

Data Protection Policy Australia

OCSIS-P-10-02

1. About this policy

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our colleagues, clients, customers and suppliers. We take our data protection responsibilities extremely seriously and recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

All colleagues are obliged to comply with this policy when processing personal data on our behalf and any breach of this policy may result in disciplinary action.

The types of personal data that we process include information about current, past and prospective suppliers, customers, tenants, landlords, colleagues, professional advisers, consultants and others we may communicate with. The personal data, which may be held electronically, on paper or other media, is subject to The Privacy Act 1988.

On 10 December 2024, the *Privacy and Other Legislation Amendment Bill 2024* (Cth) received Royal Assent. It introduces several significant amendments to the *Privacy Act 1988* (Cth).

Below is a summary of the key changes to the Privacy Act introduced by the Amendment Act, along with their commencement dates. This policy will be updated fully when all amendments come into effect.

- **New Statutory Cause of Action for Serious Invasions of Privacy:**

Individuals can take legal action against organisations or individuals for serious invasions of privacy. This includes intrusions into personal seclusion or misuse of personal information.
Effective on a date to be fixed on or by 10 June 2025.

- **Automated Decision-Making:**

New transparency obligations require organisations to update their privacy policies to disclose when decisions are made using automated processes.
Effective on 10 December 2026.

- **Doxxing Offence:**

New measures have been introduced to combat doxxing, making it illegal to share someone's personal information with the intent to harm. This offence is punishable by up to 7 years' imprisonment.

The amendments have been proposed in the Amendment Act but the doxxing offence is not yet effective. The new measures will undergo an independent review, and a report of this review must be provided within 6 months of the review's commencement. The exact date for the review's start has not yet been specified.

- **Children's Online Privacy Code:**

The Office of the Australian Information Commissioner (OAIC) is required to develop a code addressing online privacy for children. There will be a consultation period of 60 days.
Children's Online Privacy Code to be developed and registered by 10 December 2026.

- **Overseas Dataflows, Whitelist Powers:**

Ministerial powers to 'whitelist' countries that provide substantially similar privacy protections, to assist entities disclosing personal information overseas. As of yet, no official white list has been announced.

Effective on 11 December 2024.

- **New Civil Penalty and Powers to Issue Infringement and Compliance Notices:**

The OAIC has been granted new powers to issue infringement notices and compliance notices. A failure to comply with a compliance notice may result in the imposition of civil penalties.

Effective on 11 December 2024.

- **Clarification on Required Steps to Protect Personal Information:**

The Privacy Act requires that 'reasonable steps' must be taken to protect the security of personal information. The Amendment Act has clarified that this includes implementing 'technical and organisational measures'.

Effective on 11 December 2024.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects or other sources. It also sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2. Who this policy applies to

This policy applies to all Australian based colleagues, officers, consultants, contractors, casual workers and agency workers who we employ and work with. This policy does not form part of any colleague's contract of employment and may be amended at any time.

3. Responsibility for this policy

OCS Group International's board of directors has overall responsibility for the effective operation of this policy but has delegated responsibility for overseeing its implementation to the Data Protection Officer. Suggestions for change should be reported to the Data Protection Officer.

The data protection team has day-to-day responsibility for this policy, and you should refer any questions about this policy to them in the first instance at dataprotection@ocs.com

This policy is reviewed annually by the Data Protection Officer.

4. Definition of Data Protection terms

Data is information, which is stored electronically, on a computer, or in paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be an Australian or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified directly or indirectly from that data (or from other information in our possession)

A data controller is the organisation that determines the purposes and means of the processing of personal data. They are responsible for establishing practices and policies in line with legislation. OCS are the data controller of all personal data of our employees.

Data processors include any person or organisation that processes personal data on behalf of a data controller. This includes suppliers which handle personal data on behalf of OCS or its subsidiaries.

Processing is any activity that involves the use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive data includes information about a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or sex life or in relation to a criminal offence committed or alleged to have been committed by that person. Sensitive information can only be processed under specific circumstances.

5.0 Data Protection Principles - the 13 principles that are the foundation of The Privacy Act:

APP 1	Open and transparent management of personal information	Ensures that APP entities manage <u>personal information</u> in an open and transparent way. This includes having a clearly expressed and up to date APP <u>privacy policy</u> .
APP 2	Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
APP 3	Collection of solicited personal information	Outlines when an APP entity can <u>collect</u> personal information that is solicited. It applies higher standards to the collection of <u>sensitive information</u> .
APP 4	Dealing with unsolicited personal information	Outlines how APP entities must deal with unsolicited personal information.
APP 5	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.
APP 6	Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
APP 7	Direct marketing	An organisation may only use or disclose personal information for <u>direct marketing</u> purposes if certain conditions are met.
APP 8	Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
APP 9	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 <u>use or disclose</u> a government related identifier of an individual.
APP 10	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.
APP 11	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.
APP 12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given <u>access to personal information</u> held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
APP 13	Correction of personal information	Outlines an APP entity's obligations in relation to <u>correcting the personal information</u> it holds about individuals.

Anonymity

- Individuals have the option of not identifying themselves unless an exemption applies.
- For our colleagues and client information we have a legal obligation to maintain identifiable information.

Collection of solicited personal information

For personal information (other than sensitive information):

- an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities
- different requirements exist for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an organisation may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection.
- personal information must only be collected by lawful and fair means.
- personal information must be collected from the individual concerned, unless this is unreasonable or impracticable.

Notifying Data Subjects

- An organisation that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.
- The matters include:
 - the organisation's identity and contact details
 - the fact and circumstances of collection
 - whether the collection is required or authorised by law
 - the purposes of collection
 - the consequences if personal information is not collected
 - the usual disclosures of personal information
 - information about the organisation Privacy Policy
 - whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.
- OCS must take reasonable steps, before, or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

Usage or disclosure of personal information

- We can only use or disclose personal information for the purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.
- The exceptions include where:
 - the individual has consented to a secondary use or disclosure
 - the individual would reasonably expect OCS to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
 - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
 - a permitted general situation exists in relation to the secondary use or disclosure
 - a permitted health situation exists in relation to the secondary use or disclosure
 - OCS reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Cross Border Disclosure

- OCS takes all reasonable steps to ensure that any overseas recipient of personal information does not breach the privacy principles in relation to the information.
- We are accountable for any acts or practices of the overseas recipient in relation to the information that would breach the privacy principles.

Accurate and up to date

- OCS takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.
- We also take reasonable steps to ensure that the personal information we use and disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Security of Personal Information

- OCS takes all reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- When we no longer need the personal information for any purpose for which the information may be used or disclosed, we take reasonable steps to destroy the information or ensure that it is de-identified.

Access to personal information

- Where we hold personal information about an individual we give the individual access to that information on request.
- Access requests must be responded to within 30 calendar days unless an exemption applies.

Correction of personal information

- OCS will take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.
- This requirement applies where:
 - We are satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
 - the individual requests us to correct the personal information.

Reporting a Personal Data Breach

- We have put in place procedures to deal with suspected loss of or unauthorised access to personal data (a “personal data breach”) that are available on our intranet or on request from the Data Protection Officer. Each of our colleagues must comply with these procedures.
- We have 30 days to report a breach to the supervisory authority the Office of the Australian Information Commissioner (OAIC).
- If you know or suspect that a personal data breach has occurred, please do not attempt to investigate the matter yourself. Please contact the Data Protection Officer as quickly as possible at dataprotection@ocs.com

18 Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Schedule

Data Processing Activities

- Reasons/Purposes for Processing Information

We process personal information to enable us as to carry out property management services; promote and advertise our services; maintain our own accounts and records; and support and manage our colleagues.

- Type/Classes of Information Processed

We process information relevant to the above reasons/purposes. This may include:

- Personal details
- Family details
- Lifestyle and social circumstances
- Employment and education details
- Financial details
- All information contained in references

We may also process special category data that may include:

- racial or ethnic origin
- religious or other beliefs
- trade union membership
- physical or mental health details

Data Subjects include:

- customers
- tenants
- professional advisers and consultants
- complainants, enquirers
- suppliers
- landlords
- colleagues

Document Control

Version	Description	
1.0 New policy	Date live	February 2024
	Reviewed by	Sara Taylor, DPO
	Approved by	
2.0 New legislation	Date live	February 2025
	Reviewed by	Sara Taylor, DPO
	Approved by	
	Date live	
	Reviewed by	
	Approved by	