

# Privacy Policy

---

One Investment Group

10 February 2022

---

## Table of Contents

1. Application of Policy .....	2
2. Purpose of Policy.....	2
3. What information does OIG collect? .....	2
4. How does OIG collect and hold personal information?.....	3
5. What does OIG use personal information for?.....	5
6. Accessing and Amending Personal Information .....	6
7. Protection and storage of Personal Information .....	6
8. Will information be sent overseas? .....	6
9. Making OIG’s Privacy Policy available.....	7
10. Complaints .....	7
11. Notifiable Data Breach.....	8
12. Data Breach and Data Breach Response Plan.....	8
13. Privacy Officer .....	8
14. Training and Compliance .....	9
15. Review of Policy .....	9
16. Other relevant OIG Policies.....	9
17. Dictionary and Interpretation .....	9

## 1. Application of Policy

- 1.1. This policy applies to all members of the One Investment Group (**OIG**) that hold an Australian financial services licence (**AFS Licence**) to provide financial services to retail and/or wholesale clients and their **OIG Corporate Authorised Representatives** (each an **OIG Licensee**).

## 2. Purpose of Policy

- 2.1. Privacy is important and **OIG** is committed to managing personal information responsibly
- 2.2. **OIG** 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 **OIG**;
  - (b) to describe how it collects, secures, stores, uses and discloses personal information;
  - (c) to describe **OIG's** approach to Notifiable Data Breaches; and
  - (d) to set out the role of the Privacy Officer.
- 2.3. **OIG Licensees** provide a designated service for the purpose of the AML/CTF Act and must be aware how those laws impact on their obligations under the Privacy Act.

## 3. What information does **OIG** collect?

- 3.1. **OIG Licensees** in operating their business may collect personal information and in certain limited circumstances, sensitive information.

### Investors and custodial clients

- 3.2. In operating its financial services business (including establishing and administering investments, providing custodial and depository services and determining and monitoring target markets for its financial products and handling complaints) **OIG** 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 ensure compliance with the 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 **OIG**;
  - (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.

### Personal information in relation to Fund Assets

3.4. As trustee or responsible entity for a Fund, an OIG Licensee may hold an asset (for example a lease of a property or a loan to, or guaranteed, by a person) that may require it to collect the following information:

- (a) full name, date of birth, gender and contact details including telephone, address, e-mail and fax;
- (b) a copy of a driver licence and/or passport or other identification documentation for the purpose of verifying identity and residence;
- (c) tax file numbers (TFN) and bank account details for the purpose of administering payments in respect of the relevant Fund asset;
- (d) details about authorised signatories in connection with counterpart to the relevant Fund asset.

3.5. 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

3.6. OIG 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.

OIG Licensees would generally reject the application or, where *OIG's Employee Handbook* directs, the potential employee. Where the applicant or potential employee is rejected, the OIG Licensee will destroy the information collected when it is no longer legally obliged to hold it<sup>1</sup>.

## 4. How does OIG collect and hold personal information?

4.1. In collecting personal information, OIG 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 OIG's functions or activities;

---

<sup>1</sup> Part 10 of the AML/CTF Act generally requires information to be held for 7 years.

- (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 an OIG Licensee or their service provider with their personal information, but if they do not do so OIG may not be able to provide them with products or services. If an individual applies for or accepts any of OIG products or services or otherwise provides OIG with their personal information, they agree to their information being collected, held, used and disclosed as set out in this Privacy Policy. OIG may revise this Privacy Policy and will advise place the revised Privacy Policy on the OIG website or otherwise notifying individuals of the change.
- 4.3. OIG 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, OIG 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, such as a registry service provider or investment manager;
  - (b) a financial adviser or broker;
  - (c) authorised representatives, such as executors or administrators; and
  - (d) identification verification service providers.

### OIG Websites

- 4.5. If an individual uses an OIG 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 OIG's website performance and to improve the content OIG 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 OIG website. A cookie contains bits of information that enables OIG'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 OIG's website. Individuals can configure their computer to accept or reject cookies.

## 5. What does OIG use personal information for?

- 5.1. OIG 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 the OIG Licensee;
  - (b) for communication purposes including surveys and questionnaires;
  - (c) to comply with OIG's record-keeping, reporting, and tax obligations;
  - (d) to comply with other legal obligations such as laws that require OIG Licensees to "*know your customer*", to report on tax compliance and to determine a target market for its products;
  - (e) to protect legal rights and to prevent fraud and abuse;
  - (f) for quality assurance and training purposes;
  - (g) to enable OIG and its investment managers to provide information about new and existing products and services that will enhance the relationship between OIG, the relevant investment manager and individuals. However, OIG respects the right of individuals to ask OIG not to do this and will not share personal information between unrelated investment managers of different funds; and
  - (h) to handle any relevant enquiries or complaints.
- 5.2. OIG may be required by law to disclose personal information. For instance, OIG 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 OIG Licensees, such as registry services, administration of accounts and mailing of investor holding and distribution statements, it may be necessary to release information or provide access to external service providers, for instance:
- (a) to investment managers to better understand the types of investors in the funds they administer and provide services to the OIG Licensee including services in relation to target market determinations;
  - (b) to any organisations involved in providing, managing or administering OIG's products systems or services such as custodians, registries, administrators, mail houses and software and information technology providers;
  - (c) to auditors, consultants and other professional advisers;
  - (d) to appropriate advisers, such as financial, legal, or other consultancy services;

- (e) 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 OIG;
- (f) 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;
- (g) to authorities investigating (or who could potentially investigate) alleged fraudulent or suspicious transactions in relation to an investment or account.

5.4. Information about an individual or individual's dealings with OIG 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 OIG holds about them. Generally, if it is incorrect, OIG will correct it at their request.
- 6.2. An individual's right to access is subject to some exceptions allowed by law<sup>2</sup>. Where they are able to, OIG Licensees 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 OIG 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 OIG's *IT, Cyber Resilience and Disaster Recovery Policy*.

## 8. Will information be sent overseas?

- 8.1. OIG Licensees do not anticipate that its trustees, responsible entities and custodians will disclose information to overseas recipients.
- 8.2. One Registry Services when providing registry services to an OIG Licensee, may disclose personal information to data processors located in Vietnam. These data processors have contracted to abide by Australian Privacy Law and are ISO 27001 (Data Security Management Systems) compliant. OIG Licensees will take reasonable steps to ensure that any overseas recipient will deal with such personal information in a way that is consistent with the APPs.
- 8.3. Other service providers used by OIG Licensees may disclose to overseas recipients the personal information they have collected for OIG Licensees. OIG Licensees have procedures to monitor its service providers including having them confirm their compliance with the Privacy Act.

---

<sup>2</sup> For example an OIG 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 OIG Licensee considers a transaction as suspicious or as informed AUSTRAC of its suspicions.

## 9. Making OIG's Privacy Policy available

- 9.1. OIG will make its Privacy Policy available on its website and will send a printed version free of charge to those who request it<sup>3</sup>.
- 9.2. OIG Licensees ensure that a PDS or other offer document for a product offered by them, contains:
- (a) a statement as to the availability of and access to the OIG 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 OIG's obligations in respect of the collection of personal information.
- 9.3. OIG's Privacy Policy is available from OIG free of charge through:
- (a) downloading a copy in document format from OIG's website [www.oneinvestment.com.au](http://www.oneinvestment.com.au);
  - (b) Requesting a copy be emailed by emailing a request to [enquiries@oneinvestment.com.au](mailto: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 OIG and requesting a copy be mailed or emailed using OIG's postal address: PO Box R1471, Royal Exchange NSW 1225
- 9.4. If a copy of this Privacy Policy is requested in a particular format (for example, on audio disc) please contact OIG at the telephone number or postal address set out above and OIG will accommodate any reasonable request.

## 10. Complaints

- 10.1. If an individual has a complaint about the manner in which an OIG Licensee has collected, held, used, disclosed, kept, or given people access to their personal information, they may complain to OIG by phone, email, letter or in person using the details in clause 9.3 above. The individual will need to provide OIG with sufficient details regarding their complaint and during the investigation phase, OIG may ask complainants to provide additional information.
- 10.2. Complaints will be referred to OIG's Privacy Officer who will investigate and then determine the steps OIG will take to resolve the complaint.
- 10.3. OIG will notify complainants in writing of OIG's determination, generally within 30 days. If the complainant is not satisfied with OIG's determination or does not receive a response within 30 days, the complainant can contact OIG to discuss their concerns and they can refer the complaint to the Office of the Australian Information Commissioner at [www.oaic.gov.au](http://www.oaic.gov.au)

---

<sup>3</sup> The APPs, particularly APP 5, requires OIG, as an APP entity to take such steps as are reasonable in the circumstances to make the OIG Privacy Policy available



## 11. Notifiable Data Breach

- 11.1. If OIG becomes aware that there are reasonable grounds to believe an eligible data breach has occurred, OIG is obligated to notify individuals at likely risk of serious harm and OAIC as soon practicable. In any event, OIG 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, OIG 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, OIG will notify affected individuals and OAIC as soon as practicable. The notification will include OIG'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, OIG will undertake a review process to help prevent future breaches in accordance with OIG'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 OIG's Data Breach Response Plan.
- 12.4. OIG's Data Breach Response Plan assists OIG in managing a data breach. The plan forms part of OIG's incident and breach reporting process but sets out a specific framework of procedures and lines of authority for OIG staff in the event of a data breach or suspected data breach.

## 13. Privacy Officer

- 13.1. OIG has appointed a Privacy Officer to be the first point of contact in OIG 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 OIG's business and complies with the law;

- (b) ensuring that the OIG Privacy Policy and procedures are fully implemented and working effectively; and
- (c) reporting to the board of OIG any breach of the OIG 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 OIG's *Compliance Management Systems Framework*.

## 16. Other relevant OIG Policies

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

- (a) Breach and Incident Handling Policy;
- (b) IT, Cyber Resilience 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
<b>AML/CTF Act</b>	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
<b>AML/CTF Rules</b>	Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007
<b>APPs</b>	The Australian Privacy Principles set out in the Privacy Act
<b>Application Form</b>	An application form or other request to invest in a fund operated by an OIG Licensee or other method of providing its registry service provider with personal information.
<b>NDB Act</b>	Privacy Amendment (Notifiable Data Breaches) Act 2017
<b>OAIC</b>	Office of the Australian Information Commissioner
<b>Personal Information</b>	Information or an opinion (including information or an opinion forming part of a data base, whether true or not, and whether recorded in a

Term	Meaning
	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.
<b>Privacy Act</b>	Privacy Act 1988, as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 including the APPs.
<b>Sensitive Information</b>	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.