Privacy Act 2020 and the New Financial Advice Regime

There are many legislative changes taking place in the financial advice industry and it is important to understand how these relate. The aim of this paper is to provide an overview of the new Privacy Act and how its principles align with the new financial advice regime (the amendments introduced by the Financial Services Legislation Amendment Act 2019).

The focus of this paper is clients' information and how for financial advisers, as well as other professionals in the field, the new Privacy Act's provisions relate to client information.[1] Financial advice businesses and organisations need to have privacy compliance, which means clear systems for the collection and disclosure of this information. This paper discusses what we see as the most significant practical implications for adviser businesses. In particular:

- Have good data governance,
- Appoint a privacy officer, and
- Have a privacy breach response plan ready.

The Privacy Act 2020 replaces the 1993 Act and comes into force on the 1 December 2020. The new Act preserves many of the principles of the 1993 Act, as well as updates the legislation to reflect technological advances in the way businesses collect and store information. One of the main changes introduced by the new Act is the requirement to report serious privacy breaches.

In regards the financial industry, it is worth noting that other legislation that requires the use or collection of personal information takes precedence over the Privacy Act. For example, the FMC Act and the AML/CFT Act.[2]

Purpose for Collecting Clients' Information

The new Privacy Act requires businesses have a sound purpose for collecting a client's information. You need to clearly understand the purposes of collecting the information and the associated disclosure requirements.

The new Code of professional conduct for financial advice services (to come into force on the 15 March 2021) introduces the obligation of suitability of advice.[3] This, as well as new

[1] The Privacy Act covers all personal information collected or held by a New Zealand entity, or an overseas entity in the course of carrying on business in New Zealand (section 4).
[2]The Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
[3] Standard 3 Give financial advice that is suitable.

provisions introduced by the FMC Act[4] and FMC regulations, provides a clear basis as to why advisers collect client information. The Standards in the Code are consistent with the obligations under the Privacy Act. However, client information for financial advice purposes is broader than personal information under the Privacy Act.[5] It is defined as "all information about the client that is collected or held by a person who gives financial advice. That includes information in work papers and records, and the financial advice given to the client".[6]

Quantity of Information

There are significant costs and risks associated with holding information. Typically, costs and security risks increase with the quantity of information held, as well the potential for its abuse. As such, financial advisers need to carefully consider:

- Why the information is needed
- If there is there a lawful purpose for holding the information
- How the information will be used

Retention of Client Information

Another important issue is deciding how long is necessary to hold your client's information. A standard condition for financial advice provider (FAP) licensing is record keeping - FAPs need to maintain appropriate records for 7 years.[7] If after 7 years you no longer need to hold onto the information, you must get rid of it and have efficient information systems to do so. It is advisable that you should not keep the information for longer than needed and that businesses have appropriate policies in place to justify keeping it for longer. Standard 5 of the Code states that "Client information should be retained only for as long as it is required…When is no longer needed, the client information should be returned to the client or disposed of securely".

Protect Client Information

You will also need to ensure that your service providers are adequately securing and protecting information. In the new Privacy Act, businesses are responsible for information held by service providers, which includes cloud storage services.[8] This aligns with the new Code[9] as it sets out that "A person who gives financial advice must take reasonable steps to protect client information against loss and unauthorised access, use, modification, or

[4] Section 431L FSLAA.
[5] Commentary, Code Standard 5.
[6] Commentary, Code Standard 5.
[7] Standard Condition 1 (e) for full financial advice provider licenses.
[8] Privacy Act, section 11.
[9] Code Standard 5 Protect client information

disclosure".[10] In practice, this means that you need to ensure you have physical and electronic security measures in place.

For businesses that operate in a global context and share information with overseas companies, the new Privacy Act also requires you ensure that New Zealand privacy requirements are met. This is in line with GDPR rules in the EU and the way data protection regulations can apply worldwide. You will need to evaluate cross-border information flows of your business and ensure your client information is adequately protected.

Access to Information and Disclosure

Clients have the right to access personal information. The legislation provides for the Privacy Commissioner to issue an 'access direction' as well as fines up to $10,000 for a failure to comply. The record keeping condition of FAP's licenses also states that records need to be available for inspection and review by the FMA.

Privacy Breach Response Plan

One of the main changes introduced by the new Act is the requirement to report notifiable privacy breaches to the Privacy Commissioner[11], as well as notifying the individual affected or public generally.[12] A notifiable privacy breach is defined as a "breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so."[13]

In assessing whether to notify a breach, businesses must consider factors in section 113 of the Act. Generally, these include whether the information is sensitive in nature, and the action taken by the business to reduce harm.

It is advisable therefore, that adviser businesses and organisations have a privacy response plan ready. The response plan should cover the process for notification set out in section 117. This includes identifying the affected individuals, the steps taken to mitigate the breach and the details of a contact person within the business for inquiries.

Privacy Officer

The Privacy Act also sets out a general provision that all businesses and entities must appoint a privacy officer (within or outside the business).[14] The role of the officer would include:

- Development of privacy policies and procedures and provision of training to staff in their use;
- Assurance that compliance with privacy policies are met; and

[10] Code Standard 5 Protect client information
[11] Privacy Act, section 114.
[12] Privacy Act, section 115.
[13] Privacy Act, section 112.
[14] Privacy Act, section 201.

- Dealing with information requests and complaints.

Data Governance

Broadly, in view of the new Privacy Act, adviser businesses need to:

- Understand the type, purpose and duration of the information being collected within the business. This includes having clear record keeping and document destruction procedures.
- Have a privacy breach response plan.
- Appoint a privacy officer.
- If needed, update privacy statements, supplier, and client contracts.

Businesses need to have good data governance. This refers to the processes and systems for managing the availability, usability, integrity, and security of information in businesses and organisations. The introduction of new legislation provides advisers and firms with the opportunity to assess and evaluate their data standards, processes, and practices. Effective data governance can help you ensure that your client information is protected and that you meet your obligations under the Privacy Act and the new financial advice regime.

Not Legal Advice

This paper contains general information about the Privacy Act 2020 and the new financial advice regime. It is not intended as legal advice. The information is for guidance only and the authors accept no liability for claims arising directly or indirectly out of reliance placed on the information contained.