Privacy and Data Protection Bill 2014

Introduction Print

EXPLANATORY MEMORANDUM

General

The Privacy and Data Protection Bill 2014 (the Bill) establishes an information privacy and protective data security scheme for the Victorian public sector.

Clause Notes

PART 1—PRELIMINARY

Clause 1 sets out the main purposes of the Bill.

Clause 2 provides for the commencement of the Act. Clause 2(1) states that the Act comes into operation on a day or days to be proclaimed. Clause 2(2) states that Division 1 of Part 9, a consequential amendment, comes into operation on the later of the day after the day on which this Act receives the Royal Assent and the day on which section 278 of the **Victoria Police Act 2013** comes into operation. If a provision of this Bill does not come into operation before 9 December 2014, it comes into operation on that day.

Clause 3 defines words and expressions used in the Bill.

The Bill retains definitions where possible, and adapted as necessary, from the **Information Privacy Act 2000** as follows—

"Consent" can be express or implied from a particular course of conduct. This may be significant in the context of compliance with, for example, IPP 2 which allows an organisation to use personal information with the subject's consent.

This would mean, for example, that a person sending a letter to a Minister complaining about a government service in his or her Department would carry an implied consent to use that person's information to investigate the matter.

The definition of ***generally available publication*** includes information that is generally available to members of the public, whether free of charge or not, and encompasses public registers. While the Act does not apply to generally available publications, it does apply to public registers "so far as is reasonably practicable".

The definition of ***Information Privacy Principle*** (abbreviated in the Explanatory Memorandum and defined in the Act as ***IPP***) refers to the principles in Schedule 1 of the Act.
These principles were adapted from the federal Privacy Commissioner's National Principles for the Fair Handling of Personal Information, on which the Commonwealth Government's private sector privacy legislation was also based originally. Necessary changes have been made to bring them into a state-based public sector context and where there is separate legislation for the handling of health information in Victoria.

The definition of ***law enforcement agency*** includes particular organisations or individuals whose function or functions include law enforcement. The remainder of the definition, paragraphs (n) to (q), is intended to identify organisations by function. It is intended that, where an organisation exercises law enforcement functions, and even where those functions are a small part of the organisation's overall operations, it shall be defined as a law enforcement agency. For example, the Department of Environment and Primary Industries is authorised by its governing legislation to investigate and prosecute specific environmental offences. The Department of Human Services undertakes investigations into notifications of possible child abuse. The definition of law enforcement agency is intended to include such organisations, to the extent of their law enforcement functions.

The exemption available to law enforcement agencies is set out in clause 15. It will only operate in respect of a law enforcement agency's actual law enforcement functions and its community policing functions. Community policing functions are intended to refer to, for example, investigations about

missing persons, lost cattle or, in emergency situations, locating next of kin if required. The term "community policing" is not intended to refer to police work undertaken by members of the community.

The exemption is function-based for two reasons—first, in recognition of the significant number of government agencies which have law enforcement functions and, secondly, to accommodate an increasing diversity of law enforcement functions which extend beyond traditional police powers. In this way, it will have some flexibility to apply to agencies which are given law enforcement responsibilities in the future.

"Organisation" is the term adopted in Part 3 of the Bill to identify all entities which are regulated under it. The components of "organisation" are set out in clause 13.

The definition of ***personal information*** remains based on the **Privacy Act 1988** (Cth) in the interests of supporting a nationally consistent approach to the protection of information privacy. The definition only applies to information that is recorded in some form. It excludes health information, as defined in Schedule 2 of the Act, in recognition of the tailored treatment afforded to health records under the **Health Records Act 2001**.

The definition of ***public register*** includes only those registers the information on which is available to the public, whether free of charge or not. Public register information is recognised in the Act as a generally available publication. However, because of the potential for abuse through, for example, bulk commercial use of information, public registers are not immune from information privacy regulation.

The definition of ***State contract*** refers to a contract under which it is necessary for a contracted service provider to deal with personal information on behalf of an outsourcing organisation, or with the kinds of information addressed in Part 4. The reference in the definition to functions should be construed to refer only to those functions which are related to the distinctive operations of the outsourcing organisation. It would include the broader role and responsibilities that the organisation has in implementing government policies and delivering government funded services to the community. Community organisations that are contracted to deliver

government funded welfare services, for example, would be required to collect and handle any personal information associated with those services in accordance with the IPPs or an approved code of practice, and in accordance with their contractual obligations in respect of data protection in Part 4 of this Bill.

The definition of ***contracted service provider*** includes subcontractors (one or more) who undertake tasks which involve the receipt and handling of personal information. It is intended that the Commissioner has direct authority in respect of contracted service providers in Part 3, but not in Part 4.

Key new definitions included in respect of Part 3 Divisions 5, 6 and 7 and Parts 4 and 5 are—

- Approved information usage arrangement;
- Chief Statistician;
- Crime statistics data;
- Information handling provision;
- Protective data security and protective data security systems;
- Public interest determinations and temporary public interest determinations;
- Public sector data; and
- Victorian protective data security framework.

Clause 4 interprets various expressions for the purposes of the Bill.

Clause 5 sets out the objects of the Act. The objects refer a number of times to the handling of personal information. Section 3 defines the meaning of ***handling*** and ***information handling provision***.

Clause 6 describes the relationship of the Bill to other laws.

Subclause (1) provides that inconsistent provisions in any other Victorian Act will prevail over any provision of the Bill (other than Division 5, 6 or 7 of Part 3) to the extent that they are inconsistent. This will allow relevant aspects of the IPPs to overlay the operation of other Acts where requirements can be observed concurrently.

Subclause (2) specifically deals with the operation of the **Freedom of Information Act 1982** (FOI Act). When read with clause 12, it provides that none of the obligations, rights or machinery established under the FOI Act are to be affected by the Act. Any documents which are regulated under the FOI Act will continue to be so regulated and cannot be made subject to additional regulation under the Bill, except in respect of Part 4, Protective Data Security.

Clause 7 sets out rights and liabilities under the Bill. It states that the Bill must be taken not to create any general privacy right or any other rights additional to those which are specifically contained in the Bill. Similarly, nothing in the Bill is to be construed as giving rise to criminal liability except to the extent specifically described.

Clause 8 provides that the Bill binds the Crown.

PART 2—APPLICATION OF THIS ACT

Clause 9 defines ***information*** to mean personal information, public sector data, law enforcement data or crime statistics data.

Clause 10 exempts courts and tribunals from compliance with the Bill in respect of the exercise of their judicial or quasi judicial functions. The Bill will still apply to personal information collected for other functions, for example, the maintenance of staff records.

Clause 11 defines ***Parliamentary Committee*** and exempts from the application of this Bill, and from any IPP, the collection, holding, management, use, disclosure or transfer of personal information by a Parliamentary Committee in the course of carrying out its functions as a Parliamentary Committee. The clause gives effect to objects of the **Parliamentary Administration Act 2005** (No. 20 of 2005) including to promote the highest standards of governance in the administration of the Parliament of Victoria.

Clause 12 grants an exemption in respect of specified types of information that are regarded as publicly available information, including public registers. With limited exceptions, the Bill seeks only to regulate personal information and public sector data that is not publicly available.

Subclause (2) refers to the use of information held on a public register. It is intended that the Bill will apply so far as is reasonably practicable to personal information held on public registers. Such information stores are collected and held for particular purposes. While public register information should be able to be used for the, or one of the, legitimate purposes for which it was collected, it is intended that the Bill will in most cases treat uses outside those purposes as interferences with personal privacy, unless the handling is the subject of a mechanism in effect pursuant to Divisions 5, 6 and 7 of Part 3.

For example, it may be an interference with the privacy of an individual for a person to search the titles register at Land Victoria in order to identify and market products or services to a section of the Register that meets a particular socioeconomic profile. In these circumstances the organisation using that information may contravene the Act.

It is envisaged that organisations having responsibility for maintaining public registers that are made available over the internet will maintain a high standard of currency and accuracy of information on their website. In addition, it is expected that these organisations will ensure that other search engines that tap into the site, and archives that store information on it, do not retain any inaccurate data. For further guidance see OVPC, *Guidelines to Victoria's Information Privacy Principles*, 3rd edition, 2011, paras 3.34, 3.36.

PART 3—INFORMATION PRIVACY

Clause 13 lists those public sector organisations to which Part 3 of the Bill applies.

Clause 14 specifies the relationship between the provisions governing access to information under the FOI Act and the Bill. It provides that, for all documents or information that fall within the scope of the FOI Act, IPP 6 or a related applicable code of practice will not apply.

Clause 15 provides a limited exemption for law enforcement agencies. The exemption does not operate in respect of all IPPs and applies only in relation to the law enforcement and community policing functions of law enforcement agencies. That is, it does not exempt them from complying with all principles in respect

of, for example, their own staff records and other administrative matters. Community policing functions, for example, are intended to refer to such roles as licensing investigations and the operation of liquor forums, location of missing persons, providing necessary responses in public emergency and disaster situations and locating next of kin if required. The term **community policing** is not intended to refer to police work undertaken by members of the community.

Clause 16 explains what constitutes an interference with privacy of an individual.

Clause 17 explains the application of the Bill to outsourcing arrangements. It provides for differential application in respect of Part 4.

Clause 18 states that the IPPs are set out in Schedule 1. The Victorian IPPs were originally adapted from the former federal National Principles for the Fair Handling of Personal Information (the National Principles). The IPPs in Schedule 1 are reproduced from the Victorian **Information Privacy Act 2000**, in order to maintain the continuity and consistency of Victoria's privacy regime governing public sector organisations as far as possible. The IPPs must now be interpreted in light of section 13 of the **Charter of Human Rights and Responsibilities Act 2006**, which gives individuals a right not to have their privacy, family, home or correspondence unlawfully or arbitrarily interfered with.

The 13 Australian Privacy Principles (APPs), which came into force on 12 March 2014, have now replaced both the federal IPPs that previously applied to Australian and Norfolk Island Government agencies, and the National Privacy Principles (NPPs) that previously applied to private sector organisations.

The APPs regulate the handling of personal information, including health information, by Australian government agencies and some private sector organisations. A number of the APPs are significantly different from the previous federal principles, including APP 7 on the use and disclosure of personal information for the purpose of direct marketing, and APP 8 on cross-border disclosure of personal information. The ACT will enact new privacy legislation in 2014.

Victoria's IPPs do not include provisions specifically for health information. Health information privacy in Victoria continues to be regulated by the **Health Records Act 2001**. Nothing in the IPPs is intended to be taken to override any exemption in Part 2 of the Bill.

Clause 19 The Information Privacy Principles apply in relation to all personal information, whether collected by the organisation before or after the commencement of this section. It is intended that there be no gap between the operation of the **Information Privacy Act 2000** and this Bill.

Clause 20 contains the obligation, in subclause (1), for organisations to comply with the IPPs in respect of personal information that they handle. This obligation is immediate upon the commencement of the Bill. It is intended that there be no gap between the operation of the **Information Privacy Act 2000** and this Bill.

Subclause (2) describes the requirements for administering and using a public register. Although public registers contain information that is available to the public, it is intended that the personal privacy provisions of the Bill apply to their information "so far as is reasonably practicable". The rationale behind this policy is explained in clause 12.

Clause 21 provides, in subclause (1), that an organisation can discharge its duty to comply with an IPP in respect of personal information collected, held, used or disclosed by it through complying with a code of practice approved under this Part.

Organisations which handle personal information are thus given flexibility in the way that they can manage that personal information by developing codes of practice. The scheme allows approved codes of practice to set standards for information handling that differ from the default scheme as long as the standards are at least as stringent as those proposed by any IPP.

Codes can cover every part of the process of information handling, from collection to complaint handling. Alternatively, they can prescribe procedures in relation to smaller segments of the information handling process and rely on the statutory scheme for the rest. Organisations also have the freedom to

adapt a code in respect of a particular type of information they handle. See subclause (3).

A code of practice may also—

- address the issue of data matching;
- set guidelines to be followed in determining charges;
- prescribe procedures for dealing with complaints, including the appointment of an independent code administrator;
- prescribe remedies for successful complaints;
- provide for review of the code by the Commissioner; and
- provide for the expiry of the code.

Public sector bodies and councils may use a code of practice, under subclause (5), to assist them to discharge their duty to comply with the IPPs "so far as is reasonably practicable" in relation to a public register.

While public register information is publicly available, information privacy issues still arise with respect to public registers because they contain what would otherwise be personal information.

A code of practice would allow agencies and councils to outline how they will manage personal information on a public register responsibly and transparently according to their statutory obligations, and to restrict any potential for abuse.
More information about the regulation of public register information is set out in relation to clause 12.

Clause 22 sets out the mechanism for gaining approval of a code of practice. This is a formal process reflecting the legal status afforded to codes once they are approved. Subclause (1) provides that an organisation may seek approval of a code of practice or of an amendment of an approved code of practice by submitting it to the Commissioner.

If the Commissioner considers that the code (or amendment) is acceptable, he/she will so advise the Minister under subclause (3). The Minister may then recommend to the Governor in Council that the code (or amendment) be approved,

after which the approval would be noted in the Government Gazette.

Subclause (3) sets out the main criteria which the Commissioner must apply when assessing a code or variation. They are that—

- the code or amendment is consistent with the objects of this Bill;
- the code prescribes standards that are at least as stringent as the standards in the IPPs;
- the code specifies which organisations are to be bound by the code and indicates that the consent of those organisations has been obtained.

Before deciding whether or not to advise approval of a code or variation, the Commissioner, under subclause (4)—

- may consult any other person; and
- must have regard to the extent to which the public has been given an opportunity to comment on the code.

This will not necessarily mean that the Commissioner or the organisation will need to advertise a code. The circumstances of each application for approval will determine what is adequate.

Under subclause (5), a code of practice or amendment comes into operation on the day on which notice of approval is published in the Government Gazette or such later day as is expressed in the notice.

Clause 23 describes the procedure for organisations to subscribe to a code of practice that has been approved by the Commissioner.

Subclause (1) provides that an approved code of practice binds any organisation that sought and gained approval of it along with those whose consent was given at the time of approval. Any other organisation may be bound if it states that it intends to be bound by it by notice in writing given to the Commissioner.

Subclause (2) allows organisations to adopt all of an approved code or only certain parts that apply in relation to a specified class of information or activity. A notice given to the Commissioner under subclause (1) may indicate such a

qualification. The default scheme (the IPPs) will then supplement obligations in those areas not covered by code provisions.

Clause 24 specifies that an approved code has the same status as the default legislative scheme. That is, any act or practice that is a contravention of a code, even if it does not contravene an IPP, will still contravene the Bill.

Clause 25 provides for the Commissioner to establish a register of all approved codes of practice. Under subclause (2), a person may inspect the register and may obtain copies of documents for a fee set down in the regulations, if any.

Clause 26 allows a code of practice to be revoked by the same process as the approval is given in clause 22. That is, the Commissioner advises the Minister who may recommend to the Governor in Council that a code be revoked.

The Commissioner may act on his or her own initiative, or on an application for revocation made by an individual or organisation. Before deciding whether or not to advise the Minister to recommend revocation of a code or amendment, the Commissioner, under subclause (4)—

- must consult the organisation that sought approval of the code or variation;
- may consult any other person; and
- must have regard to the extent to which the public has been given an opportunity to comment on the proposed revocation.

Clause 27 preserves the validity of anything done prior to a code or amendment to a code being revoked, or a code expiring or ceasing to apply to an organisation. It also allows any proceedings or investigations relating to the period during which the code was operating, which had not been completed (or even commenced), to be completed on the terms of the code as it had operated earlier (subclauses (1) and (2)).

Subclause (3) provides that, where there has been revocation of an amendment of a code, the code will operate without that amendment from the day on which the amendment ceases to be in operation. The day an amendment ceases, through

revocation, is dealt with in clause 26. An amendment (or code) may also cease through expiry. Subclause (4) provides that an organisation (or its contracted service provider) will be bound by the original form of an IPP from the time that a code modification to that IPP ceases to operate.

Clause 28 outlines the procedure to be followed in cases where a person is incapable of making a request for access or incapable of accessing their personal information or incapable of communicating consent to an act of collection, holding, management, use, disclosure or transfer of personal information.

This procedure can apply when, as a result of one of the incapacities listed, a person is not capable of understanding the nature of giving consent or making a request for access.

In these cases, an authorised representative can act in the shoes of the individual. Subclause (4) ensures that a person can only take action as an authorised representative where the request or consent is not contrary to previously expressed wishes of the individual. The classes of persons who may qualify as authorised representatives are set out in subclause (6).

Clause 29 provides that an organisation may apply to the Commissioner for a determination that an act or practice of an organisation contravenes or may contravene an IPP (other than IPPs 4 or 6) or approved code of practice and that the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with that IPP or code of practice. The application must specify the act or practices to which the determination would apply; the relevant IPP or code of practice; and the reasons for the organisation seeking the determination. The Commissioner is expected to publish Guidelines as to what constitutes the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with that IPP or code of practice.

It is anticipated that the Commissioner will, in respect of each public interest determination and temporary public interest determination, ensure that the retention and destruction requirements applicable to other agencies with which information is to be shared are particularised.
These requirements may be expressed as conditions to the

public interest determination and temporary public interest determination.

Clause 30 provides that an application for a public interest determination may be taken to be an application for a temporary public interest determination on request.

Clause 31 provides that the Commissioner may make a public interest determination if satisfied that the public interest test set out in clause 29 has been met, having regard to specified matters.

Clause 32 provides that the effect of a public interest determination is that, in doing an act or engaging in a practice in accordance with the determination, an organisation is not required to comply with the IPP or approved code of practice to which the determination applies. It follows that the act or practice does not contravene the IPP to which the determination applies; and does not interfere with the privacy of an individual.

Clause 33 provides that a public interest determination has effect from the day of its publication until it expires, is revoked or is disallowed.

Clause 34 explains the process for amendment of a public interest determination.

Clause 35 explains the circumstances in which a public interest determination must be revoked by the Commissioner, and the procedural requirements to be met before revocation.

Clause 36 explains organisations' reporting responsibilities in respect of public interest determinations of more than 12 months' duration.

Clause 37 provides that the Commissioner may make a temporary public interest determination of up to 12 months' duration if circumstances require that a determination be made urgently.

Clause 38 sets out the requirements applicable to organisations in respect of an application for a temporary public interest determination.

Clause 39 provides that the Commissioner may make a temporary public interest determination if satisfied that the public interest test set out in subclause (1)(a) has been met, and the application raises matters that require that a determination be made urgently.

Clause 40 provides that a temporary public interest determination has effect from the day of its publication until it expires, is revoked or disallowed, or a public interest determination that has been made comes into effect.

Clause 41 explains the circumstances in which a temporary public interest determination must be revoked by the Commissioner, and the procedural requirements to be met before revocation.

Clause 42 explains that public interest determinations may be disallowed by Parliament, by means of section 15 and Part 5 of the **Subordinate Legislation Act 1994**.

Clause 43 defines the key terms ***adverse action***, ***lead party***, ***public purpose*** and ***relevant Minister*** in relation to information usage arrangements.

Clause 44 is intended to make clear that nothing in this Division requires an organisation to seek to have an information usage arrangement approved if the collection, holding, management, use, disclosure or transfer of personal information is already expressly permitted under this Bill or another enactment.

Clause 45 explains the meaning of the term "information usage arrangement" in this Division.

Information handling provisions are intended to address the situation where organisations are uncertain about the interpretation of information sharing provisions in their legislation, or there is disagreement between relevant organisations as to the correct interpretation of or interaction between information management provisions in relevant statutes.

Clause 46 explains which kinds of entities may be parties to which kinds of information usage arrangements.

Clause 47 provides for the Commissioner to receive an information usage arrangement submitted by a lead party and consider whether, in respect of the proposed arrangement, the public interest in handling of personal information in the proposed way would substantially outweigh the public interest in complying with the IPPs, or in not holding to be authorised a proposed information handling provision.

Clause 48 provides that the Commissioner must issue a report about an information usage arrangement in respect of which approval has been sought under clause 47.

Clause 49 explains the circumstances in which the Commissioner must issue a certificate approving an application for an information usage arrangement, and when the Commissioner has the discretion to refuse to issue such a certificate.

Clause 50 Subclause (1) explains who the Commissioner's report and any certificate issued in respect of an application for an information usage arrangement must be provided to. Subclause (2) sets out the Ministerial approval arrangements upon receipt of a report and a certificate.

A Minister or Ministers cannot approve an information usage arrangement unless a certificate in respect of it has been provided by the Commissioner.

Subclauses (4) and (5) require the Commissioner to publish approved information usage arrangements on the Commissioner's Internet site, however the Commissioner is not required to publish material that would disclose personal information or information which, if contained in a document, would be exempt under specified sections of the FOI Act.

Clause 51 sets out the effect of an approved information usage agreement, specifically in relation to whether it provides for acts and practices for handling personal information that modify or do not comply with an IPP (other than IPPs 4 or 6) or an approved code of practice specified in a Commissioner's certificate issued under clause 49; or whether it makes provision for handling of personal information for the purposes of an information handling provision.

Clause 52 provides that a lead party to an approved information usage arrangement may apply to the Commissioner for approval of an amendment to the arrangement. The approval process for amendment follows the process previously established for an application under the sections specified in subclause (2).

Clause 53 specifies the circumstances in which the relevant Minister must revoke the approval of an information usage arrangement and those circumstances in which the Minister has a discretion to revoke it.

The Commissioner must notify parties before notifying a Minister of the existence of grounds on which revocation must occur under subclause (1), that is, if the public interest test is no longer met in respect of variance or non-compliance with an IPP or the reasons in the application for approval of the information usage arrangement no longer apply.

The relevant Minister must notify the parties to the information usage agreement before revoking the arrangement on the ground that the reasons in the application for approval of the information usage arrangement no longer apply.

Clause 54 provides that a lead party must report to the Commissioner annually or on request in respect of the approved information usage arrangement. Content and timing of the report is to be consistent with any Guidelines published by the Commissioner.

On request the Commissioner must report to a relevant Minister about any approved information usage arrangement.
The Commissioner may report at any time to a relevant Minister about an approved information usage arrangement.

Clause 55 provides for the Commissioner to certify that a specified act or practice of an organisation is consistent with an IPP, an approved code of practice or an information handling provision.

Unless inappropriate, a certificate must include an expiry date. A certification remains in force until it expires, or is set aside earlier by a court or VCAT, and the certificate must be published on the Commissioner's Internet site.

Clause 56 provides that an individual or organisation whose interests are affected by the Commissioner's decision to issue a certificate under clause 55 may apply to VCAT for review of the decision. The Commissioner is a party to the review proceeding.

Clause 57 prescribes the threshold requirements for making a complaint to the Commissioner.

Subclause (1) allows a complaint to be made in respect of information currently or previously, but no longer, held by an organisation. Subclause (2) sets out the circumstances in which a complaint may be made to the Commissioner, as opposed to a "code administrator". Paragraph (c) of subclause (2) allows a person to make a complaint to the Commissioner where the person has complained to the relevant code administrator but

has not received an adequate response within 45 days. It is not intended that an adequate response would always be the resolution of the complaint. It may be that an adequate response, according to the circumstances, would be a letter explaining, for example, that the complaint had been received but for specified reasons could not be addressed substantively for 60 days. However, it would be expected that some form of contact would be made with the complainant within 45 days.

Under subclause (3), it is possible to consolidate complaints so that they may be by one complainant on behalf of others, with their consent. It is envisaged that this would operate in cases where there are substantially the same facts and a common respondent and where resolution of one complaint would be very likely to lead to resolution of all others. Other subclauses deal with formulation of the complaint, including specification of a respondent, assistance to be provided by staff of the Commissioner, and submission of the complaint to the Commissioner.

Clause 58 allows the Commissioner to deal with complaints referred by the Ombudsman or the Freedom of Information Commissioner.

Clause 59 specifies the manner in which children may make complaints to the Commissioner.

Clause 60 specifies the manner in which people with a disability may make complaints to the Commissioner.

Clause 61 requires the Commissioner to notify the respondent of a complaint as soon as possible after receiving it.

Clause 62 gives a discretion to the Commissioner to refuse to deal with a complaint in certain circumstances. Among other things, this clause seeks to ensure that any complaints procedures specified in a code of practice are followed first and that frivolous or vexatious complaints are screened out at the earliest opportunity.

Subclause (2) ensures that complainants and respondents are informed of the complainant's right to require the Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

Subclause (3) allows the Commissioner to undertake preliminary investigations to determine whether or not to deal with a complaint, including by inviting any person to attend the office of the Commissioner or to produce any documents.

Under subclause (4) a complainant may, within a specified period, require the Commissioner to refer a complaint to VCAT for hearing. In these circumstances, the Commissioner must so refer the complaint (subclause (5)). The Privacy Commissioner may dismiss complaints which the complainant has not asked to be referred to VCAT.

Clause 63 permits the Commissioner to refer a complaint to other specified Commissioners or the Ombudsman if the Commissioner considers that the complaint could be the subject of a complaint to them. Complainants must be notified of any referral and may take no further action under this Bill in relation to the complaint.

Clause 64 allows the Commissioner to dismiss a complaint which is subject to a long delay by the complainant. It is not envisaged that complaints would be dismissed lightly or without attempts by the Commissioner to locate the complainant or discover the reasons for delay.

Clause 65 allows the Minister to refer a complaint at any stage of its handling to VCAT for hearing. This provision would be used only in cases where the complaint related to an important issue of wider public policy. It is not intended that this clause would give the Minister the power to refer complaints to VCAT merely because the Minister was actually the complainant or named as the respondent.

Clause 66 gives the Commissioner the discretion to refuse to hear a complaint on the basis that it is not reasonably possible to conciliate. In such cases, the Commissioner must notify the parties of this assessment and, if asked in writing to do so, must refer the complaint to VCAT for hearing.

Clause 67 requires the Commissioner to make all reasonable endeavours to conciliate complaints where possible. It is expected that the vast majority of complaints will be resolved by conciliation. Other provisions in this Division support the requirement set out in this clause.

While it is intended that many complaints will be able to be resolved without the need for the Commissioner to do so, attendance may be compelled at a conciliation conference, under subclause (3).

Clause 68 gives the Commissioner the power to require any person to provide information or produce documents where the Commissioner considers that they would be relevant to a conciliation. Subclause (3) restricts this power in cases where the Secretary to the Department of Premier and Cabinet certifies that the information the subject of a request for production, if included in a document, would be classified as "exempt" under section 28(1) the FOI Act. That subsection refers to exempt documents which are Cabinet documents.

Subclause (3) is intended to operate as a supplement to clause 6(2). Clause 6(2) preserves the primacy of FOI procedures over the power of the Commissioner to compel production of documents (as opposed to information). Where the Commissioner is seeking to gain access to documents within the purview of the FOI Act, the procedure specified in that Act will continue to be the only enforceable means of access to the documents.

Clause 69 provides a mechanism for enforcement, by registration with VCAT, of conciliated agreements. Agreements which are registered are enforceable as orders of VCAT. The VCAT has a discretion to refuse to register agreements in certain circumstances, which does not affect the validity of the agreement but would prevent it from being enforced as an order.

Clause 70 provides that no evidence taken in the course of a conciliation is admissible before the Tribunal unless agreed by all parties. By this clause it is intended to encourage parties to pursue attempts at conciliation fully and frankly.

Clause 71 describes the procedure to be followed in the event that a conciliation fails.

Clause 72 allows a party or the Commissioner to apply to VCAT for an interim order pending further negotiation or conciliation of a complaint. Interim orders may only be made prior to any complaint being referred to VCAT. Subclause (3) sets out criteria for VCAT to consider in the making of an interim order. In making an interim order, VCAT may require an undertaking

as to costs and may specify the grounds under which the interim order would be lifted (subclause (6)). Subclause (8) provides that this clause is not to have any effect on VCAT's jurisdiction to make interim orders under its own Act.

Clause 73 sets out the jurisdiction of VCAT to hear information privacy complaints.

Clause 74 identifies the proper parties to a complaint before VCAT. The Commissioner will not generally be a party to complaints before VCAT, but may be joined by VCAT if required.

Clause 75 puts a limit of 30 days (with possible extension of a further 30 days) for the commencement of the hearing of a complaint referred to it by the Minister under clause 65.

Clause 76 restricts the use of documents produced to VCAT which are classified as exempt documents within the meaning of section 28(1) of the FOI Act. Subclause (2) allows VCAT to make orders about treatment of documents produced. However, in making such an order, VCAT must particularly consider subclause (4) which highlights the disclosure restrictions which are intended to apply to these documents.

Clause 77 describes what VCAT may do after hearing a complaint. In the event that VCAT finds a complaint proven, it may make the orders specified under paragraph (a) of subclause (1). Under subclause (2) these may include orders for correction or annotation of records of personal information. VCAT may also decide, under paragraph (b) of subclause (1), to make no order. If VCAT finds the complaint or part of it not proven, it may dismiss it under paragraph (c) of subclause (1).

Paragraph (d) of subclause (1) gives VCAT the power to make an order for reimbursement of the complainant for costs incurred in prosecuting the complaint regardless of the result.

Subclause (3) requires the Commissioner to report any orders relating to public registers to the relevant Minister or council. Under subclause (4) the Commissioner may also make recommendations in the report concerning legislative or administrative action in the interests of personal privacy.

Clause 78 contains the procedure for the Commissioner to issue a compliance notice. The compliance notice is designed to address serious contraventions of the IPPs or a code of practice or information usage arrangement. Where the Commissioner is satisfied that an organisation is deliberately disregarding its obligations under the Bill or where a breach is particularly serious, the Commissioner is able to direct the organisation to take action within a specified period. Failure to comply can incur large penalties.

Subclause (1) provides that the Commissioner may issue a compliance notice where two conditions are satisfied—

- an organisation or contracted service provider has contravened an IPP or an applicable code of practice or an approved information usage arrangement; and
- the act or practice is a serious or flagrant contravention, or has been repeated on at least five occasions within the previous two years.

A compliance notice requires the organisation to take specified action within a specified period to address the contravention. In circumstances where the specified period is not adequate time to address the contravention fully, an organisation will be required to give an undertaking to do so within a further specified period (subclause (3)). The Commissioner may issue a compliance notice on the Commissioner's own initiative or through the application of an individual who was a complainant under Division 8. Subclause (6) allows the Commissioner to take into account the extent to which the organisation has complied with a decision of VCAT under subdivision 5 of Division 8.

Clause 79 gives the Commissioner the powers to require any person to provide information or produce documents where the Commissioner considers that they would be relevant to making a decision whether or not to issue a compliance notice.

Subclause (3) restricts this power in cases where the Secretary to the Department of Premier and Cabinet certifies that the information the subject of a request for production, if included in a document, would be classified as an "exempt" Cabinet document under section 28(1) of the FOI Act.

Subclause (3) is intended to operate as a supplement to clause 6(2). Clause 6(2) preserves the primacy of FOI procedures over the power of the Commissioner to compel production of documents (as opposed to information). Where the Commissioner is seeking to gain access to documents within the purview of the FOI Act, the procedure specified in that Act will continue to be the only enforceable means of access to the documents.

Clause 80 gives the Commissioner the power to examine witnesses through administration of an oath or affirmation where they have been required to attend before the Commissioner under clause 79(2).

Clause 81 provides for operation of the privilege against self-incrimination. That privilege allows a person to refuse to answer a question or produce a document where the information given may tend to incriminate the person. Clause 81 is subject to clause 68(3) which prevents the Commissioner from having access to information where the Secretary to the Department of Premier and Cabinet gives a certificate under subclause (3) of clause 79.

Clause 82 specifies that it is an indictable offence for an organisation not to comply with a compliance notice. The maximum penalty in the case of a corporation is 3000 penalty units and 600 penalty units in any other case. Subclause (2) provides that a compliance notice takes effect on the later of—

- the expiry of the period specified in the notice;
- the expiry of any extended period under clause 78(3);
- the expiry of the period within which an application may be made for review of the decision to issue a notice; or
- the determination of a review in favour of the Commissioner.

Clause 83 provides that an individual or organisation affected by a compliance notice issued by the Commissioner may apply to VCAT for review of the decision to issue the notice. The Commissioner is a party to a proceeding on a review conducted in relation to this provision (subclause (3).

Subclause (2) provides that an application for review must be made within 28 days.

PART 4—PROTECTIVE DATA SECURITY

Clause 84 sets out the entities to which the protective data security provisions of the Bill in Part 4 apply. It is intended that, with limited exceptions, Part 4 will apply across the whole of Victorian government unless covered by the law enforcement data security provisions in Part 5 of the Bill.

Part 4 applies to Victorian Government Departments as public sector agencies that are public service bodies. Part 4 also applies to all Victorian Administrative Offices such as the Environment Protection Authority, the Public Records Office and the Victorian Government Solicitor's Office. Entities that are public entities or special bodies under the **Public Administration Act 2004** are, unless they are exempt under that Act in whole or in part for the purposes of this Bill, included for the purposes of Part 4.

Certain entities are explicitly excluded in subsection (2). Of these, the entities in subclause (2)(a) to (c) are exempt bodies. The health service entities cited in subclause (2)(d) to (g) that otherwise would be captured by the definition of ***public sector agency*** are excluded because they fall within the framework of Victoria's health legislation.

Provision has also been made for the Governor in Council to declare a body to be a body to which this Part applies.

Clause 85 provides that the Commissioner must develop the Victorian protective data security framework. It is recognised that a number of public sector entities have previously adapted other existing guidance on protective data security to their entity's needs. For this reason, the Victorian protective data security framework is required to be as consistent as possible with recognised existing guidance in this field as prescribed.

Both the framework and the related standards provided for in clause 86 are expected to draw on the principal elements of existing whole of Victorian government security policies, Australian and international security standards, policies, schemes, frameworks and benchmarks including alignment with the Australian Government Protective Security Policy

Framework (PSPF) in relation to data security specifically. However the Victorian standards will depart from the PSPF in a number of ways designed to support State government service delivery functions and reflect contemporary security standards.

Clause 86 provides that the Commissioner may issue general protective data security standards or customised protective data security standards tailored to specific circumstances. A customised protective data security standard will prevail over a general one to the extent of any inconsistency.

However, the Commissioner must not issue a protective data security standard unless it has been agreed by both the Attorney-General and the Minister for Technology. It is intended that ongoing consultation between relevant government departments will occur to assist in consistent future development and implementation of the framework and standards.

Clause 87 provides that protective data security standards may be amended, revoked or reissued in accordance with the procedures set out in clause 86.

Clause 88 provides that a public sector body Head for an agency or body to which Part 4 applies must ensure that that agency or body does not do an act or contravene a protective data security standard in respect of the public sector data collected, held, managed or disclosed by it or public sector data systems kept by it.

This obligation extends to ensuring that these requirements are also met by any contracted service provider for the relevant agency or body. Accordingly the public sector body Head must ensure that its contract with a contracted service provider imposes appropriate obligations on the contracted service provider to comply with any relevant protective data security standards. The Commissioner does not have direct authority over contracted service providers in respect of protective data security. However, it is considered that the general powers of the Commissioner under clause 104 would allow for the publication of model terms in respect of this obligation that are capable of being adopted into a State contract.

Clause 89 provides that within 2 years after the issue of protective data security standards, public sector body Heads must ensure that a security risk profile assessment is undertaken for their agency or body; and that a protective data security plan is developed for the agency or body that addresses the standards applicable to their agency or body. Because it is recognised that not all agencies or bodies subject to Part 4 have equal capacity or resources to meet their obligations under this Part, the Bill's head of power for the making of regulations provided for at clause 125 will enable differential application as required.

Under subclauses (2) and (3) the public sector body Head must ensure that the security risk profile assessment and plan developed for their agency or body covers its contracted service providers to the extent that the contracted service providers handle public sector data for the public sector body.

Public sector body Heads are required to ensure that the protective data security plan is reviewed if there is a significant change to their body or agency's operating environment or applicable security risks, or otherwise every 2 years. A copy of each protective data security plan must also be given to the Commissioner.

Clause 90 provides that protective data security plans are not subject to the FOI Act, because it is not considered to be in the public interest to make details of relevant entities' data security arrangements available to the public.

PART 5—LAW ENFORCEMENT DATA SECURITY

Clause 91 explains that this Part applies Victoria Police, the Chief Statistician and the Chief Statistician's employees or consultants under section 6 of the **Crime Statistics Act 2014**.

Clause 92 provides that under this Part the Commissioner may issue standards for the security and integrity of law enforcement data systems and crime statistics data systems, and for access to, and release of, law enforcement data and crime statistics data, including, but not limited to, the release of law enforcement data and crime statistics data to members of the public.

It is intended that there will be no gap in the application of the Standards for Victoria Police law enforcement data security published by the Commissioner for Law Enforcement Data

Security in July 2007, and any law enforcement data security standards issued under this Bill.

Subclauses (2) and (3) provide that the Commissioner must consult with the Chief Commissioner of Police and the Chief Statistician in developing standards applicable their functions. The Commissioner may amend, revoke and reissue law enforcement security standards in accordance with these subsections.

Clause 93 provides that a law enforcement data security standard prevails over a protective data security standard to the extent of any inconsistency.

Clause 94 requires Victoria Police not to do an act or engage in a practice that contravenes a law enforcement data security standard in respect of the law enforcement data collected, held, managed or disclosed by it or law enforcement data systems it keeps. This prohibition is also applicable to the Chief Statistician and associated employees and contractors in respect of crime statistics data.

PART 6—COMMISSIONER FOR PRIVACY AND DATA PROTECTION

Clause 95 establishes the Commissioner for Privacy and Data Protection.

Clause 96 provides that the Governor in Council may appoint a person as the Commissioner for Privacy and Data Protection. A person is not eligible for appointment as Commissioner if the person is a member of the Parliament of Victoria, or of the Commonwealth or of another State or Territory.

Clause 97 provides for the Commissioner to be paid as determined by the Governor in Council.

Clause 98 outlines the terms and conditions of appointment of the Commissioner, including period of office, terms and conditions, leave of absence and the restriction on engaging in other employment.

Subclause (6) provides that the **Public Administration Act 2004** does not apply to the Commissioner in respect of the office of Commissioner, except as provided in section 16 of that Act in relation to employees.

Clause 99 provides that the Commissioner ceases to hold office if he or she becomes insolvent, is convicted of an indictable offence or nominates for election for either House of the Parliament of Victoria, the Commonwealth or of any other State or Territory.

Subclause (2) specifies that the Privacy Commissioner may resign by notice in writing delivered to the Governor in Council.

Clause 100 contains the procedure for suspension of the Commissioner if the Governor in Council is satisfied on any ground that the Commissioner is unfit to hold to hold office.

If the Governor in Council uses the power in subclause (1) to suspend the Commissioner, the Minister must provide each House of Parliament with a full statement of the grounds of suspension within 7 sitting days (subclause (2)).

Under subclause (3), the Commissioner must be removed from office by the Governor in Council if each House of Parliament within 20 sitting days after the day when the statement was laid before it declares by resolution that the Commissioner ought to be removed from office.

If the declaration by resolution is not made within the specified time period the Governor in Council must restore the Commissioner to office (subclause (4)).

Subclause (5) provides that if the Commissioner is suspended from office under subsection (1), he or she is taken not to be the Commissioner during the period of suspension.

Clause 101 provides that the Governor in Council may appoint a person to act in the office of the Commissioner during a vacancy in that office, or where the Commissioner is absent or otherwise unable to perform the functions of the office.

The person appointed must not be a member of any Parliament in Australia.

Appointment is for a period not exceeding 6 months, and the Governor in Council may remove the acting Commissioner at any time (subclause (3)).

A person appointed as the acting Commissioner has all the powers and must perform all the duties of that office, and is entitled to the same remuneration and allowances as the Commissioner.

Clause 102 provides that an act or decision of the Commissioner or acting Commissioner is not invalid only because of a defect or irregularity relating to his or her appointment.

Clause 103 outlines the functions of the Commissioner.

Clause 104 gives the Commissioner the general power to perform his or her functions.

Clause 105 provides that the Commissioner must have regard to the objects of the Bill in performing his or her functions. The objects of the Bill are set out in Clause 5 of the Bill.

Clause 106 provides that the Commissioner may require access to data and data systems in respect of protective data security. Though the Commissioner does not have direct statutory authority in respect of the CSP, it is expected that public sector entities to which Part 4 applies could give a contractual direction to their CSP to produce data or give access to data systems to the Commissioner or otherwise cooperate with the Commissioner.

Clause 107 provides that the Commissioner may require the Chief Commissioner of Police to give the Commissioner access to law enforcement data or the Victoria Police law enforcement data system. The Chief Commissioner of Police may refuse to comply with the requirement. This provision has been included to ensure that in meeting the requirements of the Commissioner, the provision of access to data or systems does not impede the capacity of Victoria Police to carry out its law enforcement functions. The grounds upon which the Chief Commissioner may refuse to comply include instances in which giving access to law enforcement data or systems is reasonably likely to prejudice an investigation, prejudice a fair trial, disclose the identity of a confidential source of information or endanger the lives or physical safety of persons.

Clause 108 provides that the Commissioner may require the Chief Statistician to provide reasonable access to crime statistics data. The Chief Statistician may refuse to comply in the circumstances set out in subclause (3).

Clause 109 provides that the Commissioner may copy or take extracts from any data or documents accessed under clauses 106, 107 or 108 despite anything to the contrary in any other Act except the **Charter of Human Rights and Responsibilities Act 2006**.

Clause 110 provides that the Commissioner may request that a public sector body Head as defined in the **Public Administration Act 2004** provide him or her with any assistance that the Commissioner reasonably considers appropriate to perform his or her functions under this Bill relating to protective data security and law enforcement data security.

Clause 111 provides that at the request of the Minister, the Commissioner must provide the Minister with reports on any matter relating to information privacy, protective data security, crime statistics data security or law enforcement data security functions. The Minister may table a copy of such a report before each House of Parliament.

Subclause (3) allows the Commissioner, in the public interest, to publish reports and recommendations relating to any act or practice that the Commissioner considers to be an interference with the privacy of an individual or generally to the Commissioner's functions, whether or not the matters to be dealt with in any such report have been the subject of a report to the Minister.

Clause 112 provides that during the conduct of a compliance audit of a person, agency or body to which Parts 4 or 5 apply, the Commissioner may give written information to specified persons concerning any matter that the Commissioner considers warrants urgent investigation or attention.

Subclause (3) provides that the Commissioner must notify the Premier and the responsible Minister if such information is provided, and include a statement in the audit report that he or she has given information under this section during the conduct of the audit.

Clause 113 provides that the Commissioner may disclose to the IBAC any information obtained or received in the course of, or as a result of, the exercise of the functions of the Commissioner, if it is information relevant to the performance of functions or duties by the IBAC.

Subclause (2) provides that the Commissioner must notify the relevant public sector body Head of any disclosure made under subclause (1).

Clause 114 provides that any staff that are necessary for the purposes of the Bill are to be employed under Part 3 of the **Public Administration Act 2004**.

Subclause (2) provides that the Commissioner may engage as many consultants as are required to perform the Commissioner's functions under the Bill.

Clause 115 gives the Commissioner the power to delegate powers under the Act to certain persons, other than this power of delegation.

Clause 116 requires the Commissioner to make a report to the Minister by 30 September each year on the performance of the Commissioner's functions, and the exercise of powers, under the Bill during the financial year immediately preceding 30 June. The Minister must cause a copy of the report to be laid before each House of Parliament before 30 October in the year in which the report is given to the Minister.

PART 7—GENERAL

Clause 117 protects people from liability connected with taking action under the Bill.

Subclause (1) protects a person against actions for loss caused to anyone as a result of producing a document or giving any information or evidence to the Commissioner under this Bill, or giving the Commissioner access to any public sector data, crime statistics data or law enforcement data or any public sector organisation's data system, crime statistics data system or law enforcement data system under this Bill.

Subclause (2) protects a complainant against actions for loss caused to anyone as a result of the lodging of a complaint.

Subclause (3) protects an organisation, or any employee or agent of the organisation, from liability in any actions for defamation or breach of confidence or criminal offences as a result of the giving of access to information or disclosing information according to the Bill (subclauses (3) and (4)).

Subclause (5) provides that an organisation does not breach the IPPs only by reason of collecting, using, disclosing, transferring, providing access to or correcting an individual's personal information in response to a consent or request by an authorised representative whose consent or request is void by virtue of clause 28(4).

Clause 118 provides that an organisation (or person, agency or body to which Part 4 or 5 applies) and not its employee will be responsible for the actions of the employee provided that the employee was operating within the normal scope of his/her employment. For the purposes of this section, Victoria Police officers specified in subclause (3) are taken to be employees. An organisation may avoid liability under the Bill where it can show that it took reasonable precautions and exercised due diligence to prevent the relevant action from occurring. The equivalent protection applies to agents of a principal organisation acting within their authority. It does not apply to contracted service providers in their capacities as agents of an outsourcing organisation. They are excluded by clause 17(5).

Clause 119 allows an organisation to charge a prescribed fee for providing access to personal information.

Clause 120 Subclause (1) specifies the individuals to whom the secrecy provision applies. Under a general prohibition in subclause (2), a person to whom this section applies must not, either directly or indirectly, make a record of, disclose or communicate to any person any information about an individual or organisation obtained or received in the course of performing functions or duties exercising powers under this Bill or a former Act, except as provided for in subclause (3). A penalty of 60 penalty units applies.

Subclause (3) provides that a person to whom this clause applies may make a record, disclosure or communication referred to in subclause (2) by consent of the relevant individual or organisation, or if it is necessary to do so for the purposes of, or in connection with, the performance of a function or duty or the exercise of a power under this Bill or a former Act, that is, the **Information Privacy Act 2000** or the **Commissioner for Law Enforcement Data Security Act 2005**.

Clause 121 provides that the Commissioner must give notice and a reasonable opportunity to object before making disclosures or communications in relation to information obtained in consequence of the compulsory conference provisions of this Bill or the **Information Privacy Act 2000** as in force immediately before its repeal. A penalty of 60 penalty units applies.

Clause 122 prescribes a penalty for failing to comply with particular requests of the Commissioner or for obstructing the Commissioner in the performance of functions or furnishing the Commissioner with information or making a statement to the Commissioner knowing that it is false or misleading in a material particular.

Clause 123 states that, where an unincorporated organisation is found under the Bill to be guilty of an offence, each member of the committee of management of the organisation is to be taken to be guilty of the offence.

Clause 124 deals with the competency of persons to prosecute offences under the Bill.

Subclause (1) limits this to members of Victoria Police, and the Commissioner or a person authorised by the Commissioner.

Subclause (2) provides that it is to be presumed that, in the absence of evidence to the contrary, the person bringing the proceeding was authorised to bring it.

Clause 125 provides that the Governor in Council may make regulations in respect to any matter or thing required or permitted by this Bill to be prescribed or necessary to give effect to this Bill, including prescribing fees for providing access to personal information under this Bill.

Flexibility to develop regulations of differential application is provided for. For example, they may be of general or limited application or may differ according to differences in time, place or circumstance.

PART 8—REPEAL OF ACTS AND TRANSITIONAL AND SAVINGS PROVISIONS

Clause 126 provides for the repeal of the **Information Privacy Act 2000**.

Clause 127 provides for the repeal of the **Commissioner for Law Enforcement Data Security Act 2005**.

Clause 128 provides for Schedule 2, transitional and savings provisions, to have effect.

PART 9—CONSEQUENTIAL AMENDMENTS

Division 1 of Part 9 makes amendments relating to the **Victoria Police Act 2013**.

Clause 129 sets out relevant amendments to definitions in clause 3.

Clause 130 amends section 14(1) to refer to Victoria Police.

Clause 131 amends section 16(d) to refer to Victoria Police.

Clause 132 amends section 91(a) to refer to Victoria Police.

Clause 133 amends section 94(1) to refer to Victoria Police.

Clause 134 amends section 107 to refer to the relevant provision of the **Victoria Police Act 2013**.

Clause 135 amends section 118 to refer to relevant Victoria police officers.

Clause 136 amends section 124(1) to refer to police officer.

Clause 137 in Division 2 of Part 9 in respect of amendments relating to the **Legal Profession Uniform Law Application Act 2014**, this clause amends section 76(3).

Clause 138 in Division 3 of Part 9 in respect of amendments relating to the **Victorian Civil and Administrative Tribunal Act 1998** and other consequential amendments, this clause provides that Part 11A of Schedule 1 to the **Victorian Civil and Administrative Tribunal Act 1998** is repealed.

Clause 139 provides for a new Part 16AA of Schedule 1 to the **Victorian Civil and Administrative Tribunal Act 1998**.

Clause 140 provides that an Act specified in the heading to an item in Schedule 3 is amended as set out in that item.

Clause 141 provides that this Part and Schedule 3 are repealed on 9 December 2015. The repeal of this Part and Schedule 3 do not affect the amendments made by them.

SCHEDULES

SCHEDULE 1—THE INFORMATION PRIVACY PRINCIPLES

The Information Privacy Principles are re-enacted unchanged in this Bill.

Principle 1 sets out a framework for the collection of personal information, requiring, for example, organisations only to collect personal information which is necessary for their functions. Additional collection requirements specified under IPP 10 apply where sensitive information is being collected.

At the time it is collected or as soon as practicable afterwards, the organisation must take reasonable steps to ensure that individuals know who is collecting their information and why and inform them that they may gain access to it for correction. Sub-principles 1.4 and 1.5 requires organisations to collect personal information only from the subject of the information where possible or to inform the subject of the collection if information is obtained through a third party.

Principle 2 governs the use and disclosure of information held by organisations. In general, organisations must only use or disclose personal information for the purpose for which it was collected or, otherwise, with the consent of the subject. However, they are entitled to use or disclose personal information for a secondary purpose where it is related to the primary purpose of collection and the use or disclosure is within the reasonable expectations of the individual. This would be the case, for example, where the information was used to manage, evaluate or improve particular government services in relation to which the information was originally collected.

Secondary uses/disclosures are otherwise permitted in cases where there is a strong public interest in doing so. The remaining paragraphs set out the public interest grounds for secondary use and/or disclosure. These include, for example, where there is a serious threat to life (d), where disclosure is required by law (f) or for research in the public interest (c).

Paragraphs (g) and (h) of IPP 2.1 give latitude to organisations disclosing personal information to law enforcement agencies. In these circumstances the organisation holding the information would need to be satisfied that the

law enforcement agency needed the information for one of the purposes specified.

Minimal information about the purpose of collection by the law enforcement agency would usually be enough to establish that the disclosure was "reasonably necessary". Organisations may, alternatively, seek guidance from the Commissioner about what assurance they should require before releasing information to such an agency.

IPP 2.1(g) allows an organisation to disclose personal information to law enforcement agencies in these circumstances, however, it is not compelled to do so. In cases where an organisation does exercise this discretion to disclose information, IPP 2.2 requires it to make a note of the disclosure.

Principle 3 is a quality assurance principle seeking to ensure that personal information held by an organisation is accurate, complete and up to date.

Principle 4 requires organisations to protect personal information they hold from misuse, loss, unauthorised access, modification or disclosure. Organisations are also required to take reasonable steps to permanently de-identify personal information or destroy it when it is no longer needed.

Principle 5 encourages transparency by requiring organisations to document clearly their policies on management of personal information and to make those policies available to the public. Organisations must take reasonable steps to let people know, on request, what sort of personal information they hold, for what purpose and how they collect, hold, use and disclose that information.

Principle 6 provides individuals with a right to access their information and make corrections to it, where necessary. In Victoria, the Freedom of Information Act already provides a right of access to documents held by Government. The Bill does not propose to disrupt the established systems of access under this scheme by supplanting them or creating a concurrent system.

Accordingly, in the case of documents held by public sector agencies, the Freedom of Information Act will continue to be the only enforceable method of access. This arrangement is effected by clause 14 of the Bill.

However, Principle 6 applies to organisations which are not included under the Freedom of Information Act. This includes contracted service providers acting under State contracts. These organisations are required to provide access to personal information unless one of the paragraphs in sub-principle 6.1 applies. In these circumstances, the organisation is still required to consider whether the use of an intermediary would be adequate to satisfy a request for access (sub-principle 6.3).

As an alternative to access in cases where it would reveal evaluative material in connection with a commercially sensitive decision-making process, sub-principle 6.2 allows an organisation to offer an explanation instead of direct access. Sub-principle 6.4 restricts the scope for organisations to charge for access to the personal information they hold. It is intended that regulations made prescribing fees for access (clause 69) would be consistent with charges under the FOI Act. Under sub-principle 6.8, an organisation has 45 days within which to respond to requests for access.

Principle 7 imposes limits on the use of unique identifiers between public sector organisations. It provides that unique identifiers cannot be shared by different agencies except with consent of the individual or where it is necessary for their functions. Principle 7 provides a safeguard against the creation of a single identifier which could be used to cross-match data across all Government Departments.

Principle 8 preserves, where lawful and practicable, the right of individuals to remain anonymous in transactions with an organisation.

Principle 9 puts limits on the flow of information outside Victoria. An organisation is only allowed to transfer personal information outside Victoria if it reasonably believes the recipient is subject to a law, or other binding obligation, which imposes restrictions on the use of that information which are substantially similar to the Information Privacy Principles. Personal information may also be transferred with the individual's consent or if the transfer is necessary for the performance of a contract. If consent of the individual cannot practically be obtained, the organisation can only transfer the information if it is for the benefit of the individual and if the individual would be likely to consent.

Principle 10 regulates the collection of sensitive information, providing safeguards which are additional to those set out in IPP 1.

Sensitive information is defined at the beginning of the schedule as information about an individual's racial or ethnic origin, political opinions, membership of a political, professional or trade association, philosophical or religious beliefs or affiliations, membership of a trade union, sexual preferences or practices or criminal record.

In very limited circumstances, under sub-principle 10.2, this information can be collected without consent where necessary for the effective delivery of government welfare programs.

SCHEDULE 2—TRANSITIONAL AND SAVINGS PROVISIONS

Clause 1 sets out the definitions of terms used in this Schedule.

Clause 2 makes general transitional provisions in respect of the new Act. It provides that this Schedule does not affect or take away from the **Interpretation of Legislation Act 1984**.

Clause 3 provides that on and from commencement day, a reference to an old Act (that is, either the **Commissioner for Law Enforcement Data Security Act 2005** or the **Information Privacy Act 2000**) or in any Act or in any instrument made under any Act or in any other document must be read as a reference to this Act unless the context otherwise requires.

Clause 4 provides a table showing provisions from the **Information Privacy Act 2000** that are taken to be re-enacted (with modifications) by a specified provision or provisions of this Bill.

Clause 5 provides that on commencement day, the office of the Privacy Commissioner is abolished, and the incumbent goes out of office. In addition, all rights, property and assets that were vested in the Privacy Commissioner's office before that day, together with all debts, liabilities and obligations, are by force of clause 5(b) and (c), transferred to the office of the new Commissioner.

The new Commissioner also becomes a party, under clause 5(d) and (e), to any proceeding pending in any court or Tribunal to which the Privacy Commissioner was a party immediately before commencement day, and is a party to any arrangement or contract entered into by or on behalf of the Privacy Commissioner as a party and in force immediately before that day.

Clause 6 provides that on commencement day, the office of the Commissioner for Law Enforcement Data Security is abolished, and the incumbent goes out of office. In addition, all rights, property and assets that were vested in the Commissioner for Law Enforcement Data Security's office before that day, together with all debts, liabilities and obligations, are by force of clause 6(b) and (c), transferred to the office of the new Commissioner.

The new Commissioner also becomes a party, under clause 6(d) and (e), to any proceeding pending in any court or Tribunal to which the Commissioner for Law Enforcement Data Security was a party immediately before commencement day, and is a party to any arrangement or contract entered into by or on behalf of the Commissioner for Law Enforcement Data Security as a party and in force immediately before that day.

Clause 7 provides that on the commencement day, any reference to a former Commissioner (that is, the Commissioner for Law Enforcement Data Security or the Privacy Commissioner) in any Act (other than this new Act) or in any rule, regulation, order, agreement, instrument, deed or other document must, so far as it relates to any period on or after that day and if not inconsistent with the context or subject-matter, be construed as a reference to the new Commissioner.

Clause 8 provides that on the commencement day, any staff of the former Commissioners who were employed under Part 3 of the **Public Administration Act 2004** immediately before the commencement day are taken to be employed under section 114 of this Bill.

Clause 9 provides that on and after the commencement date, the Commissioner may commence or continue a prosecution for an offence committed under the old Acts.

Clause 10 applies if a reporting period has ended before the commencement day, and the Privacy Commissioner has not prepared a report of operations referred to in section 62 of the **Information Privacy Act 2000** for the period commencing on 1 July in any year and ending on 30 June in the following year ("reporting period").

Subclause (2) provides that on and after the commencement day the Commissioner must, for the reporting period, prepare a report of operations under Part 7 of the **Financial Management Act 1994** which includes the information required by section 62 of the **Information Privacy Act 2000**, which applies for the purposes of this subclause as if that section had not been repealed.

Clause 11 applies if a reporting period ends on or after the commencement day. Subclause (2) provides that on and after the commencement day the Commissioner must, for the reporting period, prepare a report which includes the information required by section 62 of the **Information Privacy Act 2000** and include that report as part of the Commissioner's first report after the end of the reporting period under clause 116 of this Bill.

Clause 12 provides that an approved code of practice under the **Information Privacy Act 2000** that was in operation immediately before that day is, on the commencement day, taken to be an approved code of practice under this Bill. Under subclause (2), on the commencement day the register of approved codes of practice kept under section 22 of the **Information Privacy Act 2000** is taken to be the register established under clause 25 of this Bill.

Clause 13 provides that this Bill applies to a complaint made but not declined, referred or finally determined under the **Information Privacy Act 2000** before the commencement day as if the complaint had been made under clause 58 of this Bill.

This Bill also applies to a compliance notice served under section 44 of the **Information Privacy Act 2000** but not set aside before the commencement day as if the compliance notice had been served under clause 78 of this Bill.

Clause 14 applies if a reporting period has ended before the commencement day, and the Commissioner for Law Enforcement Data Security has not made a report to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** for the period commencing on 1 July in any year and ending on 30 June in the following year ("reporting period").

Subclause (2) provides that on and after the commencement day the Commissioner must, for the reporting period, make a report to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005**, which applies for the purpose of this subclause as if that section had not been repealed.

Clause 15 applies if a reporting period ends on or after the commencement day. Subclause (2) provides that on and after the commencement day the Commissioner must, for the reporting period, make a report to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** and include that report as part of the Commissioner's first report after the end of the reporting period under clause 116 of this Bill. Section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** applies for the purpose of subclause (2) as if that section had not been repealed.

Clause 16 applies if a report has been made to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** before the commencement day, and that report has not been laid before each House of Parliament in accordance with that section before that day.

Subclause (2) provides that, despite the repeal of section 17 of the **Commissioner for Law Enforcement Data Security Act 2005**, section 17(2) continues to apply in respect of that report.

SCHEDULE 3—CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

The Schedule makes consequential amendments to other Victorian Acts that deal with information privacy and law enforcement data security.

References to the Information Privacy Act 2000

Because the Bill repeals the **Information Privacy Act 2000** and becomes the new principal legislation in respect of personal privacy, it is necessary to replace references to the **Information Privacy Act 2000** with references to the **Privacy and Data Protection Act 2014**.

References to the Commissioner for Law Enforcement Data Security

Because the Bill repeals the **Commissioner for Law Enforcement Data Security 2005** and provides instead for a Commissioner for Privacy and Data Protection under the new principal legislation, the **Privacy and Data Protection Act 2014**, it is necessary to replace references to the Commissioner for Law Enforcement Data Security with references to Commissioner for Privacy and Data Protection.

References to Standards under the Commissioner for Law Enforcement Data Security Act 2005

Because both law enforcement data security standards and data security standards applicable to all the entities to which Part 4 of the Bill applies may be issued under the Bill, it is necessary to replace references to Standards under the **Commissioner for Law Enforcement Data Security Act 2005** with references to Standards under the **Privacy and Data Protection Act 2014**.

References to the Privacy Commissioner

Because the Bill repeals the **Information Privacy Act 2000** including the definition of Privacy Commissioner, and provides instead for a Commissioner for Privacy and Data Protection under the Bill, the **Privacy and Data Protection Act 2014**, it is necessary to replace references to the Privacy Commissioner with references to the Commissioner for Privacy and Data Protection.

References to personal privacy

Because the Bill repeals the **Information Privacy Act 2000** and becomes the new principal legislation in respect of personal privacy, other than in the context of health information, it is necessary to replace references to personal information in connection with the **Information Privacy Act 2000** with references to personal privacy in connection with the **Privacy and Data Protection Act 2014**.