PRO-41: AUSTRALIAN PRIVACY PRINCIPLES (REV 2)

PROGRAM SUMMARY

2021/04/21

Effective From 2020-10-07 17:00:00
Effective To 2021-10-07 17:00:00
Report Date 2021-04-21 13:27:40

Standards Australian Privacy Principles

Description

The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988 (Privacy Act). They apply to any organisation or agency the Privacy Act covers.

There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information

The Australian Privacy Principles are principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies. (Source: https://www.oaic.gov.au/privacy/australian-privacy-principles/)

Scope

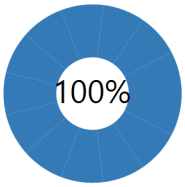
xMatters SaaS platform and services in compliance to the Australian Privacy principles.

Notes

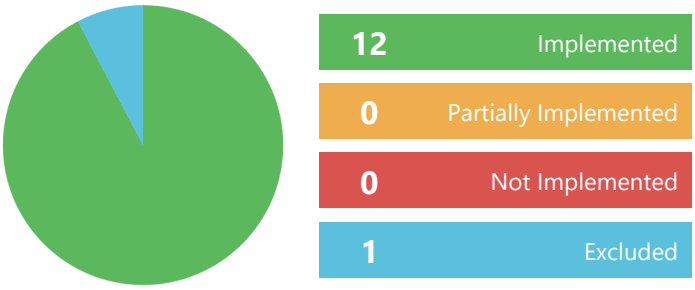
The Australian Privacy Principles (APPs) replaced the National Privacy Principles and Information Privacy Principles on 12 March 2014.

This is the text of the 13 APPs from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988. For the latest versions of these Acts visit the Federal Register of Legislation.

Overall Progress



Implementation Status



Total Controls/Policies

17

Number of Requirements

13

Requirements Per Standard

Requirement	Status	Date	Owner
AUSTRALIAN PRIVACY PRINCIPLES			
Part 1 — Consideration of personal information privacy			
APP 1	Implemented		Information Assurance Department

Open and transparent management of personal information
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

Notes

We keep our clients informed on how, when and what data is used to perform our services. xMatters Privacy Notice, Security and Privacy articles and whitepapers ensure clients are up to date with our data governance processes. xMatters stores and process all client data in Google Cloud Platform (GCP) datacenter. For more information please click here https://www.xmatters.com/trust/privacy/privacy-notice/

APP 2	Implemented		Information Assurance Department

Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Notes
Clients have total control on how their Personal Information is logged in xMatters SaaS. They can log their information and identify themselves the way they consider more appropriate using the SaaS WebUI.

Part 2 — Collection of personal information			
APP 3	Implemented		Information Assurance Department

Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.

Notes
xMatters only the necessary information for the provision of services is collected,as outlines on the Privacy Policy and Agreements.

APP 4	Implemented		Information Assurance Department

Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

Notes

Clients are responsible for entering their information on xMatters SaaS. They can also modify or delete their Personal Information at any time.

xMatters also keeps a document process for Subject Access Request (SAR).

Part 3 — Dealing with personal information

APP 5 **Implemented** Information Assurance Department

Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.

Notes

xMatters clearly states the purpose, use, processing and storage of personal information in the Privacy policy and Agreements signed with clients.

Disclosure of information with sub-processors is also disclosed and a list in annually updated and available to all clients (with an established NDA). Sub-processors are used for the provision of xMatters services. xMatters does not sell clients' information.

APP 6 **Implemented** Information Assurance Department

Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

Notes

xMatters has established processes in place to declare how we use, process and store personal information. xMatters has minimum data requirements that is a constituent receiving emergency communications: First Name, Last Name, and Email Address. Any further information provided by clients are up to the complete discretion of the client and to support their Business Case and Use Case toward the use of xMatters.

APP 7 **Implemented** Information Assurance Department

Direct Marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

Notes
xMatters collects consent for its clients to be able to send direct marketing and supporting material. Users can, at any time, opt out from marketing communications and request access to their information (SAR process).

APP 8 **Implemented** Information Assurance Department

Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

Notes

Client Data is stored in the same economic region as client is located. xMatters works with Google Cloud Platform and uses a Data Center in Sydney (primary datacenter) to store data. Further information can be found here: https://www.xmatters.com/trust/privacy/data-hosting-policy/

APP 9 **Excluded** Information Assurance Department

Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Part 4 — Integrity of personal information

APP 10 **Implemented** Rishabh Goswami

Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

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.

xMatters access the security of their data at planned intervals by conducting a Data Privacy Impact Assessment and all data is mapped for quality and privacy purposes.

APP 11 **Implemented** Information Assurance Department

Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

Notes

xMatters access the security of their data at planned intervals by conducting a Data Privacy Impact Assessment and all data is mapped for quality and privacy purposes.

There are multiple technical and administrative safeguards deployed to client data.

Part 5 — Access to, and correction of, personal information

APP 12 **Implemented** Information Assurance Department

Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

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.

APP 13 **Implemented** Information Assurance Department

Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

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.