Office of the Victorian Information Commissioner

IPP 9 – Transborder Data Flows

IPP 9 – Transborder Data Flows

On this page

9.1 The purpose of IPP 9 is to ensure that when personal information travels outside Victoria it remains subject to privacy protections.

9.2 IPP 9.1 says:

> An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if—
>
> a. the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or
> b. the individual consents to the transfer; or
> c. the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of precontractual measures taken in response to the individual's request; or
> d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
> e. all of the following apply—
> i. the transfer is for the benefit of the individual;
> ii. it is impracticable to obtain the consent of the individual to that transfer;
> iii. if it were practicable to obtain that consent, the individual would be likely to give it; or
> f. the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the IPPs.

9.3 IPP 9.1(a) will usually allow organisations to transfer personal information across state borders within Australia. To comply with IPP 9, it will usually be enough for the transferring organisation to confirm that the recipient is subject to (and accepts that it is subject to) an Australian state, territory, or Commonwealth privacy law listed in **Figure 1** below.

9.4 If the recipient is *not* subject to one of those laws or some other binding scheme or contract that imposes protections equivalent to the IPPs (for example, Western Australia), then IPP 9.1(b) – (f) must apply before the transfer can occur.

9.5 Any Victorian laws that require transborder transfers of personal information will override IPP 9 to the extent of any inconsistency.[1] Commonwealth laws may also prevail over the PDP Act. For example, mutual assistance laws may provide an alternative mechanism for authorising international data transfers relating to criminal investigations and prosecutions, and recovery of the proceeds of crime.[2]

9.6 Exemptions in the PDP Act may also allow IPP 9 to be disregarded, for example where police

[1] PDP Act, s 6(1).
[2] For information on the operation of mutual assistance laws, see the Fact Sheets, key legislation and other related documents available from
the Commonwealth Attorney-General's Department's website.

reasonably believe it is necessary not to comply with IPP 9 for particular law enforcement activities or where courts or tribunals are carrying out their judicial or quasi-judicial functions.[3]

9.7 This chapter of the Guidelines discusses common circumstances where IPP 9 issues can arise, followed by a description of each of the grounds permitting transborder disclosure in IPP 9.1(a) – (f).

Common issues involving IPP 9

Cloud services and external digital service providers

9.8 Victorian public sector organisations often use service providers that store or process information 'in the cloud' in data centres located interstate or overseas. These providers can offer different services or lower prices than equivalent providers that operate solely in Victoria.

9.9 Where organisations send personal information to a provider that stores or processes information outside Victoria, this is a transborder transfer of personal information. The sending organisation must be able to rely on one of the grounds in IPP 9.1(a) – (f), for example:

- IPP 9.1(a) – if the organisation reasonable believes the cloud service provider is subject to a substantially similar law, binding scheme or contract. This exception can apply if the recipient only stores data in a jurisdiction with equivalent privacy law, or if the recipient is a contracted service provider required to comply with the IPPs by contract and s 17 of the PDP Act.
- IPP 9.1(b) – if the organisation seeks individuals' consent for the transfer of their personal information to the cloud provider.
- IPP 9.1(f) – if the organisation can demonstrate they took reasonable steps to ensure information transferred to the cloud provider will not be held, used or disclosed inconsistently with the IPPs. Reasonable steps could include contractual or technical measures (see Case Study 9A below).

9.10 If none of the grounds in IPP 9.1 apply for a proposed transfer of information outside Victoria to a cloud service provider, then the transfer is prohibited by IPP 9. A different provider must be selected.

Case Study 9A: Using a cloud service provider in compliance with IPP 9

Organisation X is looking to use a cloud provider (CP) to store bulk data backups (including personal information).

CP is a large multinational company providing internet-based storage services. CP's standard term contract and privacy policy indicates that it stores data 'in the cloud'. It stores information in multiple countries, including the United States, which does not have privacy legislation equivalent to the PDP Act.

Organisation X considers each of the permitted grounds for transfer under IPP 9.1. Initially Organisation X considers adding terms to the contract with CP that will stipulate that CP only store its data in locations with PDP Act equivalent protections. If CP could have provided such a guarantee, Organisation X felt the transfer could be justified under IPP 9.1(a). It also considers asking CP to add a term to its contract binding CP to the IPPs. However, CP cannot guarantee the data will always be stored in such countries and refuses

[3] PDP Act, ss 10, 15, 18.

to negotiate or modify its standard terms.

Therefore, Organisation X needs to rely on one of the other exceptions in IPP 9. Consent is impractical. Organisation X decides that it will take steps to protect the personal information in the event that it is hosted in countries without substantially similar protections to the PDP Act, relying on IPP 9.1(f).

Organisation X completes a security risk assessment and privacy impact assessment for the transfer of data to CP. As a result of this assessment, it decides to encrypt all information before sending it to CP for storage and is satisfied that by encrypting the data to a sufficiently high standard, CP will not be able to access or share the personal information it is storing. Because Organisation X took reasonable steps to ensure the information cannot be used, held or disclosed in a manner inconsistent with the IPPs, it is permitted to transfer the information under IPP 9.1(f).

If Organisations X was unable to satisfy itself that one of the exceptions in IPP 9 applied, it could not use CP. It would instead need to identify a different provider that held its data in a jurisdiction with adequate privacy legislation or that would agree to be contractually bound to the IPPs or an equivalent scheme.

Outsourcing arrangements and contracted service providers

9.11 Where a Victorian government organisation outsources a function or service to a service provider outside Victoria, organisations may only transfer personal information to that service provider when one of the situations set out in IPP 9.1(a) – (f) applies.

9.12 Organisations should try to outsource functions and services and transfer personal information to contracted service providers (**CSPs**) that are bound to comply with the IPPs. A service provider is a CSP when the contract between it and the organisation includes a clause which binds the service provider to comply with the IPPs, under s 17 of the PDP Act.[4] If the CSP is bound to the IPPs, the transborder data flow will likely be permitted under IPP 9.1(a).

9.13 When organisations outsource digital services, they may use the eServices State contract[5] issued by the Victorian Government Purchasing Board. This standard State contract binds the 'Supplier' of the digital service – in other words, the recipient of the transborder data – to the IPPs.

Model Terms for Transborder Data Flows of Personal Information

9.14 Additionally, OVIC has issued Model Terms for Transborder Data Flows (**Model Terms**) which explain in detail what an organisation must do to adhere to the IPPs.

[4] PDP Act s 17(2) provides: 'A State contract may provide for the contracted service provider to be bound by the Information Privacy Principles and any applicable code of practice with respect to any act done, or practice engaged in, by the contracted service provider for the purposes of the State contract in the same way and to the same extent as the outsourcing party would have been bound by them in respect of that act or practice had it been directly done or engaged in by the outsourcing party.'

[5] The Victorian Government Purchasing Board provides standard purchase contracts for Government Owned Entities, Councils and Government Supported Organisation, available here.

9.15 The Model Terms might be used where the contractor is unfamiliar with the IPPs or a higher standard of privacy protection is required. While a simple clause that binds the recipient organisation to the IPPs under s 17 of the PDP Act will usually be sufficient to comply with IPP 9, more detailed contract terms will make it easier for the contractor to understand their IPP obligations.

9.16 The intention of the Model Terms is to impose a series of contractual obligations that is substantially similar to the IPPs. It outlines key obligations (which are based on those in the IPPs) with which the organisation must comply.

9.17 For example, the Model Terms include obligations for the recipient to notify the organisation of a security breach, and to not engage in data matching without the organisation's prior authority. Clauses like these protect an individual's privacy, promote clarity about what is (and is not) authorised by the contract, and help the organisation meet its other obligations (for example, under IPP 2 and IPP 4). Organisations are, of course, able to modify and adapt the Model Terms to fit their circumstances.

9.18 As noted above, agencies will often be able to meet the requirements of IPP 9 by imposing IPP obligations on their contractor through a clause giving effect to s 17 of the PDP Act. The Model Terms may be more appropriate where the organisation to which a service is being outsourced is unfamiliar with the IPPs, and a general clause imposing the IPPs won't communicate privacy compliance requirements clearly enough. The Model Terms provide a framework to ensure data handing and processing to be consistent with the IPPs, in language that is intended to be more easily understood by an audience not familiar with the IPPs.

Grounds under which personal information may be transferred

9.19 This section discusses each of the grounds on which personal information may be transferred outside Victoria, as set out in IPP 9.1(a) – (f). The different grounds of IPP 9.1 interact in different ways. Two or more might apply in the same situation. For example, IPP 9.1(a) and (f) commonly overlap. Consent (and implied consent), play a role in IPPs 9.1(b) and (c). IPP 9.1(d) and IPP 9.1(e) will require the organisation to anticipate either the interests of an individual or the likelihood the individual would give consent.

9.20 IPP 9.1(a) and (f) require the transfer be accompanied by privacy protections. In contrast, transfers under IPP 9.1(b) to (e) do not need to be accompanied by express privacy protections. However, transfers under IPP 9.1(b) to (e) must be in the interest, or for the benefit, of the individual.

IPP 9.1(a): Recipient bound by principles substantially similar to the IPPs

9.21 IPP 9.1(a) permits organisations to transfer data outside Victoria where they reasonably believe the recipient is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information that are substantially similar to the IPPs.

9.22 To comply with IPP 9, it will generally be sufficient for the transferring organisation to confirm that the recipient is subject to another state, territory, or Commonwealth privacy law that is equivalent to the IPPs with respect to the information that is being provided.

9.23 OVIC considers that the privacy laws in New Zealand and in most Australian states and territories are substantially similar to the IPPs, for the purpose of IPP 9.1(a). A list of states and territories with the protections available in each one is at **Figure 1**. Organisations will need to make their own assessment of the privacy laws that apply in other countries, and in Australian states that do not

have privacy legislation (Western Australia and South Australia) if they wish to transfer information relying on IPP 9.1(a).

Coverage

9.24 Organisations should check whether the proposed recipient is covered by a privacy law comparable to the PDP Act.

9.25 Not all Australian jurisdictions have privacy laws in force. In that regard, as at 19 September 2019:

- privacy laws exist in Victoria, New South Wales, the Northern Territory, Tasmania, Queensland, the Australian Capital Territory and the Commonwealth;[6]
- South Australia has adopted administrative privacy standards which have some application to South Australian public sector organisations; and
- Western Australia does not have a privacy law or administrative standards in place.

9.26 **Figure 1** is designed to help agencies identify the privacy laws in Australian jurisdictions. It also provides links to resources that will help agencies understand the coverage of those laws.

9.27 **Figure 2** provides information about privacy laws in international jurisdictions.

Figure 1: Australian Privacy Jurisdictions

	Privacy Laws or Standards	**Oversight Body**
VIC	*Privacy and Data Protection Act 2014* (Vic) Available here.	Office of the Victorian Information Commissioner (OVIC)
	Health Records Act 2001 (Vic) Available here.	Office of the Health Complaints Commissioner, Victoria (HCC)
NSW	*Privacy and Personal Information Protection Act 1998* (NSW) *Health Records and Information Privacy Act 2002* (NSW) Available here.	Information and Privacy Commission (IPC), New South Wales
QLD	*Information Privacy Act 2009* (Qld) Available here.	Office of the Information Commissioner (OIC), Queensland

[6] Health privacy laws have also been enacted in the ACT, New South Wales, Victoria and Queensland. The Queensland *Information Privacy Act 2009* applies to the health department, who must comply with the National Privacy Principles in that Act. Also, in Queensland, confidentiality of information that identifies individuals that have received public sector health services, is a requirement of the *Hospital and Health Boards Act 2011* (Qld).

TAS	*Personal Information Protection Act 2004* (Tas) Available here.	Ombudsman, Tasmania
SA	No privacy law, but see Cabinet Administrative Instruction to comply with Information Privacy Principles Instruction (originally issued in 1989, last re-issued on 20 June 2016)	Privacy Committee, South Australia
WA	No privacy law or administrative privacy regime	Not applicable
NT	*Information Act 2002* (NT) (especially Part 5) Available here.	Office of the Information Commissioner, Northern Territory
ACT	*Information Privacy Act 2014* (ACT) Available here.	Office of the Australian Information Commissioner (OAIC)
	Health Records (Privacy and Access) Act 1997 (ACT) Available here.	Australian Capital Territory, Human Rights Commission
CTH	*Privacy Act 1998* (Cth) Available here.	Office of the Australian Information Commissioner (OAIC)

Figure 2: International Privacy Jurisdictions

	Privacy Laws or Standards	**Oversight Body**
New Zealand	*Privacy Act 1993* Available here.	Office of the Privacy Commissioner
United States (federal)	No general national privacy law.	The Office of Management and Budget (OMB) issues guidance on the Privacy Act of 1974. However, the Federal Trade Commission oversees the privacy of consumers. See here.

European Union	General Data Protection Regulation (**GDPR**) OVIC Guidance on the GDPR	European Data Protection Board European Member States Oversight Bodies European Union Oversight Body: European Data Protection Supervisor Non-EU countries deemed to have an adequate level of data protection by the European Commission, see here.

Assessing if the personal information recipient is subject to substantially similar privacy protections

9.28 When assessing if the recipient of the personal information is subject to a 'substantially similar' law, binding scheme or contract, the organisation should consider whether the recipient is subject to equivalent privacy protections.

9.29 This assessment involves considerations of the extent to which:

- the recipient is subject to the relevant law, binding scheme or contract;
- principles of fair handling of personal information are effectively upheld under the law, binding scheme or contract; and
- the relevant principles are similar to Victoria's IPPs.

9.30 These considerations are essentially about:

- *Form of obligation*: what form of regulatory mechanism is used to impose fair handling obligations on the recipient? It is a law, binding scheme or contract?
- *Content of principles*: which privacy or data protection rights are included in the fair handling principles the recipient is required to uphold? Are these substantially similar to the IPPs?
- *Enforceability*: are the fair handling principles binding on the recipient and are they enforceable?

Form of obligation: Is the recipient subject to a law, binding scheme or contract?

9.31 Some examples of when a recipient may be subject to a law, binding scheme or contract include when they are:

- bound by a privacy or data protection law that applies in the recipient's jurisdiction and to the recipient specifically;
- required to comply with some other law that imposes data collection and handling obligations in respect of personal information – for example, some criminal law and taxation statutes include provisions that expressly authorise and prohibit specified uses and disclosures, permit retention of some data and require destruction after a set time or under specified circumstances and preserve a right of access to the person's own information;
- subject to an enforceable industry scheme or privacy code, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code;
- party to a contract that successfully binds them to the IPPs through s 17 of the PDP Act; or
- party to a contract that effectively incorporates the Model Terms provided by OVIC.

9.32 Recipients may not be regarded as subject to a law, binding scheme or contract where, for example:

- the privacy or data protection law or regulations (or other law or regulations) exempt the recipient from complying with some or all of the fair handling principles;
- there is an existing or proposed authority (such as a public interest determination or direction issued by a privacy commissioner or minister) allowing the recipient to breach any or all of the fair handling principles;
- the personal information being transferred is not protected under the recipient's privacy or data protection law, for example, due to a difference in definition or coverage;
- the recipient is able to opt out of the binding scheme without notice and without returning or otherwise appropriately disposing of the personal information which had been transferred; or
- the agreement is unenforceable – such is often the case with a Memorandum of Understanding or shared protocols.

Content of principles: Are the fair handling principles substantially similar to the IPPs?

9.33 IPP 9.1(a) does not require the recipient to be bound to uphold principles identical to the IPPs, or principles as stringent as the IPPs.[7] The fair handling principles applying to the recipient must be 'substantially similar'. This term suggests some variations in wording and perhaps scope of privacy principles is not barrier to the transborder data flow, recognising the principles may be tailored to meet specific needs and conditions of other jurisdictions, industries or parties to a transborder data flow. This may result in stronger or weaker protections but such principles may still be regarded as 'substantially similar' to the IPPs.

9.34 When assessing whether the fair handling principles applying to the recipient are 'substantially similar', organisations might conduct:

- a side by side comparison of the IPPs and other principles, noting their similarities and differences; and,
- an assessment of the importance of any similarities or differences, considering the essential features of the IPPs, the relevance of particular principles to the data transfer under consideration and the objects of the PDP Act.[8]

9.35 In general, personal information transferred out of Victoria should only be used and disclosed for legitimate purposes. For example, a fair handling principle that allows a recipient to use or disclose personal information for direct marketing purposes without the individual's consent may not be regarded as substantially similar to the restrictions on use and disclosure in IPP 2 (Use and Disclosure).

Enforceability: Does the law, binding scheme or contract effectively uphold fair handling principles?

9.36 It is not enough that the recipient is subject to a law, binding scheme or contract which contains fair handling principles. These principles must be 'effectively upheld'. This means the principles should be

[7] In contrast, any Code of Practice developed and approved under Part 3 of the PDP Act must prescribe standards that 'are at least as stringent as the standards prescribed by the Information Privacy Principles'; PDP Act ss 21(2), 22(3)(b).
[8] Section 8A(2) of the PDP Act requires the Information Commissioner to have regard to the objects of the PDP Act in performing his or her functions and exercising his or her powers under the PDP Act. The objects of the PDP Act are set out in s 5 and are: (a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector; (b) to balance the public interest in promoting open access to public sector information with the public interest in protecting its security; and (c) to promote awareness of responsible personal information handling practices in the public sector; and (d) to promote the responsible and transparent handling of personal information in the public sector; and (e) to promote responsible data security practices in the public sector.

enforceable.

9.37 Mechanisms should be in place to promote compliance with the principles, to enable complaints about alleged breaches to be independently investigated and to provide appropriate outcomes to resolve complaints and address the harm suffered as a result of the recipient's failure to effectively uphold the principles.

9.38 Many privacy laws in Australasia, Canada and Europe do promote compliance and investigate non-compliance though independent regulators and tribunals. Mechanisms are included to enable complaints to be made and investigated, and avenues are available to resolve disputes. Binding codes may have a code administrator who can receive complaints and provide remedies for privacy breaches.

9.39 Contracts can be more problematic as the individuals whose personal information is being transferred cannot usually enforce them. Organisations seeking to use contracts to comply with IPPs 9.1(a) or (f) should consider including mechanisms which enable:

- individuals to exercise their access and correction rights;
- complaints to be independently investigated and appropriate outcomes to be provided;
- compliance audits be undertaken; and,
- awareness measures be taken to promote compliance within the recipient organisation.

9.40 Including the Model Terms in a contract may help organisations comply with IPP 9.1(a) because the recipient is subject to a contract that effectively upholds principles for the fair handling of the information that are substantially similar to the IPPs.

IPP 9.1(b): Individual gives consent

9.41 IPP 9.1(b) allows organisations to transfer personal information interstate or overseas when they have an individual's consent. Consent should be informed, voluntary, specific, current and made with legal capacity. The concept of consent is discussed further in these Guidelines under Key Concepts and IPP 2.1(b).

9.42 For consent to be informed and specific, when seeking consent from an individual for a transborder data transfer an organisation should address (at a minimum):

- the purpose of the transfer;
- the personal information to be transferred;
- the recipient's location and where the data will be stored and any privacy laws applying to the transfer of the data. This may be problematic for some cloud storage services where data is fragmented across several jurisdictions. In these circumstances, it may be more appropriate to consider another service provider or rely on a different subsection of IPP 9.1;
- what entities will be able to access the information;
- whether and to whom the information may be further disclosed or transferred;
- how the personal information will be handled by the recipient; and
- the consequences for the individual of giving or failing to give consent.

9.43 Where personal information is transferred as part of a research project, refer to the use of consent and other mechanisms discussed in IPP 2.1(c).

9.44 IPP 9.1(b) allows an organisation to obtain consent from an individual to transfer their information to an interstate or overseas recipient who is not subject to substantially similar privacy protections. This potentially reduces the privacy protection of the information after it is transferred, so organisations

should ensure individuals are properly informed of any reasonably foreseeable privacy risks associated with the transfer prior to obtaining the individual's consent.

Case Study 9B: Validity of consent

The Complainant complained Organisation A transferred their personal information to a Software Platform Provider located in another country (which did not have similar privacy laws to Victoria) not in accordance with IPP 9.

Organisation A sought consent (under IPP 9.1(a)) from the Complainant to submit their personal information using one of the Software Platform Provider's cloud products. The Complainant consented to the transfer by Organisation A to the Software Platform Provider because the Complainant relied on Organisation A's services and did not feel they had any alternative but to agree to the transfer.

The following year the Software Platform Provider made significant changes to its cloud product and privacy features. However, Organisation A did not seek the Complainant's consent again for future transfers of their personal information.

To resolve the dispute, Organisation A agreed to allow the Complainant to submit their personal information without using a cloud product. Organisation A also agreed to improve its process to ensure the consent it seeks for transfers is valid (current, informed and voluntary).

In this case, it was appropriate to offer an alternative method of transferring information without using a cloud product, however, this will not apply to all situations involving the use of cloud or other digital products.

IPP 9.1(c): Necessary to perform a contract with the individual or for implementation of pre-contractual measures at the individual's request

9.45 IPP 9.1(c) allows organisations to transfer information outside Victoria where the transfer is necessary for:

- the performance of a contract between the individual and the organisation; or
- for the implementation of pre-contractual measures taken in response to the individual's request.

9.46 The transfer must be necessary or there must be a close connection between the data subject and the purpose of the contract. IPP 9.1(c) cannot be used for transfers of additional, non-essential information. Nor can IPP 9.1(c) be used to authorise transfers of information for a purpose unrelated to the performance of the contract or pre-contractual measures. Transfers of information carried out to implement pre-contractual measures must be initiated by the individual, not by the organisation or recipient. The meaning of 'necessary' is discussed in these Guidelines under Key Concepts and IPP 2.

9.47 In many cases, consent may be an alternative basis for the transfer. For example, the organisation

may expressly seek consent in the contract, or, in limited circumstances, consent may be implied.[9]

IPP 9.1(d): Necessary to perform a contract with a third party in the individual's interest

9.48 Under IPP 9.1(d), an organisation may transfer information outside Victoria to conclude or perform a contract with a third party in the interest of the individual who is the subject of the information being transferred.

9.49 IPP 9.1(d) deals with transfers that are beneficial to the interests of the individual. Organisations should remember the individual's interest in protecting their privacy is one of these interests. The transfer should not be carried out solely in the interest of the organisation or recipient. The individual's interest must be served and the test for necessity must be met. To be necessary, there should be a close and substantial connection between the individual's interest and the purposes of the contract.

IPP 9.1(e): For the individual's benefit where impracticable to obtain consent or consent likely to be given

9.50 IPP 9.1(e) permits a transborder data flows where the transfer is for the benefit of the individual, it is impracticable to obtain the individual's consent and the organisation reasonably believes the individual would be likely to consent.

9.51 The following three distinct requirements must all apply. The organisation must reasonably believe that:

- the transfer must be for the individual's benefit. For example, IPP 9.1(e) is likely to permit the transfer of essential personal information to help identify and assist a seriously injured person involved in an overseas or interstate accident or disaster.
- it is impracticable to obtain the consent of the individual whose personal information is the subject of the transfer. Transfers for the benefit of the individual ordinarily occur by consent, however, IPP 9.1(e) allows the transfer to proceed without consent, if it is impracticable to obtain that consent. Following the above example, it may be impracticable to obtain consent if the seriously injured person cannot communicate, or it is an emergency situation where delay to obtain consent might put the individual at risk.
- the individual would likely give their consent if they were able to be asked. If the organisation is aware of the individual having previously expressed a wish not to have their information transferred in the circumstances, IPP 9.1(e) will not authorise the transfer.

9.52 For more information, refer to the discussion of 'consent' and 'practicable' in the Key Concepts and IPP 2 (Use and Disclosure).

IPP 9.1(f): Reasonable steps to ensure data will not be handled inconsistently with the IPPs

9.53 IPP 9.1(f) authorises a transborder data flow if the organisation has taken reasonable steps to ensure the information transferred will not be held, used or disclosed by the recipient inconsistently with the IPPs.

9.54 Steps required to obtain the required reasonable belief under IPP 9.1(a) will often, in practice, amount to what is required by IPP 9.1(f). However, IPP 9.1(f) also allows transfers where the recipient is not bound by a law, binding scheme or contract which effectively upholds fair handing principles that are substantially similar to the IPPs. The focus of IPP 9.1(f) is the reasonable steps

[9] See *E v Money Transfer Service* [2006] PrivCmrA 5.

taken by the organisation, instead of the privacy obligations binding the recipient.

9.55 For example, IPP 9.1(f) might be satisfied where the organisation takes practical steps to limit the amount of information transferred, enters into agreements to clarify permissible and prohibited uses and disclosures of the transferred information and secures the information from the time of the transfer until its eventual return or destruction. These are reasonable steps which ensure the information is held consistently with IPP 2 (Use and Disclosure) and IPP 4 (Data Security). Various (and often multiple) methods might be used to satisfy IPP 9.1(f). Reasonable steps are likely to include legal, technological and administrative practices.

9.56 Some examples of reasonable steps for transferring personal information under IPP 9.1(f) might include the following:

- **Privacy Impact Assessments** (**PIAs**) – undertaking a PIA can help your organisation assess risks associated with a transfer and to implement appropriate security measures. Information about PIAs is here.
- **Technical security measures** – a number of security controls can be implemented to secure personal information being transferred to an interstate recipient (for example, end-to-end encryption and the use of at rest encryption by the recipient of the personal information). More information is in IPP 4 (Data Security).
- **Cloud security assessment** – the Victorian Government Chief Information Security Officer has produced a cloud security guide (including a sample assessment tool) to help organisations to identify risks and appropriate controls when considering using a cloud service provider
- **Victorian Protective Data Security Framework and Five Step Action Plan** – these documents may help organisations when considering the sensitivity of the personal information to be transferred and the potential impact in the event of a breach
- **Including the Model Terms in a contract** – this may help organisations comply with IPP 9.1(f) because the Model Terms are evidence of reasonable steps by the organisation to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the IPPs.

> Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

Version control table

Version	Description	Date published
IPP 9 – Transborder Data Flows 2019.B	Edits following consultation.	14 November 2019
IPP 9: Transborder Data Flows 2019.A	Consultation draft.	28 February 2019
IPP 9: Transborder Data Flows (2011)	2011 pdf version.	2011