IOOF

Privacy policy

November 2020

1 Overview

Protecting our clients' privacy is very important to us. To ensure our compliance with the Privacy Act and as part of our commitment to ensuring the safety of your private and confidential information, we have established and implemented this Policy.

1.1 Introduction

The Privacy Act requires that we handle your personal information in accordance with a set of national principles, known as the Australian Privacy Principles (APPs), which regulate the collection, use, correction, disclosure and transfer of personal information about individuals by organisations like us in the private sector.

1.2 Policy statement

The Policy explains our policies and practices with respect to the collection, use and management of your personal information and our approach to the APPs.

1.3 Scope and application

This Policy applies to IOOF Holdings Ltd and its controlled entities, which comprises APRA Regulated Entities, Responsible Entities, Australian Financial Services Licensees and all Australian business divisions (collectively referred to as "IOOF" in this Policy). Where an entity specifically adopts this Policy (for example an ASIC or APRA-regulated entity), references to IOOF are taken to be a reference to that entity. This Policy applies to IOOF's business activities carried on in Australia. In the event of any inconsistencies between the Policy requirements and IOOF's statutory duties under Australian law, the latter shall prevail.

2 Definitions and key concepts

Australian law	means an Act of the Commonwealth or of a State or Territory or regulations, or any other instrument, made under such an Act.
Australian Privacy Principle or **APP**	means the Australian Privacy Principles set out in Schedule 1 of the Privacy Act.
Breach	means an act or practice which is contrary to or inconsistent with the Privacy Act, including an APP.
Collect	means to collect personal information, usually for inclusion in a record.
Consent	means express consent or implied consent.
GDPR	means the General Data Protection Regulation (EU) 2016/679.
Health information	means personal information about the health of an individual, an individual's expressed wishes about the future provision of health services to the individual, or a health service to be provided to an individual.
Holds	means possession or control of a record that contains personal information.

Individual	means a natural person.
Know Your Customer or **KYC**	means the process of verifying a customer's identity (as required by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)) by using reliable and independent documents and information.
Notifiable Data Breaches Scheme	means the scheme under Part IIIC of the Privacy Act which requires that, in the event personal information is involved in a data breach that is likely to result in serious harm, we must notify each affected individual and the Australian Information Commissioner.
Overseas recipient	means a person who receives personal information who is not in Australia or an external Territory, not us or a subsidiary or associate of us, and not the individual to whom the personal information relates.
Personal information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Policy	means this Privacy Policy.
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Officer	means the IOOF privacy officer, responsible for managing the business impacts of privacy laws and policies across the IOOF group of companies. Refer to section 5 of this Policy for contact details.
Reasonable Steps	means the actions or efforts we undertake to comply with the Privacy Act and the APPs, which must be objectively reasonable in the circumstances.
Sensitive information	means personal information about an individual's: ◆ racial or ethnic origin ◆ political, philosophical or religious beliefs or opinions ◆ memberships or affiliations ◆ sexual preferences or practices ◆ criminal record ◆ health or genetic information ◆ biometric information.
Solicit	means to request personal information, or anything that includes personal information, from someone other than the individual.
Tax file number or **TFN**	means a tax file number as defined in Part VA of the *Income Tax Assessment Act 1936* (Cth).
Use	means to handle, manage, or undertake an activity with personal information in our effective control.

3 General obligations

3.1 Collection

3.1.1 What information do we collect?

We will collect and hold your personal information for the purposes of:

- providing advice, products and services to you
- managing and administering your products and services
- verifying your identity
- letting you know about our other products and services.

The type of information collected from you includes information that is necessary to operate your account or for us to provide advice to you. We may ask you to provide personal information such as your:

- name
- e-mail address
- residential and/or postal address
- date of birth
- telephone number
- occupation
- bank account details
- financial details
- employer
- tax file number (TFN)
- preferences and interests

This information is primarily collected from application forms you have completed, your use of our online facilities, or through ongoing communications with you or persons you authorise to communicate with us on your behalf.

There are specific circumstances in which we will ask for your consent to provide sensitive information such as:

- Health Information when you apply for insurance or from medical practitioners when you make a claim
- income information from employers when you apply for additional insurance protection or salary continuance insurance
- details of your dependents, as defined at section 10 of the *Superannuation Industry (Supervision) Act 1993* (Cth), to pay benefits in the event of your death.

We will inform you of any legal requirements for us to request information about you and the consequences of not providing that information. For example, in addition to the personal information we will obtain from you, whenever you acquire a new product or service from us, we will require documents evidencing your identity. Such evidence may include a certified copy of your driver's licence, passport or birth certificate. If you do not provide identity documentation, we may not be able to action your request.

We will solicit personal information about you where you have knowingly provided that information to us, we believe you have authorised a third party to provide that information to us, or we are obligated or authorised by law to obtain such information. Third parties that we may need to collect information from include your financial adviser, product issuer, employer, accountant or solicitor. To verify your identity for Know Your Customer (KYC) purposes, we may also solicit personal information about you from reliable identity verification service providers.

In order to identify opportunities to improve our products and services and to enhance your customer experience with us, we may also collect data from third parties. Prior to engaging any third party, a thorough due diligence process is undertaken to ensure your personal information is fully protected. This includes ensuring that sufficient security measures and relevant confidentiality and contractual arrangements are in place which, at a minimum, require the third party to handle personal information in strict accordance with our requirements under Australian privacy law.

3.1.2 What if you do not give us the information we request?

You are not obligated to give us the information that we request. However, if you do not give us the information that we ask for, or the information you give is not complete or accurate, this may:

- prevent or delay the processing of your application or claim
- affect your eligibility for specified insurance cover
- preclude us from providing you financial advice
- prevent us from contacting you about your product or services
- impact the taxation treatment of your account.

For example, we are required to ask for your TFN when you become a member of one of our superannuation products. If you choose to not give us your TFN, you may be subject to higher tax charges on your superannuation, we may not be able to locate different accounts in your name, and we may not be able to accept personal contributions.

3.2 Use of information

3.2.1 How do we use the information that we collect?

We use your personal information for the purpose for which it has been obtained and for related purposes. For example, we collect your personal information so that we are able to:

- provide financial advice to you
- establish and manage your investments and accounts
- implement your investment instructions
- establish and maintain insurance protection
- process contributions, transfer monies or pay benefits
- report the investment performance of your account
- keep you up to date on other products and services that may be of interest to you
- improve the operation of our business and enhance the delivery of our products and services.

3.3 Disclosure

3.3.1 Who do we give your information to?

For the purpose of providing the services you have requested to you (or an authorised related purpose), we may provide your information to other companies within the IOOF Group or external parties. Where personal information is disclosed, we have strict controls in place to ensure information is held, used and disclosed in accordance with the APPs.

The types of external organisations to which we may disclose your personal information include:

- organisations involved in providing, managing or administering our products or services such as actuaries, custodians, external dispute resolution services, insurers, investment managers, product issuers, alliance partners or mail houses
- your financial adviser or other advisers appointed by you
- your employer (only if you have an employer sponsored superannuation arrangement)
- funds (administrators or trustees) to which your benefit is to be transferred or rolled over
- medical practitioners and other relevant professionals, where you have applied for insurance cover or made a claim for disablement benefit
- your personal representative, or other persons who may be entitled to receive your death benefit, or a person contacted to assist us to process that benefit
- financial institutions that hold accounts for you
- professional advisers appointed by us
- third party services, to enable us to deliver better products and services to you
- businesses that have referred you to us.

Like other financial services companies, there are situations where we may also disclose your personal information where it is:

- required by law (such as to the Australian Taxation Office or pursuant to a court order)
- authorised by law (such as where we are obliged to disclose information in the public interest or to protect our interests)
- necessary to discharge obligations (such as for enforcement activities of regulatory bodies or to foreign governments for the purposes of foreign taxation)
- required to assist in law enforcement (such as to a police force).

We may also disclose your information if you give your consent.

3.3.2 Will my information be disclosed overseas?

It is generally unlikely that we will disclose your personal information overseas. However, we may occasionally use third-party service providers or offshore outsourcing services to provide services to you. Depending on the circumstances, the relevant countries will vary such that it is not practicable to list them here.

Any overseas disclosure does not affect our commitment to safeguarding your personal information and we will take reasonable steps to ensure any overseas recipient complies with the APPs.

Where it is likely that we will transfer your personal information overseas, we will either seek your consent or inform you and ensure that appropriate contractual measures are in place requiring the overseas entity to protect your personal information in accordance with our obligations under Australian privacy law.

3.4 Access and correction of information

3.3.1 Can I access my information and what if it is incorrect?

You may request access to the personal information we hold about you. We may charge a reasonable fee to cover our costs.

There may be circumstances where we are unable to give you access to the information that you have requested. If this is the case, we will inform you and explain the reasons why.

We will take reasonable steps to ensure that the personal information we collect, hold, use or disclose is accurate, complete, up to date, relevant and not misleading.

You have a right to ask us to correct any information we hold about you if you believe it is inaccurate, incomplete, out of date, irrelevant or is misleading. If we do not agree with the corrections you have supplied and refuse to correct the personal information, we will give you a written notice to that effect.

If you wish to access or correct your personal information, you may contact us through our offices or by writing to the Privacy Officer, whose contact details are set out in section 5.

3.5 Protection of personal and sensitive information that we hold

3.5.1 How do we protect the security of your information?

We have security systems, practices and procedures in place to safeguard your privacy. We may use cloud storage or third-party servers to store the personal information we hold about you. These services are subject to regular audit and the people who handle your personal information have the training, knowledge, skills and commitment to protect it from unauthorised access, disclosure or misuse.

If you use the secure adviser or client sections of our websites, we will verify your identity by your username and password. Once verified, you will have access to secured content. You are responsible for maintaining the secrecy of your login details.

3.5.2 Risks of using the internet

You should note that there are inherent security risks in transmitting information through the internet. You should assess these potential risks when deciding whether to use our online services. If you do not wish to transmit information through our website, there are other ways in which you can provide this information to us. You can, for example, contact our ClientFirst team. Refer to section 5 for ClientFirst's contact details.

3.5.3 Cookies

A “cookie” is a small text file that may be placed on a computer by a web server. Our websites may use cookies, Google Analytics and/or other analytics tools which may enable us to identify you, your browser or other information about you while you are using our site. These cookies may be permanently stored on a computer or are temporary session cookies. They are used for a variety of purposes, including security and personalisation of services. They are frequently used on websites and you can choose if and how a cookie will be accepted by configuring your preferences and options in your browser.

All browsers allow you to be notified when you receive a cookie and you may elect to either accept it or not. If you wish not to accept a cookie, this may impact the effectiveness of the website. Your internet service provider or other IT service provider should be able to assist you with setting your preferences.

3.6 Retention of your personal information

We are required by law to retain certain records of information for varying lengths of time and, in certain circumstances, permanently. Where your personal information is not required to be retained under law and is no longer required for the purpose for which it was collected, we will take reasonable steps to irrevocably destroy or de-identify it.

4 European Union General Data Protection Regulation (GDPR)

If you reside in a country that is a member of the European Economic Area (the EU and Norway, Lichtenstein and Iceland), in addition to the protection you receive under the Privacy Act, you are entitled to other protections provided by the GDPR, including, in certain circumstances, the right to:

- have your personal information erased
- access your personal information in an electronic and portable format
- restrict or object to the processing of your personal information.

5 Roles and Responsibilities

The IOOF Holdings Ltd Board is ultimately responsible for overseeing the Policy.

The Privacy Officer is responsible for updating this Policy and for managing the business impacts of privacy laws across the IOOF group of companies.

5.1 Contacting the Privacy Officer or ClientFirst

You can contact the Privacy Officer by:

mail:

Privacy Officer
IOOF
GPO Box 264
Melbourne VIC 3001

or by email: Privacy.Officer@ioof.com.au

You can contact the ClientFirst team by telephoning 1800 913 118

5.2 Complaints and breaches

If you believe that we have breached the APPs by mishandling your information, you may lodge a written complaint addressed to the Privacy Officer, whose contact details are set out in section 5.

The Privacy Officer will respond to your complaint within 30 days of its receipt.

In the event that the Privacy Officer is unable to resolve your complaint, you may lodge a Privacy Complaint with the Australian Information Commissioner. For more information, please visit the Australian Information Commissioner's website .

If you have a complaint about a breach of the GDPR, you may contact the local regulator in your European Economic Area.

We are committed to helping you have control of your personal information and so it is our practice to take reasonable steps to notify you if we are aware that we have breached your privacy.

In accordance with the Notifiable Data Breaches Scheme, if your personal information is involved in a data breach that is likely to result in serious harm to you, we will notify you and the Australian Information Commissioner.

6 Policy governance

6.1 Review and approval

Unless required earlier, this Policy is reviewed and updated annually by the Privacy Officer.

Material amendments to this Policy must be approved by the IOOF Holdings Ltd Board. Non-material amendments to the Policy may be approved by the Chief Executive Officer.

The most current version of the Policy can be obtained from our website at www.ioof.com.au/privacy

6.2 Policy owner

Questions about this policy should be directed to the Privacy Officer or to our ClientFirst team. Refer to section 5 of this Policy for contact details.