PiperAlderman

Article Information

Authors: Florian Ammer, Tom Griffith
Service: Corporate & Commercial, Privacy & Data Protection

How changes to the Privacy Act 1988 affect you

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 came into effect on 12 March 2014. It has brought about important changes to the Privacy Act 1988.

The *Privacy Act 1988* (**Act**) and the recent changes apply to businesses with an annual turnover of $3m or more, although there are some exceptions. Businesses should be aware of the changes and how they may affect their obligations in relation to privacy. Broadly, these changes include:

- a harmonisation of the Information Privacy Principles and National Privacy Principles, with the implementation of the new Australian Privacy Principles (APPs)
- a broadening of the definition of "personal information"
- greater responsibilities for destruction of information not required to be held by businesses
- a broad definition of "credit provider" which has the potential to cover many types of businesses
- new enforcement regimes, including the ability of the Information Commissioner to obtain enforceable undertakings from businesses who contravene the Act or the APPs
- an increase in the total aggregate penalties that apply to contraventions (up to $1.7m), and
- the introduction of a new Part IIIA that applies to credit reporting and credit providers.

Some of the key changes and their practical consequences are discussed below.

Personal Information – much more is now caught

Businesses should be aware that the changes include a broader definition of "personal information", being:

"information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- *whether the information or opinion is true or not; and*
- *whether the information or opinion is recorded in a material form or not"*

The key change is the absence of a requirement that an individual must be able to be identified from the information itself. Under the new definition, the individual must simply be able to be reasonably identifiable, whether from the information or by some other means.

This change broadens the reach of the Act and means that privacy obligations now apply to a greater amount of information held by businesses.

New Requirements for Privacy Policies

To comply with the changes and the new APPs, changes need to be made to the form and content of privacy policies. APP1 contains a list of matters that must be addressed in a privacy policy. They include:

- the kinds of personal information collected
- how personal information is collected, used and stored
- how an individual can seek access and correction to their personal information
- how an individual can make a complaint about a breach of the Act or the APPs, and
- whether or not personal information is likely to be disclosed to overseas recipients and if so, the countries in which they are likely to be located.

De-identification and destruction of personal information

The new APP4 and APP11 contain requirements to ensure that certain personal information no longer required to be held is either de-identified or destroyed. Information is de-identified
if the information is no longer about an identified individual. What this means for businesses is that they should implement a process to ensure compliance with these requirements. For example, such process should provide for:

- identifying the types of personal information collected
- determining whether such information is reasonably necessary to be held for one or more of the business's functions or activities, and
- de-identifying or destroying any personal information determined to be unnecessary to be held.

Depending on the nature and size of a business, these requirements can have a significant impact and may require comprehensive measures to be implemented to ensure compliance.

Part IIIA – Credit Reporting Bodies and Credit Providers

The introduction of the new Part IIIA creates additional obligations for credit reporting bodies and credit providers. The obligations relate to the collection, use and disclosure of credit information, which is defined in the Act.

Part IIIA also contains a new, broad definition of "credit provider". It extends to organisations which provide goods/services on terms allowing payment to occur more than 7 days after the goods/services are provided. A wide variety of businesses are likely to be caught by this definition.

Businesses should give consideration to whether they fall within the definition of "credit provider". If so, additional matters may need to be addressed. For example, credit providers who disclose certain credit information to credit reporting bodies (such as Dun & Bradstreet or Veda Advantage) must disclose the name and contact details of the credit reporting bodies to whom such information is disclosed.