RECENT AUSTRALIAN PRIVACY REFORMS WILL SIGNIFICANTLY IMPACT OFFSHORE SHARE INCENTIVES FOR AUSTRALIAN EMPLOYEES

By Alec Christie, Partner, DLA Piper Australia

The changes to the *Privacy Act 1988* (Cth), including the introduction of the new Australian Privacy Principles (**APPs**), significantly increase the obligations imposed on an offshore parent or related entity that collects or deals with personal information from Australian residents (ie employees) in connection with managing employee share incentive plans (**Plans**).

When the reforms become effective on 12 March 2014, many of the current practises of overseas entities that offer Australian employees the ability to participate in Plans will not, for information collected from 12 March 2014, be compliant with Australian privacy law and will need to be changed.

SIGNIFICANT NEW ATTITUDE AND TEETH FOR REGULATOR: NEW PENALTIES AND INCREASED POWERS

From 12 March 2014:

- the functions and powers of the Privacy Commissioner (the relevant government regulator) are significantly enhanced;
- the existing National Privacy Principles (**NPPs**), currently applicable to the private sector, are replaced with the new APPs which are applicable to both the public and private sectors; and
- for the first time in Australia, significant monetary penalties for both serious and repeated invasions of privacy (ie breaches of the Privacy Act/APPs) are available.

The Privacy Commissioner's increased powers under the APPs enable the regulator to, among other things:

- seek civil penalties (up to A$340,000 for an individual and A$1.7 million for a company) in cases where there is either a serious interference or repeated interferences with an individual's privacy;
- audit the handling of personal information by the private sector;
- investigate compliance of an organisation with the APPs on its own motion (ie no complaint is required in order to investigate); and
- make determinations following all investigations (ie even if the investigation is an "own motion" investigation) and apply to the Federal Court of Australia or Federal Magistrates Court to enforce such determinations.

However, the most significant "change" that has been introduced by the amendments to the Privacy Act and the new APPs is the approach and attitude (together with the increased and new powers) of the Privacy Commissioner to that of a more aggressive regulator keen to exercise the new powers and to police and enforce the provisions of the Privacy Act and the APPs!

Soon after the passing of the amendments and the new APPs, the Privacy Commissioner (Mr Timothy Pilgrim), in response to questions about the Privacy Commission's new and extended powers and the new significant fines for serious or repeated invasions of privacy, clearly flagged his future intentions by stating:

> *"From the commencement of the new laws, I will be able to accept enforceable undertakings*

and seek civil penalties … I will not shy away from using these powers in appropriate cases."

This new or re-invigorated attitude is also evident in the flurry of recent guidance documents issued by the Office of the Australian Information Commissioner (under which the Privacy Commissioner sits). These guidance documents remind us of existing obligations and the fact that many of these obligations will be the subject of a renewed focus going forward, in addition to reminding us of the new obligations applicable from 12 March 2014.

CURRENT PRACTICES AND THE EMPLOYEE RECORDS EXEMPTION

Many overseas entities that offer Australian employees the ability to participate in their Plans have relied on the local Australian subsidiary employer to collect the required information from its employees and to then forward this information on to the overseas entity, with minimal wording in the plan documentation and no additional privacy processes or policy in place in respect of the personal information provided by the employees.

This approach is based on the "*employee records*" exemption under the *Privacy Act* (which is continued, for the time being, under the revised law from 12 March 2014), whereby employment related personal information collected and disclosed by an employer from/about its employee for employment–related purposes is exempt from the provisions of the *Privacy Act*. However, there are concerns as to whether employees' personal information collected in connection with overseas Plans are for an employment related activity of the employer. Certainly, the exemption does not apply where the overseas entity collects this information directly. In practice, these possible problems are currently often overlooked.

From 12 March 2014, however, there will be a significantly increased focus on "black letter" compliance with the *Privacy Act* and APPs and any privacy "workarounds" in place or shortcomings previously overlooked will now need to be revisited.

WHAT ARE THE MAIN CHANGES THAT OVERSEAS ENTITIES THAT OPERATE PLANS NEED TO PREPARE FOR?

While the APPs in many ways mirror the current NPPs, there are some changes introduced by the amendment to the *Privacy Act* and the new APPs including, most relevantly for overseas entities offering Plans into Australia:

1. New requirements to actively maintain and notify a privacy policy and to ensure compliance (no more set and forget)

Businesses are required to manage personal information in an open and transparent way under the APPs and to notify those whose personal information they collect of a number of mandatory matters (usually contained in a privacy policy). This is similar to the current NPPs relating to "openness", but the APPs go into considerably more detail about the specific requirements that organisations must satisfy.

A business must have a clearly expressed and up–to–date privacy policy. That is, a "living document" that is reviewed and updated regularly and contains information about:

- the kinds of personal information the business collects and the purpose(s) for which it collects the information (and how it collects and holds that information);
- how an individual can access his/her personal information held by the business (and how they can have the information corrected, if necessary);
- whether the business is likely to disclose personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located (and whether such countries have appropriate privacy protections); and
- how the individual may complain about a breach of the APPs (and what the business will do to address such complaints).

Businesses also need to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs.

The APPs will require overseas entities operating Plans that collect personal information directly from Australian employees to (i) have an APP (ie Australian) compliant privacy policy and (ii) notify that privacy policy to the Australian employees prior to or at the time of collecting their information.

2. Cross-border data transfers (continuing liability for offshore incidents)

In a change from the current NPPs, the APPs generally permit cross–border disclosure of personal information, if reasonable steps are taken to ensure the overseas recipient will comply with the APPs. However, if a business discloses personal information to an overseas recipient it will remain liable for any breaches of the APPs by the overseas recipient of that information (as if the sending organisation itself had committed those breaches).

Businesses can minimise this continuing liability for personal information sent out of Australia by obtaining the individual's "informed consent" to disclose his/her personal information to an overseas recipient. However, the current wording that most organisations use to allow cross–border transfers will not comply with the new requirements of the APPs.

This will be relevant to overseas entities who directly collect and further disclose the information of the Australian employees (eg to a third party service provider). It will also be relevant to the Australian subsidiary employer which collects this personal information and then discloses/transfers it to its overseas parent entity.

3. Re-invigorated focus on obligations and enforcement (current practical "workarounds" need to be reconsidered)

As indicated above, overseas entities that offer Australian employees the ability to participate in a Plan must reconsider any practical privacy workarounds currently in place. Where the overseas entity collects the information directly from the Australian employee it will be subject to the *Privacy Act*, as amended, and the APPs and is required to appropriately notify (ie of an Australian compliant privacy policy) to and obtain any relevant consents (in particular where sensitive information is collected) from the Australian employees. It will also need to ensure that it and its processes comply with the APPs in terms of their collection, holding, use and disclosure of the personal information it collects from the Australian employees.

In addition, where the overseas entity collects the information via its local subsidiary that employs the Australian employees, we caution that this approach will need to be reconsidered in each specific circumstance to ensure that processes are implemented by the Australian subsidiary in order to benefit from the employee records exemption, if applicable.

WHAT THOSE OVERSEAS ENTITIES THAT OPERATE PLANS CAN DO NOW!

While the amendments to the *Privacy Act* and the new APPs do not become effective and applicable until 12 March 2014, we recommend that those overseas entities that offer Plans into Australia consider their relevant documentation, processes and privacy policies now. This is to ensure that all required changes (including revised processes, new wording and an Australian–compliant privacy policy for the overseas entity, where relevant) are put in place well before 12 March 2014 to avoid a rushed response in February/March 2014 for Plans in respect of which personal information is to be collected from Australian employees after 12 March 2014.

The main steps that overseas entities that operate Plans should be taking now include:

(i) examining and determining in respect of their Australian employees:

- what personal information needs to be collected, how it will be collected (and from whom – the individual or the local group entity) and the purpose(s) for which the information is being collected;
- whether their current privacy policy and the processes for notifying it/obtaining any required consents comply with the APPs; and

- whether their current internal practices with respect to the handling of that personal information (including security measures) are compliant with the APPs; and

(ii) implementing APP compliant processes, policies and documentation/relevant clauses for Plan documentation to address the findings from the gap analysis resulting from (i) above.

MORE INFORMATION

Please do not hesitate to contact Alec Christie or one of our dedicated privacy team if we can assist with the review of the wording in your current documentation, audit your current procedures and privacy policy or if you require assistance to ensure compliance with the new privacy regime effective from 12 March 2014.

Separately, if you require advice with respect to making of an offer of securities to Australian employees, please contact David Morris or Nicole Sloggett.

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

David Morris
Partner
T +61 2 9286 8371
david.p.morris@dlapiper.com

Nicole Sloggett
Senior Associate
T +61 2 9286 8528
nicole.sloggett@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

1201679720/JPS/102013