



Privacy Update: AML/CTF considerations and possible reforms

Most financial services providers would be aware of the requirements of the privacy legislation, and the 10 National Privacy Principles (“NPPs”) set out in the *Privacy Act 1988 (Cth)* (“the Privacy Act”).

Since 1988, the Privacy Act has provided privacy protection to individuals in their dealings with the public sector. In December 2001, new provisions were introduced that regulate the private sector. Thus, generally, organisations with an annual turnover of more than \$3 million must either comply with an approved privacy code or comply with the NPPs. (Organisations subject to AML/CTF obligations are also now bound by the NPPs. See below.)

The privacy legislation protects both:

- personal information, which is defined as information or an opinion about an individual whose identity is apparent from the information or opinion; and
- sensitive information in relation to racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal records and health information.

National Privacy Principles

Collection (NPP 1 and 10)

An organisation must only collect personal information that is necessary for its functions or activities, and only directly from the person if it is reasonable and practicable to do so. At the time that it collects personal information, or as soon as practicable afterwards, an organisation must make the person aware of:

- why it is collecting information about them;
- who else it might give it to.

An organisation must obtain the person’s consent before collecting sensitive information.

Use and disclosure (NPP2)

An organisation should only use or disclose personal information for the primary purpose of collection. If it is going to use personal information for a secondary purpose (e.g. marketing), an organisation must obtain the person’s consent. The use of non-sensitive personal information is allowed for direct marketing where, among other things, it is impracticable to seek the person’s consent and where the customer is told that they can opt out.

Data quality (NPP3)

An organisation must ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Data security (NPP4)

An organisation must protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. It must destroy or permanently de-identify personal information if it no longer needs it.

Openness (NPP5)

An organisation should put its privacy policy on its website. If a person asks, it should let them know what sort of personal information it holds, what purposes it holds it for and

how it collects, uses and discloses that information.

Access and correction (NPP6)

A person has a right of access to all the personal information that an organisation holds about them.

Identifiers (NPP7)

An organisation cannot collect a particular Commonwealth-government-assigned identifier (e.g. TFN) from all its customers and then use that identifier to organise and match other personal information.

Anonymity (NPP8)

An organisation must give a person the option of interacting anonymously with it if it is reasonably practicable to do so.

Trans-border data flows (NPP9)

An organisation must not disclose personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the person's consent.

Complaints handling

A person who thinks an organisation has interfered with his or her privacy can complain to the Privacy Commissioner. The Commissioner will give the organisation the opportunity to resolve the complaint directly. The Commissioner will conciliate the complaint using letters, phone calls and meetings. The Commissioner may make a formal determination. This determination can be enforced by the Federal Court.

AML/CTF obligations:

As noted above, organisations which "come under" the \$3 million turnover limit, are relieved from complying with the NPPs, unless they are also bound by the Anti Money Laundering and Counter Terrorism Financing legislation ("AML/CTF"). The AML/CTF legislation has amended the

Privacy Act, so that small businesses which are designated as "reporting entities" by the AML/CTF legislation will also be subject to the obligations of the Privacy Act.

As you may be aware, a reporting entity is a financial institution, or other person, who provides designated services. Designated services are described in detail in section 6 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* ("the AML/CTF Act"), and include services such as providing a service in the capacity of an Australian financial services licensee.

Part of a reporting entity's obligations include identifying individuals to whom it intends to provide services. Usually, this process will involve the collection and subsequent handling of individuals' personal information. Individuals will include ordinary customers, sole traders, partners, trustees and beneficiaries, executive officers and so on,

You should ensure that all personal information collected, used and disclosed by you is in accordance with the requirements of the Privacy Act. Also, your organisation should have in place a tailored Privacy Policy, which sets out the way that personal information is dealt with. We suggest that when information is collected for AML/CTF purposes, you should at all times be aware of your obligations under the Privacy Act.

Also, the amount of "Know Your Customer" information which is required to be collected and verified by reporting entities is significant, and could often include sensitive information. For example, an individual's place of birth may indicate a person's racial or ethnic origin. The Privacy Act requires organisations to handle sensitive information with a "higher degree" of care than personal information. NPP 10 only allows an organisation to collect sensitive information with the consent of the individual.

Considering the amount of information to be collected, used and disclosed by reporting entities, the Privacy Commissioner has suggested that there be a greater emphasis on privacy training within the AML/CTF program required by the AML/CTF legislation.

Reform of the Privacy Act:

In March 2009, the Federal Government announced a review of the scope of privacy law in Australia. The review was announced by Senator John Faulkner, Special Minister of State, at the Freedom of Speech Conference in Sydney on 24 March 2009.

The review has been, in part, prompted by the Australian Law Reform Commission's Review of Secrecy Laws – Issues Paper 34 *Submission to the Australian Law Reform Commission* February 2009. One of the proposed amendments is to consolidate in the Privacy Act, an individual's enforceable rights of access to and correction of their own personal information.

In its review, the Australian Law Reform Commission review made the following suggested changes to the privacy regime:

1. Increase the assessment and audit functions of the Privacy Commissioner.
2. Increase the Privacy Commissioner's discretion in relation to the investigation of individual privacy complaints.
3. Increase the Privacy Commissioner's powers to enforce remedies against organisations which breach the Privacy Act, for example, by imposing civil penalties and an undertakings regime, analogous to the powers of the Australian Competition and Consumer Commission.

The Australian Law Reform Commission also made a number of other

recommendations for changes to the Privacy Act, last year.

We will let you know when and in what form the proposed changes will become law, and how the changes will impact upon your businesses.

The law is current as at April 2009.

Please note that this paper is a summary of the law only and is not a substitute for legal advice. Holley Nethercote is able to assist companies in meeting their obligations in this area by providing practical and prompt legal advice. Licensing, training and creation of compliance programs are also available via an associated business, Compact- Compliance and Corporate Training – www.compliance-training.com.au.

We invite you to contact us:
Telephone: (03) 9670 8200
Facsimile: (03) 9670 5499
Email: law@holleynethercote.com.au
Web: www.holleynethercote.com.au