Regulation and risk collide

Managing information as an AFS licensee

Samantha Hills

With the recent spate of data breaches now extending to the financial services industry, Australian financial services licensees are racing to ensure that their information management procedures are up to scratch, fearing that they may be the next business to hit the headlines.

Information management: What do we mean?

Information management in 2023 comes under a swathe of different names. Some people refer to 'document', 'data' or 'records', rather than 'information'. Some policies focus on 'retention' and others on 'destruction'.

We recommend considering information broadly, so that your measures cover information in multiple forms, and so that they cover both personal information, as it is understood under the *Privacy Act 1988* (Privacy Act), and confidential information, which takes into account information which is confidential by virtue of the commercial relationship between the licensee and third parties or by virtue of other circumstances.

Competing considerations

The challenge for information management in 2023 is the collision of a number of regulatory and risk management considerations. Historically, the approach of a prudent licensee was often to collect information even if it was not necessarily required and to retain it for lengthy periods of time. Now, cyber and data breaches have ramifications under the Privacy Act, which contains significant penalties for data breaches and requirements to notify clients and the Office of the Australian Information Commissioner in the event of a notifiable data breach. These breaches also have ramifications under the *Corporations Act 2001* (Corporations Act), after the Federal Court, in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496, found that a licensee with inadequate cyber risk management measures in place had breached its obligations to have adequate risk management systems under section 912A of the Corporations Act.

These ramifications have to be weighed against the forces impelling a licensee to collect and keep information. These forces stem from business necessity, such as the need to collect information about a client so that advice can be given or an investment opened in their name, and regulatory requirements such as those under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and the Corporations Act. Both regulatory regimes require the collection of information for various purposes and the retention of that information for set periods of time.

Factor in other considerations which promote or mandate the retention of documents such as:

- Is there a complaint on foot in relation to which the information is relevant?
- Is the information reasonably likely to be required as evidence in a legal proceeding?

- How long does the licensee wish to retain documents to help protect it against the risk of litigation?

Information relating to representatives and third parties

When preparing our template Information Management Policy, we found that information collected by a licensee, and which is susceptible to data breaches typically falls into two buckets: information relating to representatives—including employees—and information relating to third parties with which the licensee interacts. This, of course, includes information relating to clients.

Phases of information management

The management of information may be divided into four distinct phases: collect, secure, retain and destroy.

Collect

When deciding what personal information to collect, consider the Australian Privacy Principles (APPs). APP 3 states that an entity "must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities". There are additional requirements for sensitive information. This will be a relevant consideration, for example, for licensees which collect information from individuals for advice or underwriting purposes in a life insurance context.

From a risk management perspective, it is sensible to adopt a similar approach to considering what information to collect in relation to a client which is not an individual, such as the trustee of a self-managed super fund or a family trust. That is, what information is reasonably necessary for one or more of the entity's functions or activities?

Do not be tempted to equate retail and wholesale client criteria with whether information is personal or not; these are entirely separate concepts. Personal information relates to an individual, regardless of whether they are a wholesale or retail client.

Whether or not information relates to an individual, it could well be confidential. Information will be confidential if it is given in circumstances of confidence or if it is confidential in nature, for example, you overhear someone talking about a sensitive family matter, whether or not it is specifically stated to be confidential.

For both personal and confidential information, think about what it is necessary to collect for the running of the business, from both a practical and a regulatory perspective.

From a regulatory perspective, the AML/CTF Act (if applicable) and the Corporations Act require licensees to collect (or record) a range of information in relation to clients. The former requires you to collect information in order to properly identify a client. The latter requires you to collect information for a range of purposes related to clients, such as to satisfy best interests obligations when providing personal advice to retail clients or when a complaint is made in relation to the licensee's financial products or services[1].

Both regimes also contain requirements that compel a licensee to collect information in relation to future potential, or actual, representatives. This includes employees. For licensees with an AML/CTF Program Part A, measures for employee screening will need to be in place. Under the Corporations Act, licensees have obligations such as obtaining references and compliance information from former authorising licensees of a prospective financial adviser intending to service retail clients.

Secure

A number of regimes set out security requirements for information held by licensees. These are not technical requirements from an IT perspective but, rather, principles-based regulatory requirements. For example, APP 11.1 requires an entity holding personal information to "take such steps as are reasonable in the circumstances to protect the information:

1. from misuse, interference and loss; and
2. from unauthorised access, modification or disclosure."

The Privacy (Tax File Number) Rule 2015 sets out special requirements for protecting tax file number information. These requirements include restricting access to the information.

The whistleblower protections under the Corporations Act prohibit disclosure of information relating to the identity of a whistleblower[2].

Many contractual relationships with third parties will impose obligations, either via express or implied terms, to keep information confidential. It is also possible for a party to bring an action in court for 'breach of confidence', where it imparts to another party information on the understanding that the communication is for a restricted purpose and the recipient of the information discloses it without consent.

Retain

A licensee needs to determine for how long it should keep particular types of information. Minimum recordkeeping requirements are set by the same regulatory regimes which require the licensee to collect information and keep records in the first place. *The Attorney-General's Department Privacy Act Review Report 2022* included a recommendation that the Commonwealth:

"undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information".

For example, under the AML/CTF Act, if a reporting entity makes records of the customer identification procedure, or information obtained in the course of carrying out the procedure, in respect of a particular customer, the record—or a copy of it—needs to be kept for seven years after the entity stops providing designated services to the

The quote

Personal information relates to an individual, regardless of whether they are a wholesale or retail client.

Samantha Hills, Holley Nethercote

Samantha is a partner at Holley Nethercote, working primarily in financial services law. Her expertise includes providing legal advice, chairing compliance committee meetings, conducting licensee compliance audits and facilitating training sessions for a range of financial services clients. Samantha holds a Bachelor of Arts with Honours and a Bachelor of Laws with Honours.

client[3]. For personal advice given to retail clients, Australian Securities and Investments Commission (ASIC) Class Order (CO 14/923), made under the Corporations Act, requires the licensee to keep records of the information relied on to demonstrate compliance with the best interests obligations. These records must be kept for seven years after the day the personal advice was provided to the client.

Once these minimum timeframes have elapsed, there are other issues to consider. APP 11.2 requires an entity to de-identify and destroy information once the entity no longer requires it for any purpose for which the information may be used or disclosed under the APPs.

Even if statutory retention periods have been met, the licensee should not destroy information if it relates to an existing complaint. And there are explicit obligations not to destroy information that may be used as evidence in legal proceedings[4].

Plus, the licensee needs to consider litigation risk. Statutes of limitations in the various States provide a defence to actions brought after the expiry of the limitations period. For example, in contract law or negligence, or for civil remedies under the Corporations Act, this period is six years after the cause of action arises[5]. For breach of contract, any alleged breach will generally occur while the relationship with a client—or other party—is on foot. For actions in negligence, the cause of action arises when the loss occurs. Consider the situation where a personal advice licensee gives advice to a client in 2023 to invest in a particular product, the product heads south in 2035, and the client sues the licensee in 2036. If the licensee has destroyed its records, it will struggle to defend itself in court.

This all needs to be weighed against the 'almost too hot to handle' issues of 2023: cyber security and privacy risk. As noted earlier in this article, data breaches have repercussions under the privacy regime and could also lead to an allegation by ASIC that the licensee does not have adequate risk management systems in place. The more information you collect and the longer you keep it, the more you increase these risks.

Destroy

This leads us to the final step in the life cycle of information: destroy. There is no magic here. Once you have decided on the period for which you will keep particular information, taking into account the considerations above, when the period has elapsed in relation to that information, you need to destroy it. We recommend creating a schedule that guides you on what can be destroyed when. You should build document destruction into your regular processes. It might occur daily in a large business with sophisticated systems and, perhaps, six monthly, in a small business where systems are simpler. But make sure you destroy information when your schedule says you will.

Effective destruction, like information security, will involve the help of qualified IT experts. These experts are no longer a 'nice to have' for an AFS licensee but an essential part of your compliance framework. **FS**

Help is here

Holley Nethercote has released its template Information Management Policy and a template Document Destruction Schedule, for access by HN Hub subscribers and available for purchase by other licensees. The documents are intended to help licensees navigate the difficulties of collecting, securing, retaining and destroying information in an era when privacy and cyber security loom larger than ever before.

Meanwhile, to help you navigate the landscape of information management from a regulatory perspective, refer to our template Information Management Policy and template Document Destruction Schedule. For more tailored advice, contact us here at Holley Nethercote Lawyers. Our friendly team can help you make sense of the interlacing regulatory and legal considerations affecting management of information in 2023.

1: ASIC Regulatory Guide 271: Internal dispute resolution ("RG 271") enforceable paragraph RG 271.79

2: Section 1317AAE.

3: Section 113(2).

4: Consider, for example, the Crimes Act 1958 (Victoria) – sections 254 and 255.

5:Consider, for example, the Limitation of Actions Act 1958 (Victoria). Note that these statutes do not prevent a person from bringing an action. Rather, they provide a complete defence to the defendant if the action is brought. For example, depending on the circumstances, an insurance company may elect not to take the defence because of its duty of utmost good faith.