LIFESTYLE ASSET MANAGEMENT

Privacy Policy

OUR COMMITMENT

Wealthy & Wise Lifestyle Planning Pty Limited ("WWLP") understands the importance of your privacy and is committed to protecting it. To honour our commitment, WWLP abides by the National Privacy Principles established under the Privacy Act 1988 (Cth), as amended

We believe that this statement will address any potential concerns you may have about how the personal information that you provide to WWLP is collected, held, used, corrected, disclosed and transferred. You may obtain more information on request about the way we manage your personal information by contacting us in one of the ways set out in the last section of this policy. A summary of the National Privacy Principles is available by contacting our office.

COLLECTION

As a financial planning organisation, we collect and hold personal information from our members and clients during the course of our activities. Our main purpose for collecting that personal information is to facilitate financial planning activities, insurance policies or related services. Furthermore, we are subject to certain legislative and regulatory requirements under the Corporations Law, and the Rules of Professional Conduct of the Financial Planning Association of Australia, which necessitate that we obtain and hold such information to ensure that appropriate advice, can be given. Our ability to provide comprehensive financial planning advice is dependent upon us obtaining accurate personal information.

Personal Information comprises information that allows you to be identified. It includes your name, age, gender, contact details and also the following details:

- financial needs and objectives;
- current financial circumstances, including your assets and liabilities (both actual and potential), income, expenditure, etc;
- investment preferences and aversion or tolerance to risk;
- employment history, employment circumstances;
- family structure, commitments and social security eligibility, and
- any other relevant information including medical history and/or reports.

WWLP will only collect, maintain and use personal information about you if it is necessary for us to adequately provide the services that you have requested. Circumstances in which this may be necessary include:

- preparation of a strategy document or a statement of advice;
- provision of financial planning advice;
- making securities and investment recommendations;
- reviewing your financial plan;
- reviewing securities and investment recommendations; and
- advising on and renewing risk insurance requirements.

Generally, collection of personal information will be collected in either face to face interviews, over the telephone or by way of a client data form. From time to time additional and/or updated personal information may be collected through one or more of those methods. Where reasonable and practicable, we will only collect personal information about you from you.

USE AND DISCLOSURE

We will not use or disclose personal information collected by us for any purpose other than:

(a) the purposes for which it was provided or secondary related purposes in circumstances where you would reasonably expect such use or disclosure; or

(b) where you have consented to such disclosure; or

(c) where the National Privacy Principles authorise use or disclosure in circumstances relating to public health and safety, and in connection with certain operations by or on behalf of an enforcement body; or

(d) where we are obliged pursuant to the Corporations Act, to maintain certain transaction records and make those records available for inspection by the Australian Securities and Investments Commission; or

(e) where we are required under the Rules of Professional Conduct of the Financial Planning Association of Australia, to make certain information available for inspection by the Association to ensure ongoing compliance with mandatory professional standards. This may involve the disclosure of your personal information.

(NOTE: It is a condition of our agreement with each of our representatives that they adopt and adhere to this privacy policy. You can be assured that any representative will maintain your personal information in accordance with this policy. If you have any concerns in this regard, you should contact us by any of the methods detailed at the end of this policy).

DATA QUALITY

We are required, pursuant to the Corporations Act 2001 and Rules of Professional Conduct of the Financial Planning Association of Australia, to collect sufficient information to ensure appropriate advice can by given in respect of recommendations made to our clients. If you elect not to provide us with the personal information, you may be exposed to higher risks in respect of the recommendations made to you and this may affect the adequacy or appropriateness of advice given to you.

DATA SECURITY

Your personal information is generally held in your client file. Information may also be held in a computer database. We will at all times seek to ensure that the personal information collected and held by us is protected from misuse, loss, unauthorised access, modification or disclosure. At all times your personal information is treated as confidential and any sensitive information is treated as highly confidential. Access to our premises is controlled, and after hours access is allowed only to personnel with authorisation to access the premises. All computer-based information is protected through the use of access passwords on each computer. Data is backed up each evening and stored securely.

In the event you cease to be a client of this organisation, any personal information which we hold about you will be maintained in secure storage for a period of 7 years, in accordance with legislative and professional requirements. After a period of 7 years, the information will be destroyed.

OPENNESS

We are committed to being open about how we use personal information. Where our documents ask for personal information, we will generally state the purposes for its use and to whom it may be disclosed.

ACCESS AND CORRECTION

You may request access to your personal information by contacting us by any of the methods detailed at the end of this policy. We will (subject to the following exception), provide you with access to that information by either providing you with copies of the information requested or providing you with an accurate summary of the information held. We will require you to provide evidence of your identity prior to providing access in accordance with this policy.

We will not provide you with access to your personal information if.

(f) Providing access would pose a serious threat to the life or the health of a person;

(g) Providing access would have an unreasonable impact on the privacy of others;

(h) The request for access is vexatious or frivolous;

(i) The information relating to existing or anticipated legal proceedings between us would not be discoverable in those proceedings;

(j) Providing access would reveal our intentions in relation to negotiations with you in such a way to prejudice those negotiations;

(k) Providing access would be unlawful;

(l) Denying access is required or authorised by or under law;

(m) Providing access would be likely to prejudice certain operations by or on behalf of an enforcement body or an enforcement body requests that information not be provided on the grounds of national security.

In the event we refuse you access to your personal information, we will provide you with an explanation for that refusal. We will endeavour to respond to any request for access within 14-30 days depending on the complexity of the information and/or the request. If your request is urgent please indicate this clearly.

We will endeavour to ensure that at all times, the personal information about you that we hold is up to date and accurate. In the event that you become aware, or believe, that any of the information that we hold about you is inaccurate, incomplete, or out dated, you may contact us by any of the methods detailed at the end of this policy and provide us with evidence of the inaccuracy or the incompleteness or out datedness. We will take all reasonable steps to correct the information if we agree that the information requires correcting.

IDENTIFIERS

We will not adopt as our own any identifiers that you may wish to provide to us such as Tax File Numbers, Medicare numbers etc. The *Anti-Money Laundering and Counter Terrorism Financing* Act 2006 requires that you may be "identified" before investing in a financial product. What this means is that you may be required to produce documentary evidence to confirm your identity. Your adviser will explain these requirements to you if and when appropriate.

PRIVACY COMPLAINTS

If you wish to complain about any breach or potential breach of this privacy policy or the National Privacy Principles, you should contact us by any of the methods detailed below and request that your complaint be directed to WWLP's Compliance Officer. Your complaint will be investigated and you will be issued with an acknowledgment of your complaint within 14 days of the receipt of your complaint.

It is our intention to use our best endeavours to resolve any complaint to your satisfaction. However, if you are unhappy with our response, you are entitled to contact the Office of the Privacy Commissioner on 1300 363 992 who may investigate your complaint further.

Should you have any queries or comments in relation to this Privacy Policy, please contact The Compliance Officer:

Lifestyle Asset Management Pty Ltd (ABN 58 113 067 968) 84 Nicholson Street NSW 2011 Tel: +612 9310 0888 Fax: +612 9310 0887 AFSL 288421

Australian Financial Services Licence 288421 www.wealthyandwise.com.au

Outline of amendments effective from 12 March 2014

Changes

In some ways, not a lot has changed. The APPs replace the Information Privacy Principles (IPPs), which previously applied to Commonwealth departments and agencies, and the National Privacy Principles (NPPs), which applied to certain private sector organisations. Many of the amendments are routine and simply allow for consistent terminology in the Act, with the removal of the IPPs/NPPs and the inclusion of the new APPs.
However, some changes are significant.
It is not practical to set out all the changes here, and businesses should seek advice where necessary. We include some of the major changes below.

Privacy Policy
APP1 introduces a prescriptive regime for a business' Privacy Policy in terms of content and availability. All Privacy Policies must comply with the new requirements for notification of certain matters about the personal information which is collected (APP 5).

This notification must occur at the time of the collection (either directly from the individual or from a third party) or as soon as reasonably practical after the collection. Agencies and businesses must take reasonable steps to implement processes that will ensure that they comply with the APPs.
Pseudonym
APP2 introduces a new requirement that a business must allow a person to use a pseudonym when dealing with the business (subject to limitations and practicality).

De-identifying information
APP4 creates new obligations on organisations to de-identify unsolicited information under some circumstances. Unsolicited information is personal information which a business has taken no active step to collect.
For the first time agencies and businesses will have to determine whether, if they had collected the information, they would have been permitted to do so under the Act, and whether APPs 5 to 13 apply to the information. If so, the information must be dealt with in accordance with the APPs and their Privacy Policy. If not, provided it is not a Commonwealth record and it would be lawful to do so, the agency or business must destroy or de-identify the information.
Notifying about off-shore disclosure
APP5 introduces the matters that must be notified to a person when personal information is collected. Amongst others, there is a new requirement for an agency or business to notify a person whether it is likely to disclose that person's personal information overseas, and if so, to which countries the disclosure will be likely to be made.
Direct Marketing
The use and disclosure of personal information for direct marketing is now addressed in a discrete privacy principle (rather than as an exception in NPP 2 as a secondary purpose). This is in recognition of the concern of the public for their privacy to be protected.
APP 7 prohibits direct marketing by businesses unless one of the exceptions apply (exceptions are set out in APP 7.2 to 7.5). The APPs do not apply to the extent the Do Not Call Register Act 2006 or Spam Act 2003 applies. Government agencies will generally be exempt from the prohibition against direct marketing unless it is in relation to an agency's commercial activities (s7A Act).
Cross-Border Disclosures
APP8 introduce a new accountability approach to cross-border disclosure of personal information (previously covered under NPP9).
Under APP8 and s16C of the Act, a business (including a small business operator that is governed by the Act) or agency that discloses personal information to an overseas recipient, including over the internet, may now be accountable for an act or practice of the overseas recipient that would breach the APPs (s16C Act), subject to some exceptions.

That is, if the overseas recipient is not otherwise subject to the APPs, and handles the personal information it receives from the business in a manner that breaches the APPs, the Australian business supplying the information will be taken to have breached the APPs unless an exception applies. An overseas recipient does not include an overseas office of the entity, but it does include a related company or entity in a corporate group.
While there are a number of exceptions to, and ways to indemnify the business against liability, the most practical way to avoid breaching APP8 is to notify the individual that their information will be disclosed overseas (APP 5), and obtain the consent of the individual to the overseas transfer of the information, and to the consequences of such consent.
Security
APP11 provides that agencies and businesses must take reasonable step to protect the information they hold from misuse, interference and loss, unauthorised access, modification and disclosure. This includes a new obligation to ensure that personal information cannot be 'interfered with'.
Extra Territorial application (s5 and 6)
The Privacy Act has always applied extraterritorially to an act or practice engaged in outside Australia by a business or small business operator to which the Act applies with an 'organisational link' to Australia. This principal has not changed, although the government has amended the extraterritorial provisions of the Act (ss5 and 6) by introducing the new term: 'Australian Link'.
Foreign Websites
A business that has an online presence in Australia, and collects personal information from individuals located in Australia, carries on a business in Australia (has an Australian Link) for the purpose of s5B(3)(b)(c) of the Act. It does not matter if the website is owned by a business that is located outside Australia or if the business is not incorporated in Australia.

The Act and the APPs will apply to collection, use and disclosure of the information (unless the act or practice is required by an applicable foreign law (see ss 6A and 6B Act)).

Credit Reporting

Part IIIA of the Privacy Act (Credit Reporting) has been completely revised. Some of the changes include:

New types of credit-related personal information that can be collected and held in the credit reporting system, including repayment history

Greater protection for consumers to access and correct credit-related personal information held by credit reporting bodies and credit providers

New requirements relating to charging, notification and timeframes for providing individual's with access or correcting information

Positive obligation on credit reporting agencies and credit providers to substantiate the correctness of the personal information held

The provisions in Part II make it clear whether the obligations in Part IIIA replace relevant APPs or apply in addition to APPS.

Enhanced Powers

The Australian Information Commissioner will have enhanced powers to investigate an interference with an individual's privacy and will now have the ability to:

accept enforceable undertakings

seek civil penalties in the case of serious or repeated breaches of an individual's privacy

conduct an audit/ assessment of the performance for both Commonwealth government agencies and businesses.

A serious or repeated breach of the Act will allow the Commissioner to make a determination and apply to the Federal Court to enforce the determination. Civil penalties of up to $1.7million for a corporation, $340,000 for an individual (2000 penalty units) may be sought.