MEX Exchange

PRIVACY & INFORMATION MANAGEMENT POLICY

MEX AUSTRALIA PTY LTD | ACN 155 084 058 | AFSL 416279
VERSION 1 | 29 DECEMBER 2020

Introduction

When you collect **personal information** from your client or potential client, you need to comply with the privacy laws. Personal information is any information or an opinion about a person which is reasonably capable of identifying them and includes (for example) information relating to your client's financial, taxation, health, employment and estate planning matters.

Note that information can be personal information whether or not it is recorded in a material form. An opinion or information about a person can be personal information even if it is not true.

Develop and implement a Privacy Policy

You must have adopted, and posted on your website, a clearly expressed and up-to-date policy about how you manage personal information you collect, hold, use and disclose. This policy must include information about:

- the **kinds** of personal information that you collect and hold as an entity, and **how** you collect and hold it;
- the **purposes** for which you collect, hold, use and disclose personal information;
- how an individual can **access** the personal information about them that you hold, and if necessary, seek to have that information corrected;
- how we secure our clients' personal information, and ensure that it is protected from misuse, interference, or unauthorised access, modification or disclosure;
- how an individual can **complain** about a breach of the Australian Privacy Principles;
- whether you are likely to disclose personal information to **overseas recipients**, and ,if so, the countries in which those recipients are likely to be located; and
- whether you are required to comply with the EU General Data Protection Regulations (GDPR), and, if yes, the way in which you comply with those obligations.

Give the client a privacy statement

Before collecting personal information from a new client, you must give them a privacy statement. This is a document which summarises your privacy obligations and sets out key information about who is collecting personal information about them, why it is being collected, who it may be disclosed to (including MEX) and how their personal information will be handled. The statement will also refer the client to the privacy policy posted on your website. Typically, **this statement will be included in your FSG (**although it can be given separately) **and acknowledged in your client application processes**.

Only collect relevant client information

You must only collect the type of personal information about your clients which is described and included in your Privacy Policy.

You must not collect personal information about a client from a third party unless it is unreasonable or impractical to collect it directly from the client.

When gathering information about a client, the information must be relevant for your purpose of providing financial planning services, as well as your obligation to comply with requirements imposed by law. For instance, questions about a client's job and income are directly relevant to their financial position, whereas in most circumstances, their religion or ethnic background is irrelevant. Details about religion, ethnic background, political beliefs, criminal record, trade union membership, and sexual orientation are all types of sensitive information for the purposes of the privacy legislation, and heightened obligations apply to the management of sensitive information. This is another reason to avoid collecting this information in the first instance.

Health information is also sensitive information, and this is discussed further below.

Using and disclosing your client's information

You must only collect, hold, use and disclose personal information for the purposes disclosed in your Privacy Policy.

Generally, this will be for the purpose of providing the financial products and services requested by your client. If you disclose a client's personal information for a secondary purpose, then subject to some limited exceptions, that purpose must be related to the primary purpose **and** one that the client would **reasonably expect**. Disclosure of sensitive information for a secondary purpose must be **directly** related to the primary purpose for which it was provided. Sensitive information includes disclosure of information about mental or physical health, or genetic or biometric data, which may have been collected for advice on insurance cover.

For example: it may be necessary for you to disclose some of a client's health information to an external compliance auditor for the purpose of auditing the quality of the advice you provided to them. This is allowed. However, if you disclosed your client's health information to a marketing company which wanted to sell the client medical equipment, this would breach the privacy legislation.

Use or disclosure of client personal information for **direct marketing purposes** is not permitted, unless either **express consent** has been obtained (e.g. at the time of client onboarding) or the person would reasonably expect their personal information to be used or disclosed for this purpose.

It is **not** sufficient to assume that the client would reasonably expect to receive the marketing material because of the client's profession, interest or hobby. The Australian Information Commissioner's view is that a person is not likely to have a reasonable expectation that their personal information will be used or disclosed for direct marketing purposes if the person has been notified that their personal information will only be used for a particular purpose unrelated to this.

If you wish to use your clients' personal information for the purpose of direct marketing, you should add a consent to direct marketing in your standard fact finder, and always provide a means by which a client may request not to receive direct marketing communications (also known as "opting out"), and comply with that request. This means that you must have a policy in place to track which clients do not want to receive direct marketing, and if a client has opted out of receiving direct marketing communications, you must ensure that they do not in fact receive direct marketing materials.

You may disclose a client's personal information for a purpose unrelated to providing financial advice if you have obtained your **client's written consent** to the disclosure.

Disclosing client's information to a third party (e.g. accountant)

When you disclose **personal information** of a client to a third party (e.g. accountant or lawyer), you should ensure that the third-party recipient signs a privacy agreement or acknowledgement whereby they agree to treat the personal information in accordance with the obligations set out in the privacy laws.

Keep information up to date

You must ensure that client files are regularly checked, and the client's information is kept accurate and up-to-date. You should build this policy into your regular review with clients.

Compliance tip: If you use any standard form checklists in your annual review, ensure that they include a check that the client's contact, financial and medical records (if applicable) have not changed.

Keep information secure

Ensure that your client's file is stored in a secure location which adequately protects it from misuse or loss. Hard copy filing systems should be under lock and key, and all electronic files should be password protected, with security software installed and regular back-ups taken. Client files should not be left lying around on desks or taken home, and access should only be available to appropriate persons.

Where some or all of your employees are working remotely, and are accessing clients' personal information, ensure that the employees' devices have the necessary security updates installed, and can only access your computer system via a secure remote desktop application. You should also consider whether to implement multifactor authentication procedures for remote access to systems and resources.

You also need to make sure you shred or use secure paper disposal services for hard copy documents, and have information destruction processes in place to securely dispose of electronic files.

Allow client access to their file

The law requires you to provide your client with access to their file upon receiving a reasonable request. The client also has a right to correct the personal information in their file. The exception to this rule is where the information is relevant to current or anticipated legal proceedings or a criminal investigation.

You must respond to the client's request "within a reasonable period after the request is made". In responding, you must either give access to the personal information that is requested, or notify the individual of your refusal to give access. Factors that may be relevant in deciding what is a reasonable period include the scope and clarity of a request, whether the information can be readily located and assembled, and whether consultation with the individual or other parties is required. However, as a general guide, a reasonable period should not exceed 30 calendar days.

You may have grounds to refuse an access request in some limited circumstances, including where giving access to personal information would:

- unreasonably impact on the privacy of other individuals;
- be reasonably likely to pose a serious threat to the life, health or safety of any individual (or more broadly);
- be relevant to a legal dispute you are having, or may have, with the person making the request; or
- amount to a breach of any relevant law.

Before responding to a request for access, you should seek further guidance from the compliance team in these situations.

Transferring Information Overseas

Your Privacy Policy must set out if you are likely to disclose client personal information to overseas recipients (including IT service providers if your website is hosted overseas, or you use cloud-based or web-based data storage, software or applications), and the countries where the personal information is likely to be sent.

If, for whatever reason, you need to transfer a client's personal information outside of Australia (including because your website is hosted overseas, or you store information on a cloud-based or web-based server located overseas, or you use web-based software or applications that are hosted overseas), and the privacy laws equivalent to the *Privacy Act 1988* do not apply, you must take reasonable steps to ensure that the overseas recipient complies with the Australian Privacy Principles (i.e. by including this obligation in your contractual arrangements). The compliance team can help you with this.

Treat tax file numbers with care

The **Privacy (Tax File Number) Rule 2015** (TFN Rule) regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act.

If a client file includes a **tax file number** (TFN), then the file must also include a **written authority** from the client for you to use the TFN.

You must explain the **legal basis** and **intended purpose** for collecting the client's tax file number (for example, collecting the TFN as required under taxation legislation in order to provide the client with professional services connected with that legislation). You must also make the client aware that declining to provide it is not an offence, as well as the consequences of not quoting the TFN.

Where an **accountancy practice is** operated in conjunction with your financial planning business and a client is referred to you from the accountancy side, then **a new authorisation** from the client for the TFN **must be obtained**. This is because the tax file number is now required for a different and separate purpose.

You are required to ensure that the TFN is protected by security safeguards to prevent unauthorised access, use or disclosure.

If you no longer require TFN information, you must not continue to hold it and must destroy it securely.

For example: if you collect TFN information from a client for the purpose of reporting that information to the Australian Tax Office, then after that report is made, the relevant TFN information must not be retained. One way of achieving this is to "black out" the TFN data in the relevant documents on file.

Unauthorised use or disclosure of a tax file number is an offence which carries significant penalties.

Addressing a suspected or known data breach

A **data breach** occurs when **personal information** is accessed or disclosed in an unauthorised way, or is lost.

A **data breach** could occur in a number of ways. Some examples include:

- a mobile phone, laptop or removable storage device containing personal information is lost or stolen;
- sending an email containing personal information to the wrong recipient;
- accessing or disclosing personal information outside the requirements or authorisation of their employment;
- databases or an email account containing personal information are "hacked" into or otherwise illegally accessed by an individual;
- a client file is lost or stolen;
- paper records are stolen from insecure recycling or garbage bins.

Data breaches can give rise to a range of actual or potential harms to individuals and entities.

There are data breach reporting obligations that apply to any organisation covered by the privacy legislation (which may include an individual who is an authorised representative, or a corporate authorised representative). If you suspect or know that a data breach has arisen, you must contact the compliance team immediately. You may also wish to visit the website of the OAIC to consult resources on dealing with a data breach, or seek professional advice.

Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

The actions taken following a data breach should generally follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach and evaluate the potential harm to affected individuals and, where possible, take action to remediate any risk of harm.

Step 3: Notify individuals and the OAIC if required. If the breach is an "eligible data breach", such notification may be mandatory.

Step 4: Review the incident and consider what steps can be taken to prevent future breaches.

If remedial action is successful in preventing a likely risk of serious harm to individuals, the notification obligations may not apply.

An **eligible data breach** occurs when each of the following **three criteria** are satisfied:

a) there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;

b) this is likely to result in **serious harm** to one or more individuals; and

c) the entity has not been able to prevent the likely risk of serious harm with remedial action.

"**Serious harm"** is not defined in the legislation. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

You should take into account the following (non-exhaustive) list of "relevant matters" in assessing the likelihood of serious harm:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be compromised
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security, technology or methodology:
    - was used in relation to the information, and;
    - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
    - have obtained, or who could obtain, the information;
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates; and
    - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters