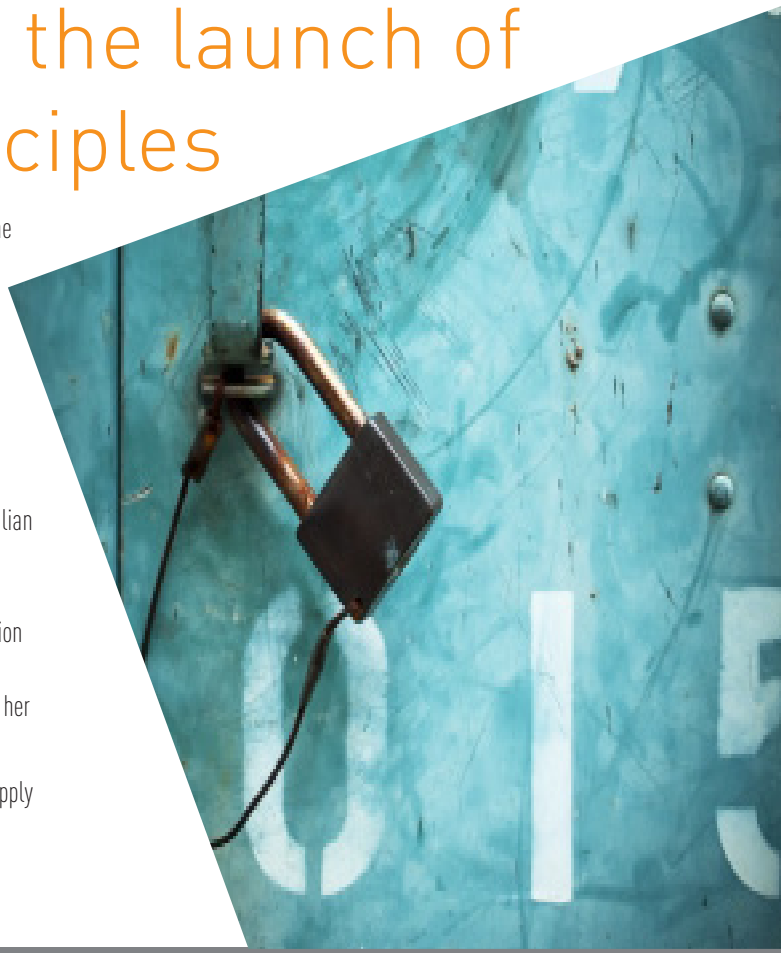
ALERT

cornwallstodart
ENHANCING SUCCESS

6 DECEMBER 2013

Privacy matters: Count down to the launch of the new Australian Privacy Principles



Overview

Australian organisations are urged to prepare for privacy reforms under the *Privacy Act 1988* (Cth) (**Act**), which are set to take effect on 14 March 2014 (**Privacy Reforms**). In this Alert, we outline the key changes to the privacy law framework and consider a number of variations to the privacy obligations that are likely to be pressure points for businesses bound by the proposed Australian Privacy Principles (**APPs**).

The planned Privacy Reforms are not particularly complex. However, they require a considered review of an organisation's inward facing and outward facing policies and procedures to ensure compliance. The management of employees' personal information will be just as important (and equally likely to give rise to a complaint) as the management of clients' personal information.

Businesses should not be dissuaded from adopting a methodical approach to the Privacy Reforms by the inexact nature of many of the privacy obligations (which incorporate concepts such as 'reasonably necessary' and 'implied consent'). Organisations should be proactive, appoint responsible personnel to oversee the implementation of the Privacy Reforms and plan to commence a privacy audit as soon as possible, to ensure the organisation is compliant from day one.

Revised framework

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), which was passed by the Senate in November 2012, imposes additional obligations on the private sector, while giving the Australian Information Commissioner (**Commissioner**) increased powers of enforcement. A new penalty system allows the Commissioner to seek a maximum penalty of $340,000 for individuals and $1.7 million for corporations. The Commissioner has the power to initiate an investigation of an organisation for breaches of the APPs on his or her own initiation.

The Privacy Reforms introduce 13 new (or revised) APPs that will apply uniformly to both private organisations and government agencies that collect and store personal information. The APPs will replace the National Privacy Principles that currently apply to the private

sector and the Information Privacy Principles that apply to the public sector. A number of the APPs are significantly different to their predecessors. APPs 1, 4, 5, 7 and 8 in particular introduce substantial changes to an organisation's obligations with regard to managing personal information.

Who must comply with the Act following the Privacy Reforms?

The definition of an 'APP entity' remains substantially unchanged. Therefore, the Act will continue to apply to any 'agency' or 'organisation' (ie an individual, body corporate, partnership, trust or unincorporated association) unless it is a 'small business operator' (**APP Entity**). In general, a 'small business operator' is a business with an annual turnover below $3 million, unless an exception applies (eg businesses that provide a health service or disclose personal information in exchange for a benefit).

Management of personal information

APP 1 outlines a foundation obligation in respect of APP Entities' management of personal information. Every APP Entity must manage personal information in a way that is open and transparent. In practice, this means that organisations must take 'reasonable steps' to ensure personal information is protected against loss, misuse or unauthorised access at every stage of the information 'life cycle', from collection to use, storage and destruction. Whether an organisation's conduct amounts to 'reasonable steps' will be highly dependent on factors specific to the APP Entity, including the nature of the personal information held, available resources and the practicability of implementing appropriate information management practices. APP Entities should keep a record of the steps taken to comply with APP 1, including a record of the reasons for not adopting a course of action that may be considered as 'best practice'.

What are the minimum requirements?

Every APP Entity must have a clearly expressed, up-to-date 'APP Privacy Policy' and formal procedures for dealing with inquiries and complaints. An APP Privacy Policy must be tailored to the APP Entity. An irrelevant or generic privacy policy is unlikely to satisfy the obligations imposed by APP 1.

Unsolicited information

APP 4 concerns unsolicited personal information (eg a curriculum vitae supplied by a potential job applicant or a customer complaint sent to an organisation's head office). An APP Entity must decide within a 'reasonable period' whether the organisation could have collected the information under APP 3 (eg the information is directly related to one or more of its functions or activities). The information must be destroyed or de-identified 'as soon as practicable' if the APP Entity would not have been entitled to collect the information pursuant to APP 3.

Notification of collection

APP 5 requires organisations to take reasonable steps to 'notify' an individual of certain matters prior to collecting personal information (or as soon as practicable after collection). This obligation will supplant the current obligation to take reasonable steps to ensure the individual 'is aware of' certain matters prior to collection. Further, APP Entities must now provide individuals with information regarding their 'APP Privacy Policy' and advise whether they are likely to disclose personal information to overseas recipients and, if practicable, the countries where prospective overseas recipients reside.

Direct marketing

APP 7 prohibits APP Entities from using or disclosing personal information for the purpose of marketing goods and services to individuals (ie direct marketing), unless an exception applies. If an organisation is permitted to use personal information for direct marketing purposes, it must provide individuals with an option to 'opt-out'. A request to 'opt-out' must be observed within a reasonable time.

Organisations may only use personal information obtained from a third party for direct marketing if the individual has expressly consented to the use of their information for that purpose (unless obtaining consent is impracticable). The direct marketing provisions of the Act apply in addition to the requirements under the *Do Not Call Register Act 2006* (Cth) and the *Spam Act 2003* (Cth).

Cross-border disclosure

APP 8 deals with cross-border disclosure of personal information. An APP Entity must take steps to ensure that the overseas entity does not conduct itself in a way that would breach the APPs, prior to disclosure of personal information. The APP Entity must also inform the individual that the APPs may not apply to the management of their personal information by the overseas entity. An APP Entity may be liable for the conduct of the overseas entity in the event that it does not reasonably believe that the recipient entity operates in accordance with a privacy regime that is comparable to Australian law.

Enforcement of the APPs

The privacy obligations imposed by the APPs should be observed not least because of the substantial penalties that may apply for non-compliance. The Commissioner will have the power (among other things) to:

- conduct an assessment (following a complaint, or on his or her own accord) to determine whether an organisation complies with the APPs;
- require an organisation to provide an enforceable undertaking to ensure that the organisation takes (or refrains from taking) a particular action(s); and
- apply to the Federal Court of Australia for a civil penalty order against an organisation, for serious or repeated breaches of the APPs.

Conclusion

Organisations are strongly advised to consider the potential impact of the Privacy Reforms on their current practices for managing staff and clients' personal information. In particular, we recommend organisations take the following preliminary steps to prepare for the reforms:

- plan a 'privacy audit' to ensure your organisation's privacy policy (and accompanying procedures) complies with the obligations imposed by the APPs. An organisation that complies with the existing National Privacy Principles may not necessarily comply with the impending APPs;
- amend internal protocols that outline how staff and third parties are to collect and handle personal information on behalf of the organisation;
- carry out a departmental evaluation to identify how various divisions of the business handle personal information in practice (eg IT, marketing, sales etc) and to determine whether staff training is indicated to ensure employees know and understand the relevant privacy obligations and protocols;
- review (and potentially re-negotiate) contracts with third parties with a view to imposing contractual obligations that require third parties to comply with the new APPs (so as to discharge the organisation's own obligations under the APPs); and
- peruse registered APP Codes to ensure your organisation meets the requisite industry standard.

Want to republish any of this newsletter?

If you would like to republish any part of this newsletter in your staff newsletter or elsewhere please contact our Marketing team on **+61 3 9608 2168**

Disclaimer

This newsletter is intended to provide general information on legal issues and should not be relied upon as a substitute for specific legal or other professional advice.

Images

All images are used courtesy of www.freedigitalphotos.net

For further information regarding the Privacy Reforms and how to get your business 'privacy reform ready' please contact:

Ian Sinclair, Partner
Phone (direct) **+61 3 9608 2166**
Mobile **+61 412 906 896**
Email **i.sinclair@cornwalls.com.au**

Lesley Naik, Lawyer
Phone (direct) **+61 3 9608 2179**
Email **l.naik@cornwalls.com.au**