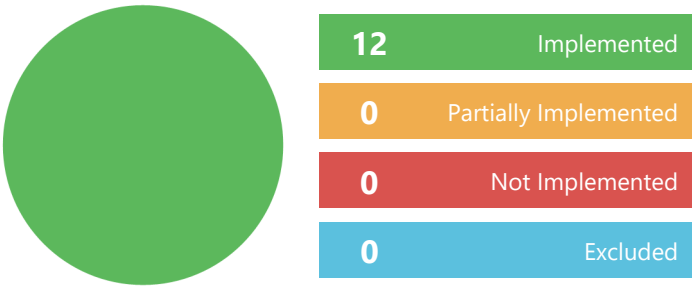
Notes

N/A

Overall Progress



Implementation Status



Total Controls/Policies

18

Number of Requirements

12

Requirements Per Standard

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

Purpose of collection of personal information
Personal information must only be collected when:
the collection is for a lawful purpose, connected with what the agency does, and it's necessary to collect the information for that purpose.

Satisfied By
- **Control:** Data Processing agreement
- **Policy:** Privacy Notice

Notes
Client data collected by xMatters is for specified, explicit and legitimate purposes, which depends on client's Business and Use case. 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 personal information
Personal information must usually be collected from the person the information is about. But sometimes it is all right to collect information from other people instead - for instance, when:
getting it from the person concerned would undermine the purpose of the collection
it's necessary so a public sector body can uphold or enforce the law
the person concerned authorises collection from someone else.

Satisfied By
- **Policy:** P-21: Privacy Code of Practice
- **Policy:** Privacy Notice
- **Control:** Data Processing agreement

Notes
All client data in xMatters systems is inputted by the clients, depending on their Business and Use case. 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

Collection of information from subject
When an agency collects personal information from the person the information is about, it has to take reasonable steps to make sure that person knows things like:
why it's being collected
who will get the information
whether the person has to give the information or whether this is voluntary
what will happen if the information isn't provided.
Sometimes there are good reasons for not letting a person know about the collection, for example, if it would undermine the purpose of the collection, or it's just not possible to tell the person.

Satisfied By

- **Control:** Data Processing agreement
- **Control:** Trust Portal

Notes

Client data that is provided to xMatters is done so by the client to support their Business and Use Case(s). 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 of personal information
Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances.

Satisfied By

- **Control:** Data Processing agreement
- **Control:** MSA (Master Service Agreement)

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

Principle 5 **Implemented** Information Assurance Department

Storage and security of personal information
It's impossible to stop all mistakes. But agencies must ensure that there are reasonable safeguards in place to prevent loss, misuse or disclosure of personal information.

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

Notes
xMatters Software as a Service (SaaS) systems operate in a Java environment that currently reside in Google Cloud Platform (GCP) Infrastructure as a Service (IaaS). The GCP IaaS is a very robust, redundant and fault tolerant network infrastructure that provides many privacy and security features that are in alignment and certified against national and international standards and frameworks.
xMatters administration and operations of the datacenters is conducted using administrative controls for access and monitoring as well as technical controls for access (including multi-factor authentication). xMatters Operations and Support Teams consist of highly capable and vetted personnel. xMatters only accesses client data and client instances when they have been permitted to do so by the client in order to address client requests (e.g. problem ticket) and for support purposes, there is no casual data access. xMatters access control and continuous monitoring logs all database access and ships the logs to a centralized Security Information and Event Management (SIEM) system.

Principle 6 **Implemented** Information Assurance Department

Access to personal information
People usually have a right to ask for access to personal information that identifies them. However, sometimes, agencies can refuse to give access to information, for instance because giving the information would:
endanger a person's safety
prevent detection and investigation of criminal offences
involve an unwarranted breach of someone else's privacy.

Satisfied By
- **Control:** Subject Access Request (SAR) Register
- **Policy:** P-15: Subject Access Request (SARS)
- **Control:** C-54: Hosted Service Agreement (HSA)
- **Control:** Data Processing agreement

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 of personal information
People have a right to ask the agency to correct information about themselves, if they think it is wrong. If the agency does not want to correct the information, it does not usually have to. But people can ask the agency to add their views about what the correct information is.

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, etc., of personal information to be checked before use
Before it uses or discloses personal information an agency must take reasonable steps to check that information 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

Agency not to keep personal information for longer than necessary
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
- **Control:** MSA (Master Service Agreement)
- **Policy:** Data Deletion Policy

Notes

Data is retained for the duration of the contract or unless indicated within theMaster 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 Datacenters. 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

Limits on use of personal information
Agencies must use personal information for the same purpose for which they collected that information. Other uses are occasionally permitted (for example because this is necessary to enforce the law, or the use is directly related to the purpose for which the agency got the information).

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

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

Limits on disclosure of personal information
Agencies can only disclose personal information in limited circumstances. One example is where another law requires them to disclose the information. Also, an agency can disclose information if it reasonably believes, for example, that
disclosure is one of the purposes for which the agency got the information
disclosure is necessary to uphold or enforce the law
disclosure is necessary for court proceedings
the person concerned authorised the disclosure
the information is going to be used in a form that does not identify the person concerned.

Satisfied By
- **Control:** C-29: Data Map
- **Control:** PII Subprocessors assessment

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

Unique identifiers
Some agencies give people a "unique identifier" instead of using their name. Examples are a driver's licence number, a student ID number, or an IRD number. An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

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