



PRO-41: AUSTRALIAN PRIVACY PRINCIPLES (REV 2)

PROGRAM SUMMARY

2020/10/15

Effective From	2020-10-07 17:00:00	Standards	Australian Privacy Principles
Effective To	2021-10-07 17:00:00		
Report Date	2020-10-15 07:42:15		

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

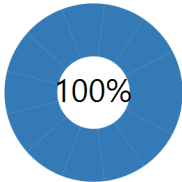
xMatters SaaS platform and services in compliance to the Australian Privacy principles.

Notes

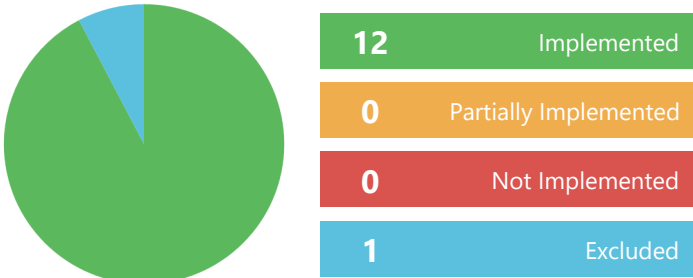
The Australian Privacy Principles (APPs) replaced the National Privacy Principles and Information Privacy Principles on 12 March 2014.

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

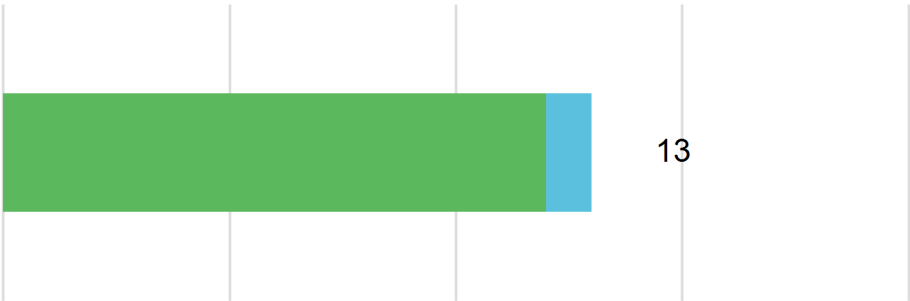
18

Number of Requirements

13

Requirements Per Standard

Australian Privacy Principles



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

Satisfied By

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

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.

Satisfied By

- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-72: Privacy Notice
- **Control:** C-29: Data Map
- **Control:** C-65: Sub-processors List

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.

Satisfied By

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

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.

Satisfied By

- **Policy:** P-72: Privacy Notice
- **Control:** Data Processing Agreement (DPA)
- **Policy:** P-15: Subject Access Request (SARS)

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.

Satisfied By

- **Control:** Data Processing Agreement (DPA)
- **Control:** C-29: Data Map
- **Policy:** P-77: Standard Contractual Clauses (SCC)
- **Control:** C-65: Sub-processors List

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.

Satisfied By

- **Control:** Data Processing Agreement (DPA)
- **Control:** C-29: Data Map
- **Policy:** P-15: Subject Access Request (SARS)

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.

Satisfied By

- **Control:** Virtual Private Networking (VPN)
- **Control:** TRUSTe/TrustARC certified
- **Control:** C-21: Access Control SaaS
- **Control:** C-17: Firewall rules audits
- **Control:** Multifactor Authentication (MfA)
- **Control:** Security Awareness and Training
- **Control:** C-40: Endpoint Security - Duplicate of C-55 Antivirus protection
- **Control:** C-34: Disaster Recovery Tests (A1122)
- **Control:** WhiteHat - Vulnerability Scan
- **Control:** C-55: Antivirus protection
- **Policy:** P-46: Cryptographic and Key Management Policy (A101)
- **Policy:** P-75: Security at xMatters

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.

Satisfied By

- **Policy:** P-72: Privacy Notice
- **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.

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.

Satisfied By

- **Policy:** P-21: Privacy Code of Practice
- **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.



Created with **StandardFusion**. Copyright ©2020 Fireloft Inc.

This product includes standards copyrighted by the American Institute of Certified Public Accountants. All rights reserved. Portions of the ISO Standard have been reproduced with permission from the Standards Council of Canada. No further reproduction or distribution of this copy is permitted by electronic transmission or any other means. Portions of this product are provided courtesy of PCI Security Standards Council, LLC ("PCI SSC"). © 2006-2015 PCI Security Standards Council, LLC. All rights reserved. PCI SSC does not endorse this product, its provider or the methods, procedures, statements, views, opinions or advice contained herein. All references to documents, materials or portions thereof made available by PCI SSC ("PCI Materials") should be read as qualified by the actual PCI Materials. For questions regarding PCI Materials, please contact PCI SSC through its web site at <https://www.pcisecuritystandards.org>.