



HEIDTMAN & CO.

LAWYERS

PRIVACY ACT

The last decade or so produced what can best be described as a "black market" of customer information, in which business people would buy and sell information to facilitate the targeted marketing of particular groups and specific demographics.



Whilst many believed that such practices were overly intrusive and overtly undesirable, they were generally allowed to continue because Australian law did not recognise a "right to privacy" as such.

The law of property (specifically intellectual property) and confidential information (areas of law traditionally used to protect information) were simply not adequate to provide protection for information that merely identified individuals.

The situation worsened with the increased accessibility and popularity of the internet, and eventually the Government introduced amendments to the *Privacy Act* 1988 (Cth), which now brings most of the private sector under the *Privacy Act* regime.



So, to whom does the *Privacy Act* apply, what are your obligations under the *Privacy Act*, and what will happen if you fail to comply with them?

To Whom Does The Privacy Act Apply?



The *Privacy Act* applies to "organisations" - generally any organisation or entity that:

- * Has an annual turnover in excess of \$3 million;
- * Discloses "personal information" (generally, information that personally identifies an individual) about another individual to anyone else for a benefit, service or advantage;
- * Provides a benefit, service or advantage to collect personal information about another individual from anyone else; or
- * Provides health services and holds "health information" (generally "personal information" relating to health).

However, some activities are specifically excluded from the operation of the *Privacy Act*. These include:

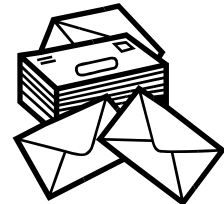
- * Certain acts and practices by employers relating to personal information of employees; and
- * The passing of personal information between related companies.

National Privacy Principles

The *Privacy Act* lays down 10 National Privacy Principles ("NPPs") with which most businesses will need to comply. The NPPs set out minimum standards of compliance for businesses when they handle personal information throughout its life cycle - from collection to use and disclosure, storage, security and accessibility.

Whilst the obligations imposed by the NPPs can seem quite vague and convoluted, the most important obligations imposed by them can be summarised as follows:

NPP 1 Collection



Organisations must not collect personal information unless the information is necessary for one or more of their functions or activities.

NPP 2 Use And Disclosure

Organisations must use or disclose personal information only for the purpose(s):

- * For which it was provided by the customer;
- * For which the customer might reasonably expect that it will be used; or
- * To which the customer has consented.

LEVEL 29, BT TOWER, 1 MARKET STREET, SYDNEY NSW 2000 TEL: (02) 9267 3388 FAX: (02) 9267 3688
E-MAIL: mailbox@heidtmans.com.au WEBSITE: www.heidtmans.com.au ADDRESS: PO Box Q77 QVB Post Shop NSW 1230

PARTNERS: DAVID HEIDTMAN, PETER CARKAGIS, ALAN McMURRAN, PENELOPE CABLE, MANUEL THEOS
CONSULTANT: WILLIAM MALOS **SENIOR ASSOCIATE:** MICHAEL TZIRTZILAKIS
ASSOCIATES: ANNE McDONALD, VANESSA MARQUEZ-VALLEJO, ADAM MAZZAFERRO

The best way to ensure you do not breach NPP 2 is to obtain the consent of the customer (preferably by signature) in all circumstances where you are using personal information and you are not sure whether the use relates directly to the services for which the customer has come to you.

The obvious example of one such "grey area" is the practice of direct marketing to customers, where a business sends out brochures, promotional material and the like in an attempt to encourage customers to use the business further. This will generally not be considered to be one of the purposes for which the customer provided the business with their personal information, and is arguably not a purpose for which the customer might reasonably expect their personal information to be used



NPP 5 Openness

Organisations must document clearly expressed and accessible policies on their management of personal information.

Businesses usually ensure compliance with this obligation by posting a "privacy policy" on their website, which is either accessible by customers via their own computers or which can be printed out for customers on the business premises.

NPP 6 Access

If an organisation holds personal information about an individual, it must provide that individual with access to this information unless circumstances make this inappropriate; for example if:

- * Access would pose a serious and

imminent threat to life or health;

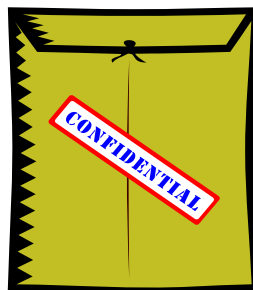
- * The request is frivolous or vexatious; or
- * Access would prejudice legal or tribunal proceedings.

NPP 10 Sensitive Information

Organisations are generally prohibited from collecting "sensitive information" about an individual (generally personal information that would normally be considered sensitive, such as information pertaining to race, religion or sexual preference), unless:

- * the individual has consented;
- * the collection is required by law; or
- * the collection is necessary to prevent or lessen a serious threat to life or health.

What Will Happen If My Business Fails To Comply With The Privacy Act?



If you fail to comply with your obligations under the *Privacy Act*, an individual whose personal information has been used in a way not permitted by the *Privacy Act* can make a complaint to the Privacy Commissioner, or the Privacy Commissioner can undertake an investigation of his own accord.

The Privacy Commissioner can then make a declaration that includes one or more of the following:

- * That a business has interfered with the privacy of an individual and that such acts should be

discontinued;

- * That a business should perform any reasonable act or course of conduct to redress any loss or damage suffered by an individual (including injury to feelings and humiliation);
- * That an individual is entitled to a specified amount of compensation; or
- * That it is inappropriate to take any further action in the matter.

Non-compliance with a declaration of the Privacy Commissioner may lead to court enforcement.

How We Can Help

Heidman & Co has experience with many of the issues raised by the *Privacy Act*, from the drafting of privacy policies to suggesting practical and innovative ways in which to continue business activities without breaching the *Privacy Act*.

The Privacy Commissioner has indicated that if a dispute arises regarding infringement of the *Privacy Act* relating to an area of "uncertainty", the dispute will usually be decided in favour of the individual to whom the personal information relates.

Accordingly, if you have any concerns or questions about the *Privacy Act*, or wish to know more about the National Privacy Principles, you should seek advice rather than risk a hefty penalty or onerous compliance order.



Heidman & Co Fact Sheets are published as a service to our clients and friends. Articles should be viewed only as a summary of the law and not as a substitute for legal consultation in a particular case. Your comments and questions are always welcome.