**TRANSBORDER DATA FLOWS OF PERSONAL INFORMATION**

**MODEL CONTRACT TERMS**

**CONTENTS**

[INTRODUCTION 3](#_Toc69821234)

[PRELIMINARIES 4](#_Toc69821235)

[Key terms 4](#_Toc69821236)

[Text of IPP 9 5](#_Toc69821237)

[MODEL TERMS 7](#_Toc69821238)

[MODEL TERMS WITH COMMENTARY 13](#_Toc69821239)

INTRODUCTION

Modern business is increasingly borderless. Digital communication technologies have made it as easy to send information to the other side of the world, as it is to send to the other side of the street. This seamlessness has allowed organisations to globalise, and regions to specialise. It has opened up enormous opportunities for innovation and efficiency.

Victorian agencies regulated by the *Privacy and Data Protection Act 2014* (Vic) are increasingly taking advantage of these opportunities. And where agencies do so, the Victorian community can benefit as well, through improved services, and more cost-effective government. But Victorians expect that their privacy will be protected, wherever their personal information is sent.

Victoria’s *Privacy and Data Protection Act 2014* (Vic)(**PDP Act**) seeks 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.’[[1]](#endnote-1)

The ten Information Privacy Principles (**IPPs**) in Schedule 1 of the PDP Act set out minimum standards for how the Victorian government must manage personal information. IPP 9 (Transborder Data Flows) outlines how an organisation may transfer personal information about an individual to someone outside Victoria.

The basic idea in IPP 9 is that when personal information travels, privacy protection should travel with it.

IPP 9 is designed to ensure an organisation will only transfer an individual's personal information out of Victoria where the personal information will have protection substantially similar to the PDP Act, or alternatively, where the individual consents, or is likely to consent.

The Office of the Victorian Information Commissioner (**OVIC**) has a number of functions and powers under the PDP Act. One of its functions is to develop and publish model terms capable of being adopted by an organisation in a contract or arrangement with a recipient of personal information being transferred by the organisation outside Victoria.[[2]](#endnote-2)

This resource contains model contract terms (**Model Terms**) regarding the transfer of personal information outside Victoria. The Model Terms may be adopted (with or without adaptation) in an organisation's contract with a recipient where personal information is transferred by the organisation outside Victoria. Some links to parts of the PDP Act and the IPPs are also explained.

This guide and the Model Terms are not prescriptive. They are intended to be tools to help organisations comply with IPP 9.

Each organisation will need to decide whether or not the Model Terms are appropriate for its own particular circumstances.

PRELIMINARIES

Key terms

IPP 9 regulates how an ‘organisation’ may transfer ‘personal information’ about an individual to someone who Victoria.

Organisation

Most of the state government, local government and Victorian statutory authorities are governed by the PDP Act. Some exemptions apply.

An ‘organisation’ is defined in the PDP Act to cover:

* a range of Victorian public sector bodies or individuals, including Ministers, Parliamentary Secretaries, public sector agencies, municipal councils, statutory authorities established or appointed for a public purpose, courts, tribunals and Victoria Police; and
* contracted service providers who have agreed to be bound by the Information Privacy Principles in the PDP Act and any applicable code of practice for acts and practices under the relevant State contract.[[3]](#endnote-3)

Personal information

‘Personal information’ is defined in the PDP Act to mean:

* information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* (Vic) (**HR Act**) applies.[[4]](#endnote-4)

For example, an individual’s name and address,[[5]](#endnote-5) telephone number[[6]](#endnote-6) and where an individual works are ‘personal information’.[[7]](#endnote-7)

Personal information must be ‘recorded’ in a physical or electronic form. The PDP Act will not apply where the information only exists in someone’s mind.

The exclusion of health information from the PDP Act reflects the Victorian Parliament’s decision to deal with the privacy of health information within the HR Act.[[8]](#endnote-8)

Application

IPP 9 applies where an organisation covered by the PDP Act (**Organisation**) transfers personal information to someone outside Victoria (**Recipient**). If the Recipient is not subject to a law or binding scheme which effectively upholds the principles of fair handling of the information similarly to the IPPs, you should consider whether to adopt the Model Terms in this Guide in any contract between the Organisation and the Recipient.

Compliance with IPP 9 is only one aspect of privacy compliance. It is likely Organisations will also need to consider the impact of other IPPs when transferring personal information to recipients outside Victoria, for example, IPP 2 (Use and Disclosure) and IPP 4 (Data Security).[[9]](#endnote-9)

Commonwealth level

At the Commonwealth level, the *Privacy Act 1988* (Cth) (**Privacy Act**) regulates the handling of personal information about individuals and provides a basis for nationally consistent regulation of privacy.[[10]](#endnote-10) The Privacy Act includes the Australian Privacy Principles that apply to the private sector and the Commonwealth public sector.

IPP 9 is similar to Australian Privacy Principle 8 (**APP 8**) in the Privacy Act. The main difference is that APP 8 deals with transfers of personal information to someone who is outside Australia.

Contracted service providers under a State contract that binds the outsourcing Organisation to comply with the IPPs for acts and practices under the contract may have to comply with both IPP 9 and APP 8 for different aspects of its activities. IPP 9 will apply to the contracted service provider's acts and practices for the purpose of meeting its obligations under a State contract with an Organisation. Nevertheless, the APPS do not apply to acts and practices under State contracts: see section 7B(5) of the Privacy Act.

Text of IPP 9

IPP 9.1 states:

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if –

* + 1. 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
		2. the individual consents to the transfer; or
		3. 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; or
		4. 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
		5. all of the following apply –
			1. the transfer is for the benefit of the individual;
			2. it is impracticable to obtain the consent of the individual to that transfer;
			3. if it were practicable to obtain that consent, the individual would be likely to give it; or
		6. 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 Information Privacy Principles.

The six bases on which personal information may be transferred to someone outside Victoria are alternatives. This means only one needs to be met. In practice, several may be fulfilled at once.

IPP 9.1(a) and IPP 9.1(f) will commonly overlap because by including appropriate clauses in an enforceable agreement with a Recipient, the Organisation may both establish the reasonable belief required under IPP 9.1(a) and take a reasonable step under IPP 9.1(f).

Not all transfers of personal information by Organisations will have features that bring them within IPP 9.1(b) to (e). For example, when an Organisation decides to provide personal information to a shared federal-state resource to assist cross-border law enforcement or revenue protection, this arrangement is unlikely to be:

* with the consent of all relevant individuals (IPP 9.1(b));
* necessary for performance of a contract with relevant individuals or in response to an individual’s request (IPP 9.1(c));[[11]](#endnote-11)
* necessary for performance of a contract in the interest of the individual (IPP 9.1(d)); or
* for the relevant individual's benefit in circumstances where it was impracticable to obtain the individual’s consent or if it was practicable the individual would likely consent (IPP 9.1(e)).

Transfers of personal information that are not within IPP 9.1(b) to (e) may be transfers permitted by IPP 2. For example, some transfers may be made under agreements[[12]](#endnote-12) made by one or more of the groupings of Federal and State Ministers who hold similar portfolio responsibilities[[13]](#endnote-13) and meet periodically to discuss and coordinate collective action across the internal borders of Australia.

Therefore, Organisations seeking to transfer personal information about an individual to someone outside Victoria will often seek to rely on IPP 9.1(a) and (f) to permit such transfers. The Model Terms, if reflected appropriately in a binding contract for the purposes of IPP 9.1(a), will assist Organisations in complying with IPP 9.1(a) or (f), or both.

The appropriate use of the Model Terms in a binding contract between an Organisation and a Recipient could lead to the conclusion that an Organisation transferring personal information outside Victoria complies 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; or
* IPP 9.1(f) because the adapted Model Terms and the way the parties have followed them during their dealings are evidence of reasonable steps by the Organisation to ensure the information which it transferred will not be held, used or disclosed by the Recipient in a manner inconsistent with the IPPs.

MODEL TERMS

These Model Terms are to be read with the rest of this guide, in particular, the Commentary in the next section, and with the PDP Act itself. This guide is not prescriptive about how the Model Terms are to be used. The Model Terms are a guide only.

The Model Terms are likely to require adaptation to the particular circumstances of the parties to any given agreement. Although the Model Terms are set out here as a stand-alone agreement, transborder dataflow clauses will often comprise only part of larger agreements dealing with many matters other than flows of personal information. In such cases, the terms ‘Recipient’ and ‘Organisation’ will need to be defined or replaced with the relevant terminology used in the larger agreement.

Model Terms for Transborder Data Flows Parties

(‘**Organisation**’)

(‘**Recipient**’)

Recitals

1. The Organisation transfers or proposes to transfer various information and data to the Recipient.
2. Some of the data which is transferred may constitute or contain Personal Information.
3. To enable the Organisation to transfer Personal Information to the Recipient consistently with the PDP Act and the IPPs, the Organisation requires that the Recipient be subject to a binding contract which effectively upholds principles for the fair handling of the Personal Information that are substantially similar to the IPPs.
4. This Agreement obliges the Recipient to observe such principles for the fair handling of Transferred Personal Information.
5. **Definitions and Interpretation**
	1. **Definitions**

In this Agreement:

Commencement Date means [insert].

**Code of Practice** means a code of practice as defined in, and approved under, the PDP Act.

**Data Subject** means an Individual about whom Personal Information is transferred by the Supplier to the Recipient.

**Individual** means a natural person.

**Information Privacy Principles** and **IPPs** means the information privacy principles contained in Schedule 1 of the PDP Act.

**Law** means any statute, regulation, order, rule or subordinate legislation, including the common law.

**OVIC** means the Office of the Victorian Information Commissioner.

**Organisation** has the meaning given in the PDP Act.

**PDP Act** means the *Privacy and Data Protection Act 2014* (Vic) as amended from time to time.

**Personal Information** has the meaning given to it in the PDP Act from time to time, and as at the Commencement Date, refers to information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* (Vic)applies.

**Transferred Personal Information** means any Personal Information transferred from the Organisation to the Recipient before, on or after the Commencement Date and includes any copy of that Personal Information and any part of that Personal Information included or incorporated in a record with other information.

* 1. **Interpretation**

In this Agreement:

* + 1. references to any statute, ordinances or other Law include all regulations and enactments made under them and all consolidations, amendments, re- enactments or replacements of them; and
		2. a reference to a party, clause, schedule, attachment or annexure is a reference to a party, clause, schedule, attachment or annexure to or of this Agreement and a reference to this Agreement includes all schedules, attachments or annexures to it.
1. **Primary Purpose**

The purpose of the transfer of Personal Information from the Organisation to the Recipient is contained in Part A of Schedule 1 of this Agreement.

1. **Subject Matter**

The nature and type of Personal Information to be transferred in the agreed format between the parties is contained in Part B of Schedule 1 of this Agreement.

1. **Organisation’s Acknowledgement**

The Recipient agrees that it is bound by the Information Privacy Principles and any applicable Code of Practice with respect to any act done, or practice engaged in, by the Recipient for the purposes of this Agreement in the same way and to the same extent as the Organisation would have been bound by them in respect of that act or practice had it been directly done or engaged in by the Organisation.

1. **Organisation's Disclosure of this Agreement**

The Organisation may disclose to any person the fact that the Recipient is a party to this Agreement for the purpose of allowing such person to assess whether Transferred Personal Information is adequately protected in the hands of the Recipient. The Organisation may also disclose a pro forma document containing terms substantially similar to the terms of this Agreement to any person for such purpose.

1. **Recipient’s Obligations**
	1. **IPPs**

Subject to sub-clauses 6.4 and 6.5, the Recipient agrees that it will not at any time do an act, or engage in a practice, in respect of Transferred Personal Information, that would breach an Information Privacy Principle.

* 1. **Specific Undertakings**

Without limiting sub-clause 6.1, the Recipient agrees that:

* + 1. it will not collect, use, disclose and otherwise handle the Transferred Personal Information for any purpose other than that provided for under clause 2 of this Agreement without the prior written permission of the Organisation or the Data Subject or where required or authorised by or under Law;
		2. it will not disclose the Transferred Personal Information to a person (wherever located) (**Further Recipient**) who is not an Organisation unless the Recipient complies with IPP 9 in respect of that disclosure as if the Recipient was an Organisation and the Further Recipient was someone who is outside Victoria for the purposes of IPP 9;
		3. unless within the purpose under clause 2, the Recipient must not match or otherwise combine any Transferred Personal Information about a Data Subject with any other Personal Information about that Data Subject from any other source without the prior written permission of the Organisation or that Data Subject’s consent or where required by Law (and where the Recipient obtains the Data Subject's consent, the Recipient will notify the Organisation in writing that such consent has been obtained);
		4. it will establish processes to comply with the IPPs including but not limited to mechanisms that will enable Data Subjects to access and correct Transferred Personal Information about them that is held by it, in a manner consistent with IPP 6;
		5. having regard to the nature of the information, the Recipient will take reasonable steps, including appropriate technological and organisational steps, to ensure the security and quality of the Transferred Personal Information, including but not limited to the prevention of unauthorised or unlawful access to the Transferred Personal Information and prevention of accidental loss, destruction or damage;
	1. **Other Matters**

The Recipient agrees and confirms that:

* + 1. it will immediately and unreservedly comply with any written instructions from the Organisation which are stated by the Organisation to be necessary for compliance with the IPPs or any guidance issued by the OVIC or other applicable Laws;
		2. it will immediately notify the Organisation, in writing, of any breach or suspected breach of its obligations under this Agreement (and of any act or omission which would have been a breach of sub-clauses 6.1 or 6.2 but for the operation of sub-clause 6.4), whether on the part of itself or its officers, employees, volunteers, agents or sub-contractors and of steps taken to repair the breach;
		3. it will allow and cooperate with any independent investigation of complaints by the Organisation, OVIC or any person or body nominated by the Organisation and provide appropriate redress to complainants for any harm arising from its failure to effectively uphold the IPPs;
		4. it will permit the Organisation or its nominee to inspect or audit its compliance under this Agreement and with the IPPs and further warrants the accuracy of records audited; and it will ensure that any of its officers, employees, volunteers, agents and sub-contractors who are able to obtain access to any Transferred Personal Information, or to whom it otherwise discloses Transferred Personal Information are made aware of, and undertake to observe, the obligations imposed on the Recipient under this clause 6; and
		5. it will ensure that any of its officers, employees, volunteers, agents and sub-contractors who are able to obtain access to any Transferred Personal Information, or to whom it otherwise discloses Transferred Personal Information are made aware of, and undertake to observe, the obligations imposed on the Recipient under this clause 6.
	1. **Limitations on Compliance with IPPs**

Sub-clauses 6.1 and 6.2 do not apply to an act or practice of the Recipient which is required by or under a Law of an Australian jurisdiction other than Victoria which applies to the Recipient.

* 1. **Compliance with Local Laws**

The Recipient will not, in respect of Transferred Personal Information, do an act, or engage in a practice, that would breach any Laws which apply to the Recipient.

1. **Indemnities and Warranties**
	1. **Recipient’s Indemnity**

Subject to the provisions of this Agreement, the Recipient at all times indemnifies and holds harmless the Organisation, its officers, employees, volunteers, agents and sub-contractors (in this clause 7 referred to as ‘those indemnified’) from and against any loss, cost (including legal costs and expenses on a solicitor/own client basis) or liability incurred or suffered by any of those indemnified arising from or in connection with any complaint, claim, suit, demand, action or proceeding by any person (including, but not limited to, any award, order or similar judgment or direction by the OVIC) where such loss or liability was caused or contributed to by the Recipient’s act or omission (or an act or omission by the Recipient’s officers, employees, agents, volunteers or sub-Organisations) in handling Transferred Personal Information, whether deliberate or not.

* 1. **Limitation on Recipient’s Indemnity**

The Recipient’s liability to indemnify the Organisation under sub-clause 7.1 will be reduced proportionally to the extent that any negligent act or omission of those indemnified directly contributed to the loss or liability.

* 1. **Recipient’s Warranties**

The Recipient warrants that:

* + 1. any Law applying to the Recipient does not prevent the Recipient from:
			1. complying with IPPs in respect of the Transferred Personal Information; and
			2. fulfilling its obligations under this Agreement;
		2. the Recipient has made itself aware (and will keep itself aware) of the requirements of the PDP Act and of the IPPs in particular.
	1. **Survival**

The warranties and indemnities set out in this clause 7 will survive the expiration or termination of this Agreement.

1. **Termination**

This Agreement will be taken to have commenced on the Commencement Date and it will continue until terminated by written agreement between the parties.

Upon the termination of this Agreement, or upon the Organisation's written request prior to the termination of this Agreement, the Recipient will:

1. return or destroy (at the Organisation's election) all Transferred Personal Information including all copies, in whatever form, of the Transferred Personal Information held or controlled by the Recipient; and
2. deliver to the Organisation, a complete and up-to-date list of all persons or other legal entities that to the Recipient's knowledge have had access to, or control of, any of the Transferred Personal Information.
3. **Governing Law**
4. The parties agree this Agreement is governed by the Law of Victoria and irrevocably submit to the non-exclusive jurisdiction of the Courts and Tribunals of Victoria.
5. The Recipient must not claim Victorian jurisdiction as inconvenient.
6. **Other Laws**

To the extent that the terms of this Agreement are inconsistent with any relevant and applicable Laws, to the extent of the inconsistency those terms will not bind the parties.

Schedule 1

Part A - Clause 2

[Insert the purpose for the transfer of Personal Information from the Organisation to the Recipient]

Part B - Clause 3

[Insert details of the nature and type of Personal Information to be transferred.]

MODEL TERMS WITH COMMENTARY

In this part of the guide, each clause of the Model Terms is reproduced in turn and followed by brief commentary as relevant.

Recitals

1. The Organisation transfers or proposes to transfer various information and data to the Recipient.
2. Some of the data which is transferred may constitute or contain Personal Information.
3. To enable the Organisation to transfer Personal Information to the Recipient consistently with the PDP Act and the IPPs, the Organisation requires that the Recipient be subject to a binding contract which effectively upholds principles for the fair handling of the Personal Information that are substantially similar to the IPPs.
4. This Agreement obliges the Recipient to observe such principles for the fair handling of Transferred Personal Information.
5. **Definitions and Interpretation**
	1. **Definitions**

In this Agreement:

Commencement Date means [insert].

**Code of Practice** means a code of practice as defined in, and approved under, the PDP Act.

**Data Subject** means an Individual about whom Personal Information is transferred by the Supplier to the Recipient.

**Individual** means a natural person.

**Information Privacy Principles** and **IPPs** means the information privacy principles contained in Schedule 1 of the PDP Act.

**Law** means any statute, regulation, order, rule or subordinate legislation, including the common law.

**OVIC** means the Office of the Victorian Information Commissioner.

**Organisation** has the meaning given in the PDP Act.

**PDP Act** means the *Privacy and Data Protection Act 2014* (Vic) as amended from time to time.

**Personal Information** has the meaning given to it in the PDP Act from time to time, and as at the Commencement Date, refers to information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* (Vic)applies.

**Transferred Personal Information** means any Personal Information transferred from the Organisation to the Recipient before, on or after the Commencement Date and includes any copy of that Personal Information and any part of that Personal Information included or incorporated in a record with other information.

* 1. **Interpretation**

In this Agreement:

* + 1. references to any statute, ordinances or other Law include all regulations and enactments made under them and all consolidations, amendments, re- enactments or replacements of them; and
		2. a reference to a party, clause, schedule, attachment or annexure is a reference to a party, clause, schedule, attachment or annexure to or of this Agreement and a reference to this Agreement includes all schedules, attachments or annexures to it.

|  |
| --- |
| **Commentary:** Both parties should understand and agree on the terms used in this type of agreement. The recitals, definition and interpretation sections should assist that mutual understanding, whether adopted exactly as in the Model Terms or amended through negotiation. Where privacy laws are inconsistent between Victoria and other jurisdiction, definitions will also need particular attention. The Recipient should be clear ‘personal information’ includes much more than obvious identifying data such as name, address and date of birth. The breadth of the term is not always appreciated. For example, the term may encompass images and biometrics. Other jurisdictions may have slightly different definitions. For example, some jurisdictions do not limit personal information to information that is recorded. Some include ‘health information’ within the meaning of ‘sensitive information’, and others may include information about identifiable deceased persons, as well as the living. ‘Sensitive information’ is a subset of personal information. It is generally afforded a higher level of privacy protection under the IPPs than other personal information. Sensitive information is defined in Schedule 1 of the PDP Act: ‘Sensitive information means information or an opinion about an individual's— * + 1. racial or ethnic origin; or
		2. political opinions; or
		3. membership of a political association; or
		4. religious beliefs or affiliations; or
		5. philosophical beliefs; or
		6. membership of a professional or trade association; or
		7. membership of a trade union; or
		8. sexual preferences or practices; or
		9. criminal record— that is also personal information.

Importantly, the Recipient must understand that the Organisation is subject to Victorian legislation and accordingly, the Recipient must meet the Organisation’s requirements before the Organisation can provide any personal information or sensitive information.For consistency, definitions and terminology are drawn as far as possible from the relevant statutes. When drafting this type of agreement, give careful consideration to what other definitions may assist the parties in understanding their obligations under the agreement. ‘Organisation’ refers to the Victorian public sector organisation transferring the personal information while ‘Recipient’ refers to the organisation or person outside of Victoria’s jurisdiction receiving the personal information. In this context, an Organisation may be public or private, profit or non-profit. If the contracting parties are identified as anything other than Organisation and Recipient, both ‘Organisation’ and ‘Recipient’ should either be defined in this clause or replaced by the appropriate reference. |

1. **Primary Purpose**

The purpose of the transfer of Personal Information from the Organisation to the Recipient is contained in Part A of Schedule 1 of this Agreement.

|  |
| --- |
| **Commentary:** Under IPP 2 and IPP 9, Victorian public sector organisations may only disclose information to another organisation under certain circumstances. Purpose is a key concept in data protection standards. The purpose behind the transfer must be clearly expressed in agreements for transborder data flows. If the transfer to the Recipient by the Organisation is in accordance with the primary purpose of collection, this should be stated clearly and the primary purpose briefly described.It is unlikely the primary purpose of initial collectionby the Organisation of personal information from or about the Data Subjects will have been to disclose the personal information to the Recipient. It will be more common the Organisation collected the personal information for some other primary purpose, without planning for the data to flow across borders. Disclosure to the Recipient may have become necessary or desirable subsequently, so a transfer across borders took place.In some circumstances, disclosure to the Recipient may be necessary for the Organisation to fulfil the primary purpose of collection. For example, personal information may be collected for the primary purpose of processing a licence application made by the Data Subject. Granting the licence may require checks with an organisation based in Canberra. In this example, the flow of the applicant’s personal information out of Victoria for the check is necessary for the primary purpose for which the information was collected.Perhaps most common will be disclosures not for the primary purpose, but disclosures permitted under IPP 2. If the purpose of the transfer is different from the primary purpose of collection, the Organisation must ensure the purpose fits at least one of the categories in IPP 2 or is otherwise exempt.When drafting clause 2, the purpose should indicate which one or more of the eight categories provided under IPP 2 will apply. Permitted types of use or disclosure (other than for primary purpose): 1. secondary purpose related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection, and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
2. the individual has consented to the use or disclosure;
3. if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual, it must be impracticable for the organisation to seek the individual's consent before the use or disclosure; and in the case of disclosure, the Organisation reasonably believes that the Recipient will not disclose the information;
4. the Organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare; or a serious threat to public health, public safety, or public welfare;
5. the Organisation has reason to suspect unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;
6. the use or disclosure is required or authorised by or under Law; or
7. the Organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency, and the Organisation makes a written note of the disclosure (IPP 2.2):
	1. the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
	2. the enforcement of laws relating to the confiscation of the proceeds of crime;
	3. the protection of the public revenue;
	4. the prevention, detection, investigation or remedying of seriously improper conduct; or
	5. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal,
8. the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and—
9. the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and
10. an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

Clarity about how the Organisation’s use or disclosure – the transfer to the Recipient – complies with IPP 2 will assist the Organisation to deal with any enquiries Data Subjects or other individuals may raise. Clarity about purpose will also assist the Recipient in its handling of the information under the Agreement. |

1. **Subject Matter**

The nature and type of Personal Information to be transferred in the agreed format between the parties is contained in Part B of Schedule 1 of this Agreement.

|  |
| --- |
| **Commentary:** The Agreement should specify what information is to be transferred and in what form.This information should be contained in a Schedule attached to the Agreement (that forms an integral part of the Agreement). The Schedule should describe the nature and type of information to be transferred, especially if it is sensitive information.* ‘Nature of information’ refers to its general category or characteristic use. For example, the nature of names, addresses and dates of birth is identifier information and the nature of bank account numbers and credit card details is financial information.
* ‘Type of information’ is more specific, for example, name, home address, tax file number, gender, ratepayer record, number of children, driver’s licence number, fines incurred or outstanding.

Where relevant, the Organisation should highlight types of sensitive information to ensure the Recipient knows it is receiving sensitive information. As outlined above, sensitive information has increased protection requirements. **SAMPLE*****Schedule 1, Part B (Clause 3 refers)****Personal Information to be transferred -**Nature: identifiers; financial; driver details**Types:**First Names* *Middle Names* *Surnames* *Gender**Dates of Birth* *Home Addresses**Home & Mobile Phone Numbers* *Drivers licence numbers**Bank account numbers* *Credit card numbers****Sensitive Information****Ethnicity**Political opinions**Membership of a political association**Criminal record data* *Philosophical beliefs* *Religious beliefs* *Sexuality***Part B of Schedule 1** should also indicate the **extent of the information** to be transferred, using whatever measure or measures are most relevant, convenient and clear in the context. For example:***SAMPLE*** ***Part B Schedule 1****Number of records:**Approximately 500 A4 pages* *(or)**XX [number] of files of digital data containing XX [number] megabytes.**Number of Data Subjects:**Approximately XX [number] persons.* Detail about the extent of the information to be transferred can help comply with IPP 4 (Data Security). It may also help Organisations comply with IPP 3 (Data Quality) because it clearly tells the Recipient what data it will need to keep accurate, complete and up-to-date, and the data can serve the purposes of the transfer. Being able to get a swift understanding of what and how much personal information has been involved in a transfer may be helpful if any problem occurs. Details of amounts of data transferred also assist with audits and, if they become necessary, investigations. If media coverage or regulator interest ensues, the reputation of the Organisation or the Recipient will be at risk and an adequate response will be important.It is likely the parties would also benefit by specifying the **method of transfer**. Data will travel in digital form by various methods that may lead to its loss. For example, data may travel by electronic means (for example, XML data feeds, e-mails with attachments or extranets), on CDs, DVDs or USB keys (‘memory sticks’) sent by courier/mail or in a laptop computer. Cases exist of serious losses of information travelling by each of these methods. If the data in those cases had been adequately encrypted, the problems would not have been so serious. |

1. **Organisation’s Acknowledgement**

The Recipient agrees that it is bound by the Information Privacy Principles and any applicable Code of Practice with respect to any act done, or practice engaged in, by the Recipient for the purposes of this Agreement in the same way and to the same extent as the Organisation would have been bound by them in respect of that act or practice had it been directly done or engaged in by the Organisation.

|  |
| --- |
| **Commentary:** The wording of clause 4 aligns with s 17(2) of the PDP Act. It ensures the Recipient complies with the IPPs in the same manner as the organisation is bound by the IPPs. |

1. **Organisation's Disclosure of this Agreement**

The Organisation may disclose to any person the fact that the Recipient is a party to this Agreement for the purpose of allowing such person to assess whether Transferred Personal Information is adequately protected in the hands of the Recipient. The Organisation may also disclose a pro forma document containing terms substantially similar to the terms of this Agreement to any person for such purpose.

|  |
| --- |
| **Commentary:** The Organisation’s obligations under the PDP Act include obligations to give notice about purpose of collection and usual disclosures (IPP 1.3), to take reasonable steps to ensure data security (IPP 4), an obligation to be open about how it handles personal information, such as a privacy policy (IPP 5), and an obligation to allow data subjects to access and correct their personal information (IPP 6).The Organisation’s handling of personal information may be subject to audit or investigation by OVIC, who may require access to transborder dataflow agreements in specific cases to ascertain whether the records are maintained according to the IPPs (ss 8C and 8D of the PDP Act). For the most part, disclosure of pro forma agreements that contain substantially similar terms is likely to satisfy the more general openness requirements of the IPPs.Clause 5 ensures the Recipient is aware the Organisation has obligations under the PDP Act and that fulfilment and oversight of those obligations may entail scrutiny of the agreement or its terms by persons other than the parties, for example, a regulatory oversight body such as OVIC. |

1. **Recipient’s Obligations**
	1. **IPPs**

Subject to sub-clauses 6.4 and 6.5, the Recipient agrees that it will not at any time do an act, or engage in a practice, in respect of Transferred Personal Information, that would breach an Information Privacy Principle.

* 1. **Specific Undertakings**

Without limiting sub-clause 6.1, the Recipient agrees that:

* + 1. it will not collect, use, disclose and otherwise handle the Transferred Personal Information for any purpose other than that provided for under clause 2 of this Agreement without the prior written permission of the Organisation or the Data Subject or where required or authorised by or under Law;
		2. it will not disclose the Transferred Personal Information to a person (wherever located) (**Further Recipient**) who is not an Organisation unless the Recipient complies with IPP 9 in respect of that disclosure as if the Recipient was an Organisation and the Further Recipient was someone who is outside Victoria for the purposes of IPP 9;
		3. unless within the purpose under clause 2, the Recipient must not match or otherwise combine any Transferred Personal Information about a Data Subject with any other Personal Information about that Data Subject from any other source without the prior written permission of the Organisation or that Data Subject’s consent or where required by Law (and where the Recipient obtains the Data Subject's consent, the Recipient will notify the Organisation in writing that such consent has been obtained);
		4. it will establish processes to comply with the IPPs including but not limited to mechanisms that will enable Data Subjects to access and correct Transferred Personal Information about them that is held by it, in a manner consistent with IPP 6;
		5. having regard to the nature of the information, the Recipient will take reasonable steps, including appropriate technological and organisational steps, to ensure the security and quality of the Transferred Personal Information, including but not limited to the prevention of unauthorised or unlawful access to the Transferred Personal Information and prevention of accidental loss, destruction or damage;
	1. **Other Matters**

The Recipient agrees and confirms that:

* + 1. it will immediately and unreservedly comply with any written instructions from the Organisation which are stated by the Organisation to be necessary for compliance with the IPPs or any guidance issued by the OVIC or other applicable Laws;
		2. it will immediately notify the Organisation, in writing, of any breach or suspected breach of its obligations under this Agreement (and of any act or omission which would have been a breach of sub-clauses 6.1 or 6.2 but for the operation of sub-clause 6.4), whether on the part of itself or its officers, employees, volunteers, agents or sub-contractors and of steps taken to repair the breach;
		3. it will allow and cooperate with any independent investigation of complaints by the Organisation, OVIC or any person or body nominated by the Organisation and provide appropriate redress to complainants for any harm arising from its failure to effectively uphold the IPPs;
		4. it will permit the Organisation or its nominee to inspect or audit its compliance under this Agreement and with the IPPs and further warrants the accuracy of records audited; and it will ensure that any of its officers, employees, volunteers, agents and sub-contractors who are able to obtain access to any Transferred Personal Information, or to whom it otherwise discloses Transferred Personal Information are made aware of, and undertake to observe, the obligations imposed on the Recipient under this clause 6; and
		5. it will ensure that any of its officers, employees, volunteers, agents and sub-contractors who are able to obtain access to any Transferred Personal Information, or to whom it otherwise discloses Transferred Personal Information are made aware of, and undertake to observe, the obligations imposed on the Recipient under this clause 6.
	1. **Limitations on Compliance with IPPs**

Sub-clauses 6.1 and 6.2 do not apply to an act or practice of the Recipient which is required by or under a Law of an Australian jurisdiction other than Victoria which applies to the Recipient.

* 1. **Compliance with Local Laws**

The Recipient will not, in respect of Transferred Personal Information, do an act, or engage in a practice, that would breach any Laws which apply to the Recipient.

|  |
| --- |
| **Commentary:** Clause 6 makes the key elements of a data protection scheme enforceable against the Recipient. It is the main clause for transferring the obligations that the PDP Act imposes on the Organisation to the Recipient with the Transferred Personal Information. In some ways, clause 6 forms a checklist for the Organisation and the Recipient. An alternative formulation to sub-clause 6.2(a) is: ‘it will only use or disclose the Transferred Personal Information for the primary purpose provided for under clause 2 of this Agreement or for another purpose if that use or disclosure is permitted under the IPPs.’ This formulation is sufficient for the Organisation to comply with IPP 9, although the formulation in the Model Term 6.2(a) offers the Organisation more assurance. Sub-clause 6.2(c) addresses data-matching – a practice often relevant to a transborder dataflow – but only to the extent IPP 9 permits. Sub-clause 6.3 recognises the dynamic nature of information flows and information handling. It considers the training, oversight, early warnings and adjustments necessary when large datasets of personal information move from the hands of those who are familiar with the circumstances of collection – sometimes referred to as the ‘best custodian’ – into the hands of rganisations less familiar with the idiosyncrasies of the dataset.Sub-clause 6.4 provides an act or practice of the Recipient in respect of Transferred Personal Information which would breach an IPP or sub-clause 6.2 is not a breach of the Agreement if it is required by an Australian Law which applies to the Recipient. Such an act or practice must be notified under sub-clause 6.3(b). Sub-clause 6.4(b) and 6.3(b) should be considered with sub-clause 7.4, in which the Recipient warrants, as at the date of the Agreement, that legislation applying to the Recipient does not prevent the Recipient from complying with the IPPs in respect of the Transferred Personal Information. Accompanying transborder dataflows within Australia with coherent privacy protection standards is complex. The task would be simplified to some extent by the adoption of one uniform set of information privacy principles applying to all Organisations and Recipients. |

1. **Indemnities and Warranties**
	1. **Recipient’s Indemnity**

Subject to the provisions of this Agreement, the Recipient at all times indemnifies and holds harmless the Organisation, its officers, employees, volunteers, agents and sub-contractors (in this clause 7 referred to as ‘those indemnified’) from and against any loss, cost (including legal costs and expenses on a solicitor/own client basis) or liability incurred or suffered by any of those indemnified arising from or in connection with any complaint, claim, suit, demand, action or proceeding by any person (including, but not limited to, any award, order or similar judgment or direction by the OVIC) where such loss or liability was caused or contributed to by the Recipient’s act or omission (or an act or omission by the Recipient’s officers, employees, agents, volunteers or sub-Organisations) in handling Transferred Personal Information, whether deliberate or not.

* 1. **Limitation on Recipient’s Indemnity**

The Recipient’s liability to indemnify the Organisation under sub-clause 7.1 will be reduced proportionally to the extent that any negligent act or omission of those indemnified directly contributed to the loss or liability.

* 1. **Recipient’s Warranties**

The Recipient warrants that:

* + 1. any Law applying to the Recipient does not prevent the Recipient from:
			1. complying with IPPs in respect of the Transferred Personal Information; and
			2. fulfilling its obligations under this Agreement;
		2. the Recipient has made itself aware (and will keep itself aware) of the requirements of the PDP Act and of the IPPs in particular.
	1. **Survival**

The warranties and indemnities set out in this clause 7 will survive the expiration or termination of this Agreement.

|  |
| --- |
| **Commentary:** Clause 7 requires the Recipient indemnify the Organisation for any actions or omissions of the Recipient (and those working for it) that may adversely affect the Organisation. The indemnity would be reduced proportionally to the contribution by the Organisation and those working for the Organisation. The Recipient’s warranties are important to giving transborder data protection substance in practice. In effect, the Recipient warrants that, while it is not bound by the PDP Act as an Organisation, it will comply regardless as if it were an Organisation that is bound. |

1. **Termination**

This Agreement will be taken to have commenced on the Commencement Date and it will continue until terminated by written agreement between the parties.

Upon the termination of this Agreement, or upon the Organisation's written request prior to the termination of this Agreement, the Recipient will:

1. return or destroy (at the Organisation's election) all Transferred Personal Information including all copies, in whatever form, of the Transferred Personal Information held or controlled by the Recipient; and
2. deliver to the Organisation, a complete and up-to-date list of all persons or other legal entities that to the Recipient's knowledge have had access to, or control of, any of the Transferred Personal Information.

|  |
| --- |
| **Commentary:** The Organisation will need to consider what complying with IPP 4, in particular IPP 4.2, will require for personal information transferred outside Victoria.Information transferred to achieve a short-term purpose should be destroyed or returned oncethe purposes are fulfilled. If the transfer is for a long-term purpose, the Organisation may need to consider whether the terms of the Agreement are sufficient. Where destruction is effective and the preferred option, the Organisation should obtain written confirmation from the Recipient that destruction has happened. When digital data is involved, destruction is usually more complex than mere deletion from one place in an electronic information system. Copies and the hard disks and archives of multiple users need to be considered, and back-up regimes may present a significant challenge.The Organisation’s legally enforceable privacy obligations do not expire after a certain period, nor does the Recipient’s indemnity. Giving attention to the details of how personal information will be destroyed or returned is a good way to avoid privacy breaches in the future.  |

1. **Governing Law**
2. The parties agree this Agreement is governed by the Law of Victoria and irrevocably submit to the non-exclusive jurisdiction of the Courts and Tribunals of Victoria.
3. The Recipient must not claim Victorian jurisdiction as inconvenient.

|  |
| --- |
| **Commentary:** Clause 9 presumes the parties will want Victorian Law to apply, but leaves open the option for Organisations to bring proceedings in the Recipient’s jurisdiction. Having the Victorian Civil and Administrative Tribunal (**VCAT**) and Victorian courts remain the principal interpreters of the PDP Act and the IPPs promotes coherent development of case law.  |

1. **Other Laws**

To the extent that the terms of this Agreement are inconsistent with any relevant and applicable Laws, to the extent of the inconsistency those terms will not bind the parties.

|  |
| --- |
| **Commentary:** Clause 10 ensures the provisions of the Agreement are severable and enforceable in the event any are inconsistent with existing laws. This is a standard clause and may be dispensed with if the Agreement already contains similar provisions. |

1. PDP Act section 5(a). [↑](#endnote-ref-1)
2. PDP Act section 8C(1)(b). [↑](#endnote-ref-2)
3. PDP Act section 13. [↑](#endnote-ref-3)
4. PDP Act section 3. [↑](#endnote-ref-4)
5. Duggan v Moira Shire Council, Unreported, VCAT Reference No. G394/2004 (Senior Member Preuss, 9 February 2005); Complainant P v Local Council [2005] VPrivCmr 2; Complainant D v Minister [2003] VPriv Cmr 4; Complainant H v Local Council [2004] VPrivCmr 2. [↑](#endnote-ref-5)
6. **An individual’s mobile telephone number**: Complainant K v Local Council [2004] VPrivCmr 5; an individual’s work telephone number:*Complainant M v Tertiary Institution* [2004] VPrivCmr 7. [↑](#endnote-ref-6)
7. Seven Network (Operations) Ltd v Media Entertainment & Arts Alliance (2004) 148 FCR 145. [↑](#endnote-ref-7)
8. An organisation under the PDP Act may also be an organisation under the HR Act. The HR Act contains Health Privacy Principle (HPP) 9, which is similar to IPP 9 except that HPP 9 deals with the transfer of ‘health information’ (not ‘personal information’ under the PDP Act) to someone who is outside Victoria. So if the organisation transfers information containing ‘personal information’ under the PDP Act as well as ‘health information’ under the HR ACt to someone who is outside Victoria, the organisation will need to comply with both IPP 9 and HPP 9 unless the organisation is relevantly exempt under the PDP Act and the HR Act. [↑](#endnote-ref-8)
9. The website of the Office of the Victorian Information Commissioner contains information such as Guidelines and resources about the IPPs and other relevant background materials for reference. [↑](#endnote-ref-9)
10. *Privacy Act 1988* (Cth) section 2A(c). [↑](#endnote-ref-10)
11. Note this sub-clause refers (among other things) to transfers ‘necessary … for the implementation of pre-contractual measures taken in response to the individual’s request’. The requirement for a request from the individual will probably mean the sub-clause may rarely be relevant to large-scale government data transfers. Alternatively, transfers may be authorised by another Victorian statute. [↑](#endnote-ref-11)
12. Some agreements, such as Memoranda of Understanding, may not be binding and therefore would not be regarded as a ‘binding scheme or contract’ for the purposes of IPP 9.1(a). Moreover, multi- jurisdictional bodies, such as Ministerial Councils, may not be directly subject to the PDP Act where they are exempt from the definition of ‘public sector organisation’ as being an ‘exempt body’ under s 4 of the *Public Administration Act 2004* (Vic). [↑](#endnote-ref-12)
13. For example, Council of Australian Governments (COAG, comprising the Prime Minister, Premiers and Chief Ministers) or various Ministerial Councils, such as the Standing Committee of Attorneys-General (SCAG), the Australian Health Ministers’ Conference (AHMC) and the Australasian Police Ministers’ Council. [↑](#endnote-ref-13)