AUSTRALIAN PRIVACY TOOLBOX FOR THE TECHNOLOGY SECTOR

By Alec Christie, Partner, DLA Piper

The new Australian Privacy Principles attempt to keep pace with changing technology, emerging privacy issues and developments in privacy law in Australia and internationally.

This "Toolbox" will help you prepare for the increased focus on privacy compliance and the increasing emphasis on privacy in respect of Big Data, Cloud and Tech products which are now provided in many industries, particularly the financial services sector. It will also assist you to tune up your Australian privacy processes and policies in readiness for the new Australian Privacy Principles (**"APPs"**) which become effective from ***12 March 2014***.

1. The Privacy Commissioner's increased powers, fines and reinvigorated approach

Issue/trend: Due to the existing privacy regime in Australia having few, if any, enforcement "teeth" and because the current regulator is best described as "passive", there has been patchy compliance with (and a minimal understanding of) Australia's existing privacy law in the Technology Sector in Australia.

The amendments to the privacy law, including the introduction of the new APPs, herald a new era for privacy law in Australia. The combination of penalties of up to $1.7 million for organisations for a serious invasion of privacy or repeated invasions of privacy ($340,000 for individuals) and the additional investigatory powers given to a renewed and reinvigorated regulator, we expect, will significantly increase the importance of privacy compliance and the likelihood of investigations and enforcement of Australian privacy law.

Please see our **Top 10** as regards to some of the common general privacy misconceptions and misunderstandings in Australia (and the Asia Pacific region).

Tip: All Tech organisations carrying on business in Australia that access personal information (whether by collecting directly from individuals or indirectly by collecting personal information from customers) will now be separately and independently obliged to comply with Australian privacy law/the APPs.

Please see our **New APPs Update** and **Impact on Government Agencies Update** for a more detailed discussion of the areas that are impacted by the new APPs and our earlier **Consumer Action Update** in respect of possible direct consumer actions.

2. The new offshore transfer regime

Issue/trend: The new APPs turn the existing National Privacy Principle with respect to overseas transfer of personal information on its head. From 12 March 2014, Australian organisations are now obliged to "ensure" that the overseas entity receiving personal information from an Australian company complies with Australian privacy law (ie the APPs). In addition, the Australian entity will remain liable for breaches of the APPs by the overseas recipient (except in limited cases). As well as, the transfer of personal information offshore, access by offshore third parties to an Australian managed database is also now classified as an offshore disclosure.

Tip: Customers need to do due diligence on their provider before disclosing information and must include relevant obligations in contracts with respect to complying with the APPs and an indemnity for any breach of the APPs by the offshore provider/recipient. Tech providers must acquaint themselves with their obligations under the APPs, limit any indemnity to damages caused directly by their actions and insist (possibly with a cross indemnity) that the Australian customer obtains all necessary

privacy consents. The customer should also be obliged to provide all necessary notifications under Australian privacy law to facilitate the disclosure of the information to the overseas provider/recipient.

Again, please see our recent **New APPs Update** for further details.

BIG DATA

3. Re-identification of data, re-notification and re-consent

Issue/trend: Big Data (and the analytics that go with it) is becoming more common in Australia, especially for businesses in the retail and financial services sectors. The concern is that Australian privacy law does not specifically deal with Big Data and so the APPs must be applied from first principles and, when applied on such a basis, any "re-identification" of information (ie that can be linked to an individual) will trigger independent and separate privacy obligations of the organisation undertaking the Big Data analytics at the time of such re-identification (where it will be considered to be itself "collecting" that personal information). Obviously, given that vast data sets and numbers of potential individuals involved it is a complex and costly exercise to re-consent and re-notify all such individuals on this deemed "collection".

Tip: Before embarking on Big Data analytics, consideration must be given to one's own data and that acquired from third parties or accumulated from public sources to determine if the appropriate consents have been obtained/notifications made to enable the Big Data analytics to occur and to avoid the cost of re-consent and re-notification.

We discuss both the issues and practical solutions in detail in our **Big Data Update**.

THE MOBILE/APP ENVIRONMENT

4. Privacy compliance for Apps

Issue/trend: One of the focuses identified by the Privacy Commissioner is in the App/Mobile environment where they are keen to ensure that clear and transparent privacy policies and processes are implemented. That is, not just that privacy processes and policies are followed in respect of Apps (which is substantially missing at present) but also that the privacy policies and processes are adapted and transformed for the mobile environment with consideration given to how best to communicate these to individuals over this platform.

Tip: We recommend that privacy processes and compliance with the Australian privacy law be rolled out across all Apps and other applications on the mobile platform as a priority. In addition, consideration must be given to the best method of modifying the privacy policies and processes to suit the mobile/App environment.

We address both the issues raised by the Privacy Commissioner and suggested solutions in more detail in our recent **Mobile/App Update** and **Updated App Update**.

CLOUD

5. Offshore transfer of personal information – Customer consent obligations and ongoing liability

Issue/trend: Cloud will continue to be a hot topic for 2014 with more and more Australian organisations considering a move to the Cloud. Privacy in the Cloud continues to be one of the biggest concerns in relation to moving into this space, even if this is sometimes overstated. Given the overseas transfer/disclosure obligations and the additional obligation to name countries where the personal information may be held/disclosed, there is real concern that many offshore Cloud providers will not be suitable for and unable to satisfy the Australian customer's new privacy obligations.

Tip: Australian customers need to ensure that they implement relevant privacy policies for (including obtaining relevant consents and making relevant notifications to) their customers in order to enable a move to the Cloud. Overseas Cloud vendors need to be aware of the changed obligations of Australian customers (a more onerous privacy compliance regime) including the obligation to inform individuals where their personal information may be stored in the Cloud (ie the countries) and their ongoing liability for breaches of the APPs by the cloud provider overseas. Cloud vendors will need to update their processes and terms and conditions accordingly.

We deal with these issues and possible solutions in more detail in our **Cloud Update**.

SECURITY

6. Vendor IT security

Issue/trend: Another focus identified by the Privacy Commissioner is the area of security which has been restated and reinforced as an obligation under the new APPs. This little understood privacy obligation requires organisations to take "reasonable steps" to keep secure any personal information collected or held (whether this be on one's own servers, in the Cloud, offshored, outsourced or the like). As an indication of how seriously the Privacy Commissioner is taking this overlooked privacy obligation, he issued a 32 page guidance on what "reasonable steps", in respect of security, look like to the Privacy Commissioner.

Tip: Tech providers must realise that Australian customers will now have a significant interest in what security they have – whether as an outsource, offshore, Cloud or other provider.

In our **Security Update** and **De-identification Update** we review the security guidance from the Privacy Commissioner and comment in more detail on the practical solutions suggested.

FINANCIAL SERVICES

7. New APRA Prudential Guidelines on Managing Data Risk

Issue/trend: In addition to the new APPs, Tech organisations supplying to the financial services sector in Australia must be aware of the new Prudential Practice Guidelines on Managing Data Risk, recently finalised by APRA which (together with APRA's existing guidance on IT security) provide additional obligations on financial services entities regulated by APRA with respect to data collection, management, control and security. These obligations are additional to the obligations under the APPs for the relevant financial services sector organisations.

Tip: Be aware of these additional obligations (which are significantly more onerous than those under the new APPs) for Australian financial services entities regulated by APRA. You need to consider the best ways to meet these obligations if you wish to continue doing business with such entities.

The issues and concerns raised by APRA and the suggested practical solutions are discussed in detail in our **Data Risk Guidance Update**.

HELP IS AVAILABLE!

Please do not hesitate to contact Alec Christie or one of our dedicated Tech Sector specialist privacy team to learn more about (or for our assistance with) any of the matters raised above or to ensure your compliance with the new APPs.

Alec Christie
Partner
T +61 2 9286 8237
Alec.Christie@dlapiper.com

CONTACT YOUR NEAREST DLA PIPER OFFICE:

BRISBANE

Level 29, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 38, 201 Elizabeth Street
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 4144
sydney@dlapiper.com

www.dlapiper.com

1201757584