Version No. 003

Information Privacy Act 2000

Act No. 98/2000

Version incorporating amendments as at 1 July 2002

TABLE OF PROVISIONS

Version No. 003

Information Privacy Act 2000

Act No. 98/2000

Version incorporating amendments as at 1 July 2002

The Parliament of Victoria enacts as follows:

PART 1—PRELIMINARY

1. *Purposes*

The main purposes of this Act are—

(a) to establish a regime for the responsible collection and handling of personal information in the Victorian public sector;

(b) to provide individuals with rights of access to information about them held by organisations, including information held by contracted service providers;

(c) to provide individuals with the right to require an organisation to correct information about them held by the organisation, including information held by contracted service providers;

(d) to provide remedies for interferences with the information privacy of an individual;

(e) to provide for the appointment of a Privacy Commissioner.

2. *Commencement*

(1) Subject to sub-section (2), this Act comes into operation on a day or days to be proclaimed.

(2) If a provision referred to in sub-section (1) (except section 81) does not come into operation before 1 September 2001, it comes into operation on that day.

3. ***Definitions***

In this Act—

"applicable code of practice", in relation to an organisation, means an approved code of practice by which the organisation is bound;

"approved code of practice" means a code of practice approved under Part 4 as varied and in operation for the time being;

"body" means body (whether incorporated or not);

"child" means a person under the age of 18 years;

"code administrator", in relation to a code of practice, means an independent code administrator appointed in accordance with the code to whom complaints may be made in accordance with the code alleging a contravention of the code;

"Commonwealth-regulated organisation" means an agency within the meaning of the Privacy Act 1988 of the Commonwealth and to which that Act applies;

"consent" means express consent or implied consent;

"correct", in relation to personal information, means alter that information by way of amendment, deletion or addition;

"Council" has the same meaning as in the **Local Government Act 1989**;

"disability" has the same meaning as in the **Disability Services Act 1991**;

"enactment" means an Act or a Commonwealth Act or an instrument of a legislative character made under an Act or a Commonwealth Act;

"Federal Privacy Commissioner" means the Privacy Commissioner appointed under the Privacy Act 1988 of the Commonwealth;

"generally available publication" means a publication (whether in paper or electronic form) that is generally available to members of the public and includes information held on a public register;

"illness" means a physical, mental or emotional illness, and includes a suspected illness;

"individual" means a natural person;

"Information Privacy Principle" means any of the Information Privacy Principles set out in Schedule 1;

"insolvent under administration" means—

(a) a person who is an undischarged bankrupt; or

(b) a person for whom a debt agreement has been made under Part IX of the Bankruptcy Act 1966 of the Commonwealth (or the corresponding provisions of the law of another jurisdiction) if the debt agreement has not ended or has not been terminated; or

(c) a person who has executed a deed of arrangement under Part X of the Bankruptcy Act 1966 of the Commonwealth (or the corresponding provisions of the law of another

jurisdiction) if the terms of the deed have not been fully complied with; or

(d) a person whose creditors have accepted a composition under Part X of the Bankruptcy Act 1966 of the Commonwealth (or the corresponding provisions of the law of another jurisdiction) if a final payment has not been made under that composition;

"IPP" means Information Privacy Principle;

"law enforcement agency" means—

(a) the police force of Victoria or of any other State or of the Northern Territory; or

(b) the Australian Federal Police; or

(c) the National Crime Authority; or

(d) the Commissioner appointed under section 8A of the **Corrections Act 1986**; or

(e) the Business Licensing Authority established under Part 2 of the **Business Licensing Authority Act 1998**; or

(f) a commission established by a law of Victoria or the Commonwealth or of any other State or a Territory with the function of investigating matters relating to criminal activity generally or of a specified class or classes; or

(g) an agency responsible for the performance of functions or activities directed to—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences

or breaches of a law imposing a penalty or sanction for a breach; or

(ii) the management of property seized or restrained under laws relating to the confiscation of the proceeds of crime or the enforcement of such laws, or of orders made under such laws; or

(h) an agency responsible for the execution or implementation of an order or decision made by a court or tribunal, including an agency that—

(i) executes warrants; or

(ii) provides correctional services, including a contractor within the meaning of the **Corrections Act 1986**, or a sub-contractor of that contractor, but only in relation to a function or duty or the exercise of a power conferred on it by or under that Act; or

(iii) makes decisions relating to the release of persons from custody; or

(i) an agency responsible for the protection of the public revenue under a law administered by it;

S. 3(1) def. of "officer" amended by No. 44/2001 s. 3(Sch. item 64).

"officer", in relation to a body corporate, has the meaning given by section 82A of the Corporations Act;

"organisation" means a person or body that is an organisation to which this Act applies by force of Division 1 of Part 2;

"parent", in relation to a child, includes—

(a) a step-parent;

(b) an adoptive parent;

(c) a foster parent;

(d) a guardian;

(e) a person who has custody or daily care and control—

of the child;

S. 3(1) def. of "personal information" amended by No. 2/2001 s. 107(a).

"personal information" means 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** applies;

"personal privacy" means privacy of personal information;

"Privacy Commissioner" means Privacy Commissioner appointed under Part 7;

"public register" means a document held by a public sector agency or a Council and open to inspection by members of the public (whether or not on payment of a fee) by force of a provision made by or under an Act other than the **Freedom of Information Act 1982** or the **Public Records Act 1973** containing information that—

(a) a person or body was required or permitted to give to that public sector agency or Council by force of a provision made by or under an Act; and

(b) would be personal information if the document were not a generally available publication;

"public sector agency" means an Agency or public authority within the meaning of the **Public Sector Management and Employment Act 1998**;

"State contract" means a contract between an organisation and another person or body (whether an organisation for the purposes of this Act or not) under which services are to be provided to one (the outsourcing organisation) by the other (the contracted service provider) in connection with the performance of functions of the outsourcing organisation, including services that the outsourcing organisation is to provide to other persons or bodies;

"third party", in relation to personal information, means a person or body other than the organisation holding the information and the individual to whom the information relates;

"Tribunal" means Victorian Civil and Administrative Tribunal established by the **Victorian Civil and Administrative Tribunal Act 1998**.

4. ***Interpretative provisions***

(1) For the purposes of this Act, an organisation holds personal information if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria.

(2) If a provision of this Act refers to an IPP by a number, the reference is a reference to the IPP designated by that number.

(3) A reference in this Act to a contracted service provider is a reference to a person or body in the capacity of contracted service provider and includes a reference to a subcontractor of the contracted service provider (or of another such subcontractor) for the purposes (whether direct or indirect) of the State contract.

(4) Without limiting section 37(a) of the **Interpretation of Legislation Act 1984**, a reference in this Act to an organisation using a neuter pronoun includes a reference to an organisation that is a natural person, unless the contrary intention appears.

5. ***Objects of Act***

The objects of this Act are—

(a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;

(b) to promote awareness of responsible personal information handling practices in the public sector;

(c) to promote the responsible and transparent handling of personal information in the public sector.

6. ***Relationship of this Act to other laws***

(1) If a provision made by or under this Act is inconsistent with a provision made by or under any other Act that other provision prevails and the provision made by or under this Act is (to the extent of the inconsistency) of no force or effect.

(2) Without limiting sub-section (1), nothing in this Act affects the operation of the **Freedom of Information Act 1982** or any right, privilege, obligation or liability conferred or imposed under that Act or any exemption arising under that Act.

7. ***Nature of rights created by this Act***

(1) Nothing in this Act—

(a) gives rise to any civil cause of action; or

(b) without limiting paragraph (a), operates to create in any person any legal right enforceable in a court or tribunal—

otherwise than in accordance with the procedures set out in this Act.

(2) A contravention of this Act does not create any criminal liability except to the extent expressly provided by this Act.

8. ***Act binds the Crown***

(1) This Act binds the Crown in right of Victoria and, so far as the legislative power of the Parliament permits, the Crown in all its other capacities.

(2) Nothing in this Act makes the Crown in any of its capacities liable to be prosecuted for an offence.

———————

PART 2—APPLICATION OF THIS ACT

Division 1—Public Sector Organisations

9. ***Application of Act***

(1) This Act applies to—

(a) a Minister;

(b) a Parliamentary Secretary, including the Parliamentary Secretary of the Cabinet;

(c) a public sector agency;

(d) a Council;

(e) a body established or appointed for a public purpose by or under an Act;

(f) a body established or appointed for a public purpose by the Governor in Council, or by a Minister, otherwise than under an Act;

(g) a person holding an office or position established by or under an Act (other than the office of member of the Parliament of Victoria) or to which he or she was appointed by the Governor in Council, or by a Minister, otherwise than under an Act;

(h) a court or tribunal;

(i) the police force of Victoria;

(j) a contracted service provider, but only in relation to its provision of services under a State contract which contains a provision of a kind referred to in section 17(2);

(k) any other body that is declared, or to the extent that it is declared, by an Order under sub-section (2)(a) to be an organisation for the purposes of this sub-section—

excluding any person or body that is a Commonwealth-regulated organisation or declared, or to the extent that it is declared, by an Order under sub-section (2)(b) not to be an organisation for the purposes of the relevant paragraph of this sub-section.

(2) The Governor in Council may, by Order published in the Government Gazette—

(a) declare a body to be, either wholly or to the extent specified in the Order, an organisation for the purposes of sub-section (1); or

(b) declare a body referred to in paragraph (e) or (f) of sub-section (1), or a person holding an office or position referred to in paragraph (g) of sub-section (1), not to be an organisation for the purposes of that paragraph, either wholly or to the extent specified in the Order.

(3) The Minister may only recommend to the Governor in Council the making of an Order under sub-section (2)(b) in respect of a body or person if satisfied that the collection, holding, management, use, disclosure and transfer by that body or person of personal information is more appropriately governed by another scheme (whether contained in an enactment or given legislative force by an enactment) which would apply if that person or body were not an organisation for the purposes of the relevant paragraph of sub-section (1), either wholly or to the extent specified in the Order.

(4) A person or body to which this Act applies by force of sub-section (1) is an organisation for the purposes of this Act, either wholly or to the relevant extent.

(5) This section is subject to Division 2.

Division 2—Exemptions

10. ***Courts, tribunals, etc.***

Nothing in this Act or in any IPP applies in respect of the collection, holding, management, use, disclosure or transfer of personal information—

(a) in relation to its or his or her judicial or quasi-judicial functions, by—

(i) a court or tribunal; or

(ii) the holder of a judicial or quasi-judicial office or other office pertaining to a court or tribunal in his or her capacity as the holder of that office; or

(b) in relation to those matters which relate to the judicial or quasi-judicial functions of the court or tribunal, by—

(i) a registry or other office of a court or tribunal; or

(ii) the staff of such a registry or other office in their capacity as members of that staff.

11. ***Publicly-available information***

(1) Nothing in this Act or in any IPP applies to a document containing personal information, or to the personal information contained in a document, that is—

(a) a generally available publication; or

(b) kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(c) a public record under the control of the Keeper of Public Records that is available for public inspection in accordance with the **Public Records Act 1973**; or

(d) archives within the meaning of the Copyright Act 1968 of the Commonwealth.

(2) Sub-section (1) does not take away from section 16(4) which imposes duties on a public sector agency or a Council in administering a public register.

12. ***Freedom of Information Act 1982***

Nothing in IPP 6 or any applicable code of practice modifying the application of IPP 6 or prescribing how IPP 6 is to be applied or complied with applies to—

(a) a document containing personal information, or to the personal information contained in a document, that is—

(i) a document of an agency within the meaning of the **Freedom of Information Act 1982**; or

(ii) an official document of a Minister within the meaning of that Act—

and access can only be granted to that document or information, and that information can only be corrected, in accordance with the procedures set out in, and in the form required or permitted by, that Act; or

(b) a document containing personal information, or to the personal information contained in a document, to which access would not be granted under the **Freedom of Information Act 1982** because of section 5(3) or 6 of that Act.

S. 12(b) amended by No. 2/2001 s. 107(b).

13. ***Law enforcement***

It is not necessary for a law enforcement agency to comply with IPP 1.3 to 1.5, 2.1, 6.1 to 6.8, 7.1 to 7.4, 9.1 or 10.1 if it believes on reasonable grounds that the non-compliance is necessary—

(a) for the purposes of one or more of its, or any other law enforcement agency's, law enforcement functions or activities; or

(b) for the enforcement of laws relating to the confiscation of the proceeds of crime; or

(c) in connection with the conduct of proceedings commenced, or about to be commenced, in any court or tribunal; or

(d) in the case of the police force of Victoria, for the purposes of its community policing functions.

PART 3—INFORMATION PRIVACY

14. *Information Privacy Principles*

(1) The Information Privacy Principles are set out in Schedule 1.

(2) Nothing in any Information Privacy Principle affects the operation or extent of any exemption arising under Division 2 of Part 2 and those Principles must be construed accordingly.

(3) For the purposes of this Act, an act done or practice engaged in by an organisation is an interference with the privacy of an individual if, and only if, the act or practice is contrary to, or inconsistent with an Information Privacy Principle or an applicable code of practice.

15. *Application of IPPs*

(1) IPP 1 and IPP 10 apply only in relation to information collected on or after the commencement of this section.

(2) The remaining Information Privacy Principles apply in relation to all personal information, whether collected by the organisation before or after the commencement of this section.

16. *Organisations to comply with IPPs*

(1) On and from the first anniversary of the commencement of section 15, an organisation must not do an act, or engage in a practice, that contravenes an Information Privacy Principle in respect of personal information collected, held, managed, used, disclosed or transferred by it.

(2) Sub-section (1) does not apply to the doing of an act, or the engaging in of a practice, by an organisation that, but for this sub-section, would

constitute a contravention of an Information Privacy Principle, if—

(a) the doing of the act or the engaging in of the practice is necessary for the performance of a contract to which the organisation is a party entered into by the organisation before 26 May 2000; and

(b) the act is done or the practice is engaged in before the second anniversary of the commencement of section 15 or the end of any extension of that period granted in relation to that contract under sub-section (3).

(3) On the application of an organisation before the second anniversary of the commencement of section 15 or before the expiry of any extension of that period granted under this sub-section, the Privacy Commissioner may grant an extension of that period in relation to a specified contract if he or she is of the opinion that the organisation is doing its best—

(a) to comply with the IPPs consistent with its obligations under the contract; and

(b) to seek to have the contract re-negotiated to enable the organisation to comply fully with the IPPs.

(4) A public sector agency or a Council must, in administering a public register, so far as is reasonably practicable not do an act or engage in a practice that would contravene an Information Privacy Principle in respect of information collected, held, managed, used, disclosed or transferred by it in connection with the administration of the public register if that information were personal information.

17. ***Effect of outsourcing***

(1) Subject to this section, the status or effect for the purposes of this Act of an act or practice is not affected by the existence or operation of a State contract.

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

(3) If a provision of a kind referred to in sub-section (2) is in force under a State contract, the Information Privacy Principles and any applicable code of practice apply to an act done, or practice engaged in, by the contracted service provider in the same way and to the same extent as they would have applied to the outsourcing organisation in respect of that act or practice had it been directly done or engaged in by the outsourcing organisation.

(4) An act or practice that is an interference with the privacy of an individual done or engaged in by a contracted service provider for the purposes of the State contract must, for the purposes of this Act and any applicable code of practice, be taken to have been done or engaged in by the outsourcing organisation as well as the contracted service provider unless—

(a) the outsourcing organisation establishes that a provision of a kind referred to in sub-section (2) was in force under the State contract at the relevant time in relation to the act or practice; and

(b) the IPP or applicable code of practice to which the act or practice is contrary, or with which it is inconsistent, is capable of being enforced against the contracted service provider in accordance with the procedures set out in this Act.

(5) Section 68(1) does not apply to an act done or practice engaged in by a contracted service provider acting within the scope of a State contract.

PART 4—CODES OF PRACTICE

18. *Codes of practice*

(1) An organisation can discharge its duty to comply with an Information Privacy Principle in respect of personal information collected, held, managed, used, disclosed or transferred by it by complying with a code of practice approved under this Part and binding on the organisation.

(2) A code of practice may—

(a) modify the application of any one or more of the Information Privacy Principles by prescribing standards, whether or not in substitution for any Information Privacy Principle, that are at least as stringent as the standards prescribed by the Information Privacy Principle; or

(b) prescribe how any one or more of the Information Privacy Principles are to be applied, or are to be complied with.

(3) A code of practice may apply in relation to any one or more of the following—

(a) any specified information or class of information;

(b) any specified organisation or class of organisation;

(c) any specified activity or class of activity;

(d) any specified industry, profession or calling or class of industry, profession or calling.

(4) A code of practice may also—

(a) impose controls on an organisation that matches data for the purpose of producing or verifying information about an identifiable individual; or

(b) in relation to charging—

(i) set guidelines to be followed in determining charges; or

(ii) prescribe circumstances in which no charge may be imposed; or

(c) prescribe—

(i) procedures for dealing with complaints alleging a contravention of the code, including the appointment of an independent code administrator to whom complaints may be made; or

(ii) remedies available where a complaint is substantiated; or

(d) provide for the review of the code by the Privacy Commissioner; or

(e) provide for the expiry of the code.

(5) Sub-section (1) applies also to a public sector agency or a Council in seeking to discharge its duty to comply, so far as is reasonably practicable, with an Information Privacy Principle in relation to a public register as imposed by section 16(4) and this Part has effect accordingly.

19. ***Process for approval of code of practice or code variation***

(1) An organisation may seek approval of a code of practice, or of a variation of an approved code of practice, by submitting the code or variation to the Privacy Commissioner.

(2) The Governor in Council, on the recommendation of the Minister acting on the advice received from the Privacy Commissioner under sub-section (3), may by notice published in the Government Gazette approve a code of practice or a variation of an approved code of practice.

(3) The Privacy Commissioner may advise the Minister to recommend to the Governor in Council that a code of practice, or a variation of an approved code of practice, be approved if in his or her opinion—

(a) the code or variation is consistent with the objects of this Act in relation to the personal information to which the code applies; and

(b) the code of practice prescribes standards that are at least as stringent as the standards prescribed by the Information Privacy Principles; and

(c) the code specifies the organisations bound (either wholly or to a limited extent) by the code or a way of determining the organisations that are, or will be, bound (either wholly or to a limited extent) by the code; and

(d) only organisations that consent to be bound by the code are, or will be, bound by the code.

(4) Before deciding whether or not to advise the Minister to recommend approval of a code of practice or of a variation of an approved code of practice, the Privacy Commissioner—

(a) may consult any person or body that the Privacy Commissioner considers it appropriate to consult; and

(b) must have regard to the extent to which members of the public have been given an opportunity to comment on the code or variation.

(5) A code of practice or variation comes into operation at the beginning of—

(a) the day on which the notice of approval under sub-section (2) is published in the Government Gazette; or

(b) such later day as is expressed in that notice as the day on which the code or variation comes into operation.

20. ***Organisations bound by code of practice***

(1) An approved code of practice binds—

(a) any organisation—

(i) that sought approval of it; or

(ii) that consents to be bound by the approved code; and

(b) any organisation that, by notice in writing given to the Privacy Commissioner, states that it intends to be bound by the approved code of practice as it is then in operation and that is capable of applying to the organisation.

(2) A notice under sub-section (1)(b) may indicate an intention that the organisation be bound by the approved code of practice—

(a) generally; or

(b) only in respect of specified information or a specified class of information collected, held, used or disclosed by it; or

(c) only in respect of any specified activity or class of activity.

(3) A notice under sub-section (1)(b) has no effect unless the Privacy Commissioner approves it.

(4) The Privacy Commissioner may approve a notice under sub-section (1)(b) if satisfied that the approved code of practice is capable of applying to the organisation to the extent set out in the notice.

(5) An organisation is bound by an approved code of practice—

(a) in the case of an organisation referred to in sub-section (1)(a), on and from the coming into operation of the code; and

(b) in the case of an organisation referred to in sub-section (1)(b), on and from the date expressed in the notice under that sub-section as the date on and from which the organisation will be bound by the code or the date on which the organisation is notified of the Privacy Commissioner's approval of the notice, whichever is the later.

(6) An organisation bound by an approved code of practice may, by notice in writing given to the Privacy Commissioner, state that it intends to cease to be bound by that code.

(7) An organisation ceases to be bound by an approved code of practice on and from the date of the notice under sub-section (6) or such later date as is expressed in that notice as the date on and from which the organisation will cease to be bound by the code.

21. ***Effect of approved code***

If an approved code of practice is in operation and binding on an organisation, an act done, or practice engaged in, by the organisation that contravenes the code, even though that act or practice would not otherwise contravene any Information Privacy Principle, is, for the purposes of this Act, deemed to be a contravention of an

Information Privacy Principle and may be dealt with as provided by that code and this Act.

22. ***Codes of practice register***

(1) The Privacy Commissioner must cause a register of all approved codes of practice to be established and maintained and for that purpose may determine the form of the register.

(2) A person may during business hours—

(a) inspect the register and any documents that form part of it; or

(b) on the payment of any fee required by the regulations, obtain a copy of any entry in, or document forming part of, the register.

23. ***Revocation of approval***

(1) The Governor in Council, on the recommendation of the Minister acting on advice received from the Privacy Commissioner under sub-section (3), may by notice published in the Government Gazette revoke the approval of a code of practice or of a variation of an approved code of practice.

(2) The Privacy Commissioner may act under sub-section (1) on his or her own initiative or on an application for revocation made to him or her by an individual or organisation.

(3) The Privacy Commissioner may advise the Minister to recommend to the Governor in Council that a code of practice, or a variation of an approved code of practice, be revoked.

(4) Before deciding whether or not to advise the Minister to recommend revocation of the approval of a code of practice or of a variation of an approved code of practice, the Privacy Commissioner—

(a) must consult the organisation that sought approval of the code or variation and may consult any other person or body that the Privacy Commissioner considers it appropriate to consult; and

(b) must have regard to the extent to which members of the public have been given an opportunity to comment on the proposed revocation.

(5) An approved code of practice or approved variation ceases to be in operation at the beginning of—

(a) the day on which the notice of revocation under sub-section (1) is published in the Government Gazette; or

(b) such later day as is expressed in that notice as the day on which the code or variation ceases to be in operation.

24. ***Effect of revocation of approval or variation or expiry of approved code***

(1) The revocation of the approval of a code of practice or of a variation of an approved code of practice, or the expiry of an approved code of practice, or the ceasing of an organisation to be bound by a code of practice, does not—

(a) revive anything not in force or existing at the time at which the revocation, expiry or cessation becomes operative; or

(b) affect the previous operation of the code or anything duly done or suffered under, or in relation to, the code; or

(c) affect any right, privilege, obligation or liability acquired, accrued or incurred under, or in relation to, the code; or

(d) affect any penalty incurred in respect of any contravention of the code or in respect of any offence against section 48(1) committed in relation to a compliance notice issued because of any contravention of the code; or

(e) affect any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability or penalty as is mentioned in paragraphs (c) and (d)—

and any such investigation, legal proceeding or remedy may be instituted, continued or enforced and any such penalty may be imposed as if the code or variation had not been revoked or the code had not expired or the organisation had not ceased to be bound by the code.

(2) Subject to sub-section (1), if a variation of an approved code of practice is revoked, the code takes effect without that variation as from the beginning of the day on which the variation ceases to be in operation in all respects as if the variation had not been made.

(3) Nothing in this section prevents the application to an organisation of an IPP (without any modification) on and from the day on which an applicable code of practice, that modified the application of that IPP, ceases to be in operation.

———————

PART 5—COMPLAINTS

Division 1—Making a Complaint

25. ***Complaints***

(1) An individual in respect of whom personal information is, or has at any time been, held by an organisation may complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual.

(2) A complaint may be made under sub-section (1) if—

(a) there is no applicable code of practice in relation to the holding of the information by the organisation; or

(b) there is an applicable code of practice in relation to the holding of the information by the organisation but that code does not provide for the appointment of a code administrator to whom complaints may be made; or

(c) there is an applicable code of practice in relation to the holding of the information by the organisation that provides for the appointment of a code administrator and not less than 45 days before complaining under sub-section (1) the individual complained to the code administrator in accordance with the procedures set out in that code but has received no response or a response that the individual considers to be inadequate.

(3) In the case of an act or practice that may be an interference with the privacy of 2 or more individuals, any one of those individuals may make a complaint under sub-section (1) on behalf of all of the individuals with their consent.

(4) A complaint must be in writing and lodged with the Privacy Commissioner by hand, facsimile or other electronic transmission or post.

(5) It is the duty of employees in the office of the Privacy Commissioner to provide appropriate assistance to an individual who wishes to make a complaint and requires assistance to formulate the complaint.

(6) The complaint must specify the respondent to the complaint.

(7) If the organisation represents the Crown, the State shall be the respondent.

(8) If the organisation does not represent the Crown and—

(a) is a legal person, the organisation shall be the respondent; or

(b) is an unincorporated body, the members of the committee of management of the organisation shall be the respondents.

(9) A failure to comply with sub-section (6) does not render the complaint, or any step taken in relation to it, a nullity.

26. ***Complaint referred to Privacy Commissioner***

The Privacy Commissioner may treat a complaint referred to him or her by the Ombudsman under section 15A of the **Ombudsman Act 1973** as if it were a complaint made under section 25(1).

27. *Complaints by minors and people with an impairment*

(1) A complaint may be made—

(a) by a child; or

(b) on behalf of a child by—

(i) a parent of the child; or

(ii) any other individual chosen by the child or by a parent of the child; or

(iii) any other individual who, in the opinion of the Privacy Commissioner, has a sufficient interest in the subject-matter of the complaint.

(2) A child who is capable of understanding the general nature and effect of choosing an individual to make a complaint on his or her behalf may do so even if he or she is otherwise incapable of exercising powers.

(3) If an individual is unable to complain because of impairment, a complaint may be made on behalf of that individual by—

(a) another individual authorised by that individual to complain on his or her behalf; or

(b) if that individual is unable to authorise another individual, any other individual on his or her behalf who, in the opinion of the Privacy Commissioner, has a sufficient interest in the subject-matter of the complaint.

(4) In this section, **"impairment"** has the same meaning as in the **Equal Opportunity Act 1995**.

Division 2—Procedure after a Complaint is Made

28. *Privacy Commissioner must notify respondent*

The Privacy Commissioner must notify the respondent in writing of the complaint as soon as practicable after receiving it.

29. *Circumstances in which Privacy Commissioner may decline to entertain complaint*

(1) The Privacy Commissioner may decline to entertain a complaint made under section 25(1) by notifying the complainant and the respondent in writing to that effect within 90 days after the day on which the complaint was lodged if the Privacy Commissioner considers that—

(a) the act or practice about which the complaint has been made is not an interference with the privacy of an individual; or

(b) the act or practice is subject to an applicable code of practice and all appropriate mechanisms for seeking redress available under that code have not been exhausted; or

(c) although a complaint has been made to the Privacy Commissioner about the act or practice, the complainant has not complained to the respondent; or

(d) the complaint to the Privacy Commissioner was made more than 45 days after the complainant became aware of the act or practice; or

(e) the complaint is frivolous, vexatious, misconceived or lacking in substance; or

(f) the act or practice is the subject of an application under another enactment and the subject matter of the complaint has been, or

is being, dealt with adequately under that enactment; or

(g) the act or practice could be made the subject of an application under another enactment for a more appropriate remedy; or

(h) the complainant has complained to the respondent about the act or practice and either—

(i) the respondent has dealt, or is dealing, adequately with the complaint; or

(ii) the respondent has not yet had an adequate opportunity to deal with the complaint; or

(i) the complaint was made under section 27, on behalf of a child or a person with an impairment, by an individual who has an insufficient interest in the subject matter of the complaint.

(2) A notice under sub-section (1) must state that the complainant, by notice in writing given to the Privacy Commissioner, may require the Privacy Commissioner to refer the complaint to the Tribunal for hearing under Division 5.

(3) If the act or practice could be made the subject of an application under—

(a) the Privacy Act 1988 of the Commonwealth; or

(b) the **Ombudsman Act 1973**—

the Privacy Commissioner may refer the complaint to the Federal Privacy Commissioner or the Ombudsman, as the case may be, and notify the complainant and the respondent in writing of the referral.

(4) Before declining to entertain a complaint, the Privacy Commissioner may, by notice in writing, invite any person—

(a) to attend before the Privacy Commissioner, or an employee in the office of the Privacy Commissioner, for the purpose of discussing the subject matter of the complaint; or

(b) to produce any documents specified in the notice.

(5) Within 60 days after receiving the Privacy Commissioner's notice declining to entertain a complaint, the complainant, by notice in writing given to the Privacy Commissioner, may require him or her to refer the complaint to the Tribunal for hearing under Division 5.

(6) The Privacy Commissioner must comply with a notice under sub-section (5).

(7) If the complainant does not notify the Privacy Commissioner under sub-section (5), the Privacy Commissioner may dismiss the complaint.

(8) As soon as possible after a dismissal under sub-section (7), the Privacy Commissioner must, by written notice, notify the complainant and the respondent of the dismissal.

(9) A complainant may take no further action under this Act in relation to the subject matter of a complaint dismissed under this section.

30. ***Privacy Commissioner may dismiss stale complaint***

(1) The Privacy Commissioner may dismiss a complaint if he or she has had no substantive response from the complainant in the period of 90 days following a request by the Privacy Commissioner for a response in relation to the complaint.

(2) As soon as possible after a dismissal under sub-section (1), the Privacy Commissioner must, by notice in writing, notify the complainant and the respondent of the dismissal.

(3) A complainant may take no further action under this Act in relation to the subject matter of a complaint dismissed under this section.

31. ***Minister may refer a complaint direct to Tribunal***

(1) If the Minister considers that the subject matter of a complaint raises an issue of important public policy, the Minister may refer the complaint directly to the Tribunal for hearing under Division 5, whether or not the Privacy Commissioner has considered it or the complaint is in the process of being conciliated.

(2) The Minister is not a party to a proceeding on a complaint referred to the Tribunal under sub-section (1) unless joined by the Tribunal.

32. ***What happens if conciliation is inappropriate?***

(1) If the Privacy Commissioner does not consider it reasonably possible that a complaint may be conciliated successfully under Division 3, he or she must notify the complainant and the respondent in writing.

(2) A notice under sub-section (1) must state that the complainant, by notice in writing given to the Privacy Commissioner, may require the Privacy Commissioner to refer the complaint to the Tribunal for hearing under Division 5.

(3) Within 60 days after receiving the Privacy Commissioner's notice under sub-section (1), the complainant, by notice in writing given to the Privacy Commissioner, may require him or her to refer the complaint to the Tribunal for hearing under Division 5.

(4) The Privacy Commissioner must comply with a notice under sub-section (3).

(5) If the complainant does not notify the Privacy Commissioner under sub-section (3), the Privacy Commissioner may dismiss the complaint.

(6) As soon as possible after a dismissal under sub-section (5), the Privacy Commissioner must, by written notice, notify the complainant and the respondent of the dismissal.

(7) A complainant may take no further action under this Act in relation to the subject matter of a complaint dismissed under this section.

Division 3—Conciliation of Complaints

33. ***Conciliation process***

(1) If the Privacy Commissioner considers it reasonably possible that a complaint may be conciliated successfully, he or she must make all reasonable endeavours to conciliate the complaint.

(2) Sub-section (1) does not apply to a complaint—

(a) that the Privacy Commissioner has declined to entertain under section 29 or dismissed under section 30; or

(b) that the Minister has referred to the Tribunal under section 31.

(3) The Privacy Commissioner may require a party to attend a conciliation either personally or by a representative who has authority to settle the matter on behalf of the party.

34. ***Power to obtain information and documents***

(1) If the Privacy Commissioner has reason to believe that a person has information or a document relevant to a conciliation under this Division, the Privacy Commissioner may give to the person a written notice requiring the person—

(a) to give the information to the Privacy Commissioner in writing signed by the person or, in the case of a body corporate, by an officer of the body corporate; or

(b) to produce the document to the Privacy Commissioner.

(2) If the Privacy Commissioner has reason to believe that a person has information relevant to a conciliation under this Division, the Privacy Commissioner may give to the person a written notice requiring the person to attend before the Privacy Commissioner at a time and place specified in the notice to answer questions relevant to the complaint.

(3) The Privacy Commissioner is not entitled to require an agency within the meaning of the **Freedom of Information Act 1982** or a Minister to give any information if the Secretary to the Department of Premier and Cabinet furnishes to the Privacy Commissioner a certificate certifying that the giving of that information (including in answer to a question) would involve the disclosure of information which, if included in a document of the agency or an official document of the Minister, would cause the document to be an exempt document of a kind referred to in section 28(1) of the **Freedom of Information Act 1982**.

(4) The Privacy Commissioner may not conduct an investigation in respect of a certificate under sub-section (3) or question whether the information is of a kind referred to in section 28(1) of the **Freedom of Information Act 1982** or a decision to sign such a certificate.

34A. ***Referral of complaint to Health Services Commissioner***

S. 34A inserted by No. 2/2001 s. 108.

If the complaint could be made the subject of a complaint under the **Health Records Act 2001**, the Privacy Commissioner may refer the complaint to the Health Services Commissioner and notify the complainant and the respondent in writing of the referral.

35. ***Conciliation agreements***

(1) If, following conciliation, the parties to the complaint reach agreement with respect to the subject matter of the complaint—

(a) at the request of any party made within 30 days after agreement is reached, a written record of the conciliation agreement is to be prepared by the parties or the Privacy Commissioner; and

(b) the record must be signed by or on behalf of each party and certified by the Privacy Commissioner; and

(c) the Privacy Commissioner must give each party a copy of the signed and certified record.

(2) Any party, after notifying in writing the other party, may lodge a copy of the signed and certified record with the Tribunal for registration.

(3) Subject to sub-section (4), the Tribunal must register the record and give a certified copy of the registered record to each party.

(4) If the Tribunal, constituted by a presidential member, considers that it may not be practicable to enforce, or to supervise compliance with, a conciliation agreement, the Tribunal may refuse to register the record of the agreement.

(5) On registration, the record must be taken to be an order of the Tribunal in accordance with its terms and may be enforced accordingly.

(6) The refusal of the Tribunal to register the record of a conciliation agreement does not affect the validity of the agreement.

36. ***Evidence of conciliation is inadmissible***

Evidence of anything said or done in the course of a conciliation is not admissible in proceedings before the Tribunal or any other legal proceedings relating to the subject matter of the complaint, unless all parties to the conciliation otherwise agree.

37. ***What happens if conciliation fails?***

(1) If the Privacy Commissioner has attempted unsuccessfully to conciliate a complaint, he or she must notify the complainant and the respondent in writing.

(2) A notice under sub-section (1) must state that the complainant, by notice in writing given to the Privacy Commissioner, may require the Privacy Commissioner to refer the complaint to the Tribunal for hearing under Division 5.

(3) Within 60 days after receiving the Privacy Commissioner's notice under sub-section (1), the complainant, by notice in writing given to the Privacy Commissioner, may require the Privacy Commissioner to refer the complaint to the Tribunal for hearing under Division 5.

(4) The Privacy Commissioner must comply with a notice under sub-section (3).

(5) If the complainant does not notify the Privacy Commissioner under sub-section (3), the Privacy Commissioner may dismiss the complaint.

(6) As soon as possible after a dismissal under sub-section (5), the Privacy Commissioner must, by written notice, notify the complainant and the respondent of the dismissal.

(7) A complainant may take no further action under this Act in relation to the subject matter of a complaint dismissed under this section.

Division 4—Interim orders

38. ***Tribunal may make interim orders before hearing***

(1) A complainant or a respondent or the Privacy Commissioner may apply to the Tribunal for an interim order to prevent any party to the complaint from acting in a manner prejudicial to negotiations or conciliation or to any decision or order the Tribunal might subsequently make.

(2) An application may be made under sub-section (1) at any time before the complaint is referred to the Tribunal.

(3) In making an interim order, the Tribunal must have regard to—

(a) whether or not the complainant has established a prima facie case with respect to the complaint; and

(b) any possible detriment or advantage to the public interest in making the order; and

(c) any possible detriment to the complainant's or the respondent's case if the order is not made.

(4) An interim order applies for the period, not exceeding 28 days, specified in it and may be extended from time to time by the Tribunal.

(5) The party against whom the interim order is sought is a party to the proceeding on an application under sub-section (1).

(6) In making an interim order, the Tribunal—

(a) may require any undertaking as to costs or damages that it considers appropriate; and

(b) may make provision for the lifting of the order if specified conditions are met.

(7) The Tribunal may assess any costs or damages referred to in sub-section (6)(a).

(8) Nothing in this section affects or takes away from the Tribunal's power under section 123 of the **Victorian Civil and Administrative Tribunal Act 1998** to make orders of an interim nature in a proceeding in the Tribunal in respect of a complaint.

Division 5—Jurisdiction of the Tribunal

39. *When may the Tribunal hear a complaint?*

(1) The Tribunal may hear a complaint—

(a) referred to it by the Privacy Commissioner under section 29, 32 or 37;

(b) referred to it by the Minister under section 31.

(2) The Tribunal also has the jurisdiction conferred by section 38.

(3) Where a certificate has been given in respect of a document under section 34(3) or 45(3), the powers of the Tribunal do not extend to reviewing the decision to give the certificate and shall be limited to determining whether a document has been properly classified as an exempt document of a kind referred to in section 28(1) of the **Freedom of Information Act 1982**.

40. ***Who are the parties to a proceeding?***

(1) The complainant and the respondent are parties to a proceeding in respect of a complaint referred to in section 39(1).

(2) The Privacy Commissioner is not a party to a proceeding in respect of a complaint referred to in section 39(1)(a) unless joined by the Tribunal.

41. ***Time limits for certain complaints***

(1) The Tribunal must commence hearing a complaint within 30 days after its referral to the Tribunal if the complaint was referred to it by the Minister under section 31.

(2) The Tribunal, constituted by a presidential member, may extend the period of 30 days under sub-section (1) by one further period of not more than 30 days.

42. ***Inspection of exempt documents by Tribunal***

(1) Subject to sub-section (2) and to any order made by the Tribunal under section 51(2) of the **Victorian Civil and Administrative Tribunal Act 1998**, the Tribunal must do all things necessary to ensure that—

(a) any document produced to the Tribunal in proceedings under this Act that is claimed to be an exempt document of a kind referred to in section 28(1) of the **Freedom of Information Act 1982**, or the contents of

that document, is not disclosed to any person other than—

(i) a member of the Tribunal as constituted for the proceedings; or

(ii) a member of the staff of the Tribunal in the course of the performance of his or her duties as a member of that staff; and

(b) the document is returned to the respondent at the conclusion of the proceedings.

(2) The Tribunal may make such orders as it thinks necessary having regard to the nature of the proceedings.

(3) If the applicant is represented by a qualified legal practitioner, orders under sub-section (2) may include an order that the contents of a document produced to the Tribunal that is claimed to be an exempt document be disclosed to that legal practitioner.

(4) In making an order under sub-section (2), the Tribunal must be guided by the principle that the contents of a document that is claimed to be an exempt document should not normally be disclosed except in accordance with an order of the Tribunal under section 51(2) of the **Victorian Civil and Administrative Tribunal Act 1998**.

(5) If a complaint under section 39 relates to a document or part of a document in relation to which disclosure has been refused on the grounds specified in section 28 of the **Freedom of Information Act 1982**, the Tribunal may, if it regards it as appropriate to do so, announce its findings in terms which neither confirm nor deny the existence of the document in question.

43. ***What may the Tribunal decide?***

(1) After hearing the evidence and representations that the parties to a complaint desire to adduce or make, the Tribunal may—

(a) find the complaint or any part of it proven and make any one or more of the following orders—

(i) an order restraining the respondent, or the organisation of which the respondents are members of the committee of management, from repeating or continuing any act or practice the subject of the complaint which the Tribunal has found to constitute an interference with the privacy of an individual;

(ii) an order that the respondent perform or carry out any reasonable act or course of conduct to redress any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of the act or practice the subject of the complaint;

(iii) an order that the complainant is entitled to a specified amount, not exceeding $100 000, by way of compensation for any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of the act or practice the subject of the complaint;

(iv) if the act or practice the subject of the complaint is subject to an approved code of practice, an order that the code administrator take specified steps in the matter, which may include using conciliation or mediation, securing an apology or undertaking as to future conduct from the respondent or the payment of compensation, not exceeding $100 000, by the respondent; or

(b) find the complaint or any part of it proven but decline to take any further action in the matter; or

(c) find the complaint or any part of it not proven and make an order that the complaint or part be dismissed; or

(d) in any case, make an order that the complainant is entitled to a specified amount to reimburse the complainant for expenses reasonably incurred by the complainant in connection with the making of the complaint and the proceedings held in respect of it under this Act.

(2) In an order under sub-paragraph (i) or (ii) of paragraph (a) of sub-section (1) arising out of a breach of IPP 6.5 or 6.6, the Tribunal may include an order that—

(a) an organisation or respondent make an appropriate correction to the personal information; or

(b) an organisation or respondent attach to the record of personal information a statement provided by the complainant of a correction sought by the complainant.

(3) If an order of the Tribunal relates to a public register, the Privacy Commissioner must, as soon as practicable after its making, report the order to the Minister responsible for the public sector agency or Council that administers that public register.

(4) The Privacy Commissioner may include in a report under sub-section (3) recommendations in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of personal privacy.

PART 6—ENFORCEMENT OF INFORMATION PRIVACY PRINCIPLES

44. *Compliance notice*

(1) The Privacy Commissioner may serve a compliance notice on an organisation, if it appears to him or her that—

(a) the organisation has done an act or engaged in a practice in contravention of an Information Privacy Principle, including an act or practice that is in contravention of an applicable code of practice; and

(b) the act or practice—

(i) constitutes a serious or flagrant contravention; or

(ii) is of a kind that has been done or engaged in by the organisation on at least 5 separate occasions within the previous 2 years.

(2) A compliance notice requires the organisation to take specified action within a specified period for the purpose of ensuring compliance with the Information Privacy Principle or applicable code of practice.

(3) If the Privacy Commissioner is satisfied, on the application of an organisation on which a compliance notice is served, that it is not reasonably possible to take the action specified in the notice within the period specified in the notice, the Privacy Commissioner may extend the period specified in the notice on the giving to him or her by the organisation of an undertaking to take the specified action within the extended period.

(4) The Privacy Commissioner may only extend a period under sub-section (3) if an application for the extension is made before the period specified in the notice expires.

(5) The Privacy Commissioner may act under sub-section (1) on his or her own initiative or on an application by an individual who was a complainant under Part 5.

(6) In deciding whether or not to serve a compliance notice, the Privacy Commissioner may have regard to the extent to which the organisation has complied with a decision of the Tribunal under Division 5 of Part 5.

45. ***Power to obtain information and documents***

(1) If the Privacy Commissioner has reason to believe that a person has information or a document relevant to a decision to serve a compliance notice under section 44(1), the Privacy Commissioner may give to the person a written notice requiring the person—

(a) to give the information to the Privacy Commissioner in writing signed by the person or, in the case of a body corporate, by an officer of the body corporate; or

(b) to produce the document to the Privacy Commissioner.

(2) If the Privacy Commissioner has reason to believe that a person has information relevant to a decision to serve a compliance notice under section 44(1), the Privacy Commissioner may give to the person a written notice requiring the person to attend before the Privacy Commissioner at a time and place specified in the notice to answer questions relevant to the decision.

(3) The Privacy Commissioner is not entitled to require an agency within the meaning of the

Freedom of Information Act 1982 or a Minister to give any information if the Secretary to the Department of Premier and Cabinet furnishes to the Privacy Commissioner a certificate certifying that the giving of that information (including in answer to a question) would involve the disclosure of information which, if included in a document of the agency or an official document of the Minister, would cause the document to be an exempt document of a kind referred to in section 28(1) of the **Freedom of Information Act 1982**.

(4) The Privacy Commissioner may not conduct an investigation in respect of a certificate under sub-section (3) or question whether the information is of a kind referred to in section 28(1) of the **Freedom of Information Act 1982** or a decision to sign such a certificate.

46. ***Power to examine witnesses***

(1) The Privacy Commissioner may administer an oath or affirmation to a person required under section 45(2) to attend before the Privacy Commissioner and may examine the person on oath or affirmation.

(2) The oath or affirmation to be taken or made by a person for the purposes of this section is an oath or affirmation that the answers the person will give will be true.

47. ***Protection against self-incrimination***

(1) It is a reasonable excuse for a natural person to refuse or fail to give information or answer a question or to produce a document when required to do so under this Part if giving the information or answering the question or producing the document might tend to incriminate the person.

(2) This section does not limit section 45(3).

48. ***Offence not to comply with compliance notice***

(1) An organisation must comply with a compliance notice served on it under section 44(1) that is in effect.

Penalty: In the case of a body corporate, 3000 penalty units;

In any other case, 600 penalty units.

(2) A compliance notice served under section 44(1) does not take effect—

(a) until the expiry of the period specified in the notice; or

(b) until the expiry of any extended period fixed under section 44(3); or

(c) until the expiry of the period within which an application for review of the decision to serve the notice may be made to the Tribunal under section 49(1); or

(d) if an application is made under section 49(1) for review of the decision to serve the notice, unless and until the review has been determined in favour of the Privacy Commissioner—

whichever is the later.

(3) An offence against sub-section (1) is an indictable offence.

49. ***Application for review***

(1) An individual or organisation whose interests are affected by a decision of the Privacy Commissioner under section 44(1) to serve a compliance notice may apply to the Tribunal for review of the decision.

(2) An application for review must be made within 28 days after the later of—

(a) the day on which the decision is made; or

(b) if, under the **Victorian Civil and Administrative Tribunal Act 1998**, the individual or organisation requests a statement of reasons for the decision, the day on which the statement of reasons is given to the individual or organisation or the individual or organisation is informed under section 46(5) of that Act that a statement of reasons will not be given.

(3) The Privacy Commissioner is a party to a proceeding on a review under this section.

PART 7—PRIVACY COMMISSIONER

50. *Privacy Commissioner*

(1) There shall be a Privacy Commissioner who shall be appointed by the Governor in Council.

(2) The Privacy Commissioner shall not be a member of the Parliament of Victoria or of the Commonwealth or of any other State or a Territory.

51. *Remuneration and allowances*

The Privacy Commissioner is entitled to be paid the remuneration and allowances that are determined by the Governor in Council.

52. *Terms and conditions of appointment*

(1) Subject to this Part, the Privacy Commissioner holds office for the period, not exceeding 7 years, that is specified in the instrument of appointment but is eligible for re-appointment.

(2) Subject to this Part, the Privacy Commissioner holds office on the terms and conditions determined by the Governor in Council.

(3) The Privacy Commissioner is entitled to leave of absence as determined by the Governor in Council.

(4) The Privacy Commissioner must not engage, directly or indirectly, in paid employment outside the duties of Privacy Commissioner.

(5) The **Public Sector Management and Employment Act 1998** does not apply to the Privacy Commissioner in respect of the office of Privacy Commissioner, except as provided in section 16 of that Act.

53. ***Vacancy, resignation***

(1) The Privacy Commissioner ceases to hold office if he or she—

(a) becomes an insolvent under administration; or

(b) is convicted of an indictable offence or an offence which, if committed in Victoria, would be an indictable offence; or

(c) nominates for election for either House of the Parliament of Victoria or of the Commonwealth or of any other State or a Territory.

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

54. ***Suspension of Privacy Commissioner***

(1) The Governor in Council may suspend the Privacy Commissioner from office.

(2) The Minister must cause to be laid before each House of Parliament a full statement of the grounds of suspension within 7 sitting days of that House after the suspension.

(3) The Privacy 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 is laid before it declares by resolution that the Privacy Commissioner ought to be removed from office.

(4) The Governor in Council must remove the suspension and restore the Privacy Commissioner to office unless each House makes a declaration of the kind specified in sub-section (3) within the time specified in that sub-section.

55. ***Acting appointment***

(1) The Governor in Council may appoint a person to act in the office of Privacy Commissioner—

(a) during a vacancy in that office; or

(b) during a period or all periods when the person holding that office is absent from duty or is, for any reason, unable to perform the duties of the office.

(2) An appointment under sub-section (1) is for the period, not exceeding 6 months, that is specified in the instrument of appointment.

(3) A person is not eligible to be appointed under sub-section (1) if the person is a member of the Parliament of Victoria or of the Commonwealth or of any other State or a Territory.

(4) The Governor in Council may at any time remove the acting Privacy Commissioner from office.

(5) While a person is acting in the office of the Privacy Commissioner in accordance with this section, the person—

(a) has, and may exercise, all the powers and must perform all the duties of that office under this Act; and

(b) is entitled to be paid the remuneration and allowances that the Privacy Commissioner would have been entitled to for performing those duties.

56. ***Validity of acts and decisions***

An act or decision of the Privacy Commissioner or acting Privacy Commissioner is not invalid only because—

(a) of a defect or irregularity in or in connection with his or her appointment; or

(b) in the case of an acting Privacy Commissioner, that the occasion for so acting had not arisen or had ceased.

57. ***Staff***

(1) There may be employed under Part 3 of the **Public Sector Management and Employment Act 1998** any employees that are necessary for the purposes of this Act.

(2) The Privacy Commissioner may engage as many consultants as are required for the exercise of his or her functions.

58. ***Functions***

The functions of the Privacy Commissioner are—

(a) to promote an understanding and acceptance of the Information Privacy Principles and of the objects of those Principles;

(b) in accordance with Part 4, to consider at the request of an organisation whether to advise the Minister to recommend to the Governor in Council the approval of a code of practice (or of a variation of an approved code of practice) in relation to that organisation;

(c) in accordance with Part 4, to consider at the request of an individual or organisation, or on his or her own initiative, whether to advise the Minister to recommend to the Governor in Council the revocation of the approval of a code of practice or of a variation of an approved code of practice;

(d) to issue guidelines in relation to the development of codes of practice and variations of a kind referred to in paragraph (b);

(e) to issue guidelines on procedures to be adopted, consistent with the procedures under the **Freedom of Information Act 1982**, where—

(i) the organisation holding the personal information is an agency within the meaning of that Act or a Minister; and

(ii) the personal information is contained in a document of the agency, or an official document of a Minister, within the meaning of that Act;

(f) to 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;

(g) to examine the practice of an organisation with respect to personal information maintained by that organisation for the purpose of ascertaining whether or not the information is maintained according to the Information Privacy Principles or any applicable code of practice;

(h) subject to this Act, to receive complaints about an act or practice of an organisation—

(i) that may contravene an Information Privacy Principle; or

(ii) that may interfere with the privacy of an individual or may otherwise have an adverse effect on the privacy of an individual—

and, if the Privacy Commissioner considers it appropriate to do so, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the complaint;

(i) to issue compliance notices under Part 6 and to carry out an investigation for this purpose;

(j) to conduct or commission audits of records of personal information maintained by an organisation for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles or any applicable code of practice;

(k) to monitor and report on the adequacy of equipment and user safeguards;

(l) to examine and assess any proposed legislation that would require or authorise acts or practices of an organisation that may, in the absence of the legislation, be interferences with the privacy of an individual or that may otherwise have an adverse effect on the privacy of an individual, and to report to the Minister the results of the examination and assessment;

(m) to undertake research into, and to monitor developments in, data processing and computer technology (including data matching and data linkage) to ensure that any adverse effects of such developments on personal privacy are minimised, and to report to the Minister the results of the research and monitoring;

(n) to make reports and recommendations to the Minister, or the Minister responsible for a public sector agency or a Council administering a public register, in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of personal privacy;

(o) for the purpose of promoting the protection of personal privacy, to undertake educational programs on the Privacy Commissioner's own behalf or in co-operation with other persons or bodies whose functions concern the protection of personal privacy;

(p) to make public statements in relation to any matter affecting personal privacy or the privacy of any class of individual;

(q) to receive and invite representations from members of the public on any matter affecting personal privacy;

(r) to consult and co-operate with other persons and bodies concerned with personal privacy;

(s) to provide advice (with or without a request) to any individual or organisation on any matter relevant to the operation of this Act;

(t) to examine and assess (with or without a request) the impact on personal privacy of any act or practice, or proposed act or practice, of an organisation;

(u) to make suggestions to any individual or organisation in relation to any matter that concerns the need for, or the desirability of, action by that individual or organisation in the interests of personal privacy;

(v) to gather information that, in the opinion of the Privacy Commissioner, will assist the Privacy Commissioner in carrying out his or her functions under this Act;

(w) to review any approved code of practice, whether or not expressly authorised to do so by the code.

59. ***Powers***

The Privacy Commissioner has power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions.

60. ***Privacy Commissioner to have regard to certain matters***

The Privacy Commissioner must have regard to the objects of this Act in the performance of his or her functions and the exercise of his or her powers under this Act.

61. ***Delegation***

(1) The Privacy Commissioner may, by instrument, delegate to an employee referred to in section 57(1) any of his or her powers under this Act other than this power of delegation.

(2) The Privacy Commissioner may, by instrument, delegate to any person any of his or her powers under Division 3 of Part 5.

62. ***Annual reports***

The Privacy Commissioner must each year include the following information in the report of operations of the office under Part 7 of the **Financial Management Act 1994**—

(a) the number of audits of records of personal information conducted under section 58(j) during the preceding financial year; and

(b) the organisations in respect of which those audits were conducted.

63. ***Other reports***

(1) In addition to the report of operations under Part 7 of the **Financial Management Act 1994**, the Privacy Commissioner may report to the Minister on any act or practice that the Privacy Commissioner considers to be an interference with the privacy of an individual, whether or not a complaint has been made under section 25(1).

(2) The Minister may cause a copy of a report referred to in sub-section (1) to be laid before each House of the Parliament.

(3) The Privacy Commissioner may from time to time, in the public interest, publish reports and recommendations relating generally to the Privacy Commissioner's functions under this Act or to any matter investigated by the Privacy Commissioner, whether or not the matters to be dealt with in any such report have been the subject of a report to the Minister.

PART 8—GENERAL

64. *Capacity to consent or make a request or exercise right of access*

(1) If an IPP or an applicable code of practice requires the consent of an individual to the collection, use or disclosure of personal information or to the transfer of personal information to someone who is outside Victoria, the power to give that consent may be exercised on behalf of an individual who is incapable of giving consent by an authorised representative of that individual, if the consent is reasonably necessary for the lawful performance of functions or duties or exercise of powers in respect of the individual by the authorised representative.

(2) If an IPP or an applicable code of practice empowers an individual to request access to, or the correction of, personal information or confers on an individual a right of access to personal information, the power to make that request, or the right of access, may be exercised—

(a) by the individual personally, except if the individual is a child who is incapable of making the request; and

(b) by an authorised representative of the individual if—

(i) the individual is incapable of making the request or exercising the right of access; and

(ii) the personal information to be accessed is reasonably necessary for the lawful performance of functions or duties or exercise of powers in respect of the individual by the authorised representative.

(3) For the purposes of sub-sections (1) and (2), an individual is incapable of giving consent, making the request or exercising the right of access if he or she is incapable by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder of—

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right of access (as the case requires); or

(b) communicating the consent or refusal of consent, making the request or personally exercising the right of access (as the case requires)—

despite the provision of reasonable assistance by another individual.

(4) An authorised representative of an individual must not give consent or request access to, or the correction of, personal information if the authorised representative knows or believes that the consent or request does not accord with the wishes expressed, and not changed or withdrawn, by the individual before he or she became incapable of giving consent or requesting access and any purported consent given or request made in those circumstances is void.

(5) An organisation may refuse a request by an authorised representative of an individual for access to the personal information of the individual if the organisation reasonably believes that access by the authorised representative may endanger the individual.

(6) In this section, **"authorised representative"**, in relation to an individual, means a person who is—

(a) a guardian of the individual; or

(b) an attorney for the individual under an enduring power of attorney; or

(c) an agent for the individual within the meaning of the **Medical Treatment Act 1988**; or

(d) an administrator or a person responsible within the meaning of the **Guardianship and Administration Act 1986**; or

(e) a parent of an individual, if the individual is a child; or

(f) otherwise empowered under law to perform any functions or duties or exercise powers as an agent of or in the best interests of the individual—

except to the extent that acting as an authorised representative of the individual is inconsistent with an order made by a court or tribunal.

65. ***Failure to attend etc. before Privacy Commissioner***

A person must not, without reasonable excuse—

(a) refuse or fail—

(i) to attend before the Privacy Commissioner; or

(ii) to be sworn or make an affirmation; or

(iii) to give information; or

(iv) to answer a question or produce a document—

when so required by the Privacy Commissioner under this Act; or

(b) wilfully obstruct, hinder or resist the Privacy Commissioner or an employee in the office of the Privacy Commissioner or a delegate of the Privacy Commissioner in—

(i) performing, or attempting to perform, a function or duty under this Act; or

(ii) exercising, or attempting to exercise, a power under this Act; or

(c) furnish information or make a statement to the Privacy Commissioner knowing that it is false or misleading in a material particular.

Penalty: 60 penalty units.

66. ***Protection from liability***

(1) A person who lodges a complaint under section 25(1) is not personally liable for any loss, damage or injury suffered by another person by reason only of the lodging of the complaint.

(2) A person who produces a document, or gives any information or evidence, to the Privacy Commissioner under this Act is not personally liable for any loss, damage or injury suffered by another person by reason only of that production or giving.

(3) Sub-section (4) applies where—

(a) a person has been provided by an organisation with access to personal information; and

(b) the access was required by IPP 6 or an applicable code of practice or the organisation, or an employee or agent of the organisation acting within the scope of his or her actual or apparent authority, believed in good faith that the access was required by IPP 6 or an applicable code of practice.

(4) The provision of access to personal information in the circumstances referred to in sub-section (3)—

(a) is not to be regarded as making the organisation, or any employee or agent of the organisation, liable for defamation or breach of confidence or guilty of a criminal offence by reason only of the provision of access; or

(b) is not to be regarded as making any person who provided the personal information to the organisation liable for defamation or breach of confidence in respect of any publication involved in, or resulting from, the provision of access by reason only of the provision of access; or

(c) must not be taken for the purpose of the law relating to defamation or breach of confidence to constitute an authorisation or approval of the publication of the information by the person who is provided with access to it.

(5) An organisation is not in breach of the Information Privacy Principles or an applicable code of practice by reason only of—

(a) collecting, using, disclosing or transferring personal information; or

(b) providing access to personal information; or

(c) correcting personal information—

of an individual in response to a consent or request by an authorised representative whose consent or request is void by virtue of section 64(4).

67. ***Secrecy***

(1) A person who is, or has been, the Privacy Commissioner, an acting Privacy Commissioner, a delegate of the Privacy Commissioner, an employee in the office of the Privacy Commissioner or a consultant engaged by the Privacy Commissioner must not, directly or indirectly, make a record of, disclose or communicate to any person any information relating to the affairs of any individual or organisation acquired in the performance of functions or duties or the exercise of powers under this Act, unless—

(a) 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 Act; or

(b) the individual or organisation to whom the information relates gives written consent to the making of the record, disclosure or communication.

Penalty: 60 penalty units.

(2) Without limiting sub-section (1), the Privacy Commissioner must not disclose or communicate to any person, other than a person employed in the office of the Privacy Commissioner, any information given to the Privacy Commissioner pursuant to a requirement made under Division 3 of Part 5 or Part 6 (including information contained in a document required to be produced to the Privacy Commissioner) unless he or she has—

(a) notified the person from whom the information was obtained of the proposal to disclose or communicate that information; and

(b) given that person a reasonable opportunity to object to the disclosure or communication.

Penalty: 60 penalty units.

68. ***Employees and agents***

(1) Any act done or practice engaged in on behalf of an organisation by an employee or agent of the organisation acting within the scope of his or her actual or apparent authority is to be taken, for the purposes of this Act including a prosecution for an offence against this Act, to have been done or engaged in by the organisation and not by the employee or agent unless the organisation establishes that it took reasonable precautions and exercised due diligence to avoid the act being done or the practice being engaged in by its employee or agent.

(2) If, for the purpose of investigating a complaint or a proceeding for an offence against this Act, it is necessary to establish the state of mind of an organisation in relation to a particular act or practice, it is sufficient to show—

(a) that the act was done or practice engaged in by an employee or agent of the organisation acting within the scope of his or her actual or apparent authority; and

(b) that the employee or agent had that state of mind.

69. ***Charges for access***

An organisation may charge an individual the prescribed fee for providing access to personal information under this Act.

70. ***Offences by organisations or bodies***

If this Act provides that an organisation or body is guilty of an offence, that reference to an organisation or body must, if the organisation or body is unincorporated, be read as a reference to each member of the committee of management of the organisation or body.

71. ***Prosecutions***

(1) A proceeding for an offence against this Act may only be brought by—

(a) a member of the police force; or

(b) the Privacy Commissioner; or

(c) a person authorised to do so, either generally or in a particular case, by the Privacy Commissioner.

(2) In a proceeding for an offence against this Act it must be presumed, in the absence of evidence to the contrary, that the person bringing the proceeding was authorised to bring it.

72. ***Supreme Court—limitation of jurisdiction***

It is the intention of section 7 to alter or vary section 85 of the **Constitution Act 1975**.

73. ***Regulations***

(1) The Governor in Council may make regulations for or with respect to any matter or thing required or permitted by this Act to be prescribed or necessary to be prescribed to give effect to this Act.

(2) Without limiting sub-section (1), the Governor in Council may make regulations prescribing fees for providing access to personal information under this Act.

PART 9—AMENDMENT OF CERTAIN ACTS

74. ***Amendment of Parliamentary Committees Act 1968***

In section 4D(a) of the **Parliamentary Committees Act 1968**, after sub-paragraph (iii) **insert**—

"(iiia) unduly requires or authorises acts or practices that may have an adverse effect on personal privacy within the meaning of the **Information Privacy Act 2000**; or".

75. ***Amendment of Magistrates' Court Act 1989***

In Schedule 4 to the **Magistrates' Court Act 1989**, after item 38 **insert**—

"39. ***Non-compliance with compliance notice***

Offences under section 48(1) of the **Information Privacy Act 2000**.".

76. ***Amendment of Subordinate Legislation Act 1994***

In section 21(1) of the **Subordinate Legislation Act 1994**, after paragraph (g) **insert**—

"(ga) unduly requires or authorises acts or practices that may have an adverse effect on personal privacy within the meaning of the **Information Privacy Act 2000**;".

77. ***Amendment of Public Sector Management and Employment Act 1998***

In section 16(1) of the **Public Sector Management and Employment Act 1998**, after paragraph (h) **insert**—

"(i) the Privacy Commissioner in relation to the office of the Privacy Commissioner.".

78. ***Amendment of Victorian Civil and Administrative Tribunal Act 1998***

In Schedule 1 to the **Victorian Civil and Administrative Tribunal Act 1998**, after Part 11 **insert—**

"PART 11A—INFORMATION PRIVACY ACT 2000

40A. ***Intervention by Privacy Commissioner***

The Privacy Commissioner may intervene at any time in a proceeding under the **Information Privacy Act 2000**.

40B. ***Notification in other proceedings***

(1) If an application is made under section 38 (interim order) or a referral under section 31 (Minister's referral) of the **Information Privacy Act 2000**, the principal registrar must notify the Privacy Commissioner.

(2) Sub-clause (1) does not apply in the case of an application by the Privacy Commissioner under section 38 of the **Information Privacy Act 2000**.

40C. ***Privacy Commissioner may apply for interim injunction***

The Privacy Commissioner may apply for an order granting an interim injunction under section 123 in a proceeding under the **Information Privacy Act 2000** whether or not he or she is a party to that proceeding.

40D. ***Compulsory conference***

The presiding member at a compulsory conference in a proceeding under the **Information Privacy Act 2000** may refer

any matter to the Privacy Commissioner for investigation, negotiation or conciliation.

40E. ***Settlement offers***

Sections 112 to 115 do not apply to a proceeding under the **Information Privacy Act 2000**.".

79. ***New section 15A inserted in Ombudsman Act 1973***

In the **Ombudsman Act 1973**, after section 15 **insert—**

"15A. ***Referral of complaint***

If the complaint could be made the subject of an application under the **Information Privacy Act 2000**, the Ombudsman may refer the complaint to the Privacy Commissioner and notify the complainant and the respondent in writing of the referral.".

80. ***New section 20B inserted in Ombudsman Act 1973***

In the **Ombudsman Act 1973**, after section 20A **insert—**

"20B. ***Communication of information to the Privacy Commissioner***

The Ombudsman or the Acting Ombudsman may communicate to the Privacy Commissioner appointed under the **Information Privacy Act 2000** any information obtained or received in the course or as a result of the exercise of the functions of the Ombudsman under this Act, being information relevant to the performance of functions or duties by the Privacy Commissioner.".

81. ***Amendment of Information Privacy Act 2000***

In section 3 of the **Information Privacy Act 2000**, in the definition of "Commonwealth-regulated organisation" after "agency" **insert** ", or an organisation, ".

SCHEDULES

SCHEDULE 1

THE INFORMATION PRIVACY PRINCIPLES

In these Principles—

"sensitive information" means information or an opinion about an individual's—

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record—

that is also personal information;

Sch. 1 def. of "unique identifier" amended by No. 2/2001 s. 107(c).

"unique identifier" means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name but does not include an identifier within the meaning of the **Health Records Act 2001**.

1. ***Principle 1—Collection***

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of—

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. ***Principle 2—Use and Disclosure***

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless—

(a) both of the following apply—

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) 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—

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information; or

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent—

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety, or public welfare; or

(e) the organisation has reason to suspect that 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; or

(f) the use or disclosure is required or authorised by or under law; or

(g) 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—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(h) the Australian Security Intelligence Organization (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and—

(i) 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

(ii) 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.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(g), it must make a written note of the use or disclosure.

3. ***Principle 3—Data Quality***

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

4. ***Principle 4—Data Security***

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

5. ***Principle 5—Openness***

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. ***Principle 6—Access and Correction***

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that—

(a) providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders—

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (j) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, the organisation—

(a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and

(b) may refuse access to the personal information until the fee is paid.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must—

(a) provide access, or reasons for the denial of access; or

(b) correct the personal information, or provide reasons for the refusal to correct the personal information; or

(c) provide reasons for the delay in responding to the request for access to or for the correction of personal information—

as soon as practicable, but no later than 45 days after receiving the request.

7. ***Principle 7—Unique Identifiers***

7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.

7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless—

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless—

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or

(b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8. ***Principle 8—Anonymity***

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9. ***Principle 9—Transborder Data Flows***

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—

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply—

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the

information inconsistently with the Information Privacy Principles.

10. ***Principle 10—Sensitive Information***

10.1 An organisation must not collect sensitive information about an individual unless—

(a) the individual has consented; or

(b) the collection is required under law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns—

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if—

(a) the collection—

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

Sch. 2 repealed by No. 2/2001 s. 107(d).

* * * * *

ENDNOTES

1. General Information

Minister's second reading speech—

Legislative Assembly: 26 May 2000

Legislative Council: 3 October 2000

The long title for the Bill for this Act was "to establish a regime for the responsible collection and handling of personal information in the Victorian public sector, to amend the **Parliamentary Committees Act 1968**, the **Ombudsman Act 1973**, the **Subordinate Legislation Act 1994** and certain other Acts and for other purposes."

Constitution Act 1975:

Section 85(5) statement:

Legislative Assembly: 26 May 2000

Legislative Council: 3 October 2000

Absolute majorities:

Legislative Assembly: 5 September 2000

Legislative Council: 26 October 2000

The **Information Privacy Act 2000** was assented to on 12 December 2000 and came into operation as follows:

Sections 1–80, Schedules 1, 2 on 1 September 2001: section 2(2); section 81 not yet proclaimed.

2. Table of Amendments

This Version incorporates amendments made to the **Information Privacy Act 2000** by Acts and subordinate instruments.

Health Records Act 2001, No. 2/2001

Assent Date:	10.4.01
Commencement Date:	S. 107(b)(c) on 16.11.01: Government Gazette 15.11.01 p. 2839; ss 107(a)(d), 108 on 1.7.02: s. 2(2)
Current State:	This information relates only to the provision/s amending the **Information Privacy Act 2000**

Corporations (Consequential Amendments) Act 2001, No. 44/2001

Assent Date:	27.6.01
Commencement Date:	S. 3(Sch. item 64) on 15.7.01: s. 2
Current State:	This information relates only to the provision/s amending the **Information Privacy Act 2000**

---

3. Explanatory Details

No entries at date of publication.