New Privacy Laws

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 and Privacy Regulation 2013 both commenced on 12 March 2014. They represent the most significant changes in the legislation since it was first introduced in 1988. They introduce new requirements, for both privacy policies and associated procedures.

These requirements apply to Australian businesses having a turnover over $3m, as well as government agencies, health services providers and entities trading in personal information. Different requirements apply to:

- Personal Information – Information/opinions about an identified or reasonably identifiable individual, e.g. name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and references or other commentary.

- Sensitive Information – Health, genetic or biometric information about an individual or information/opinions about or implying an individual's 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 or criminal record.

The main changes are as follows:

1. OAIC powers – The powers of the Office of the Australian Information Commissioner ("OAIC") have been greatly expanded, with power to investigate privacy law breaches (following a complaint or on its own initiative), obtain enforceable undertakings and/or apply to the court for a civil penalty of up to $340,000 in the case of an individual or up to $1.7 million in the case of a company. A misconception seems to be arising, to the effect that substantial penalties will be common. Although the potential for substantial penalties should be taken seriously, the guidelines issued by the OAIC indicate that the OAIC will generally try to resolve privacy disputes by conciliation.

2. Credit reporting - a number of new restrictions and requirements have been imposed.

3. Privacy principles – The previous National Privacy Principles ("NPP") have been renamed the Australian Privacy Principles ("APP") and there are 13 new principles. The main requirements of the new principles are as follows:

    a) Privacy policy - An organisation must now have a written privacy policy. It must be readily available free of charge. It must contain a considerable amount of information which would not normally have been included in the past, e.g. the kinds of information collected, how it is collected, held, used or disclosed, the purpose for which it is collected, held, used or disclosed, how an individual may access it and seek

BANNERMANS LAWYERS
T: (02) 9929 0226 M: 0403 738 996 ABN: 61 649 876 437
E: dbannerman@bannermans.com.au W: www.bannermans.com.au
P: PO Box 514 NORTH SYDNEY NSW 2059 AUSTRALIA

correction, how an individual may complain and how the complaint will be dealt with and whether it is likely to be disclosed to overseas recipients and if so, which countries are involved.

b) Compliance program - An organisation must now have a compliance program. Most of the principles are framed so as to require a proactive approach. An organisation's privacy policy and associated procedures must be reviewed from time to time. The OAIC guidelines suggest that there should be at least annually.

c) Anonymity/Pseudonymity - An organisation must allow an individual to deal with the organisation anonymously or using a pseudonym, unless identification is required by law or it is impractical for the organisation to deal with persons who have not identified themselves.

d) Collection and use of solicited personal information - The requirements are slightly more restrictive, e.g. collection of sensitive information requires the consent of the relevant individual and collection of other personal information requires lawful and fair means and collection only from the relevant individual, where practical. However, some exemption categories have been introduced, including "Permitted General Situations", which include some action taken regarding safety, law enforcement or military activity or legal proceedings/dispute resolution.

e) Collection and use of unsolicited personal information - There is now provision for an organisation to action and possibly destroy or de-identify unsolicited personal information. The OAIC guidelines suggest that information provided in excess of what was requested should be treated as unsolicited.

f) Collection notices - An organisation must, at the time of collecting personal information, if practical and otherwise as soon as practical after collecting the information, take reasonable steps to notify the individual of specified matters or otherwise ensure that the relevant individual is aware of those matters. A misconception seems to be arising, to the effect that an organisation must issue a collection notice to an individual, after collecting personal information about the individual However, the OAIC's guidelines suggest that it will often be possible to satisfy this requirement by a statement at the point of collection and that there will be situations in which no action is required, e.g. where information is collected on an on-going basis in relation to the same matter.

g) Direct marketing - An organisation must not use or disclose personal information about an individual for direct marketing, unless the organisation has the individual's consent (in the case of sensitive information) or the individual would reasonably expect the organisation to use the information for that purpose (in the case of other personal information), the organisation provides a simple means by which the individual may opt out of further marketing material and the marketing material includes a statement drawing individual's attention to that option.

h) Maintenance, access and correction - Expanded obligations now apply regarding maintenance of accuracy of information, ensuring security of information, provision of access to information, correction of information and destruction/de-identification of information when it is no longer required. These are framed so as to require organisations to act proactively, necessitating establishment of procedures to deal with these issues and a compliance program.

i) Trans border data flows - Increased restrictions and obligations have been imposed regarding disclosure of personal information to overseas recipients. A misconception seems to be arising, to the effect that use of emerging technologies, such as cloud computing resources, will be prohibited or

T: (02) 9929 0226 M: 0403 738 996 ABN: 61 649 876 437
E: dbannerman@bannermans.com.au W: www.bannermans.com.au
P: PO Box 514 NORTH SYDNEY NSW 2059 AUSTRALIA

restricted. That is not the case, where there is no disclosure of personal information to overseas recipient.

Most organisations probably do not comply with the new requirements. This should be addressed, by conducting a privacy audit, with a view to developing a privacy policy compliant with the new legislation, as well as establishing associated procedures and a compliance program.

Prepared by Bannermans Lawyers
20 March 2014

BANNERMANS LAWYERS
T: (02) 9929 0226 M: 0403 738 996 ABN: 61 649 876 437
E: dbannerman@bannermans.com.au W: www.bannermans.com.au
P: PO Box 514 NORTH SYDNEY NSW 2059 AUSTRALIA