PLN Australia
Pacific Legal Network

Australian Privacy Law Update: your obligations when sending information across borders further clarified under revised APP Guidelines

Written by John Ridgway
15/05/2015

In March 2014, the Australian Government streamlined Australian Privacy law introducing the new Privacy Regulation 2013(Regulations) under the amended Privacy Act 1988 (**Privacy Act**). The Regulations applied a new principles-based approach to protecting the personal information of Australians, including the introduction of 13 new Australian Privacy Principles (**APPs**).[1]

The revised APP Guidelines (Guidelines) released on 1 April 2015 by the Office of the Australian Information Commissioner (**OAIC**) clarify some of the ambiguity in the application of the APPs. In particular, the Guidelines clarify those matters the OAIC will take into consideration when exercising its powers to enforce the APPs and Regulations and provide examples of the APPs in action.

Are you sending information collected in Australia overseas?

If you are a business operating in Australia and you send personal information overseas for purposes including cloud-based storage, payment facilitation, processing, or service delivery, APP 8 is likely to apply to you.

The key obligations under APP 8 are:

- you must take *"reasonable steps to ensure that the overseas recipient does not breach the APPs"*; and
- you *remain accountable* for any acts or practices of that overseas recipient regarding any break of the APPs.

There are exceptions to these requirements which were clarified by the Guidelines (see a further discussion below).

Is it 'use' by or 'disclosure' to a third party?

It is 'disclosure', not 'use', that is regulated under APP 8; however, 'disclosure' and 'use' are not defined under the Privacy Act or Regulations and this leads to some confusion.

The Guidelines suggest that a ***disclosure*** occurs when an APP entity makes personal information accessible or visible to others **and releases** the subsequent handling of the personal

information **from its effective control**. This focuses on the act done by the disclosing party, not the actions or knowledge of the recipient. This will occur in most contracting relationships.

Some common examples of disclosure are:

- An Australian based retailer outsourcing the payment processing (and therefore collection of customer's personal information) of goods or services ordered though their website to an overseas contractor;
- Outsourcing reference checks, as part of a recruitment drive, by providing applicant's personal information to overseas business; and
- Reliance on international parent companies to provide technical and billing support which requires access to an Australian customer database (including personal information)

By contrast, an APP entity uses personal information when it handles and manages personal information **within its effective control**. For example, where an entity provides personal information to an overseas recipient, via a server in a different overseas location, a disclosure would not usually occur until the personal information has reached the overseas recipient.

What is good practice to comply with APP 8?

The Regulations require "reasonable steps" to be taken by an Australian business if it is disclosing personal information overseas. The Guidelines provide that the reasonable steps to be taken will depend upon factors such as:

- The sensitivity of the information being disclosed;
- The nature of the relationship between your business and who you are disclosing to;
- The nature of the potential adverse consequences for the individual whose personal information may be mishandled;
- The operational safeguards implements by your contractor; and
- The practicability of measures required to be implemented (especially time and cost).

In most situations the OAIC would expect an enforceable contract between your business and your overseas contractor to include:

- **What** type of personal information you be disclosing and the **purpose** for which it will be disclosed;
- A requirement that you **contractor comply with the APPs** (including by imposing similar standards on any third party sub-contractors);
- The implementation of a **complaint handling process**; and
- A **data breach response plan**.

What about the exceptions to taking ''reasonable steps''?

One key exception to taking reasonable steps to ensure personal information disclosed to overseas contractors is protected is if there is a **substantially similar law** or binding scheme in the country of receipt. The OAIC is responsible for determining whether there is a "reasonable basis for believing that the law is substantially similar." The OAIC will apply a rigorous threshold for being "substantially similar" and will expect a privacy or data protection law, or binding, enforceable industry standard. Therefore this exception should be applied with caution.

Another exception is where personal information is disclosed after the individual is expressly informed and consents to the disclosure. In accordance with the Guidelines, there must be a clear written or oral statement explaining that your business:

- Will not be accountable under the Privacy Act; and
- The individual will not be able to seek redress under the Privacy Act.

However, the statement must be made at the time consent is sought; your business cannot rely on any prior knowledge of the individual and you must explain the practical effects and risks associated with the disclosure.

Are you a foreign company with an Australia link?

Where previously, the privacy legislation simply prohibited trans-national disclosure, the APPs now regulate businesses with an "Australian link". An Australian link includes where an organisation carries on business in Australia; and collects or holds personal information in Australia.

This includes where you:

- Have a place of business in Australia;
- Have an agent acting on its behalf in Australia;
- Australia is one of the countries on the drop down menu appearing on the entity's website;
- Web content that forms part of carrying on the business, was uploaded by or on behalf of the entity, in Australia;
- Business or purchase orders are assessed or acted upon in Australia; and
- The entity is the registered proprietor of trademarks in Australia.

If you satisfy these definitions, the full complement of APPs will apply to your operations to protect the privacy of Australian individual's personal information.

What should you do?

Ensuring that you protect your business from potential risks from overseas contractors through carefully drafted contracts is paramount. As these guidelines and responsibilities apply from March 2014, it is also important to review the terms of existing key contracts that involve the disclosure of personal information.

[1] The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

Contact

For more information please contact:

John Ridgway
Head of Legal Services
T +61 410 520 416
E j.ridgway@pln.com.au