A SIMPLE GUIDE TO COMPLIANCE WITH AUSTRALIAN PRIVACY LAWS

ASPECT LEGAL CHEAT SHEET SERIES

A publication of aspect legal

aspectlegal

New Privacy Laws – **Should You Care?**

New privacy laws come into effect on 12 March 2014. The changes are important to understand because the powers of the Privacy Commissioner have been ramped up and businesses that fail to comply with the laws may be liable for fines of up to $1.7 million.

The new laws may be relevant to you and you should read this article if ***any*** of the following could apply to your business:

- It provides **health services** or **holds health information** – for example if you are a doctor, dentist, naturopath, chiropractor, pharmacy, gym or weight loss clinic;
- It makes money or gets any other benefit from disclosing personal information – for example if you sell or trade your database of personal information with other businesses or if you provide recruitment or head hunting services;
- It has contracts with any government departments **(including government panel contracts);**
- It has an **annual turnover of above $3 million;** or
- It has **related entities that are located overseas.**

What's changed?

Firstly, there has been a change in terminology. The 10 "National Privacy Principles" or "NPPs" (which currently apply to the certain private organisations) and the 11 "Information Privacy Principles" or "IPPs" (which currently apply to government agencies) will be replaced by a unified set of 13 "Australian Privacy Principles" or "APPs".

ASPECT TIP:
Update your privacy policy and privacy statements to reflect the new terminology.

Who must comply?

The APPs apply to agencies and to organisations whose annual turnover is more than $3 million. The APPs also apply to businesses that provide health services and which hold health information (other than employee records), and to businesses that disclose personal information for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information. The laws refer to these organisations and businesses as "APP entities".

ASPECT TIP:
If your organisation's turnover is the proximity of this $3 million cap, speak to one of our lawyers, who can give you more detailed guidance on how to calculate the annual turnover for the purposes of these laws.

Special provisions apply to contracted service providers and subcontractors that handle personal information under a Commonwealth contract. The definition of "Commonwealth contract" is broad.

ASPECT TIP:
If you have any contracts with government departments – including government panel contracts – speak with one of our lawyers to determine whether and how you must comply with the APPs and other privacy obligations under the contract

Note that the laws extend to acts and practices that occur outside Australia. If your organisation is part of a larger group (including group companies that are located overseas), in certain circumstances, the acts and practices (and breaches) by your related group entities, will be deemed to be your acts and practices (and breaches).

ASPECT TIP:
Review your group-wide information handling practices to ensure group-wide compliance with the laws because a breach by a related group entity could come back to bite you in Australia

Online businesses with no physical presence in Australia, but that collect personal information from individuals who are physically in Australia, must also comply with the laws.

The Australian Privacy Principles
New Issues to Take Note Of

The most significant of the new APPs for businesses are set out below:

APP 1 and **5** - Open and Transparent Management and Notification of the Collection of Personal Information

You must take reasonable steps in the circumstances to implement APP-compliant practices, procedures and systems. You must have a clear and up-to-date Privacy Policy that is made available and free of charge (e.g. on your website). APP 1 now prescribes a list of matters that must be included in your Privacy Policy. APP 5 requires you to take reasonable steps to notify the individual of certain listed matters at or before (or if it is not practicable, as soon as practicable after) the time that you collect their personal information. This is often described in practice as the "Privacy Statement" and is usually a short form notice.

ASPECT TIP:
Check your privacy policy and privacy statements address all the matters required by APP 1 and APP 5. See here for the lists of requirements

APP 2 - Anonymity and Pseudonymity

You must give individuals the option when dealing with you, to not identify themselves, or to use a pseudonym – unless otherwise required by law, or if it is impracticable to deal with an individual who has not identified themselves or used a pseudonym.

APP 4 - Unsolicited personal information

APP 4 gives unsolicited personal information the same sort of protection as solicited information. If you receive unsolicited personal information, you must, within a reasonable period, determine whether you could have collected it under APP 3. If you could not have collected that information under APP 3, and the information is not contained in a Commonwealth record, then you must destroy or de-identify the information as soon as practicable.

ASPECT TIP:
Have a system in place for identifying and handling unsolicited personal information in accordance with the new laws

APP 6 – Use Or Disclosure Of Personal Information

You must not use or disclose personal information for a "secondary purpose" unless the individual has consented. If no consent has been given, you may use or disclose the personal information for a secondary purpose in certain circumstances such as if the individual would reasonably expect that you use or disclose their information for a secondary purpose and the secondary purpose is related to the primary purpose (or directly related, in the case of sensitive information); the use or disclosure is required or authorised by law; a permitted general situation exists, or a permitted health situation exists.

If you collect the information from a related body corporate, then your related body corporate's primary purpose will be treated as your primary purpose for collection.

APP 7 - Direct marketing

Direct marketing is prohibited unless an exception applies and certain rules are followed. For example, you must not use personal information for direct marketing purposes unless that information was collected from the individual, and they would expect it to be used for direct marketing, it is easy for the individual to opt out of the direct marketing and they have not opted out. There are different rules for when the information isn't collected from the individual, or when the individual wouldn't expect their personal information to be used for direct marketing. There are also specific requirements for contracted services providers for a Commonwealth contract.

You can only use or disclose sensitive information for direct marketing purposes if the individual has consented.

This APP does not apply to the Do Not Call Register and Spam Acts.

ASPECT TIP:
Review your marketing system to ensure that personal information falls within the exceptions that permit direct marketing

APP 8 - Disclosing information offshore

You must give individuals the option when dealing with you, to not identify themselves, or to use a pseudonym – unless otherwise required by law, or if it is impracticable to deal with an individual who has not identified themselves or used a pseudonym.

ASPECT TIP:
Consider whether you disclose personal information outside of Australia, for example by outsourcing, off-shoring or cloud computing.

Also, contracts with overseas entities that have access to personal information should reflect an agreement by that entity to comply with the APPs.

ASPECT TIP:
Check whether your agreements with any overseas organisations that may have access to personal information you store (e.g. hosting companies) include an obligation for them to comply with the APPs and consider obtaining an indemnity from them should they breach the APPs.

Information Handling Tips **for Businesses**

Below are some other personal information handling tips for your business:

- Start preparing for the changes to privacy laws now
- Have your privacy policy and privacy statements reviewed to ensure they comply with the new requirements
- Make sure your IT systems are secure
- Don't collect personal information that is unnecessary for your business or "just in case" it becomes necessary
- If you do need to collect personal information, tell them why you are doing this, what the information will be used for and how long it will be kept
- Make it clear who will have access to that personal information, including any third parties
- Take steps to destroy or de-identify personal information that is no longer required, subject to other record keeping requirements

Let us know if you need help in getting ready for the new privacy laws. If you would like your privacy policy and privacy statements reviewed or updated, or if you would just like to discuss any questions you might have, contact us on (02) 8006 0830 or send an email to enquiries@aspectlegal.com.au

In the meantime, if you'd like to know more information about the APPs, including comparison guides, checklists, and presentations for staff training, you can find them here.

Privacy Pack | Contact Us | Training

Email:
enquiry@aspectlegal.com.au

Phone Number:
02 8006 0830

Office Location:
Top Floor, 6/10 Rodborough Road
Frenchs Forest
NSW 2086