Changes to the Privacy Act now in effect - are you prepared?

Pieter Oomens and Theonie Trianta | April 2014 | Commercial Disputes and Transactions

Summary

On 12 March 2014, the changes to the *Privacy Act 1988* ('Act') as a result of the *Privacy Amendment (Enhancing Privacy Protection) Act* (2012) came into effect. The purpose of the amendments to the Act was to assist in enhancing the protection of individuals' personal information. In other words, businesses and agencies now have stricter obligations as to how they collect, store and use personal information.

Who must comply?

Generally, all Federal and Australian Capital Territory Government Agencies ('Agencies') as well as 'Organisations' (being private sector organisations with an annual turnover of more than $3 million) and all private health service providers must comply with the Act. Small Business Operators, being businesses with an annual turnover of less than $3 million may, in some circumstances, still be required to comply with the provisions regulating credit providers.

.

Expansion of the definition of 'personal information'

The Privacy Act sets out the rights and obligations in respect of an individual's 'personal information'. The Act has expanded the definition of 'personal information' to be:

> '*information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
> *(a) Whether the information or opinion is true or not; and*
> *(b) Whether the information or opinion is recorded in a material form or not '.*

Accordingly, personal information is any information that may identify a person. Such information may include a person's name, credit card details, contact details, address and may extend to information relating to online activity such as their IP address or online purchase history.

Australian Privacy Principles

Previously, Agencies were required to comply with eleven Information Privacy Principles while Organisations were required to comply with ten National Privacy Principles. The amended Act has consolidated these principles into one set of principles, namely the Australian Privacy Principles ('APPs').

The new APPs are as follows:

APP 1- Open and transparent management of personal information
APP 2- Anonymity and Pseudonymity
APP3- Collection of solicited personal information
APP4 - Dealing with unsolicited personal information
APP5 - Notification of the collection of personal information
APP6 - Use or disclosure of personal information
APP7- Direct marketing
APP8 - Cross border disclosure
APP9 - Adoption, use or disclosure of government related identifiers
APP10 - Quality
APP11 - Security
APP12 - Access
APP13 - Correction

All Organisations and Agencies (collectively, 'APP Entities') must comply with the APPs. Broadly speaking, some of the new obligations for APP Entities under the amended Act (subject to some exceptions) include:

- The obligation for APP Entities to have a more prescriptive privacy policy which is publicly available;
- Dealing with individuals on a pseudonymous basis unless it is impracticable;
- Obtaining consent from individuals before collecting sensitive information;
- Providing collection statements outlining prescribed information to individuals before collecting personal information;
- Complying with new obligations when dealing with unsolicited personal information;
- Refraining from using personal information for direct marketing purposes unless the individual would reasonably expect such use and the APP entity provides a simple method to 'opt out';
- Taking reasonable steps to ensure overseas recipients of personal information do not breach the APPs in respect of that information.
- Ensuring personal information collected is relevant and protected from interference; and
- Ensuring systems are in place to access and correct personal information.

Credit Providers

Broadly speaking, Credit Providers are banks, Organisations and Small Business Providers who provide credit (including credit cards) during the course of their business. This may also extend to suppliers who hold accounts for the supply of goods or services to customers whereby payment in full is deferred by at least 7 days.

The amended Act inserts a new Part IIIA into the Privacy Act, which governs privacy and credit information, being a specific type of personal information. This new Part IIIA is supplemented by the Credit Reporting Privacy Code ('CR Code') which was approved by the Australian Information Commissioner on 22 January 2014, and also came into effect on 12 March 2014. This will affect many clients who are classified as 'Credit Providers', namely banks and Organisations or small business. Some of the key new requirements are highlighted below.

Credit Reporting Policy

Credit Providers must have a clearly expressed, up-to-date and publicly available policy about the management of credit information collected by the provider. The Act and the CR Code prescribe information that must be included in this policy.

Notification Requirements

Credit Providers must now notify individuals of certain information when collecting personal and credit information that it is likely to disclose to a credit reporting body. The CR Code and the amended Act specify certain information that must be included within the notification, namely with respect to collection, complaints handling procedures, overseas disclosures and access.

Access and correction

There are significant changes to the requirements of Credit Providers to provide access to and correct credit information. These changes prescribe certain time limitations and procedures to be adopted in responding to and complying with requests to access and/or correct credit information.

Turks LEGAL

Also, if a Credit Provider holds credit eligibility information about an individual that it believes is inaccurate, out of date, incomplete, irrelevant or misleading, it must on its own initiative take reasonable steps to correct such information and ensure data derived from that information is correct.

Complaints handling

Importantly, the amended Act gives individuals the explicit right to complain to Credit Providers in relation to most acts or practices under Part IIIA or the CR Code.

Credit Providers may be required to consult with other credit providers or credit reporting bodies to deal with a complaint but may not refer that complaint for resolution. The amended Act prescribes certain procedures and time limitations in dealing with complaints. Credit Providers should have a compliant complaints handling system incorporating these changes.

Recognised External Dispute Resolution Schemes ('EDRS')

The amended Act provides the Privacy Commissioner with power to recognise an EDRS for the purpose of handling privacy-related complaints. Generally, if an individual is not satisfied with a Credit Provider's response to a complaint, it may file the complaint with the EDRS for resolution.

All Credit Providers are generally required to become members of a recognised EDRS before they are permitted to disclose credit information to a credit reporting body, or in other words, participate in the credit reporting system.

On 28 February 2014, the Privacy Commissioner announced that the requirement for commercial credit providers (as distinct from consumer credit providers) to join an EDRS to participate in the credit reporting system would be suspended for 12 months (to 12 March 2015). At this stage, from 12 March 2015 all commercial Credit Providers will need to join an EDRS to continue disclosing information to credit reporting bodies.

Penalties

The amended Act has introduced civil penalties for breaches of certain provisions of the Act. Where a civil penalty is ordered or an Organisation, Agency or Credit Provider has been found guilty of an offence, an individual affected by the conduct may also apply for compensation from that entity (on top of any penalties ordered by a court).

Further, some parts of the amended Act carry criminal penalties, such as the unauthorised use and disclosure of false and misleading information.

What should Agencies, Organisations and Credit Providers do?

Agencies and Organisations should conduct an audit of their practices and procedures in collecting, storing, using and disclosing personal information (and in some cases credit information) to ensure they comply with the new privacy regime. Access, correction and complaints handling practices must also be reviewed. Agencies and organisations must ensure that their privacy policies are up to date and compliant with the new regime.

Credit Providers should also conduct an audit of their practices and procedures in relation to collecting, storing, using and disclosing of credit information so it is compliant with the new provisions affecting Credit Providers. Credit Providers must also ensure that they have drafted a credit reporting policy and considered whether they will join an EDRS scheme (which, as the law presently stands, must be done by 12 March 2015) to continue participating in the credit reporting system.

Turks LEGAL

TurkAlert

For more information, please contact:

Pieter Oomens
Partner
T: 02 8257 5709
M: 0417 268 334
pieter.oomens@turkslegal.com.au

Theonie Trianta
Lawyer