Privacy Policy

One Registry Services

7 January 2026

PUBLIC

Table of Contents

1. Application of Policy

1.1. This policy applies to all members of the One Registry Services Group (**ORS**) including One Registry Services Pty Ltd (ACN 141 757 360).

2. Purpose of Policy

2.1. Privacy is important and ORS is committed to managing personal information responsibly

2.2. ORS considers having a documented approach to how it collects, secures, stores, uses and discloses personal information is important and this policy is designed:

(a) to assist in identifying the personal and sensitive information held by ORS;

(b) to describe how it collects, secures, stores, uses and discloses personal information;

(c) to describe ORS's approach to Notifiable Data Breaches; and

(d) to set out the role of the Privacy Officer.

2.3. ORS may assist clients to meet their obligations under the AML/CTF Act and in respect of their Tax Compliance obligations and must be aware how those laws impact on their obligations under the Privacy Act.

3. What information does ORS collect?

3.1. ORS in operating its registry services business may collect personal information and in certain limited circumstances, sensitive information.

3.2. ORS in providing registry services to its clients, including in establishing and administering investments, and performing investor verification and tax compliance, ORS may collect the following information:

(a) full name, prior or other names, date of birth, gender;

(b) contact details including:

(i) postal, residential and email addresses; and
(ii) telephone, mobile and fax numbers;

(c) a copy of a driver licence and/or passport or other identification documentation for the purpose of verifying identity and residence and to assist clients with their compliance with any relevant requirements including AML/CTF Act, foreign tax compliance reporting or Australian withholding tax;

(d) tax file numbers (TFN) and bank account details for the purpose of administering investor accounts and tax reporting and withholding;

(e) investor contribution details and investment choice;

(f) details about authorised signatories on investments or accounts with ORS;

(g) detailed contact information about the relevant financial adviser; and

(h) copies of any relevant trust deeds, partnership agreements or constitutions, which may be relevant to comply with the AML/CTF Act.

3.3. It may, on occasion also be necessary in each case to obtain other details, including information relating to powers of attorney or for probate and estate administration.

Sensitive Information

3.4. ORS may collect sensitive information in respect of:

(a) Investors, during their review of AML/CTF review, for example where a potential investor is identified as high risk because they have a criminal record or a political party affiliation; or

(b) Potential employees where pre-appointments checks such as bankruptcy and criminal record are performed.

ORS would generally reject the application or, where *OIG's Employee Handbook* directs, the potential employee. Where the applicant or potential employee is rejected, ORS will destroy the information collected when it is no longer legally obliged to hold it[1].

4. How does ORS collect and hold personal information?

4.1. In collecting personal information, ORS will:

(a) disclose how it manages personal information in an open and transparent way;

(b) not collect personal information unless that information is reasonably necessary for the one or more of ORS's functions or activities;

(c) only collect information by lawful and fair means;

(d) only collect personal information from the individual unless it is unreasonable or impracticable to do so; and

(e) if it receives personal information that was not solicited, destroy that information.

4.2. An individual is not required to provide ORS or their client with their personal information, but if that individual does not do so, ORS may not be able to provide them with services. If an individual submits an Application Form, that individual is deemed to agree to their personal information being collected, held, used and disclosed as set out in this Privacy Policy. ORS may revise this Privacy Policy and will advise place the revised Privacy Policy on the ORS website or otherwise notifying individuals of the change.

4.3. ORS may collect personal information in various ways including from application forms or other documents, telephone, email, letters or other correspondence and from websites and other social media channels. Wherever practicable, ORS will collect information about individuals from them directly.

4.4. However, it may be necessary at times to collect information about individuals from other external sources, such as:

(a) a service provider or investment manager;

(b) a financial adviser or broker;

[1] *Part 10 of the AML/CTF Act generally requires information to be held for 7 years.*

(c) an online application provider;

(d) authorised representatives, such as executors or administrators; and

(e) identification verification service providers.

ORS Websites

4.5. If an individual uses an ORS website the following types of information may be collected and analysed for statistical purposes:

(a) the number of users who visit the website;

(b) the number of pages viewed; and

(c) traffic patterns.

4.6. This is anonymous statistical data and no attempt is made to identify users or their browsing activities. This data is used only to evaluate ORS's website performance and to improve the content ORS displays to the audience.

4.7. Other information, such as browser type, is included in a 'cookie' that is sent to the user's computer when they complete certain tasks on the ORS website. A cookie contains bits of information that enables ORS's servers to identify and interact efficiently with the user's computer. Cookies are designed to provide a better, more customised website experience, and to make it easier for users to use ORS's website. Individuals can configure their computer to accept or reject cookies.

5. What does ORS use personal information for?

5.1. ORS generally only uses and discloses information for the purpose for which it was disclosed or related purposes which would reasonably be expected. Those purposes include:

(a) to establish and administer investments or other relationships with ORS clients;

(b) to provide to its clients under its registry services agreements or, at the direction of its clients, to provide to other service providers of its clients;

(c) for communication purposes including surveys and questionnaires;

(d) to comply with ORS's clients' record-keeping, reporting, and tax obligations;

(e) to comply with other legal obligations such as laws that require ORS's clients to "*know your customer*", to report on tax compliance and to determine a target market for its products;

(f) to protect legal rights and to prevent fraud and abuse;

(g) for quality assurance and training purposes;

(h) to enable ORS and its clients to provide information about new and existing products and services that will enhance the relationship between ORS, the relevant client and individuals. However, ORS respects the right of individuals to ask ORS not to do this and will not share personal information between unrelated clients of different funds; and

(i) to handle any relevant enquiries or complaints.

5.2. ORS (either on its own account or on behalf of its clients) may be required by law to disclose personal information. For instance, ORS may be required to provide details to:

(a) Australian Government regulators such as the Australian Securities and Investments Commission, the Australian Tax Office, the Australian Transaction Reports and Analysis Centre and to other regulatory or government entities;

(b) the Australian Financial Complaints Authority (AFCA) or the Australian Information Commissioner;

(c) as required by a court order (including in Family Law matters);

(d) other regulatory or governmental entities outside of Australia.

5.3. In order to meet the needs of and provide services to individuals dealing with ORS, it may be necessary to release information or provide access to external service providers, for instance:

(a) the trustees and responsible entities that have engaged ORS to provide them with registry services;

(b) to investment managers to better understand the types of investors in the funds they administer and provide services to the relevant trustee or responsible entity (including in relation to their design and distribution obligations);

(c) to any organisations involved in providing, managing or administering the products systems or services of ORS's clients such as custodians, investment managers, administrators, mail houses and software and information technology providers;

(d) to auditors, consultants and other professional advisers;

(e) to appropriate advisers, such as financial, legal, or other consultancy services;

(f) to a legal personal representative, attorney or any other person who may be entitled to receive the proceeds from an individual's investment or account with ORS;

(g) to other financial institutions who hold an account in an investor's name, for example, where amounts have been transferred to or from that account;

(h) to authorities investigating (or who could potentially investigate) alleged fraudulent or suspicious transactions in relation to an investment or account;

(i) to on-line application provider; and

(j) to lenders.

5.4. Information about an individual or individual's dealings with ORS is not and will not be sold to any other company, individual, or group.

6. Accessing and Amending Personal Information

6.1. Individuals may request access to any personal information ORS holds about them. Generally, if it is incorrect, ORS will correct it at their request.

6.2. An individual's right to access is subject to some exceptions allowed by law[2]. Where they are able to, ORS will notify individuals of the basis for any denial of access to their personal information.

7. Protection and storage of Personal Information

7.1. All personal information ORS collects will be held securely.

7.2. Personal information is protected from unauthorised access through the use of secure passwords, user logins or other security procedures. Developments in security and encryption technology are reviewed regularly as detailed in ORS's *IT, Cyber Resilience and Disaster Recovery Policy*.

8. Will information be sent overseas?

8.1. ORS may disclose personal information outside of Australia including to our third-party suppliers located in Vietnam and cloud-computing services. ORS will ensure these data processors contracted to abide by privacy rules at least as robust as Australian Privacy Law and are ISO 27001 (Information Security Management Systems) compliant. When an individual provides their personal information to ORS, they are deemed to consent to the disclosure of their information outside of Australian and to acknowledge that ORS is not required to ensure that overseas recipients handle that personal information in compliance with the Privacy Act. ORS will, however, take reasonable steps to ensure that any overseas recipient will deal with personal information disclosed to them in a way that is consistent with the APPs.

8.2. ORS's clients, and other service providers used by ORS's clients, may disclose to overseas recipients the personal information ORS has collected for their clients and individuals may need to read more than ORS's privacy policy.

9. Making ORS's Privacy Policy available

9.1. ORS will make its Privacy Policy available on its website and will send a printed version free of charge to those who request it [3].

9.2. ORS ensure that an Application Form, contains:

(a) a statement as to the availability of and access to the ORS Privacy Policy;

(b) a general statement as to the substantial aspects of the policy that may impact on investors in the product; and

(c) a general statement as to ORS's obligations in respect of the collection of personal information.

9.3. ORS's Privacy Policy is available free of charge through:

---

[2] *For example an ORS Licensee may deny access where the information is the subject of a suspicious matter report made to AUSTRAC. Under s.41 of the AML/CTF Act it is a criminal offence to tip-off the customer that the ORS Licensee considers a transaction as suspicious or as informed AUSTRAC of its suspicions.*

[3] *The APPs, particularly APP 5, requires ORS, as an APP entity to take such steps as are reasonable in the circumstances to make the ORS Privacy Policy available*

(a) downloading a copy in document format from ORS's website www.oneregistryservices.com.au;

(b) Requesting a copy be emailed by emailing a request to enquiries@oneinvestment.com.au;

(c) Telephoning us and requesting a copy be mailed or emailed by calling (02) 8277 0000 (+612 8277 0000 for international callers);

(d) Writing to ORS and requesting a copy be mailed or emailed using ORS's postal address: PO Box R1471, Royal Exchange NSW 1225

9.4. If a copy of this Privacy Policy in requested in a particular format (for example, on audio disc) please contact ORS at the telephone number or postal address set out above and ORS will accommodate any reasonable request.

10. Complaints

10.1. If an individual has a complaint about the manner in which ORS has collected, held, used, disclosed, kept, or given people access to their personal information, they may complain to ORS by phone, email, letter or in person using the details in clause 9.3 above. The individual will need to provide ORS with sufficient details regarding their complaint and during the investigation phase, ORS may ask complainants to provide additional information.

10.2. Complaints will be referred to ORS's Privacy Officer who will investigate and then determine the steps ORS will take to resolve the complaint.

10.3. ORS will notify complainants in writing of ORS's determination, generally within 30 days. If the complainant is not satisfied with ORS's determination or does not receive a response within 30 days, the complainant can contact ORS to discuss their concerns and they can refer the complaint to the Office of the Australian Information Commissioner at www.oaic.gov.au

11. Notifiable Data Breach

11.1. If ORS becomes aware that there are reasonable grounds to believe an eligible data breach has occurred, ORS is obligated to notify individuals at likely risk of serious harm and OAIC as soon practicable. In any event, ORS must take all reasonable steps to ensure that their assessment is completed and the OAIC and potentially affected individuals are contacted within 30 days of the organisation becoming aware of the data breach.

11.2. If there is a suspected or actual data breach which may compromise personal information, ORS will promptly undertake an assessment of the incident. Where relevant, immediate steps will be taken to contain the breach. These steps may include limiting any further access or distribution of the affected personal information, or the possible compromise of other personal information.

11.3. If the unauthorised access, disclosure or loss of personal information is likely to cause serious harm to one or more individuals and the likely risk of serious harm has not been prevented by remedial action, ORS will notify affected individuals and OAIC as soon as practicable. The notification will include ORS's identity and contact details, a description of the incident, the kind of information concerned and any recommended steps for affected individuals.

11.4. Following any data breach incident, ORS will undertake a review process to help prevent future breaches in accordance with ORS's Data Breach Response Plan and Breach Reporting Template.

12. Data Breach and Data Breach Response Plan

12.1. A Data Breach occurs when either personal information or sensitive information is lost or subjected to unauthorised access, modification, use of disclosure or other misuse or interference.

12.2. The data breaches can be caused or exacerbated by a range of factors, affect different types of personal information or sensitive information and give rise to a range of actual or potential harms to individuals, organisations and government agencies.

12.3. The data breaches are required to be assessed and reported under this Privacy Policy, the Breach and Incident Handling Policy and ORS's Data Breach Response Plan.

12.4. ORS's Data Breach Response Plan assists ORS in managing a data breach. The plan forms part of ORS's incident and breach reporting process but sets out a specific framework of procedures and lines of authority for ORS staff in the event of a data breach or suspected data breach.

13. Privacy Officer

13.1. ORS has appointed a Privacy Officer to be the first point of contact in ORS when privacy issues arise either internally or externally.

13.2. The Privacy Officer is responsible for:

(a) developing and implementing a privacy policy that suits ORS's business and complies with the law;

(b) ensuring that the ORS Privacy Policy and procedures are fully implemented and working effectively; and

(c) reporting to the board of ORS any breach of the ORS Privacy Policy.

14. Training and Compliance

14.1. The implementation of (including training on) and monitoring of compliance with this policy is undertaken in accordance with OIG's *Compliance Management Systems Framework*.

14.2. Compliance with this policy is mandatory and any actual non-compliance must be reported and assessed through the normal incident/ breach reporting process. Any deliberate act of non-compliance by any employee may result in disciplinary action.

15. Review of Policy

This policy will be reviewed at the intervals and in the manner described in ORS's *Risk Management Framework*.

16. Other relevant ORS Policies

In addition to the *Compliance Management Systems Framework*, other ORS relevant policies and procedures are:

(a) Breach and Incident Handling Policy;

(b) Information Technology Policy and Business Continuity and Disaster Recovery Policy;

(c) OIG's Employee Handbook;

(d) Data Breach Response Plan.

17. Dictionary and Interpretation

17.1. In this policy, a reference to a person performing an act, for example *Director, Operations*, that person may delegate the performance of the relevant act to another, for example *Manager, Operations* provided they adequately supervise their delegate.

17.2. In addition to the terms defined in the Compliance Management Systems Framework, when used in this policy, the following capitalised terms have the meanings set out below:

Term	Meaning
AML/CTF Act	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
AML/CTF Rules	Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007
Application Form	An application form or other request to invest in a fund operated by a client of ORS or other method of providing ORS with personal information.
APPs	The Australian Privacy Principles set out in the Privacy Act
NDB Act	Privacy Amendment (Notifiable Data Breaches) Act 2017
OAIC	Office of the Australian Information Commissioner
Personal Information	Information or an opinion (including information or an opinion forming part of a data base, whether true or not, and whether recorded in a material form or not) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes credit card details, information gathered on websites and mobile telephone numbers linked to user names and mailing lists.
Privacy Act	Privacy Act 1988, as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 including the APPs.
Sensitive Information	Is a subset of personal information and includes information or an opinion about a person's racial or ethnic origin, political or religious belief, philosophical beliefs, membership of professional or trade associations or unions, sexual preferences and practices and criminal record. It also includes health information and genetic information about an individual that is not otherwise health information.
Tax Compliance	*Tax Laws Amendment (Implementation of the Common Reporting Standard) Act 2016* (Cth) (**CRS**) and *Foreign Account Tax Compliance Act (**FATCA**)* as applicable under Australian and intergovernmental agreements and any other tax reporting compliance obligations.