

SEMINAR MATERIALS

Privacy Act reforms: from the NPPs to the APPs

Assessing the impact on the private sector

July 2010

PRESENTER

Jeremy Douglas-Stewart
LLB (Hons), BEc, BA

Principal Consultant
Privacy Law Consulting Australia

PRESIDIAN
LEGAL PUBLICATIONS

Disclaimer

The seminar, these seminar materials and comments by the seminar presenter are not intended to be, nor do they constitute, legal advice. Whilst the seminar and seminar materials aim to provide detailed information on privacy laws, certain issues may have been omitted and statutory provisions not addressed in order to fit within seminar delivery time-frames. Likewise, explanations provide generalised summaries of the law and, as such, do not constitute comprehensive or exhaustive statements of the law. You should seek legal and/or other professional advice, as appropriate, based on your specific circumstances before acting or relying on any of the contents of the seminar, seminar materials and/or comments of the seminar presenter.

Copyright

All legislative materials herein are reproduced by permission but do not purport to be the official or authorised versions. They are subject to Commonwealth of Australia copyright.

Copyright in this publication, excluding that relating to legislation, is owned and/or administered by Presidian Legal Publications. For reproduction or publication beyond that permitted by the *Copyright Act 1968*, permission should be sought in writing and addressed to the Copyright Officer.

© Presidian Legal Publications, Adelaide, 2010
All rights reserved

Publisher details

61 Carrington St, Adelaide
GPO Box 625 Adelaide SA 5001
DX 175 Adelaide
tel 1300 66 13 96
fax (08) 8278 9382

CONTENTS

Introduction	4
Australian Privacy Principles	7
APP 1—open and transparent management of personal information	7
APP 2—anonymity and pseudonymity	9
APP 3—collection of solicited personal information	10
APP 4—receiving unsolicited personal information	13
APP 5—notification of the collection of personal information	14
APP 6—use or disclosure of personal information	15
APP 7—direct marketing	19
APP 8—cross-border disclosure of personal information	24
APP 9—adoption, use or disclosure of government related identifiers	28
APP 10—quality of personal information	30
APP 11—security of personal information	31
APP 12—access to personal information	31
APP 13—correction of personal information	34

Australian Privacy Law Handbook

by J Douglas-Stewart (forthcoming release: September 2010)

This publication provides a detailed guide to privacy law and practice in the private and public (federal and ACT) sectors. Written in a plain-English style for privacy officers, records managers and lawyers, the text is designed to enable users to readily identify privacy obligations and to apply the laws in practice.

Practical commentary provides guidance on how privacy laws apply in the context of specific activities, ranging from core issues such as disclosing information to third parties, dealing with contractors and handling information during recruitment to peripheral issues such as disclosing health information for medical research and dealing with children.

The text includes extensive commentary and tools to assist in developing compliance measures, such as privacy policies, collection notices, consent forms, step-by-step guides and guidance on conducting privacy audits and privacy impact assessments.

The publication is updated three times per year. Each update is accompanied by an *Australian Privacy Law Bulletin* providing a report on privacy developments.

For further information, go to: www.presidian.com.au/aplh.html

To request notification of release, send a blank email to notify@presidian.com.au with "APLH" in the subject line.



PRESIDIAN
LEGAL PUBLICATIONS

Introduction

The seminar provides a detailed overview of proposed changes to the *Privacy Act 1988* (Cth) following the release of the Government's exposure draft legislation (on 24 June 2010) setting out the Australian Privacy Principles (APPs) which are to replace the private sector National Privacy Principles (NPPs) (as well as the public sector Information Privacy Principles (IPPs)).

The seminar aims to:

- provide an overview of the proposed APPs;
- undertake a gap analysis between the APPs and NPPs identifying:
 - APP obligations that are the same as, or similar to, existing NPP obligations;
 - new obligations under the APPs;
- assess the impact of the new obligations (based on the level of existing obligations);
- provide insight into how the new obligations may apply in practice;
- provide an overview of other proposed changes to the Act.

The seminar is based on an assumed familiarity with the NPPs.

Overview of Privacy Act reforms

The Government has opted to implement its reforms to the Privacy Act over two stages.

Stage one

The exposure draft legislation constitutes the first part of the Government's reforms to the Privacy Act. It has been over 20 years since the Act was originally drafted and the Government is seeking to ensure the Act remains appropriate and relevant to business practices and consumer expectations in the 21st Century. Each subsequent part of the reforms will be referred to a Senate Committee for consideration. The Government anticipates that there will be three other parts referred to the Committee as part of the "stage one" reforms. These will address:

- credit reporting – this will replace Part IIIA of the existing Act;
- the handing of health information – currently, many provisions providing for specific regulation of dealings with health information are contained in the NPPs and IPPs. These provisions do not currently appear in the APPs as the Government has not yet decided on the best location for them in the new Act;
- reforms to the functions and powers of the Office of the Privacy Commissioner (with the existing office to become part of a new Office of the Australian Information Commissioner following the commencement of the *Freedom of Information (Reform) Act 2010* and the *Australian Information Commissioner Act 2010* principally on 1 November 2010).

Once the Senate Committee has reported on all of the parts, the Government has stated that the Bill will be consolidated and introduced into Parliament.

The Senate Committee is due to report:

- on the APP exposure draft legislation by 21 September 2010; and
- on all exposure drafts of Australian privacy amendment legislation by 1 July 2011.

Stage two

The Government has indicated that its second stage of reforms will address:

- proposals to clarify or remove certain exemptions from the Privacy Act (eg exemptions for small businesses, employee records and media organisations);
- the possible introduction of a statutory cause of action for serious invasion of privacy;
- serious data breach notifications;
- privacy and decision making issues for children and authorised representatives;

- handling of personal information under the *Telecommunications Act 1997*; and
- national harmonisation of privacy laws (partially considered in stage one).

The Government has not, however, set a time-frame within which these matters will be addressed.

Additional sources of regulation – regulations, rules, guidelines and privacy codes

The draft legislation envisages the following sources of additional regulation:

- Australian Privacy Rules (s 21) – these will be binding rules made by the Australian Information Commissioner. It is currently envisaged that these will apply in relation to:
 - APP 3(3)(g)(ii) regarding a collection to assist in locating a missing person; and
 - APP 6(2)(g)(ii) regarding a use or disclosure to assist in locating a missing person;
- regulations (s 22);
- non-binding Guidelines – these will be made by the Australian Information Commissioner; and
- privacy codes – which enable organisations to draft their own privacy codes that, once approved, will become legally binding in place of the APPs (although there has been a very limited uptake of these codes under the existing Act).

Terminology – “entity”, “organisation” and “agency”

The APPs refer to “entities” to capture both organisations and agencies. Some of the APPs, however, refer specifically to organisations or agencies where there are different provisions applying to each type of entity.

Coverage of the Act

At this stage, the Government is not proposing to make any significant changes to the coverage of the Act. In particular:

- the definition of “personal information” will effectively remain the same;
- the requirement that information must be held in a record for the Act to apply (s 16B) will remain;
- key exemptions will remain, including those relating to:
 - small business operators (ss 6D-6EA);
 - personal, family and household affairs (s 16E);
 - emergencies and disasters (Part VIA).

As noted above, the Government proposes to clarify or remove certain exemptions from the Privacy Act in “stage two” of the reforms.

In regards to extra-territorial operation, the Act currently applies to an act or practice engaged in outside of Australia where:

- it is engaged in by an organisation (but not by an agency); and
- the act or practice relates to information about an Australian citizen or permanent resident.

Under the proposed changes, the Act will apply to an act or practice engaged in outside Australia where:

- it is engaged in by an organisation *or* an agency; and
- the act relates to information about any person (ie including a foreigner) provided the entity that is dealing with the information has an Australian link (as defined by s 19(3)).

In practice, this extension in coverage is likely to have little impact for most organisations. For those that do have overseas operations, many are likely to already handle personal information about foreigners in the same way as information about Australian citizens and permanent residents.

Summary of key new obligations

The reforms to the Privacy Act will require all organisations that are bound by it to review their information handling practices to ensure compliance with the new requirements.

Key reforms relate to:

- privacy notices, requiring the inclusion of additional information, including about third party collections and overseas disclosures;
- privacy policies, requiring the inclusion of specific information, including about overseas disclosures;
- use and disclosure of personal information for direct marketing, including the provision of opt-out facilities;
- overseas disclosures, whereby organisations will be liable for breaches of the APPs by an overseas recipient;
- collection and handling of unsolicited information;
- correction of information;
- obligations to ensure activities and decisions are not based on irrelevant information;
- express obligations to implement compliance programs.

Comparative table of APPs and NPPs

APPs	NPPs
APP 1 – open and transparent management of personal information	NPP 1 – Collection
APP 2 – anonymity and pseudonymity	NPP 2 – use and disclosure
APP 3 – collection of solicited personal information	NPP 3 – data quality
APP 4 – receiving unsolicited personal information	NPP 4 – data security
APP 5 – notification of the collection of personal information	NPP 5 – openness
APP 6 – use or disclosure of personal information	NPP 6 – access and correction
APP 7 – direct marketing	NPP 7 – identifiers
APP 8 – cross-border disclosure of personal information	NPP 8 – anonymity
APP 9 – adoption, use or disclosure of government related identifiers	NPP 9 – transborder data flows
APP 10 – quality of personal information	NPP 10 – sensitive information
APP 11 – security of personal information	
APP 12 – access to personal information	
APP 13 – correction of personal information	

Australian Privacy Principles

APP 1—open and transparent management of personal information

- (1) The object of this principle is to ensure that entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

- (2) An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that:
- (a) will ensure that the entity complies with the Australian Privacy Principles; and
 - (b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles.

Purpose (APP 1(2))

The Government's *Companion Guide – Australian Privacy Principles* (June 2010) outlines the purpose of APP 1 as follows (at 9):

The requirement for open and transparent management ... will emphasise that entities should first plan *how* they will handle personal information before they collect and process it.

The principle is also intended to outline that part of complying with the Australian Privacy Principles is making sure that entities consider their privacy obligations when planning new systems.

This is part of international moves towards a “privacy by design” approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception. (emphasis in original)

Accordingly, APP 1(2) aims to ensure that entities take a *proactive* approach to privacy compliance (ie foreseeing privacy risks and putting systems in place to avoid such risks eventuating), rather than a *reactive* one (eg resolving privacy issues and complaints as they arise, resulting in privacy policies and procedures being developed piecemeal).

Equivalent NPPs

Obligations under APP 1(2) have no express equivalent under the NPPs (although such obligations are, to a large extent, implicit).

Impact of changes (APP 1(2))

Level of impact: medium

(i) *Measures to ensure compliance (APP 1(2)(a))*

Whilst the NPPs do not contain an express requirement that an organisation must take reasonable steps to implement practices, procedures and systems to ensure compliance with the NPPs, many organisations already have in place such measures as part of their privacy compliance regimes. For such organisations, APP 1(2)(a) will have little impact as it is merely formalising practical measures already implemented.

However, APP 1(2)(a) will have ramifications for organisations that have *not* adopted practices, procedures and systems to ensure compliance where it would be reasonable for them to do so. Organisations that fall within this category may include:

- medium size businesses;
- small businesses (with a turnover of less than \$3m) that trade in personal information;
- small health service providers (eg medical centres); and
- large organisations which:
 - have adopted a risk-management strategy to address privacy issues as they arise; or

- have opted not to invest resources in developing privacy compliance regimes based on a view that privacy is not a sufficiently relevant compliance issue for their organisation to warrant the expenditure.

Such organisations will need to:

- consider whether it is reasonable for them to adopt practices, procedures and systems to ensure compliance (in view of factors such as the sensitivity of information held and cost); and
- if so – develop and maintain them.

(ii) “Deal with inquiries” about compliance (APP 1(2)(b))

The obligation under APP 1(2)(b) to have in place practices, procedures and systems to enable an entity “to deal with inquiries” regarding compliance with the APPs has the *potential* to be significant, including for large organisations with well established privacy regimes. Similar obligations exist under NPP 5 (“Openness”) which requires an organisation to be open and transparent regarding what types of personal information it holds and how it is handled. However, APP 1(2)(b) has a slightly different focus; namely, on enquiries regarding compliance, as opposed to types of information held and how such information is handled.

In effect, APP 1(2)(b) will require organisations to have in place practices and procedures that require staff to respond in an appropriate way to privacy enquiries. Depending on the circumstances, it may be “reasonable” to “deal with inquiries” by providing customers with a copy of the organisation’s privacy policy (assuming it is sufficiently detailed and accurate to address the issues raised). In other instances, it may require more onerous steps, such as requiring the relevant staff to refer the enquiry to a manager or Privacy Officer who can provide an informed and considered explanation in response to the specific issues raised.

The type of scenario that is likely trying to be avoided under APP 1(2)(b) is where a customer raises a legitimate privacy issue, for example, with a customer services officer when completing an application form (eg “Why are you asking for this information?” or “Who will this information be disclosed to?”) and the customer service officer in effect provides a response that avoids or deflects the question (eg “Don’t worry. Information is treated confidentially and we won’t disclose it to anyone”, even though this is not correct, or “There is nothing to be concerned about – we comply with privacy laws.”). Responses such as these would not appear to meet APP 1(2)(b) requirements to have systems in place to enable the organisation “to deal with inquiries or complaints”.

Privacy policy

- (3) An entity must have a clearly expressed and up-to-date policy (the **privacy policy**) about the management of personal information by the entity.
- (4) Without limiting subsection (3), the privacy policy must contain the following information:
 - (a) the kinds of personal information that the entity collects and holds;
 - (b) how the entity collects and holds personal information;
 - (c) the purposes for which the entity collects, holds, uses and discloses personal information;
 - (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
 - (e) how an individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;
 - (f) whether the entity is likely to disclose personal information to overseas recipients;
 - (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the privacy policy.

Equivalent NPPs (APP 1(3) and (4))

APP 1(3) reflects obligations under NPP 5 (“Openness”) which in effect requires organisations to have a privacy policy. However, NPP 5 merely requires an organisation to set out in the policy its “policies

on its management of personal information”. APP 1(3) goes further by stating specific types of information that must be included in the privacy policy and, as such, is significantly more prescriptive.

“Overseas recipients” (APP 1(4)(f))

A disclosure to an overseas recipient will, in addition to including a transfer of information to a person overseas, also encompass circumstances where information that is stored in Australia (eg on a network) is accessed by someone overseas.

Impact of changes (APP 1(3) and (4))

Level of impact: medium.

Organisations will need to redraft their privacy policies to ensure they meet the requirements of APP 1(3).

The types of information referred to in APP 1(4)(a)-(e) are commonly included in privacy policies and can be readily inserted into existing policies if not already included.

In regards to APP 1(4)(f) and (g), regarding disclosures to overseas recipients, organisations will need to review the circumstances in which they are likely to disclose information to persons in other countries. However, more importantly (and this is likely to be of concern to some organisations), organisations will be required to state information which, in effect, could reveal information about their operational arrangements and inner-workings (in particular, their outsourcing practices and location of foreign service providers) which they may consider to be commercially confidential information.

For example, many organisations that engage in business process outsourcing to overseas firms (eg outsourcing back-office functions, such as accounts or dictation transcription, or front-office functions, such as call centre operations) take steps to ensure that information about such practices is not publicly available. In view of the need to disclose such information, the impact of the obligations for such organisations will be significant.

The notification obligations are, however, relatively limited as they only relate to whether information is disclosed to persons overseas and the country of the recipients. They do not, for example, require an organisation to state the name of the recipient, the purpose for which the information is disclosed or the nature of the activities of, or goods or services provided by, the recipient.

Availability of privacy policy etc.

- (5) An entity must take such steps as are reasonable in the circumstances to make its privacy policy available:
 - (a) free of charge; and
 - (b) in such form as is appropriate.
- (6) If an individual requests a copy of an entity’s privacy policy in a particular form, the entity must take such steps as are reasonable in the circumstances to give the individual a copy in that form.

Form of privacy policy (APP 1(6))

Ideally, guidance from the Privacy Commissioner will clarify whether it will be sufficient in all cases for organisations to make privacy policies available in electronic and, if appropriate, hardcopy formats. If not, organisations may also need to make privacy policies available in alternative formats where it is reasonable to do so – for example, by providing a verbal explanation for a blind person.

APP 2—anonymity and pseudonymity

- (1) Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.

SAMPLE ONLY



Pages 10-23 are not part of this sample.

APP 8—cross-border disclosure of personal information

- (1) Before an entity discloses personal information about an individual to a person (the *overseas recipient*):
- (a) who is not in Australia; and
 - (b) who is not the entity or the individual;
- the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.
- (2) Subsection (1) does not apply to the disclosure of personal information about an individual (the *affected individual*) by an entity to the overseas recipient if:
- (a) the entity reasonably believes that:
 - (i) the overseas recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
 - (ii) there are mechanisms that the affected individual can access to take action to enforce that protection of the law or binding scheme; or
 - (b) both of the following apply:
 - (i) the entity expressly informs the affected individual that if he or she consents to the disclosure of the information, subsection (1) will not apply to the disclosure;
 - (ii) after being so informed, the affected individual consents to the disclosure; or
 - (c) the disclosure of the information is required or authorised by or under an Australian law, or an order of a court or tribunal; or
 - (d) each of the following applies:
 - (i) the entity is an agency;
 - (ii) the disclosure of the information is required or authorised by or under an international agreement relating to information sharing;
 - (iii) Australia is a party to the international agreement; or
 - (e) both of the following apply:
 - (i) the entity reasonably believes that the disclosure of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
 - (ii) it is unreasonable or impracticable to obtain the affected individual's consent to the disclosure; or
 - (f) both of the following apply:
 - (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
 - (ii) the entity reasonably believes that the disclosure of the information is necessary for the entity to take appropriate action in relation to the matter; or
 - (g) each of the following applies:
 - (i) the entity is an agency;
 - (ii) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities by, or on behalf of, an enforcement body;
 - (iii) the overseas recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body; or
 - (h) both of the following apply:
 - (i) the entity is an agency;
 - (ii) the entity reasonably believes that the disclosure of the information is necessary for the entity's diplomatic or consular functions or activities; or

- (i) the entity is the Defence Force and the entity reasonably believes that the disclosure of the information is necessary for any of the following occurring outside Australia:
- (i) war or warlike operations;
 - (ii) peacekeeping or peace enforcement;
 - (iii) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

Equivalent NPPs

NPP 9 (“Transborder data flows”) regulates transfers of personal information to persons overseas. Broadly speaking, the requirements under APP 8 reflect those under NPP 9, although there are significant differences between the two principles.

Additional obligations

A key difference between APP 8 and NPP 9 is that APP 8 applies to *disclosures* to persons overseas whereas NPP 9 applies to *transfers* of information to persons overseas. The Government adopts the view that the former is broader as, in addition to encompassing transfers of information to persons overseas, it also includes circumstances where information that is stored in Australia (eg on a network) is accessed by (ie disclosed to) a person overseas.

Other significant differences between APP 8 and NPP 9 are addressed below.

Reasonable steps to ensure recipient complies with APPs (APP 8(1))

An organisation will be permitted to make a disclosure to an overseas recipient where it takes reasonable steps in the circumstances to ensure that the recipient does not breach the APPs in relation to the information.

What constitutes “reasonable steps” will depend on the circumstances. Contractual measures are likely to be a primary method through which such steps will be taken, either by:

- requiring the recipient to comply with the APPs as though it were bound by them; or
- by stating the specific standards and privacy protections that are required to be met and implemented in relation to each phase of the information handling process to ensure APP obligations are fulfilled (eg by stating the purposes for which the information may be used, prohibiting any disclosure, specifying security requirements, requiring destruction of records following completion of services, including powers to conduct on-site audits of information handling practices etc).

Whether a general contractual provision of the former type would be sufficient to amount to “reasonable steps” is unclear. In relation to public sector agencies’ obligations under s 95B of the *Privacy Act 1988* to take contractual measures to ensure contractors do not engage in an act or practice that would breach the APPs if it were engaged in by the relevant agency, the Privacy Commissioner has indicated that a general contractual term of this nature would not be sufficient to meet s 95B requirements (see the Commissioner’s *Private Sector Information Sheet 14 – Privacy Obligations for Commonwealth Contracts* (2001) at p 4).

By virtue of APP 8(1)(b), APP 8 does not place any restrictions on disclosures by an organisation to the individual concerned or to overseas divisions of the same organisation (ie the same legal entity). This will permit, for example, an Australian company to enable an employee on assignment in another country to access personal information on the company’s network. It would not, however, permit the company to disclose the information to a sister corporation (owned by the same parent company) in another country since, whilst the information would remain with the relevant corporate group, it would result in a disclosure of the information to a separate legal entity.

An entity is not required to take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information if one of the exceptions under APP 8(2) applies. The exceptions under APP 8(2)(a) and (b) are likely to be the two most commonly relied upon by organisations.

Liability for breach by overseas recipient (APP 8(1) and s 20)

Where an entity discloses personal information to a person outside Australia pursuant to APP 8(1), proposed new s 20 of the Act (“Acts and practices of overseas recipients of personal information”) provides that if the recipient engages in an act or practice that would breach the APPs if it were bound by them, the recipient’s act or practice will be deemed to have been engaged in by the organisation. Accordingly, the organisation will be potentially liable for the recipient’s breach. There is no equivalent provision extending liability in this way under the NPPs or other existing provisions of the Act.

An entity will not be liable for a breach by an overseas recipient where the relevant disclosure was made pursuant to an exception under APP 8(2). Accordingly, there will be a *strong* incentive for organisations to avoid reliance on APP 8(1) by ensuring overseas disclosures fall within the ambit of APP 8(2).

Law/binding scheme substantially similar to APPs and enforceable by individual (APP 8(2)(a))

The exemption under APP 8(2)(a) is similar to that under NPP 9(a) which requires the relevant organisation to reasonably believe that the recipient is subject to a law, binding scheme or contract which effectively upholds principles substantially similar to the NPPs.

APP 8(2)(a) refers to a law or scheme that is at least “substantially similar”. The Government’s *Companion Guide – Australian Privacy Principles* (June 2010) states (at 13):

This means that the level of protection must be substantially similar, or provide a higher level of protection, when considered against the overall level of protection offered by the Australian Privacy Principles. It is not intended that each Australian Privacy Principle should be replicated.

APP 8(2)(a) refers only to a law or binding scheme that imposes standards substantially similar to the APPs – unlike NPP 9(a), it makes no reference to a “contract”. Accordingly, organisations will no longer be able to rely on contractual provisions to impose appropriate standards of protection in order to permit an overseas disclosure.

Further, APP 8(2)(a)(ii) adds a significant additional requirement – namely, that there be mechanisms that the individual concerned can access to enforce that protection of the law or binding scheme. The Government’s *Companion Guide* provides (at 13) “[f]or these purposes ‘binding scheme’ is intended to ... include self-regulatory or other international arrangements that provide the necessary level of protection”.

Among other things, whether, for example, an Australian can enforce the law or scheme will depend on its extra-territorial application (eg how it applies in relation to foreigners and whether foreigners have rights to lodge complaints under it).

In regards to APP 8(2) requirements, ideally, the Privacy Commissioner would publish a list of countries that have laws and enforcement mechanisms that meet the requirements of APP 8(2)(a)(i) and (ii). In the absence of any such guidance, organisations will generally need to seek professional advice on a case-by-case basis before disclosing personal information to a person in another country for the first time.

Notification that APP 8(1) will not apply and consent (APP 8(2)(b))

APP 8(2)(b) provides that, if an organisation obtains consent to the relevant disclosure and, before doing so, notifies the individual that APP 8(1) will not apply (ie that providing consent will mean that the organisation will not be required to take reasonable steps to ensure the recipient does not breach the APPs in relation to the information), it is permitted to make the disclosure.

Accordingly, organisations will be able to ensure the applicability of APP 8(2)(b) by amending their privacy collection notices and consent forms to meet the relevant requirements.

SAMPLE ONLY



Pages 27-36 are not part of this sample.