DATA PROTECTION LAWS OF THE WORLD

Australia

DLA PIPER

Downloaded: 26 May 2018

AUSTRALIA

Last modified 24 January 2018

LAW

Data privacy/protection in Australia is currently made up of a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities with an annual turnover of at least A$3 million and all Commonwealth Government and Australian Capital Territory Government agencies.

The Privacy Commissioner has power under the Privacy Act to conduct investigations (including own motion investigations), ensure compliance with the Privacy Act and seek civil penalties for a serious/egregious breach or for repeated breaches of the APPs where remediation has not been implemented.

Australian States and Territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies (and private businesses' interaction with them). These acts are:

- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania), and
- Privacy and Data Protection Act 2014 (Victoria).

There are also various other pieces of State and Federal legislation that impact on or relate to data protection. For example, the Telecommunications Act 1997 (Cth), the National Health Act 1953 (Cth), the Health Records and Information Privacy Act 2002 (NSW), the Health Records Act 2001 (Vic) and the Workplace Surveillance Act 2005 (NSW) all impact privacy/data protection for specific types of data or for specific activities.

Further, specific regulators have expressed their expectations as to the behavior and controls which regulated entities would have in place (for example, in the case of financial services institutions, the Australian Prudential and Regulatory Authority and, in the case of corporations generally, the Australian Securities and Investment Commission). Finally, over the course of 2017, State and Federal legislation has been amended to reflect an enhanced focus on the protection of minors online. The Attorney-General of New South Wales indicated in November 2016, that the intention of the NSW Government was to table legislation in 2017 which would provide for personal civil rights of action for certain serious interferences of an individual's privacy, this legislation is yet to be tabled. While motivated through specific high-profile instances of "revenge porn" and similar, it is entirely possible that the legislation (if enacted) could have a broader reach. Our focus here, however, is on the application of the Privacy Act to private sector entities.

Private sector entities are referred to as 'organisations'. Under the Privacy Act/the APPs, an organisation can be an:

- individual
- body corporate
- partnership
- other unincorporated association, or
- a trust.

DEFINITIONS

Definition of personal data

Personal Data (which is referred to as 'personal information' in Australia) means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not.

Definition of sensitive personal data

Sensitive Personal Data (which is referred to as 'sensitive information' in Australia) means information or an opinion about:

- 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 orientation or practices
- criminal record that is also personal information
- health information about an individual
- genetic information about an individual that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric identification or verification, or
- biometric templates.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner ("Privacy Commissioner") operating under and through the Office of the Australian Information Commissioner ("OAIC") is the national data protection regulator responsible for overseeing compliance with the Privacy Act. Its website is currently http://www.oaic.gov.au/.

REGISTRATION

Australia does not maintain a register of controllers or of processing activities. There is no requirement under the current data protection regime (ie the Privacy Act) for an organisation to notify/report to the Office of the Privacy Commissioner on the processing of personal information.

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer, but it is good and usual practice under the current law and guidance has been issued by the Privacy Commissioner strongly recommending it.

COLLECTION & PROCESSING

An organisation must not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.

Under the Privacy Act organisations must also take steps, as are reasonable in the circumstances, to ensure that the personal information that the organisation collects is accurate, up-to-date and correct.

At or before the time personal information is collected, or as soon as practicable afterwards, an organisation must take reasonable steps to make an individual aware of:

- its identity and how to contact it
- why it is collecting (or how it will use the) information about the individual
- to whom it might give the personal information
- any law requiring the collection of personal information
- the main consequences (if any) for the individual if all or part of the information is not provided
- the fact that the organisation's privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organisation will deal with such complaint
- whether the organisation is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Organisations usually comply with these notification requirements by including the above information in a privacy policy and requiring individuals to accept the terms of that privacy policy prior to collecting their personal information.

One of the biggest issues in practice in respect of collection and compliance with the Privacy Act for organisations is the failure to appreciate that the obligations with respect to the mandatory notification requirements outlined above also apply to any personal information they collect from/via a third party. That is, a separate and independant obligation to notify the mandatory matters arises on the receipt of personal information from a third party, as though the organization had collected such personal information directly from the individual. In contrast to Europe, Australian privacy law does not distinguish between a 'data processor' and a 'data controller'.

An organisation must not use or disclose personal information about an individual unless one or more of the following applies:

- the personal information was collected for the primary purpose of such disclosure or a secondary purpose related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for that secondary purpose
- the individual consents
- the information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual's consent and (among other things) the individual is told that they can opt out of receiving marketing from the organisation
- a 'permitted general situation' or 'permitted health situation' exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public
- it is required or authorised by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organisations are required to also ensure that:

- each direct marketing communication provides a simple means by which the individual can opt-out
- the individual has not previously requested to opt-out of receiving direct marketing communications.

The above direct marketing requirements are additional to the specific commercial electronic messaging requirements outlined below under the heading "Electronic Marketing" although apply to all forms of direct marketing not only electronic marketing.

Where 'sensitive information' is processed there are additional protections under the Privacy Act which generally provide that an organisation is not allowed to collect sensitive information from an individual unless certain limited requirements are met, including one or more of the following:

- the individual has consented to the collection and the collection of the sensitive information is reasonably necessary for one or more of the entity's functions or activities
- collection is required or authorised by law or a court/tribunal order
- a 'permitted general situation' or 'permitted health situation' exists; for example the information is required to establish or defend a legal or equitable claim or he/she is a serious treat to the life or health of the individual or the public
- the entity is an enforcement body and the collection is reasonably necessary for that entity's functions or activities
- the entity is a non-profit organisation and the information relates to the activities of the organisation and solely to the members of the organisation (or to individuals who have regular contact with the organisation relating to its activities).

An organisation must, on request by an individual, give that individual access to the personal information (and the ability to correct inaccurate, out of date or irrelevant information) that is held about the individual unless particular circumstances apply which allow the organisation to limit the extent to which access is given (and to which correction is performed). These include emergency situations, specified business imperatives and law enforcement or other public interests.

Organisations must also provide individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with that organisation unless it is impractical to do so or the organisation is required (or authorised) by law to deal with identified individuals.

TRANSFER

Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organisation outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing/transferring entity will generally remain liable for any act(s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where:

- the organisation reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although it is a step towards ensuring compliance with the 'reasonable steps' requirement)
- the individual consents to the transfer However, under the Privacy Act the organisation must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organisation will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs
- a 'permitted general situation' applies, or
- the disclosure is required or authorised by law or a court/tribunal order.

SECURITY

An organisation must have appropriate security measures in place (ie 'take reasonable steps') to protect any personal information it retains from misuse and loss and from unauthorised access, modification or disclosure. The Privacy Commissioner has issued a 32 page detailed guidance document on what it considers to be "reasonable steps" in the context of security of personal

information, which we recommend be reviewed and implemented. Depending on the organisation, and how and by which government agency it is regulated, as noted above specific requirements or expectations may also exist and with which organisations should be familiar. An organisation must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purpose(s) for which it was collected

BREACH NOTIFICATION

There is currently no obligation to report breaches to affected individuals or to the OAIC, however, from 22 February 2018 entities with existing obligations to comply with the APPs under the Privacy Act must comply with madatory reporting requirements under the mandatory data breach notification regime.

The mandatory data breach notification includes data breaches which relate to:

- Personal information;
- Credit reporting information;
- Credit eligibility information; or
- Tax file numbers.

In summary, the regime requires organisations to notify the OAIC and affected individuals of "eligible data breaches" (in accordance with the required contents of a notice). An "eligible data breach" occurs when the following conditions are satisfied in relation to personal information, credit reporting information, credit eligibility information or tax file information:

1. both of the following conditions are satisfied:
    1. there is unauthorised access to, or unauthorised disclosure of, the information; and
    2. a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates; or
2. the information is lost in circumstances where:
    1. unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
    2. assuming that unauthorised access or unauthorised access disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates.

Whilst "serious" harm is not defined in the legislation, the OAIC has released guidance on how serious harm may be interpreted and assessed by organisations.

The regime also imposes obligations on organisations to assess whether an eligible data breach has occurred where the organisation suspects (on reasonable grounds) that an eligible data breach has occurred, but that suspicion does not amount to reasonable grounds to believe that an eligible data breach has occured. Importantly, the OAIC has released guidance indicating that such assessments must be undertaken by organisations within 30 days of any suspected data breach.

There are various exceptions to the requirement to notify affected individuals and/or the OAIC of a data breach notification including in instances where law enforcement related activities are being carried out or where there is a written declaration by the Privacy Commission.

ENFORCEMENT

The Privacy Commissioner is responsible for the enforcement of the Privacy Act and will investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made. Generally, the Privacy Commissioner prefers mediated outcomes between the complainant and the relevant organisation. Importantly, where the Privacy Commissioner undertakes an investigation of a complaint which is not settled, it is required to ensure that the results of that investigation are publicly available. Currently, this is undertaken by disclosure through the OAIC website of the entire investigation report.

The Privacy Commissioner may also investigate any 'interferences with the privacy of an individual' (ie any breaches of the APPs) on its own initiative (ie where no complaint has been made) and the same remedies as below are available.

After investigating a complaint, the Privacy Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organisation rectify its conduct or that the organisation redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and/or humiliation). Furthermore, fines of up to A$360,000 for an individual and A$1.8 million for corporations may be requested by the Privacy Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals.

ELECTRONIC MARKETING

The sending of electronic marketing (which is referred to as 'commercial electronic messages' in Australia) is regulated under *SPAM Act 2003* (Cth) ('SPAM Act') and enforced by the Australian Communications and Media Authority.

Under the SPAM Act a commercial electronic message must not be sent without the prior 'opt-in' consent of the recipient. In addition, each electronic message (which the recipient has consented to receive) must contain a functional unsubscribe facility to enable the recipient to opt-out from receiving future electronic marketing.

A failure to comply with the SPAM Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to A$1.7 million per day.

ONLINE PRIVACY

There are no laws or regulations in Australia specifically relating to online privacy, beyond the application of the Privacy Act and State and Territory privacy laws relating to online / e-privacy, the collection of location and traffic data, or the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organisation must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information. App developers must also ensure that the collection of customers' personal information complies with the Privacy Act and the Privacy Commissioner has released detailed guidance on this.

KEY CONTACTS

Peter Jones
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +61292868356
peter.jones@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.