Authorised Version No. 010

Privacy and Data Protection Act 2014

No. 60 of 2014

Authorised Version incorporating amendments as at
1 September 2017

TABLE OF PROVISIONS

Authorised Version No. 010

Privacy and Data Protection Act 2014

No. 60 of 2014

Authorised Version incorporating amendments as at
1 September 2017

The Parliament of Victoria enacts:

Part 1—Preliminary

1 Purposes

The purposes of this Act are—

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

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

(c) to establish a protective data security regime for the Victorian public sector; and

(d) to establish a regime for monitoring and assuring public sector data security; and

(e) to provide for the appointment of the Privacy and Data Protection Deputy Commissioner; and

S. 1(e) substituted by No. 20/2017 s. 78.

(f) to repeal the **Information Privacy Act 2000** and the **Commissioner for Law Enforcement Data Security Act 2005** and make consequential amendments to other Acts.

2 Commencement

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

(2) Division 1 of Part 9 comes into operation on the later of—

(a) the day after the day on which this Act receives the Royal Assent; and

(b) the day on which section 278 of the **Victoria Police Act 2013** comes into operation.

(3) Division 2 of Part 9 comes into operation on the later of—

(a) the day after the day on which this Act receives the Royal Assent; and

(b) the day on which section 157 of the **Legal Profession Uniform Law Application Act 2014** comes into operation.

(4) If a provision of this Act (other than a provision referred to in subsection (2) or (3)) does not come into operation before 9 December 2014, 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 Division 3 of Part 3 as amended and in operation for the time being;

approved information usage arrangement means an information usage arrangement approved under Division 6 of Part 3;

body means body (whether incorporated or not);

Chief Commissioner of Police means the Chief Commissioner of Police appointed under section 17 of the **Victoria Police Act 2013**;

S. 3 def. of *Chief Commissioner of Police* amended by No. 60/2014 s. 129(a).

Chief Statistician means the person employed as the Chief Statistician under section 4 of the **Crime Statistics Act 2014**;

child means a person under the age of 18 years;

* * * * *

S. 3 def. of *Commissioner* repealed by No. 20/2017 s. 79(b).

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;

contracted service provider means a person or body who provides services under a State contract;

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**;

crime statistics data means—

(a) any law enforcement data obtained by the Chief Statistician from the Chief Commissioner of Police under section 7 of the **Crime Statistics Act 2014**; or

(b) any information derived from data referred to in paragraph (a) by the Chief Statistician or an employee or consultant referred to in section 6 of the **Crime Statistics Act 2014** in the performance of functions under that Act, other than information published by the Chief Statistician under section 5(1)(a) of that Act;

crime statistics data system means a database kept by the Chief Statistician (whether in computerised or other form and however described) containing crime statistics data;

current certificate means a certificate issued under section 55(1) that has not expired or been set aside;

data security standards means—

(a) protective data security standards; or

(b) law enforcement data security standards;

de-identified, in relation to personal information, means personal information that no longer relates to an identifiable individual or an individual who can be reasonably identified;

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 Australian Information Commissioner Act 2010 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;

handling, in relation to personal information, means collection, holding, management, use, disclosure or transfer of personal information;

IBAC means the Independent Broad-based Anti-corruption Commission established under section 12 of the **Independent Broad-based Anti-corruption Commission Act 2011**;

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

Information Commissioner means the Information Commissioner appointed under section 6C of the **Freedom of Information Act 1982**;

S. 3 def. of *Information Commissioner* inserted by No. 20/2017 s. 79(a).

information handling provision means a provision of an Act that permits handling of personal information—

(a) as authorised or required by law or by or under an Act; or

(b) in circumstances or for purposes required by law or by or under an Act;

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

information usage arrangement has the meaning given by section 45;

IPP means Information Privacy Principle;

S. 3 def. of *law enforcement agency* amended by No. 60/2014 s. 129(b).

law enforcement agency means—

(a) Victoria Police; or

(b) the police force or police service of another State or a Territory; or

(c) the Australian Federal Police; or

(d) the Australian Crime Commission established under section 7 of the Australian Crime Commission Act 2002 of the Commonwealth; or

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

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

(g) 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

(h) the Chief Examiner and Examiners appointed under Part 3 of the **Major Crime (Investigative Powers) Act 2004**; or

(i) the IBAC; or

(j) the sheriff within the meaning of the **Sheriff Act 2009**; or

(k) the Victorian Inspectorate; or

(l) the Adult Parole Board established by section 61 of the **Corrections Act 1986**; or

(m) the Youth Parole Board within the meaning of the **Children, Youth and Families Act 2005**; or

(n) 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

(o) an agency responsible for the execution or implementation of an order or decision made by a court or tribunal; or

(p) an agency that provides correctional services, including a contractor within the meaning of the **Corrections Act 1986**, or a subcontractor 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

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

S. 3 def. of *law enforcement data* amended by No. 60/2014 s. 129(c).

law enforcement data means any information obtained, received or held by Victoria Police—

(a) for the purpose 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) for the purposes of its community policing functions;

S. 3 def. of *law enforcement data security standards* amended by No. 20/2017 s. 106(1)(a).

law enforcement data security standards means the standards issued, amended or reissued by the Information Commissioner under section 92;

S. 3 def. of *law enforcement data system* amended by No. 60/2014 s. 129(d).

law enforcement data system means a database kept by Victoria Police (whether in computerised or other form and however described) containing law enforcement data;

S. 3 def. of *legal practitioner* inserted by No. 20/2017 s. 79(a).

legal practitioner means an Australian legal practitioner;

S. 3 def. of *member of staff* inserted by No. 20/2017 s. 79(a).

member of staff, of the Office of the Victorian Information Commissioner, means a person employed or engaged under section 6Q of the **Freedom of Information Act 1982**;

notice to produce or attend means a notice issued under section 68 or 79, and includes a notice as varied under section 83B;

S. 3 def. of *notice to produce or attend* inserted by No. 20/2017 s. 79(a).

Office of the Victorian Information Commissioner means the Office of the Victorian Information Commissioner established under the **Freedom of Information Act 1982**;

S. 3 def. of *Office of the Victorian Information Commissioner* inserted by No. 20/2017 s. 79(a).

organisation means a person or body to which Part 3 applies under section 13;

parent, in relation to a child, includes—

(a) the father and mother of the child; and

(b) the spouse of the father or mother of the child; and

(c) the domestic partner of the father or mother of the child; and

(d) a person who has custody of the child; and

(e) a person whose name is entered as the parent of the child in the register of births in the Register maintained by the Registrar of Births, Deaths and Marriages under Part 7 of the **Births, Deaths and Marriages Registration Act 1996**; and

(f) a person who acknowledges that they are the parent of the child by an instrument of the kind described in section 8(2) or (2A) of the **Status of Children Act 1974**; and

(g) a person in respect of whom a court has made a declaration or a finding or order that the person is the parent of the child;

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;

S. 3 def. of *Privacy and Data Protection Deputy Commissioner* inserted by No. 20/2017 s. 79(a).

Privacy and Data Protection Deputy Commissioner means the Privacy and Data Protection Deputy Commissioner appointed under section 8H;

protective data security plan means a plan prepared under section 89;

S. 3 def. of *protective data security standards* amended by No. 20/2017 s. 106(1)(b).

protective data security standards means the standards issued by the Information Commissioner under section 86 or amended or reissued under section 87;

public interest determination means a determination made under section 31;

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) under an Act or regulation (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 under an Act or regulation; and

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

public sector agency means a public service body or a public entity within the meaning of the **Public Administration Act 2004**;

public sector body Head has the meaning given in the **Public Administration Act 2004**;

public sector data means any information (including personal information) obtained, received or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body;

public sector data system includes—

(a) information technology for storage of public sector data, including hardware and software; and

(b) non-electronic means for storage of public sector data; and

(c) procedures for dealing with public sector data, including by use of information technology and non-electronic means;

public service body Head has the meaning given in the **Public Administration Act 2004**;

State contract means a contract between an organisation, or a person, agency or body to which Part 4 or 5 of this Act applies, and another person or body (whether or not this Act or a Part of this Act applies to the person or body) under which services are provided to one party (the ***outsourcing party***) by the other party (the ***contracted service provider***) in connection with the performance of the functions of the outsourcing party, including services that the outsourcing party provides to other persons or bodies;

temporary public interest determination means a temporary public interest determination made under section 39;

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;

Victorian Inspectorate means the Victorian Inspectorate established under section 8 of the **Victorian Inspectorate Act 2011**;

Victorian protective data security framework means the Victorian protective data security framework developed under section 85.

4 Interpretation

(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 an individual, unless the contrary intention appears.

5 Objects

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; and

(b) to balance the public interest in promoting open access to public sector information with the public interest in protecting its security; and

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

(d) to promote the responsible and transparent handling of personal information in the public sector; and

(e) to promote responsible data security practices in the public sector.

6 Relationship of this Act to other laws

(1) If a provision made by or under this Act (other than Division 5, 6 or 7 of Part 3) relating to an Information Privacy Principle or applicable code of practice 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 subsection (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 Rights and liabilities

(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 1A—Functions, powers of Information Commissioner and appointment of Privacy and Data Protection Deputy Commissioner

Pt 1A (Headings and ss 8A–8P) inserted by No. 20/2017 s. 80.

Division 1—Performance of functions

8A Functions of Information Commissioner

S. 8A inserted by No. 20/2017 s. 80.

(1) The Information Commissioner has the following functions—

(a) functions relating to information privacy set out in section 8C;

(b) functions relating to protective data security and law enforcement data security set out in section 8D;

(c) functions conferred on the Information Commissioner by or under this Act;

(d) functions conferred on the Information Commissioner by or under any other Act.

(2) The Information Commissioner must have regard to the objects of this Act in the performance of the Commissioner's functions and the exercise of the Commissioner's powers under this Act.

(3) Except where expressly provided in this Act, the Information Commissioner is not subject to the direction or control of the Minister in respect of the performance of the Information Commissioner's duties and functions and the exercise of the Information Commissioner's powers.

S. 8B inserted by No. 20/2017 s. 80.

8B Functions of Privacy and Data Protection Deputy Commissioner

(1) The Privacy and Data Protection Deputy Commissioner has the following functions—

(a) functions relating to information privacy set out in section 8C(2);

(b) functions relating to protective data security and law enforcement data security set out in section 8D(2);

(c) any function conferred by the Information Commissioner on the Deputy Commissioner by authorisation under section 8F;

(d) any other function conferred on the Information Commissioner by or under this Act, except—

(i) a function of the Information Commissioner referred to in section 8A(1)(d); or

(ii) a function of the Information Commissioner referred to in section 8C(1) or 8D(1); or

(iii) a function of the Information Commissioner referred to in section 8F; or

(iv) a function of the Information Commissioner referred to in section 8O; or

(v) issuing directions under section 8P; or

(vi) making reports under section 116.

(2) The Privacy and Data Protection Deputy Commissioner must have regard to the objects of this Act in the performance of the Deputy Commissioner's functions and the exercise of the Deputy Commissioner's powers under this Act.

(3) Except where expressly provided in this Act, the Privacy and Data Protection Deputy Commissioner is not subject to the direction or control of the Minister in respect of the performance of the Deputy Commissioner's duties and functions and the exercise of the Deputy Commissioner's powers.

8C Information privacy functions

S. 8C inserted by No. 20/2017 s. 80.

(1) The Information Commissioner has the following functions in relation to information privacy—

(a) in accordance with Division 3 of Part 3, to undertake activities relating to the development and approval of codes of practice;

(b) to develop and publish model terms capable of being adopted by an organisation in a contract or arrangement with a recipient of personal information being transferred by the organisation outside Victoria;

(c) to make public interest determinations and temporary public interest determinations in accordance with Division 5 of Part 3;

(d) to approve information usage arrangements in accordance with Division 6 of Part 3;

(e) 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;

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

(g) to issue guidelines and other materials in relation to the Information Privacy Principles and information usage arrangements;

(h) to undertake reviews of any matters relating to information privacy, as requested by the Minister;

(i) to make reports or recommendations in relation to information privacy as provided for by section 111.

(2) The Information Commissioner and the Privacy and Data Protection Deputy Commissioner each have the following functions in relation to information privacy—

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

(b) 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;

(c) to issue certificates under Division 7 of Part 3;

(d) subject to this Act—

(i) to receive complaints about an act or practice of an organisation; and

(ii) if appropriate to do so, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the complaint;

(e) to issue compliance notices under Division 9 of Part 3 and to carry out an investigation for that purpose;

(f) 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;

(g) to consult and cooperate with persons and bodies concerned with information privacy;

(h) to undertake research in relation to matters relating to information privacy.

8D Protective data security and law enforcement data security functions

S. 8D inserted by No. 20/2017 s. 80.

(1) The Information Commissioner has the following functions in relation to protective data security and law enforcement data security—

(a) to issue protective data security standards and law enforcement data security standards;

(b) to develop the Victorian protective data security framework;

(c) to issue guidelines and other materials in relation to protective data security standards;

(d) to undertake reviews of any matters relating to protective data security, as requested by the Minister;

(e) to undertake reviews of any matters relating to law enforcement data security and crime statistics data security, as requested by the Minister;

(f) to make reports or recommendations in relation to data security as provided for by section 111.

(2) The Information Commissioner and the Privacy and Data Protection Deputy Commissioner each have the following functions in relation to

protective data security and law enforcement data security—

(a) to promote the uptake of protective data security standards by the public sector;

(b) to conduct monitoring and assurance activities, including audits, to ascertain compliance with data security standards;

(c) to refer findings of monitoring and assurance activities, including audits, to an appropriate person or body for further action;

(d) to undertake research in relation to matters relating to protective data security and law enforcement data security relevant to the public sector, particularly relating to information and communications technology;

(e) to retain copies of protective data security plans.

S. 8E inserted by No. 20/2017 s. 80.

8E Performance of concurrent functions

If a function may be performed by the Information Commissioner and the Privacy and Data Protection Deputy Commissioner, that function may be performed by—

(a) the Information Commissioner; or

(b) the Privacy and Data Protection Deputy Commissioner; or

(c) the Information Commissioner and the Privacy and Data Protection Deputy Commissioner.

S. 8F inserted by No. 20/2017 s. 80.

8F Information Commissioner may confer functions on Privacy and Data Protection Deputy Commissioner

(1) The Information Commissioner may in writing authorise the Privacy and Data Protection Deputy Commissioner to perform any of the following

functions of the Information Commissioner, as specified in the authorisation—

(a) to undertake activities in relation to the development or approval of a specified code of practice;

(b) to develop and publish specified 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;

(c) to make a specified public interest determination or a specified temporary public interest determination in accordance with Division 5 of Part 3;

(d) to approve a specified information usage arrangement;

(e) to issue a specified protective data security standard or a specified law enforcement data standard;

(f) to review or amend the Victorian protective data security framework, as specified;

(g) to issue guidelines and other materials in relation to a specified protective data security standard.

(2) The Information Commissioner may at any time in writing revoke an authorisation under this section, and on that revocation may continue and complete any action commenced under the authorisation by the Privacy and Data Protection Deputy Commissioner.

S. 8G inserted by No. 20/2017 s. 80.

8G General powers of Information Commissioner and Privacy and Data Protection Deputy Commissioner

(1) The Information Commissioner has power to do all things that are necessary or convenient to be done for or in connection with the performance of the Information Commissioner's functions.

(2) The Privacy and Data Protection Deputy Commissioner has power to do all things that are necessary or convenient to be done for or in connection with the performance of the Deputy Commissioner's functions.

Division 2—Privacy and Data Protection Deputy Commissioner

S. 8H inserted by No. 20/2017 s. 80.

8H Appointment of Privacy and Data Protection Deputy Commissioner

(1) The Governor in Council may appoint an eligible person as the Privacy and Data Protection Deputy Commissioner.

(2) A person is not eligible for appointment as the Privacy and Data Protection Deputy Commissioner if the person is—

(a) a member of the Parliament of Victoria or of the Commonwealth or of another State or a Territory; or

(b) a member of a council.

(3) A person may hold office as Privacy and Data Protection Deputy Commissioner for not more than 2 terms (whether consecutive terms or otherwise).

8I Terms and conditions of appointment of Privacy and Data Protection Deputy Commissioner

S. 8I inserted by No. 20/2017 s. 80.

(1) The appointment of the Privacy and Data Protection Deputy Commissioner is to be for the period, not exceeding 5 years, set out in the instrument of appointment.

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

(3) Subject to section 8H(3), the Privacy and Data Protection Deputy Commissioner may be reappointed.

(4) The Privacy and Data Protection Deputy Commissioner is entitled to leave of absence as determined by the Governor in Council.

(5) The Privacy and Data Protection Deputy Commissioner must not directly or indirectly engage in paid employment outside the duties of the relevant office.

8J Remuneration

S. 8J inserted by No. 20/2017 s. 80.

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

8K Vacancy and resignation of Privacy and Data Protection Deputy Commissioner

S. 8K inserted by No. 20/2017 s. 80.

(1) The Privacy and Data Protection Deputy Commissioner ceases to hold office if the office holder—

(a) resigns by notice in writing delivered to the Minister; or

(b) becomes an insolvent under administration; or

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

(d) nominates for election for the Parliament of Victoria or of the Commonwealth or of another State or a Territory; or

(e) nominates for election as a member of a council; or

(f) is removed from office under section 8L.

(2) The Privacy and Data Protection Deputy Commissioner's resignation under subsection (1)(a) takes effect on—

(a) the day on which it is received by the Minister; or

(b) if a later day is specified in the notice, on that day.

S. 8L inserted by No. 20/2017 s. 80.

8L Suspension and removal from office

(1) The Governor in Council, on the recommendation of the Minister, may suspend or remove the Privacy and Data Protection Deputy Commissioner from office on any of the following grounds—

(a) misconduct;

(b) neglect of duty;

(c) inability to perform the duties of the office;

(d) any other ground on which the Governor in Council is satisfied that the Privacy and Data Protection Deputy Commissioner should not hold office.

(2) If the Privacy and Data Protection Deputy Commissioner is removed from office, the Minister must cause a full statement of the grounds for removal to be presented to each House of Parliament within 10 sitting days of that House after the removal.

8M Acting Privacy and Data Protection Deputy Commissioner

S. 8M inserted by No. 20/2017 s. 80.

(1) The Governor in Council, on the recommendation of the Minister, may appoint an eligible person to act as the Privacy and Data Protection Deputy Commissioner—

(a) during a vacancy in the office of the Deputy Commissioner; or

(b) during any period, or all periods, when the Deputy Commissioner is absent from duty or from the State or, for another reason, cannot perform the functions of the office.

(2) A person is not eligible for appointment to act as the Privacy and Data Protection Deputy Commissioner if the person is—

(a) a member of the Parliament of Victoria or of the Commonwealth or of another State or a Territory; or

(b) a member of a council.

(3) An appointment under subsection (1) is for the period, not exceeding 12 months, set out in the instrument of appointment.

(4) The Governor in Council, on the recommendation of the Minister, may at any time remove the acting Privacy and Data Protection Deputy Commissioner from office.

(5) While a person is acting in the office of the Privacy and Data Protection Deputy Commissioner, the person—

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

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

S. 8N inserted by No. 20/2017 s. 80.

8N Validity of acts and decisions

An act or decision of the Privacy and Data Protection Deputy Commissioner or acting Privacy and Data Protection Deputy Commissioner is not invalid only because—

(a) of a defect or irregularity in or in connection with the appointment of the Privacy and Data Protection Deputy Commissioner or acting Privacy and Data Protection Deputy Commissioner; or

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

Division 3—General

S. 8O inserted by No. 20/2017 s. 80.

8O Delegation

(1) The Information Commissioner may by instrument delegate to the Privacy and Data Protection Deputy Commissioner or a member of staff of the Office of the Victorian Information Commissioner any of the Information Commissioner's functions and powers under this Act except this power of delegation.

(2) The Information Commissioner may by instrument delegate to the Privacy and Data Protection Deputy Commissioner or any member of staff of the Office of the Victorian Information Commissioner a function or power relating to information privacy, protective data security or law enforcement data security conferred on the Information Commissioner by or under any other Act.

(3) With the written consent of the Information Commissioner, the Privacy and Data Protection Deputy Commissioner may by instrument delegate to a member of staff any of the Deputy Commissioner's functions and powers (including any function or power delegated under subsection (1)) except this power of delegation.

8P Directions

S. 8P inserted by No. 20/2017 s. 80.

The Information Commissioner may issue directions to the Privacy and Data Protection Deputy Commissioner or to any member of staff of the Office of the Victorian Information Commissioner for the purposes of this Act in relation to the performance of functions under this Act other than in relation to the following—

(a) certifying consistency of an act or practice under section 55; or

(b) the conciliation of a complaint under Subdivision 3 of Division 8 of Part 3.

Part 2—Application of this Act

9 Definition

In this Part, ***information*** means—

(a) personal information; or

(b) public sector data; or

(c) law enforcement data; or

(d) crime statistics data.

10 Courts, tribunals etc.

Nothing in this Act or in any Information Privacy Principle or any data security standard applies in respect of the collection, holding, management, use, disclosure or transfer of information—

(a) in relation to its or the holder's 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 their 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.

10A Royal Commissions etc.

S. 10A inserted by No. 67/2014 s. 147(Sch. 2 item 28).

(1) Nothing in this Act or in any Information Privacy Principle or any data security standard applies in respect of the collection, holding, management, use, disclosure or transfer of information by a Royal Commission, a Board of Inquiry or a Formal Review for the purposes of, or in connection with, the performance of its functions.

(2) In this section—

Board of Inquiry has the same meaning as in the **Inquiries Act 2014**;

Formal Review has the same meaning as in the **Inquiries Act 2014**;

Royal Commission means—

(a) a Royal Commission established under the **Inquiries Act 2014**; or

(b) a Royal Commission established under the prerogative of the Crown.

11 Parliamentary Committees

(1) Nothing in this Act or in any Information Privacy Principle or any data security standard applies in respect of the collection, holding, management, use, disclosure or transfer of information by a Parliamentary Committee in the course of carrying out its functions as a Parliamentary Committee.

(2) In this section—

Parliamentary Committee means—

(a) a Joint Investigatory Committee, or the House Committee, within the meaning of the **Parliamentary Committees Act 2003**; or

(b) a committee of the Legislative Council or the Legislative Assembly.

12 Publicly-available information

(1) Nothing in this Act or in any Information Privacy Principle or any data security standard applies to any 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) Subsection (1) does not take away from section 20(2) which imposes duties on a public sector agency or a Council in administering a public register.

Part 3—Information privacy

Division 1—Application of this Part

13 Public sector organisations to which this Part applies

(1) Subject to subsection (2), this Part applies to the following—

(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 the person was appointed by the Governor in Council, or by a Minister, otherwise than under an Act;

(h) a court or tribunal;

(i) Victoria Police;

S. 13(1)(i) substituted by No. 21/2015 s. 3(Sch. 1 item 41.1).

(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 subsection (3)(a) to be an organisation for the purposes of this subsection.

(2) This Part does not apply to a person or body referred to in subsection (1) that is—

(a) a Commonwealth-regulated organisation; or

(b) declared, or to the extent that it is declared, by an Order under subsection (3)(b) not to be an organisation for the purposes of subsection (1)(e), (f) or (g).

(3) The Governor in Council may, on the recommendation of the Minister, 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 subsection (1); or

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

(4) The Minister may only recommend to the Governor in Council the making of an Order under subsection (3)(b) in respect of a body or person if satisfied that—

(a) another scheme (whether contained in an enactment or given legislative force by an enactment) would apply to the collection, holding, management, use, disclosure and transfer by that body or person of personal information if that person or body were not an organisation for the purposes of subsection (1), either wholly or to the extent specified in the Order; and

(b) the collection, holding, management, use, disclosure and transfer by that body or person of personal information is more appropriately governed by that other scheme.

14 Exemption—Freedom of Information Act 1982

(1) 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 document containing personal information or to the personal information contained in a document if—

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

(b) access can only be granted to the document or information, or the information can only be corrected, in accordance with that Act.

(2) 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 document containing personal information or to the personal information contained in a document if—

(a) the document is an official document of a Minister within the meaning of the **Freedom of Information Act 1982**; and

(b) access can only be granted to the document or information, or the information can only be corrected, in accordance with that Act.

(3) 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 document containing personal information or to the personal information contained in a document if access would not be granted to the document under the **Freedom of**

Information Act 1982 because of section 5(3), 6 or 6AA of that Act.

15 Exemption—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 noncompliance 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

S. 15(d) amended by No. 21/2015 s. 3(Sch. 1 item 41.2).

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

16 What is an interference with privacy of an individual?

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—

(a) an Information Privacy Principle or an applicable code of practice; or

(b) a public interest determination or a temporary public interest determination; or

(c) an approved information usage arrangement; or

(d) a current certificate.

17 Effect of outsourcing

(1) Subject to this section, the status or effect for the purposes of this Act (other than Part 4) 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 party would have been bound by them in respect of that act or practice had it been directly done or engaged in by the outsourcing party.

(3) If a provision of a kind referred to in subsection (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 party in respect of that act or practice had it been directly done or engaged in by the outsourcing party.

(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 (other than Part 4) and any applicable code of practice, be taken to have been done or engaged in by the outsourcing party as well as the contracted service provider unless—

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

(b) the Information Privacy Principle 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 118(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.

Division 2—Information Privacy Principles

18 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 Part 2 or section 14 or 15 and those Principles must be construed accordingly.

19 Application of Information Privacy Principles

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

20 Organisations to comply with Information Privacy Principles

(1) 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) 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.

(3) Subsections (1) and (2) do not apply if the act or practice is permitted under—

(a) a public interest determination; or

(b) a temporary public interest determination; or

(c) an approved information usage arrangement.

Division 3—Codes of practice

21 Codes of practice

(1) An organisation may 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 Division 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 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 Information Commissioner; or

S. 21(4)(d) amended by No. 20/2017 s. 106(5).

(e) provide for the expiry of the code.

(5) Subsection (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 20(2) and this Part has effect accordingly.

22 Process for approval of code of practice or code amendment

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

S. 22(1) amended by No. 20/2017 s. 106(6)(a).

(2) The Governor in Council, on the recommendation of the Minister acting on the advice received from the Information Commissioner under subsection (3), may by notice published in the Government Gazette approve a code of practice or an amendment to an approved code of practice.

S. 22(2) amended by No. 20/2017 s. 106(6)(a).

(3) The Information Commissioner may advise the Minister to recommend to the Governor in Council that a code of practice, or an amendment to an approved code of practice, be approved if in the Information Commissioner's opinion—

S. 22(3) amended by No. 20/2017 s. 106(6).

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

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

(c) the code specifies—

(i) the organisations bound (either wholly or to a limited extent) by the code; or

(ii) 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.

S. 22(4) amended by No. 20/2017 s. 106(6)(a).

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

S. 22(4)(a) amended by No. 20/2017 s. 106(6)(a).

(a) may consult any person or body that the Information 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 amendment.

(5) A code of practice or an amendment to an approved code of practice comes into operation at the beginning of—

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

(b) any later day stated in the notice as the day on which the code or amendment comes into operation.

23 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 written notice given to the Information 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.

S. 23(1)(b) amended by No. 20/2017 s. 106(6)(a).

(2) A notice under subsection (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, managed, used, disclosed or transferred by it; or

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

(3) A notice under subsection (1)(b) has no effect unless the Information Commissioner approves it.

S. 23(3) amended by No. 20/2017 s. 106(6)(a).

(4) The Information Commissioner may approve a notice under subsection (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.

S. 23(4) amended by No. 20/2017 s. 106(6)(a).

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

(a) in the case of an organisation referred to in subsection (1)(a), on and after the coming into operation of the code; and

(b) in the case of an organisation referred to in subsection (1)(b), on and after the later of—

(i) the date stated in the notice as the date on and after which the organisation will be bound by the code; or

S. 23(5)(b)(ii) amended by No. 20/2017 s. 106(6)(b).

(ii) the date on which the organisation is notified of the Information Commissioner's approval of the notice.

S. 23(6) amended by No. 20/2017 s. 106(6)(a).

(6) An organisation bound by an approved code of practice may, by written notice given to the Information 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 after the date of the notice under subsection (6) or any later date stated in that notice as the date on and after which the organisation will cease to be bound by the code.

24 Effect of approved code

(1) 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, is, for the purposes of this Act, taken to be a contravention of an Information Privacy Principle and may be dealt with as provided by that code and this Act.

(2) Subsection (1) has effect whether or not that act or practice would otherwise contravene any Information Privacy Principle.

25 Codes of practice register

(1) The Information Commissioner must cause a register of all approved codes of practice to be established and maintained.

S. 25(1) amended by No. 20/2017 s. 106(2).

(2) The Information Commissioner may determine the form of the register.

S. 25(2) amended by No. 20/2017 s. 106(2).

(3) 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 prescribed fee, obtain a copy of any entry in, or document forming part of, the register.

26 Revocation of approval

(1) The Governor in Council, on the recommendation of the Minister acting on advice received from the Information Commissioner under subsection (2), may by notice published in the Government Gazette revoke the approval of a code of practice or of an amendment to an approved code of practice.

S. 26(1) amended by No. 20/2017 s. 106(6)(a).

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

S. 26(2) amended by No. 20/2017 s. 106(6)(a).

(3) The Information Commissioner may act under subsection (2) on the Information Commissioner's own initiative or on an application for revocation made by an individual or organisation.

S. 26(3) amended by No. 20/2017 s. 106(6).

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

S. 26(4) amended by No. 20/2017 s. 106(6)(a).

S. 26(4)(a) amended by No. 20/2017 s. 106(6)(a).

(a) must consult the organisation that sought approval of the code or amendment and may consult any other person or body that the Information 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 amendment ceases to be in operation at the beginning of—

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

(b) any later day stated in that notice as the day on which the code or amendment ceases to be in operation.

27 Effect of revocation of approval or amendment or expiry of approved code

(1) The revocation of the approval of a code of practice or of an amendment to an approved code of practice, or the expiry of an approved code of practice, or the ceasing of an organisation to be bound by an approved 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 82(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 referred to in paragraphs (c) and (d).

(2) Any investigation, legal proceeding or remedy referred to in subsection (1)(e) may be commenced, continued or enforced, and any penalty may be imposed, as if the code or amendment had not been revoked or the code had not expired or the organisation had not ceased to be bound by the code.

(3) Subject to subsection (1), if an amendment to an approved code of practice is revoked, as from the beginning of the day on which the amendment ceases to be in operation, the code takes effect as if it had not been amended.

(4) Nothing in this section prevents the application to an organisation of an Information Privacy Principle (without any modification) on and after the day on which an applicable code of practice, that modified the application of that Information Privacy Principle, ceases to be in operation.

Division 4—Capacity to consent or make a request or exercise right of access

28 Capacity to consent or make a request or exercise right of access

(1) If an Information Privacy Principle or an applicable code of practice requires the consent of an individual to the collection, holding, management, use or disclosure of personal

information or to the transfer of personal information to someone who is outside Victoria, an authorised representative of the individual may give that consent if—

(a) the individual is incapable of giving consent; and

(b) 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 Information Privacy Principle 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 that right of access, may be exercised—

S. 28(2)(a) substituted by No. 64/2016 s. 16.

(a) by—

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

(ii) a supportive attorney acting under a supportive attorney appointment, within the meaning of the **Powers of Attorney Act 2014**; 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 subsections (1) and (2), an individual is incapable of giving consent, making the request or exercising the right of access if the individual is incapable (despite the provision of reasonable assistance by another individual) 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).

(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 the individual became incapable of giving consent or requesting access and any purported consent given or request made in those circumstances is of no effect.

(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—

(a) means a person who is—

(i) a guardian of the individual; or

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

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

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

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

(vi) 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; and

(b) does not include a person acting as an authorised representative of the individual if that acting is inconsistent with an order made by a court or tribunal;

disability has the same meaning as in the **Disability Act 2006**.

Division 5—Public interest determinations and temporary public interest determinations

Subdivision 1—Public interest determinations

29 Public interest determination

(1) An organisation may apply to the Information Commissioner, in writing, for a determination that—

S. 29(1) amended by No. 20/2017 s. 106(2).

(a) an act or a practice of an organisation contravenes or may contravene a specified Information Privacy Principle (other than IPP 4 or 6) or an approved code of practice; and

(b) the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with that Information Privacy Principle or approved code of practice.

(2) The application for a public interest determination must specify—

(a) the act or practice to which the determination would apply; and

(b) the relevant Information Privacy Principle or approved code of practice; and

(c) the reasons for the organisation seeking the determination.

(3) A public interest determination must not be made in respect of IPP 4 or 6.

(4) On receipt of the application, the Information Commissioner must publish, as the Information Commissioner thinks fit, a notice—

S. 29(4) amended by No. 20/2017 s. 106(2).

(a) stating that the application has been received; and

(b) inviting persons whose interests would be affected by the determination to make submissions in relation to the application; and

(c) stating a time period for making submissions in relation to the application.

S. 29(5) amended by No. 20/2017 s. 106(2).

(5) The Information Commissioner must prepare a draft determination and send a copy to the applicant and each person who has made a submission under subsection (4).

S. 29(6) amended by No. 20/2017 s. 106(2).

(6) The Information Commissioner may invite the applicant and any person who has made a submission under subsection (4) to attend a conference about the draft determination.

30 Application taken to be application for temporary public interest determination on request

S. 30(1) amended by No. 20/2017 s. 106(2).

(1) On request of the applicant, the Information Commissioner may first deal with an application under section 29 as if it were an application for a temporary public interest determination.

S. 30(2) amended by No. 20/2017 s. 106(2).

(2) If the Information Commissioner deals with the application as if it were an application for a temporary public interest determination—

(a) for the purposes of Subdivision 2, the application is taken to have been made under section 38; and

S. 30(2)(b) amended by No. 20/2017 s. 106(2).

(b) the Information Commissioner may continue to consider the application under this Subdivision, whether or not a temporary public interest determination is made.

31 Information Commissioner may make public interest determination[1]

S. 31 (Heading) amended by No. 20/2017 s. 106(3).

(1) The Information Commissioner may make a public interest determination on application under section 29 if satisfied that the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with the specified Information Privacy Principle or approved code of practice.

S. 31(1) amended by No. 20/2017 s. 106(7)(a).

(2) In deciding whether to make a public interest determination, the Information Commissioner must have regard to—

S. 31(2) amended by No. 20/2017 s. 106(7)(a).

(a) whether not permitting the organisation to do the act or engage in the practice would be in the public interest; and

(b) the objects of this Act; and

(c) any submissions received under section 29; and

(d) any matters raised before the Information Commissioner in a conference under section 29.

S. 31(2)(d) amended by No. 20/2017 s. 106(7)(a).

(3) A public interest determination must include a statement of reasons for making the determination.

(4) A public interest determination must be published on the Internet site of the Information Commissioner.

S. 31(4) amended by No. 20/2017 s. 106(7)(a).

32 Effect of public interest determination

S. 32 amended by No. 20/2017 s. 106(5).

If the Information Commissioner makes a public interest determination, the organisation is not required to comply with the specified Information Privacy Principle or approved code of practice to

the extent specified in the determination in doing the act or engaging in the practice.

33 Duration of public interest determination

A public interest determination has effect on and after the day of publication until the earliest of the following—

(a) the expiry date (if any) specified in the determination;

(b) the determination is revoked under section 35;

(c) the determination is disallowed by the Parliament or a House of the Parliament.

34 Amendment of public interest determination

S. 34(1) amended by No. 20/2017 s. 106(5).

(1) The organisation may apply to the Information Commissioner for the approval of an amendment to the public interest determination.

(2) Sections 29(2) to (6), 31, 32 and 33 apply to an application under subsection (1)—

(a) as if a reference to a public interest determination were a reference to the amendment in respect of which approval is sought; and

(b) with any other necessary modifications.

35 Revocation of public interest determination

S. 35(1) amended by No. 20/2017 s. 106(2).

(1) The Information Commissioner must revoke a public interest determination if satisfied that—

(a) the public interest in the organisation doing the act or engaging in the practice no longer substantially outweighs the public interest in complying with the Information Privacy Principle or approved code of practice specified in the determination; or

(b) the reasons set out in the application for the determination no longer apply.

(2) Before revoking a public interest determination, the Information Commissioner must give the organisation written notice stating—

S. 35(2) amended by No. 20/2017 s. 106(2).

(a) that the Information Commissioner intends to revoke the determination; and

S. 35(2)(a) amended by No. 20/2017 s. 106(2).

(b) the reasons for the intended revocation; and

(c) that the organisation may make a submission as to why the determination should not be revoked.

(3) The Information Commissioner must consider any submission received under subsection (2)(c) within the period stated in the notice before revoking the public interest determination.

S. 35(3) amended by No. 20/2017 s. 106(2).

36 Reporting and review

(1) An organisation that is subject to a public interest determination of more than 12 months' duration must report to the Information Commissioner—

S. 36(1) amended by No. 20/2017 s. 106(2).

(a) annually; and

(b) at any other time, as requested by the Information Commissioner.

S. 36(1)(b) amended by No. 20/2017 s. 106(2).

(2) Within 60 days after receiving a report under subsection (1), the Information Commissioner must review the public interest determination and consider whether to revoke or amend it.

S. 36(2) amended by No. 20/2017 s. 106(2).

Subdivision 2—Temporary public interest determinations

37 Temporary public interest determination

S. 37 amended by No. 20/2017 s. 106(5).

The Information Commissioner may make a temporary public interest determination for a period not exceeding 12 months if circumstances require that a determination be made urgently.

38 Application for temporary public interest determination

S. 38(1) amended by No. 20/2017 s. 106(2).

(1) An organisation may apply to the Information Commissioner, in writing, for a temporary public interest determination.

(2) The application must specify—

(a) the act or practice to which the determination would apply; and

(b) the relevant Information Privacy Principle or approved code of practice; and

(c) the reasons for the organisation seeking the determination, and why the determination is required urgently.

(3) An application for a temporary public interest determination cannot be made in respect of IPP 4 or 6.

S. 38(4) amended by No. 20/2017 s. 106(2).

(4) On receipt of the application, the Information Commissioner must publish, as the Information Commissioner thinks fit, a notice stating that the application has been received.

39 Information Commissioner may make temporary public interest determination[2]

S. 39 (Heading) amended by No. 20/2017 s. 106(3).

S. 39(1) amended by No. 20/2017 s. 106(7)(a).

(1) The Information Commissioner may make a temporary public interest determination on an application under section 38 if satisfied that—

(a) the public interest in the organisation doing the act or engaging in the practice substantially outweighs the public interest in complying with the relevant Information Privacy Principle or approved code of practice; and

(b) the application raises matters that require that a determination be made urgently.

(2) In deciding whether to make a temporary public interest determination, the Information Commissioner must have regard to— S. 39(2) amended by No. 20/2017 s. 106(7)(a).

(a) whether not permitting the organisation to do the act or engage in the practice is in the public interest; and

(b) the objects of this Act.

(3) A temporary public interest determination must not be made in respect of IPP 4 or 6.

(4) A temporary public interest determination must include a statement of reasons for making the determination.

(5) A temporary public interest determination must specify the date of expiry of the determination which must not be more than 12 months after the determination is published under subsection (6).

(6) A temporary public interest determination must be published on the Internet site of the Information Commissioner. S. 39(6) amended by No. 20/2017 s. 106(7)(a).

40 Duration of temporary public interest determination

A temporary public interest determination has effect on and after the day of publication until the earliest of the following—

(a) the expiry date specified in the determination;

(b) the determination is revoked under section 41;

(c) the determination is disallowed by the Parliament or a House of the Parliament;

(d) if a public interest determination is made, the day that determination takes effect.

41 Revocation of temporary public interest determination

S. 41(1) amended by No. 20/2017 s. 106(2).

(1) The Information Commissioner must revoke a temporary public interest determination if satisfied that—

(a) the public interest in the organisation doing the act or engaging in the practice no longer substantially outweighs the public interest in complying with the Information Privacy Principle or approved code of practice specified in the determination; or

(b) the reasons set out in the application for the determination no longer apply.

S. 41(2) amended by No. 20/2017 s. 106(2).

(2) Before revoking a temporary public interest determination, the Information Commissioner must give the organisation a written notice stating—

S. 41(2)(a) amended by No. 20/2017 s. 106(2).

(a) that the Information Commissioner intends to revoke the determination; and

(b) the reasons for the intended revocation; and

(c) that the organisation may make a submission as to why the determination should not be revoked.

(3) The Information Commissioner must consider any submission received under subsection (2)(c) within the period stated in the notice, before revoking the temporary public interest determination.

S. 41(3) amended by No. 20/2017 s. 106(2).

Subdivision 3—Disallowance of determinations

42 Disallowance of determinations

(1) A public interest determination or temporary public interest determination is subject to disallowance by the Parliament.

(2) Section 15 and Part 5 of the **Subordinate Legislation Act 1994** apply for the purposes of subsection (1) as though—

(a) a determination were a statutory rule (within the meaning of that Act); and

(b) notice of the making of the statutory rule had been published in the Government Gazette when the determination was published on the Internet site of the Office of the Victorian Information Commissioner.

S. 42(2)(b) amended by No. 20/2017 s. 106(8).

Division 6—Information usage arrangements

43 Definitions

In this Division—

adverse action means any action that may adversely affect the rights, benefits, privileges, obligations or interests of a specific individual;

lead party, in relation to an information usage arrangement, means—

(a) if one organisation is a party to the information usage arrangement, that organisation; or

(b) if more than one organisation is a party to the information usage arrangement—

(i) the organisation which has the agreement of the other parties to seek approval under section 47; or

(ii) if the arrangement is amended, the organisation which has the agreement of the other parties to seek approval of a further amendment under section 52;

public purpose means—

(a) compliance with a law; or

(b) the performance of functions by a public sector agency or a Council, or an agency of the Commonwealth, another State or a Territory; or

(c) the provision of a service in the public interest to the public or a section of the public;

relevant Minister, in relation to an approved information usage arrangement, means each responsible Minister who approved the arrangement under section 50(2)(a) or (b).

44 Approval of arrangement not required if information use otherwise permitted

To avoid doubt, nothing in this Division requires an organisation to seek approval of an information usage arrangement if the collection, holding, management, use, disclosure or transfer of personal information is expressly permitted by or under this Act or another enactment.

45 Meaning of *information usage arrangement*

(1) In this Division, an ***information usage arrangement*** is an arrangement that—

(a) sets out acts or practices for handling personal information to be undertaken in relation to one or more public purposes; and

(b) for any of those acts or practices, does any one or more of the following—

(i) modifies the application of a specified Information Privacy Principle (other than IPP 4 or 6) or an approved code of practice;

(ii) provides that the practice does not need to comply with a specified Information Privacy Principle (other than IPP 4 or 6) or an approved code of practice;

(iii) permits handling personal information for the purposes of an information handling provision.

(2) An information usage arrangement must—

(a) specify the parties to the arrangement; and

Note

See section 46 as to who can be a party to an information usage arrangement.

(b) specify the personal information or type of personal information to be handled under the arrangement; and

(c) describe how the arrangement would facilitate one or more public purposes; and

(d) if handling personal information under the arrangement modifies or provides for noncompliance with an Information Privacy Principle or an approved code of practice—

(i) identify the Information Privacy Principle or approved code of practice; and

(ii) state how the Information Privacy Principle or approved code of practice would be modified or not complied with; and

(e) if the arrangement would be for the purposes of an information handling provision—

(i) identify the provision; and

(ii) describe the effect of the provision; and

(f) for every party to the arrangement—

(i) describe the personal information or type of personal information that the party could disclose or transfer to other parties to the arrangement; and

(ii) state the manner in which a party could use personal information, including whether a party could disclose that information to another person or body and in what circumstances; and

(g) for every organisation that is a party to the arrangement—

(i) state adverse actions that an organisation could reasonably be expected to take as a result of handling personal information under the arrangement; and

(ii) specify the procedure that an organisation must follow before taking adverse action as a result of handling of personal information under the arrangement.

(3) An information usage arrangement may include an expiry date. However, if an information usage arrangement does not do so, it must include the reason why it does not do so.

46 Parties to an information usage arrangement

The parties specified in an information usage arrangement may only be—

(a) in the case of a single party, an organisation (other than a contracted service provider); and

(b) otherwise, an organisation (other than a contracted service provider) and one or more of the following—

(i) another organisation;

(ii) a person or body that is an agency of the Commonwealth, another State or a Territory;

(iii) any other person or body (including a private sector body) that is not an organisation, whether or not located within Victoria.

47 Information Commissioner to consider information usage arrangement

S. 47 (Heading) amended by No. 20/2017 s. 106(3).

(1) A lead party may apply for approval of an information usage arrangement by submitting to the Information Commissioner an information usage arrangement.

S. 47(1) amended by No. 20/2017 s. 106(2).

S. 47(2) amended by No. 20/2017 s. 106(2).

(2) The Information Commissioner may—

S. 47(2)(a) amended by No. 20/2017 s. 106(2).

(a) direct each organisation that is a party to the information usage arrangement to consult with any person that the Information Commissioner considers appropriate; and

S. 47(2)(b) amended by No. 20/2017 s. 106(2).

(b) consult any person that the Information Commissioner considers appropriate.

S. 47(3) amended by No. 20/2017 s. 106(2).

(3) If the arrangement would modify the application of, or provide for noncompliance with, a specified Information Privacy Principle or an approved code of practice, the Information Commissioner must consider whether the public interest in handling personal information under the information usage arrangement in the way specified under section 45(2)(d) would substantially outweigh the public interest in complying with the specified Information Privacy Principle or approved code of practice.

S. 47(4) amended by No. 20/2017 s. 106(2).

(4) If the arrangement is for the purposes of an information handling provision, the Information Commissioner must consider whether the public interest in treating the handling of personal information as being permitted for the purpose of the information handling provision would substantially outweigh the public interest in treating that handling of information as not being permitted for the purpose of the information handling provision.

48 Information Commissioner's report

S. 48 (Heading) amended by No. 20/2017 s. 106(4).

(1) The Information Commissioner must issue a report about the information usage arrangement in respect of which approval has been sought under section 47.

S. 48(1) amended by No. 20/2017 s. 106(9)(a).

(2) The Information Commissioner's report may consider the appropriateness of all aspects of the information usage arrangement, including the parties.

S. 48(2) amended by No. 20/2017 s. 106(9)(b).

(3) If the information usage arrangement is for the purposes of an information handling provision, the Information Commissioner's report must state whether, in the Information Commissioner's opinion, the provision stated under section 45(2)(e) is an information handling provision.

S. 48(3) amended by No. 20/2017 s. 106(9)(b).

49 Information Commissioner's certificate

S. 49 (Heading) amended by No. 20/2017 s. 106(4).

(1) If—

S. 49(1) amended by No. 20/2017 s. 106(2).

(a) an application is made under section 47 for approval of an information usage arrangement; and

(b) the arrangement would modify the application of, or provide for non-compliance with, a specified Information Privacy Principle or an approved code of practice; and

(c) the Information Commissioner is satisfied that the public interest in handling personal information under the information usage arrangement in the way specified under section 45(2)(d) would substantially

S. 49(1)(c) amended by No. 20/2017 s. 106(2).

outweigh the public interest in complying with the specified Information Privacy Principle or approved code of practice—

the Information Commissioner must issue a certificate to that effect in respect of the information usage arrangement.

S. 49(2) amended by No. 20/2017 s. 106(2).

(2) If—

(a) an application is made under section 47 for approval of an information usage arrangement for the purposes of an information handling provision; and

S. 49(2)(b) amended by No. 20/2017 s. 106(2).

(b) the Information Commissioner is satisfied that the public interest in treating the handling of personal information as being permitted for the purpose of the information handling provision would substantially outweigh the public interest in treating that handling of information as not being permitted for the purpose of the information handling provision—

the Information Commissioner must issue a certificate to that effect in respect of the information usage arrangement.

(3) A certificate may apply to matters in both subsections (1) and (2).

S. 49(4) amended by No. 20/2017 s. 106(2).

(4) The Information Commissioner may refuse to issue a certificate in respect of an information usage arrangement if the Information Commissioner considers that a public interest determination would be more appropriate in the circumstances.

S. 49(5) amended by No. 20/2017 s. 106(2).

(5) The Information Commissioner must refuse to issue a certificate in respect of an information usage arrangement if the Information Commissioner is not satisfied of the matters set out in section 47(3) or (4) or both, as applicable.

(6) The Information Commissioner must give written notice to the lead party as soon as practicable of a refusal under subsection (4) or (5).

S. 49(6) amended by No. 20/2017 s. 106(2).

(7) An application for approval under section 47 is taken to be refused on the day the lead party is notified in accordance with subsection (6).

50 Ministerial approval of information usage arrangement[3]

(1) The Information Commissioner must send a report issued under section 48 and a copy of any certificate issued under section 49 in relation to an information usage arrangement to—

S. 50(1) amended by No. 20/2017 s. 106(7)(a).

(a) the responsible Minister for each organisation that is a party to the arrangement; and

(b) if the arrangement authorises the handling of personal information for the purposes of an information handling provision, the responsible Minister for that provision.

(2) After receiving the report and a certificate from the Information Commissioner, the information usage arrangement may be approved—

S. 50(2) amended by No. 20/2017 s. 106(7)(a).

(a) in the case of a single party, by the responsible Minister for the lead party; or

(b) otherwise, by agreement of the responsible Ministers for each organisation that is a party to the arrangement.

(3) An information usage arrangement cannot be approved under this section unless the Information Commissioner has issued a certificate in relation to the arrangement.

S. 50(3) amended by No. 20/2017 s. 106(7)(a).

(4) Subject to subsection (5), the Information Commissioner must cause an approved information usage arrangement to be published on the Internet site of the Information Commissioner.

S. 50(4) amended by No. 20/2017 s. 106(7)(a).

S. 50(5) amended by No. 20/2017 s. 106(7)(a).

(5) The Information Commissioner is not required to publish any part of an approved information usage arrangement that would disclose—

(a) personal information; or

S. 50(5)(b) amended by No. 20/2017 s. 81.

(b) information that, if contained in a document, would make that document an exempt document under section 29(b), 29A, 31, 31A or 34 of the **Freedom of Information Act 1982**.

51 Effect of approved information usage arrangement

S. 51(1) amended by No. 20/2017 s. 106(10).

(1) If an approved information usage arrangement provides for acts and practices for handling personal information that modify or do not comply with an Information Privacy Principle (other than IPP 4 or 6) or approved code of practice specified in the Information Commissioner's certificate issued under section 49, the parties to the arrangement are not required to comply with the Information Privacy Principle or approved code of practice in respect of those acts or practices to the extent specified in the certificate.

(2) If an approved information usage arrangement provides for the handling of personal information for the purposes of an information handling provision, the handling of that information in accordance with the arrangement is taken to be permitted for the purposes of that provision.

52 Amendment of approved information usage arrangement

S. 52(1) amended by No. 20/2017 s. 106(5).

(1) The lead party to an approved information usage arrangement may apply to the Information Commissioner for the approval of an amendment to the arrangement.

(2) Sections 47(2), (3) and (4), 48, 49, 50 and 51 apply to an application under subsection (1)—

(a) as if a reference to an information usage arrangement were a reference to the amendment in respect of which approval is sought; and

(b) with any other necessary modifications.

53 Revocation of approval of information usage arrangement

(1) The relevant Minister must revoke the approval of an information usage arrangement if the relevant Minister—

(a) is notified by the Information Commissioner that any ground set out in subsection (3)(a) exists; or

S. 53(1)(a) amended by No. 20/2017 s. 106(2).

(b) becomes aware that a ground set out in subsection (3)(b) exists.

(2) The relevant Minister may revoke the approval of an information usage arrangement on request of the Information Commissioner or any party that is an organisation.

S. 53(2) amended by No. 20/2017 s. 106(2).

(3) The grounds for revocation under subsection (1) are—

(a) if the information usage arrangement modifies or provides for noncompliance with a specified Information Privacy Principle or approved code of practice, the Information Commissioner is no longer satisfied that the public interest in information handling under the arrangement substantially outweighs the public interest in complying with the Information Privacy Principles; or

S. 53(3)(a) amended by No. 20/2017 s. 106(2).

(b) the reasons in the application for approval of the information usage arrangement no longer apply.

S. 53(4) amended by No. 20/2017 s. 106(2).

(4) The Information Commissioner must give written notice to the parties to the information usage arrangement before notifying the Minister of the existence of a ground for revocation set out in subsection (3)(a).

(5) The relevant Minister must give written notice to the parties to the information usage arrangement before revoking the arrangement on a ground set out in subsection (3)(b).

54 Reporting requirements for approved information usage arrangements

S. 54(1) amended by No. 20/2017 s. 106(2).

(1) The lead party to an approved information usage arrangement must report to the Information Commissioner about the arrangement—

(a) annually; and

S. 54(1)(b) amended by No. 20/2017 s. 106(2).

(b) at any other time, as requested by the Information Commissioner.

S. 54(2) amended by No. 20/2017 s. 106(2).

(2) The content and timing of a report under subsection (1)(a) must be consistent with any guidelines published by the Information Commissioner.

S. 54(3) amended by No. 20/2017 s. 106(2).

(3) The Information Commissioner, on request of a relevant Minister, must report to the relevant Minister about an approved information usage arrangement.

S. 54(4) amended by No. 20/2017 s. 106(2).

(4) The Information Commissioner may report to a relevant Minister about an approved information usage arrangement at any time.

Division 7—Certification

55 Information Commissioner may certify consistency of act or practice

S. 55 (Heading) amended by No. 20/2017 s. 106(3).

(1) The Information Commissioner may certify that a specified act or practice of an organisation is consistent with—

S. 55(1) amended by No. 20/2017 s. 106(11)(a).

(a) an Information Privacy Principle; or

(b) an approved code of practice; or

(c) an information handling provision.

(2) The certificate remains in effect until any expiry date specified in the certificate, unless it is earlier set aside by a court or VCAT.

(3) The certificate must include an expiry date, unless it is inappropriate to do so in all the circumstances.

(4) A person who does an act or engages in a practice in good faith in accordance with a current certificate does not contravene the relevant Information Privacy Principle or approved code of practice or the relevant information handling provision (as the case requires).

(5) A certificate under this section must be published on the Internet site of the Office of the Victorian Information Commissioner.

S. 55(5) amended by No. 20/2017 s. 106(11)(b).

56 Review of decision to issue certificate

(1) An individual or organisation whose interests are affected by the decision to issue the certificate under section 55(1) may apply to VCAT for review of the decision.

S. 56(2) amended by No. 20/2017 s. 106(5).

(2) The Information Commissioner is a party to a proceeding on a review under this section.

Division 8—Information privacy complaints

Subdivision 1—Making a complaint

57 Complaints

S. 57(1) amended by No. 20/2017 s. 106(12)(a).

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

(2) A complaint relating to an Information Privacy Principle or an applicable code of practice may be made under subsection (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—

(i) not less than 45 days before complaining under subsection (1) the individual complained to the code administrator in accordance with the procedures set out in that code; and

(ii) the individual 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 subsection (1) on behalf of all of the individuals with their consent.

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

S. 57(4) amended by No. 20/2017 s. 106(12)(a).[4]

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

(6) The respondent to a complaint is—

(a) if the organisation represents the Crown, the State; or

(b) if the organisation does not represent the Crown and—

(i) is a legal person, the organisation; or

(ii) is an unincorporated body, the members of the committee of management of the organisation.

(7) A failure to comply with subsection (5) does not render the complaint, or any step taken in relation to it, a nullity.

58 Complaint referred to Information Commissioner

S. 58 (Heading) amended by No. 20/2017 s. 106(3).

(1) The Information Commissioner may treat a complaint referred to the Commissioner by the Ombudsman under section 16I of the

S. 58(1) amended by No. 20/2017 s. 106(5).

Ombudsman Act 1973 as if it were a complaint made under section 57(1).

S. 58(2) repealed by No. 20/2017 s. 82.

* * * * *

59 Complaints by minors

(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

S. 59(1)(b)(iii) amended by No. 20/2017 s. 106(5).

(iii) any other individual who, in the opinion of the Information 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 the child's behalf may do so even if the child is otherwise incapable of exercising powers.

60 Complaints by people with a disability

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

(a) another individual authorised by that individual to complain on the individual's behalf; or

S. 60(1)(b) amended by No. 20/2017 s. 106(5).

(b) if that individual is unable to authorise another individual, any other individual on the individual's behalf who, in the opinion of the Information Commissioner, has a

sufficient interest in the subject matter of the complaint.

(2) In this section—

disability has the same meaning as in the **Equal Opportunity Act 2010**.

Subdivision 2—Procedure after a complaint is made

61 Information Commissioner must notify respondent

S. 61 (Heading) amended by No. 20/2017 s. 106(3).

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

S. 61 amended by No. 20/2017 s. 106(5).

62 Circumstances in which Information Commissioner may decline to entertain complaint[5]

S. 62 (Heading) amended by No. 20/2017 s. 106(3).

(1) The Information Commissioner may decline to entertain a complaint made under section 57(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 Information Commissioner considers that—

S. 62(1) amended by No. 20/2017 s. 106(13)(a).

(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 Information Commissioner about the act or practice, the complainant has not complained to the respondent; or

S. 62(1)(c) amended by No. 20/2017 s. 106(13)(a).

S. 62(1)(d) amended by No. 20/2017 s. 106(13)(a).

(d) the complaint to the Information 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 60, on behalf of a child or a person with a disability, by an individual who has an insufficient interest in the subject matter of the complaint.

S. 62(2) amended by Nos 21/2015 s. 3(Sch. 1 item 41.3), 20/2017 s. 106(13)(a).

(2) A notice under subsection (1) must state that the complainant, by notice in writing given to the Information Commissioner, may require the Information Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

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

S. 62(3) amended by No. 20/2017 s. 106(13)(a).

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

S. 62(3)(a) amended by No. 20/2017 s. 106 (13)(a).

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

(4) Within 60 days after receiving the Information Commissioner's notice declining to entertain a complaint, the complainant, by notice in writing given to the Information Commissioner, may require the Information Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

S. 62(4) amended by Nos 21/2015 s. 3(Sch. 1 item 41.3), 20/2017 s. 106 (13)(a)(b).

(5) The Information Commissioner must comply with a notice under subsection (4).

S. 62(5) amended by No. 20/2017 s. 106(13)(a).

(6) If the complainant does not notify the Information Commissioner under subsection (4), the Information Commissioner may dismiss the complaint.

S. 62(6) amended by No. 20/2017 s. 106(13)(a).

(7) As soon as possible after a dismissal under subsection (6), the Information Commissioner must, by written notice, notify the complainant and the respondent of the dismissal.

S. 62(7) amended by No. 20/2017 s. 106(13)(a).

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

S. 63 (Heading) amended by No. 20/2017 s. 106(3).

63 Information Commissioner may refer complaint

S. 63(1) amended by No. 20/2017 s. 106(14).

(1) The Information Commissioner may refer a complaint if the Information Commissioner considers that the complaint could be the subject of a complaint to—

(a) the Federal Privacy Commissioner under the Privacy Act 1988 of the Commonwealth; or

(b) the Disability Services Commissioner under the **Disability Act 2006**; or

S. 63(1)(c) repealed by No. 20/2017 s. 83(1).

* * * * *

(d) the Ombudsman under the **Ombudsman Act 1973**; or

S. 63(1)(e) amended by No. 22/2016 s. 240.

(e) the Health Complaints Commissioner under the **Health Records Act 2001**; or

(f) the Commission for Children and Young People under the **Commission for Children and Young People Act 2012**; or

(g) the Mental Health Complaints Commissioner under the **Mental Health Act 2014**.

S. 63(1A) inserted by No. 20/2017 s. 83(2).

(1A) The Information Commissioner may decide to deal with a complaint as if it were a complaint made under the **Freedom of Information Act 1982** if the Information Commissioner considers that the complaint could be dealt with more effectively or appropriately under that Act.

(2) The Information Commissioner must notify the complainant and the respondent in writing of the referral or decision under subsection (1A).

S. 63(2) amended by No. 20/2017 ss 83(3), 106(14)(a).

(3) A complainant may take no further action under this Act in relation to the subject matter of a complaint referred under this section or dealt with under the **Freedom of Information Act 1982**.

S. 63(3) amended by No. 20/2017 s. 83(4).

64 Information Commissioner may dismiss stale complaint

S. 64 (Heading) amended by No. 20/2017 s. 106(3).

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

S. 64(1) amended by No. 20/2017 s. 106(2).

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

S. 64(2) amended by No. 20/2017 s. 106(2).

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

65 Minister may refer a complaint direct to VCAT

(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 VCAT for hearing under Subdivision 5, whether or not the Information Commissioner has considered it or the complaint is in the process of being conciliated.

S. 65(1) amended by No. 20/2017 s. 106(5).

(2) The Minister is not a party to a proceeding on a complaint referred to VCAT under subsection (1) unless joined by VCAT.

66 What happens if conciliation is inappropriate?

S. 66(1) amended by No. 20/2017 s. 106(6)(a).

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

S. 66(2) amended by No. 20/2017 s. 106(6)(a).

(2) A notice under subsection (1) must state that the complainant, by notice in writing given to the Information Commissioner, may require the Information Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

S. 66(3) amended by No. 20/2017 s. 106(6).

(3) Within 60 days after receiving the Information Commissioner's notice under subsection (1), the complainant, by notice in writing given to the Information Commissioner, may require the Information Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

S. 66(4) amended by No. 20/2017 s. 106(6)(a).

(4) The Information Commissioner must comply with a notice under subsection (3).

S. 66(5) amended by No. 20/2017 s. 106(6)(a).

(5) If the complainant does not notify the Information Commissioner under subsection (3), the Information Commissioner may dismiss the complaint.

S. 66(6) amended by No. 20/2017 s. 106(6)(a).

(6) As soon as possible after a dismissal under subsection (5), the Information 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.

Subdivision 3—Conciliation of complaints

67 Conciliation process

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

S. 67(1) amended by No. 20/2017 s. 106(2).

(2) Subsection (1) does not apply to a complaint—

(a) that the Information Commissioner has declined to entertain under section 62, referred under section 63 or dismissed under section 64; or

S. 67(2)(a) amended by No. 20/2017 s. 106(2).

(b) that the Minister has referred to VCAT under section 65.

(3) The Information 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.

S. 67(3) amended by No. 20/2017 s. 106(2).

68 Information Commissioner may issue notice to produce or attend

S. 68 substituted by No. 20/2017 s. 84.

If the Information Commissioner has reason to believe that a person has information or a document relevant to a conciliation under this Subdivision, the Information Commissioner may serve a notice to produce or attend on the person, in accordance with Division 10.

69 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

S. 69(1)(a) amended by No. 20/2017 s. 106(2).

prepared by the parties or the Information Commissioner; and

S. 69(1)(b) amended by No. 20/2017 s. 106(2).

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

S. 69(1)(c) amended by No. 20/2017 s. 106(2).

(c) the Information 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 VCAT for registration.

(3) Subject to subsection (4), VCAT must register the record and give a certified copy of the registered record to each party.

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

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

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

70 Evidence of conciliation is inadmissible

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

71 What happens if conciliation fails?

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

S. 71(1) amended by No. 20/2017 s. 106(6)(a).

(2) A notice under subsection (1) must state that the complainant, by written notice given to the Information Commissioner, may require the Information Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

S. 71(2) amended by No. 20/2017 s. 106(6)(a).

(3) Within 60 days after receiving the Information Commissioner's notice under subsection (1), the complainant, by notice in writing given to the Information Commissioner, may require the Information Commissioner to refer the complaint to VCAT for hearing under Subdivision 5.

S. 71(3) amended by No. 20/2017 s. 106(6).

(4) The Information Commissioner must comply with a notice under subsection (3).

S. 71(4) amended by No. 20/2017 s. 106(6)(a).

(5) If the complainant does not notify the Information Commissioner under subsection (3), the Information Commissioner may dismiss the complaint.

S. 71(5) amended by No. 20/2017 s. 106(6)(a).

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

S. 71(6) amended by No. 20/2017 s. 106(6)(a).

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

Subdivision 4—Interim orders

72 VCAT may make interim orders before hearing

S. 72(1) amended by No. 20/2017 s. 106(5).

(1) A complainant or a respondent or the Information Commissioner may apply to VCAT 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 VCAT might subsequently make.

(2) An application may be made under subsection (1) at any time before the complaint is referred to VCAT.

(3) In making an interim order, VCAT 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 VCAT.

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

(6) In making an interim order, VCAT—

(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) VCAT may assess any costs or damages referred to in subsection (6)(a).

(8) Nothing in this section affects or takes away from VCAT'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 VCAT in respect of a complaint.

Subdivision 5—Jurisdiction of VCAT

73 When may VCAT hear a complaint?

(1) VCAT may hear any of the following—

(a) a complaint referred to it by the Information Commissioner under section 62, 66 or 71;

S. 73(1)(a) amended by No. 20/2017 s. 106(5).

(b) a complaint referred to it by the Minister under section 65.

(2) VCAT also has the jurisdiction conferred by section 72.

(3) If a certificate has been given in respect of a document under section 83J(2), the powers of VCAT—

S. 73(3) amended by No. 20/2017 s. 85.

(a) do not extend to reviewing the decision to give the certificate; and

(b) are 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**.

74 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 73(1).

S. 74(2) amended by No. 20/2017 s. 106(5).

(2) The Information Commissioner is not a party to a proceeding in respect of a complaint referred to in section 73(1)(a) unless joined by VCAT.

75 Time limits for complaints referred by the Minister

(1) VCAT must commence hearing a complaint within 30 days after its referral to VCAT if the complaint was referred to it by the Minister under section 65.

(2) VCAT, constituted by a presidential member, may extend the period of 30 days under subsection (1) by one further period of not more than 30 days.

76 Inspection of exempt documents by VCAT

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

(a) any document produced to VCAT 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 VCAT as constituted for the proceedings; or

(ii) a member of the staff of VCAT in the course of the performance of the member's duties as a member of that staff; and

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

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

S. 76(3) amended by No. 60/2014 s. 137.

(3) If the applicant is represented by an Australian legal practitioner, orders under subsection (2) may include an order that the contents of a document produced to VCAT that is claimed to be an exempt document be disclosed to that practitioner.

(4) In making an order under subsection (2), VCAT 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 VCAT under section 51(2) of the **Victorian Civil and Administrative Tribunal Act 1998**.

(5) If a complaint under section 73 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**, VCAT 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.

77 What may VCAT decide?

(1) After hearing the evidence and representations that the parties to a complaint desire to adduce or make, VCAT 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 VCAT 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 subsection (1)(a)(i) or (ii) arising out of a breach of IPP 6.5 or 6.6, VCAT 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.

S. 77(3) amended by No. 20/2017 s. 106(2).

(3) If an order of VCAT relates to a public register, the Information 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.

S. 77(4) amended by No. 20/2017 s. 106(2).

(4) The Information Commissioner may include in a report under subsection (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.

Division 9—Enforcement of Information Privacy Principles and approved information usage arrangements

78 Compliance notice

S. 78(1) amended by No. 20/2017 s. 106(6)(a).

(1) The Information Commissioner may serve a compliance notice on an organisation, if it appears to the Information Commissioner 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) or an approved information usage arrangement; 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, applicable code of practice or approved information usage arrangement.

S. 78(3) amended by No. 20/2017 s. 106(6)(a).

(3) If the Information 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 Information Commissioner may extend the period specified in the notice on the organisation giving the Information Commissioner an undertaking to take the specified action within the extended period.

S. 78(4) amended by No. 20/2017 s. 106(6)(a).

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

S. 78(5) amended by No. 20/2017 s. 106(6).

(5) The Information Commissioner may act under subsection (1) on the Information Commissioner's own initiative or on an application by an

individual who was a complainant under Division 8.

(6) In deciding whether or not to serve a compliance notice, the Information Commissioner may have regard to the extent to which the organisation has complied with a decision of VCAT under Subdivision 5 of Division 8.

S. 78(6) amended by No. 20/2017 s. 106(6)(a).

79 Power to compel production of documents or attendance of witness

S. 79 substituted by No. 20/2017 s. 86.

If the Information Commissioner reasonably believes that a person has information or a document relevant to a decision to serve a compliance notice under section 78(1), the Information Commissioner may serve a notice to produce or attend on the person in accordance with Division 10.

* * * * *

Ss 80, 81 repealed by No. 20/2017 s. 87.

82 Offence not to comply with compliance notice

(1) An organisation must comply with a compliance notice served on it under section 78(1) that is in effect.

Penalty: 600 penalty units, in the case of an individual;

3000 penalty units, in the case of a body corporate.

(2) A compliance notice served under section 78(1) does not take effect until the latest of the following—

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

(b) the expiry of any extended period fixed under section 78(3);

(c) the expiry of the period within which an application for review of the decision to serve the notice may be made to VCAT under section 83(1);

S. 82(2)(d) amended by No. 20/2017 s. 106(5).

(d) if an application is made under section 83(1) for review of the decision to serve the notice, the review has been determined in favour of the Information Commissioner.

(3) An offence against subsection (1) is an indictable offence.

83 Application for review

S. 83(1) amended by No. 20/2017 s. 106(2).

(1) An individual or organisation whose interests are affected by a decision of the Information Commissioner under section 78(1) to serve a compliance notice may apply to VCAT 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.

S. 83(3) amended by No. 20/2017 s. 106(2).

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

Division 10—Notices to produce or attend

Pt 3 Div. 10 (Heading and ss 83A–83K) inserted by No. 20/2017 s. 88.

83A Notice to produce or attend

S. 83A inserted by No. 20/2017 s. 88.

(1) A notice to produce or attend may require a person—

(a) to produce a specified document to the Information Commissioner by or before a specified time and in a specified manner; or

(b) to attend at a specified time and place on a specified date to produce documents to the Information Commissioner; or

(c) to attend an examination before the Information Commissioner to give evidence and to produce documents at a specified time and place on a specified date; or

(d) to attend the Information Commissioner at a specified time and place to produce a specified document.

(2) A notice under subsection (1) must contain the following information—

(a) a statement that—

(i) failure to comply with the notice without reasonable excuse may be an offence; and

(ii) includes the maximum penalty for that offence;

(b) examples of what may constitute a reasonable excuse for failing to comply with the notice.

S. 83B inserted by No. 20/2017 s. 88.

83B Variation or revocation of a notice to produce or attend

(1) The Information Commissioner, by further written notice served on a person, may at any time vary or revoke a notice to produce or attend served on the person.

(2) A notice varying or revoking a notice to produce or attend must be served in accordance with section 83C.

S. 83C inserted by No. 20/2017 s. 88.

83C Service of notice to produce documents or to attend

(1) Subject to subsection (2), a notice to produce or attend must be served at a reasonable time, being not less than 7 days before the date on which the person is required to attend or otherwise comply with the notice.

(2) The Information Commissioner may serve a notice to attend requiring immediate attendance by a person if—

(a) the Information Commissioner considers on reasonable grounds that a delay in the person's attendance is likely to result in—

(i) evidence being lost or destroyed; or

(ii) the commission of an offence; or

(iii) the escape of the person on whom the notice is served; or

(iv) serious prejudice to the purpose for which the notice was issued; or

(b) the person on whom the notice is served consents to immediate attendance.

(3) A notice to produce or attend directed to a natural person must be served by serving a copy of the notice on the person personally.

(4) A notice to produce or attend directed to a body corporate must be served by leaving a copy of the notice at the registered office or principal place of business of the body corporate with a person apparently employed at that office or place and who is apparently at least 18 years of age.

(5) Subsection (4) is in addition to, and not in derogation of, sections 109X and 601CX of the Corporations Act.

83D Office of the Information Commissioner to report to the Victorian Inspectorate on issue of notice to produce or attend

S. 83D inserted by No. 20/2017 s. 88.

Within 3 days after the issue of a notice to produce or attend, the Information Commissioner must give a written report to the Victorian Inspectorate specifying—

(a) the name of the person to whom the notice relates; and

(b) the reasons why the notice was issued.

83E Power to take evidence on oath or affirmation

S. 83E inserted by No. 20/2017 s. 88.

(1) The Information Commissioner may require a person attending an examination, in accordance with a notice to attend, to give evidence on oath or affirmation.

(2) The Information Commissioner, or a person authorised to do so by the Commissioner, may administer an oath or affirmation to a person for the purposes of subsection (1).

(3) A person must not, without reasonable excuse, refuse or fail to take an oath or make an affirmation when required to do so by the Information Commissioner under subsection (1).

Penalty: 60 penalty units.

(4) A person does not commit an offence against subsection (3) unless, before the person is required to take the oath or make the affirmation, the Information Commissioner informs the person that refusal or failure to do so without reasonable excuse is an offence.

S. 83F inserted by No. 20/2017 s. 88.

83F Legal advice and representation

A person may seek legal advice, and be represented by a legal practitioner in relation to—

(a) a notice to produce or attend that is directed to the person and the notice relates to—

(i) a conciliation conducted by the Information Commissioner; or

(ii) the issue of a compliance notice by the Information Commissioner; or

(b) the person's rights, liabilities, obligations and privileges in relation to the notice to produce or attend.

S. 83G inserted by No. 20/2017 s. 88.

83G Protection of legal practitioners and persons—notice to produce or attend

(1) A legal practitioner representing the person who is served with a notice to produce or attend has the same protection and immunity as a legal practitioner has in representing a party in a proceeding in the Supreme Court.

(2) A person who is served with a notice to produce or attend has the same protection and immunity as a witness has in a proceeding in the Supreme Court.

S. 83H inserted by No. 20/2017 s. 88.

83H Failure to comply with notice to produce or attend

A person who is served with a notice to produce or attend, must not, without reasonable excuse, refuse or fail to comply with a requirement set out in the notice—

(a) to attend before the Information Commissioner; or

(b) to give information; or

(c) to answer a question or produce a document.

Penalty: 60 penalty units.

83I Reasonable excuse—self-incrimination

S. 83I inserted by No. 20/2017 s. 88.

Without limiting what is a reasonable excuse for the purposes of section 83H, it is a reasonable excuse to refuse or fail to comply with a requirement of the notice if the giving of the information or production of the document may tend to incriminate the person.

83J Reasonable excuse—cabinet documents and legal professional privilege

S. 83J inserted by No. 20/2017 s. 88.

(1) Without limiting what is a reasonable excuse for the purposes of section 83H, it is a reasonable excuse for a person to refuse or fail to comply with a requirement of the notice if—

(a) the information or document—

(i) is an exempt document under section 28 of the **Freedom of Information Act 1982**; or

(ii) is information that if included in a document would make that document an exempt document under that section 28; or

(b) the information or document is subject to legal professional privilege or client legal privilege.

(2) The Secretary to the Department of Premier and Cabinet may certify that information or a document described in subsection (1)(a)—

(a) in the case of information, is information which, if included in a document, would make the document an exempt document of a kind referred to in section 28(1) of the **Freedom of Information Act 1982**;

(b) in the case of a document, is or, if it existed, would be an exempt document of a kind referred to in section 28(1) of the **Freedom of Information Act 1982**.

S. 83K inserted by No. 20/2017 s. 88.

83K Statutory secrecy not a reasonable excuse

(1) It is not a reasonable excuse for a person to refuse or fail to comply with the notice as a result of—

(a) any obligation imposed on that person, by any enactment or rule of law, to maintain secrecy in relation to the production of the document or information or the answer to a question; or

(b) any restriction imposed on that person, by any enactment or rule of law, that prohibits the disclosure of the document, information or the answer to a question.

(2) Nothing in this section affects the operation of—

(a) Part 7 of the **Protected Disclosure Act 2012**; or

(b) Division 3 of Part 2 of the **Independent Broad-based Anti-corruption Commission Act 2011**.

Part 4—Protective data security

Division 1—Application of Part

84 Application of Part

(1) Subject to subsection (2), this Part applies to—

(a) a public sector agency; and

(b) a body that is a special body, within the meaning of section 6 of the **Public Administration Act 2004**; and

(c) a body declared under subsection (3) to be a body to which this Part applies.

(2) This Part does not apply to the following—

(a) a Council;

(b) a university within the meaning of the **Education and Training Reform Act 2006**;

(c) a body to which, or to the governing body of which, the government of another jurisdiction, or a person appointed or body established under the law of another jurisdiction, has the right to appoint a member, irrespective of how that right arises;

(d) a public hospital within the meaning of the **Health Services Act 1988**;

(e) a public health service within the meaning of the **Health Services Act 1988**;

(f) a multi-purpose service within the meaning of the **Health Services Act 1988**;

(g) an ambulance service, within the meaning of the **Ambulance Services Act 1986**.

(3) The Governor in Council, by Order published in the Government Gazette, may declare a body to be a body to which this Part applies.

Division 2—Protective data security framework

S. 85 (Heading) amended by No. 20/2017 s. 106(3).

85 Information Commissioner to develop Victorian protective data security framework

S. 85(1) amended by No. 20/2017 s. 106(5).

(1) The Information Commissioner must develop the Victorian protective data security framework for monitoring and assuring the security of public sector data.

S. 85(1A) inserted by No. 20/2017 s. 89.

(1A) The Information Commissioner may from time to time review or amend the Victorian protective data security framework.

(2) The Victorian protective data security framework must be as consistent as possible with standards relating to information security (including international standards) prescribed for the purposes of this section.

Division 3—Protective data security standards

S. 86 (Heading) amended by No. 20/2017 s. 106(3).

86 Information Commissioner may issue protective data security standards

S. 86(1) amended by No. 20/2017 s. 106(2).

(1) The Information Commissioner may issue standards, consistent with the Victorian protective data security framework, for the security, confidentiality and integrity of public sector data and access to public sector data (***protective data security standards***).

(2) The Information Commissioner may issue—

S. 86(2) amended by No. 20/2017 s. 106(2).

(a) protective data security standards that apply to any agency or body referred to in section 84(1) (***general protective data security standards***); or

(b) protective data security standards (***customised protective data security standards***) that apply—

(i) to a specified agency or body referred to in section 84(1) and all information handled by that agency or body; or

(ii) to one or more specified agencies or bodies referred to in section 84(1) and to—

(A) any specified information or class of information handled by those agencies or bodies; or

(B) any specified activity or class of activity of those agencies or bodies.

(3) If a general protective data security standard issued is inconsistent with a customised protective data security standard, the customised protective data security standard prevails to the extent of the inconsistency.

(4) The Information Commissioner must not issue a protective data security standard unless it has been agreed bythe Attorney-General and the Minister for Technology.

S. 86(4) amended by No. 20/2017 s. 106(2).

87 Amendment, revocation or reissue of standards

(1) The Information Commissioner may amend, revoke or reissue a protective data security standard.

S. 87(1) amended by No. 20/2017 s. 106(5).

(2) For the purpose of subsection (1), section 86 applies—

(a) as if a reference to the issue of a protective data security standard were a reference to the amendment, revocation or reissue of a protective data security standard (as the case requires); and

(b) with any other necessary modifications.

88 Compliance with protective data security standards

(1) A public sector body Head for an agency or a body to which this Part applies must ensure that the agency or body does not do an act or engage in a practice that contravenes a protective data security standard, in respect of—

(a) public sector data collected, held, managed, used, disclosed or transferred by it; and

(b) public sector data systems kept by it.

(2) A public sector body Head for an agency or a body to which this Part applies must ensure that a contracted service provider of the agency or body does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.

Division 4—Protective data security plans

89 Protective data security plans

(1) Within 2 years after the issue of protective data security standards applying to an agency or body to which this Part applies, the public sector body Head must ensure that—

(a) a security risk profile assessment is undertaken for the agency or body; and

(b) a protective data security plan is developed for the agency or body that addresses the protective data security standards applicable to that agency or body.

(2) A security risk profile assessment of an agency or body must include an assessment of any contracted service provider of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.

(3) A protective data security plan developed for an agency or body must address compliance by any contracted service provider of the agency or body with the protective data security standards applicable to that agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.

(4) A public sector body Head must ensure that the protective data security plan prepared under this section is reviewed—

(a) if there is a significant change in the operating environment or the security risks relevant to the agency or body; or

(b) otherwise, every 2 years.

(5) A public sector body Head for the agency or body must ensure that a copy of the protective data security plan is given to the Information Commissioner.

S. 89(5) amended by No. 20/2017 s. 106(5).

90 Exemption—Freedom of Information Act 1982

The **Freedom of Information Act 1982** does not apply to a protective data security plan.

Part 5—Law enforcement data security

91 Application of Part

This Part applies to—

S. 91(a) substituted by No. 60/2014 s. 132.

(a) Victoria Police; and

(b) the Chief Statistician; and

(c) an employee or consultant employed or engaged under section 6 of the **Crime Statistics Act 2014**.

S. 92 (Heading) amended by No. 20/2017 s. 106(3).

92 Information Commissioner may issue law enforcement data security standards

S. 92(1) amended by No. 20/2017 s. 106(15).

(1) The Information Commissioner may issue standards for—

(a) the security and integrity of law enforcement data systems and crime statistics data systems; and

(b) access to, and release of, law enforcement data and crime statistics data, including, but not limited to, the release of law enforcement data and crime statistics data to members of the public.

S. 92(2) amended by No. 20/2017 s. 106(15).

(2) The Information Commissioner must consult with the Chief Commissioner of Police in developing law enforcement data security standards.

S. 92(3) amended by No. 20/2017 s. 106(15).

(3) The Information Commissioner must consult with the Chief Statistician in developing law enforcement data security standards in relation to crime statistics data and crime statistics data systems.

(4) The Information Commissioner may amend, revoke and reissue law enforcement security standards in accordance with subsection (2) or (3), as the case requires.

S. 92(4) amended by No. 20/2017 s. 106(15).

93 Inconsistency with protective data security standards

If a law enforcement data security standard is inconsistent with a protective data security standard, the law enforcement security standard prevails to the extent of the inconsistency.

94 Compliance with law enforcement data security standards

(1) Victoria Police must not do an act or engage in a practice that contravenes a law enforcement data security standard, in respect of—

S. 94(1) amended by No. 60/2014 s. 133.

(a) law enforcement data collected, held, used, managed, disclosed or transferred by it; or

(b) law enforcement data systems kept by it.

(2) A person referred to in section 91(b) or (c) must not do an act or engage in a practice that contravenes a law enforcement data security standard, in respect of—

(a) crime statistics data collected, held, used, managed, disclosed or transferred by the person; or

(b) crime statistics data systems kept by the person.

Pt 6 (Heading) substituted by No. 20/2017 s. 90.

Part 6—General powers of Information Commissioner

Pt 6 Div. 1 (Heading and ss 95–102) repealed by No. 20/2017 s. 91.

* * * * *

Pt 6 Div. 2 (Heading) substituted as Pt 6 Div. 1 (Heading) by No. 20/2017 s. 92.

Division 1—General powers of Information Commissioner

S. 103 repealed by No. 20/2017 s. 93.

* * * * *

S. 104 repealed by No. 20/2017 s. 94.

* * * * *

S. 105 repealed by No. 20/2017 s. 95.

* * * * *

S. 106 (Heading) amended by No. 20/2017 s. 106(3).

S. 106 amended by No. 20/2017 ss 96, 106(6).

106 Information Commissioner may require access to data and data systems from public sector body Heads

The Information Commissioner may require the relevant public sector body Head to give the Information Commissioner free and full access at all reasonable times to the following as is necessary to enable the Information Commissioner to perform the Information Commissioner's functions under section 8D(1)(d) and (2)(b)—

(a) any public sector data (including any document on which such data is recorded); or

(b) any public sector organisation's data system.

107 Information Commissioner may require access to data and data systems from Chief Commissioner of Police

S. 107 (Heading) amended by No. 20/2017 s. 106(16).

(1) The Information Commissioner may require the Chief Commissioner of Police to give the Information Commissioner free and full access at all reasonable times to the following as is necessary to enable the Information Commissioner to perform the Information Commissioner's functions under section 8D(1)(e) and (2)(b)—

S. 107(1) amended by No. 20/2017 ss 97, 106(17).

(a) any law enforcement data (including any document on which such data is recorded); or

(b) the Victoria Police law enforcement data system.

(2) The Chief Commissioner of Police may refuse to comply with a requirement of the Information Commissioner under subsection (1) if the Chief Commissioner considers that giving access to law enforcement data or a law enforcement data system would, or would be reasonably likely to—

S. 107(2) amended by No. 20/2017 s. 106(17)(b).

(a) prejudice the investigation of a breach or possible breach of the law or prejudice the enforcement or proper administration of the law in a particular instance; or

(b) prejudice the fair trial of a person or the impartial adjudication of a particular case or disclose data that is of such a nature that it would be privileged from production in

legal proceedings on the ground of legal professional privilege or client legal privilege; or

(c) disclose, or enable a person to ascertain, the identity of a confidential source of information in relation to the enforcement or administration of the law; or

(d) endanger the lives or physical safety of persons engaged in or in connection with law enforcement or persons who have provided confidential information in relation to the enforcement or administration of the law.

S. 107(3) amended by No. 60/2014 s. 134(1).

(3) Section 19 of the **Victoria Police Act 2013** does not apply to any power, discretion, function, authority or duty of the Chief Commissioner of Police under this section.

Note to s. 107(3) repealed by No. 60/2014 s. 134(2).

* * * * *

S. 107(4) inserted by No. 60/2014 s. 134(3).

(4) A police officer who is a Deputy Commissioner appointed under section 21 of the **Victoria Police Act 2013** may exercise the powers and perform the functions of the Chief Commissioner of Police under this section as if the Deputy Commissioner were the Chief Commissioner of Police.

S. 108 (Heading) amended by No. 20/2017 s. 106(3).

108 Information Commissioner may request access to crime statistics data

S. 108(1) amended by No. 20/2017 ss 98, 106(6).

(1) The Information Commissioner may require the Chief Statistician to give the Information Commissioner free and full access at all reasonable times to any crime statistics data (including any document on which crime statistics

data is recorded) or any crime statistics data system as is necessary to enable the Information Commissioner to perform the Information Commissioner's functions under section 8D(1)(e) and (2)(b).

S. 108(2) amended by No. 20/2017 s. 106(6)(a).

(2) Subject to subsection (3), the Chief Statistician must comply with a requirement of the Information Commissioner under this section.

S. 108(3) amended by No. 20/2017 s. 106(6)(a).

(3) The Chief Statistician may refuse to comply with a requirement of the Information Commissioner under this section if the Chief Statistician considers that giving access to that data or system would, or would be reasonably likely to—

(a) prejudice the investigation of a breach or possible breach of the law or prejudice the enforcement or proper administration of the law in a particular instance; or

(b) prejudice the fair trial of a person or the impartial adjudication of a particular case or disclose data that is of such a nature that it would be privileged from production in legal proceedings on the ground of legal professional privilege or client legal privilege; or

(c) disclose, or enable a person to ascertain, the identity of a confidential source of information in relation to the enforcement or administration of the law; or

(d) endanger the lives or physical safety of persons engaged in or in connection with law enforcement or persons who have provided confidential information in relation to the enforcement or administration of the law.

S. 109 (Heading) amended by No. 20/2017 s. 106(3).

S. 109 amended by No. 20/2017 s. 106(5).

109 Information Commissioner may copy or take extracts from data

Despite anything to the contrary in any other Act (other than the **Charter of Human Rights and Responsibilities Act 2006**) or law, the Information Commissioner may make copies of, or take extracts from, any data or document accessed under section 106, 107 or 108.

S. 110 amended by No. 20/2017 s. 106(18).

110 Public sector body Heads to provide assistance

The Information Commissioner may request a public sector body Head to provide any assistance that the Information Commissioner reasonably considers appropriate to perform the Information Commissioner's functions under this Act relating to protective data security and law enforcement data security.

111 Reports to the Minister and other reports

S. 111(1) amended by No. 20/2017 s. 106(19).

(1) At the request of the Minister, the Information Commissioner must report to the Minister on any matter relating to the Information Commissioner's information privacy, protective data security, law enforcement data security or crime statistics data security functions.

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

S. 111(3) amended by No. 20/2017 s. 106(19)(a).

(3) The Information Commissioner may publish, in the public interest, reports and recommendations—

S. 111(3)(a) amended by No. 20/2017 s. 106(19)(a).

(a) relating to any act or practice that the Information Commissioner considers to be an interference with the privacy of an individual; or

(b) generally relating to the Information Commissioner's functions under this Act.

S. 111(3)(b) amended by No. 20/2017 s. 106(19)(b).

(4) The Information Commissioner may publish a report under subsection (3) whether or not the matters to be dealt with in the report have been the subject of a report to the Minister.

S. 111(4) amended by No. 20/2017 s. 106(19)(a).

112 Disclosure during course of compliance audit—data security

(1) At any time during the conduct of a compliance audit of a person, agency or body to which Part 4 or 5 applies, the Information Commissioner may give written information to a person or body referred to in subsection (2) concerning any matter that the Information Commissioner considers requires urgent investigation or attention.

S. 112(1) amended by No. 20/2017 s. 106(2).

(2) For the purpose of subsection (1), the following persons and bodies are specified—

(a) the IBAC;

(b) the Victorian Inspectorate;

(c) the Ombudsman;

(d) the Chief Commissioner of Police;

(e) the Director of Public Prosecutions;

(f) a prescribed person or body.

(3) If the Information Commissioner gives information under this section, the Information Commissioner must—

S. 112(3) amended by No. 20/2017 s. 106(2).

(a) notify the Premier and the responsible Minister for the person, agency or body; and

(b) include a statement in the audit report that the Information Commissioner has given information to a person or body under this section during the conduct of the audit.

S. 112(3)(b) amended by No. 20/2017 s. 106(2).

113 Disclosure to the IBAC

S. 113(1) amended by No. 20/2017 s. 106(2).

(1) The Information Commissioner may disclose any information obtained or received in the course or as a result of the exercise of the functions of the Information Commissioner under this Act, if it is information relevant to the performance of functions or duties by the IBAC.

S. 113(2) amended by No. 20/2017 s. 106(2).

(2) The Information Commissioner must notify the relevant public sector body Head of any disclosure made under subsection (1).

Pt 6 Div. 3 (Heading) substituted as Pt 6 Div. 2 (Heading) by No. 20/2017 s. 99.

Division 2—Reporting

S. 114 repealed by No. 20/2017 s. 100.

* * * * *

S. 115 repealed by No. 20/2017 s. 101.

* * * * *

116 Annual reports

S. 116(1) amended by No. 20/2017 s. 106(20).

(1) The Information Commissioner must make a report to the Minister by 30 September in each year on the performance of the Information Commissioner's functions, and the exercise of the Information Commissioner's powers, under this Act during the financial year ending on the immediately preceding 30 June.

(2) The Minister must cause a copy of a report given to the Minister under subsection (1) to be laid before each House of Parliament before 30 October in the year in which the report is given to the Minister.

Part 7—General

117 Protection from liability

(1) A person is not personally liable for any loss, damage or injury suffered by another person by reason only that the person—

(a) produces a document, or gives any information or evidence, to the Information Commissioner under this Act; or

S. 117(1)(a) amended by No. 20/2017 s. 106(2).

(b) gives the Information Commissioner access to any public sector data, law enforcement data or crime statistics data or any public sector organisation's data system, law enforcement data system or crime statistics data system under this Act.

S. 117(1)(b) amended by No. 20/2017 s. 106(2).

(2) A person who lodges a complaint under section 57(1) is not personally liable for any loss, damage or injury suffered by another person by reason only of the lodging of the complaint.

(3) Subsection (4) applies if—

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

(b) either—

(i) the access was required by IPP 6 or an applicable code of practice; or

(ii) the organisation, or an employee or agent of the organisation acting within the scope of the employee's or agent's 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 subsection (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 the information.

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

(a) collecting, holding, managing, 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 28(4).

118 Employees and agents

(1) Any act done or practice engaged in on behalf of an organisation, or a person, agency or body to which Part 4 or 5 applies by an employee or agent of the organisation, person, agency or body acting within the scope of the employee's or agent's 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, person, agency or body and not by the employee or agent unless the organisation, person, agency or body 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, person, agency or body, 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, person, agency or body, acting within the scope of the employee's or agent's actual or apparent authority; and

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

S. 118(3) substituted by No. 60/2014 s. 135.

(3) For the purposes of this section, each of the following is an employee of Victoria Police—

(a) the Chief Commissioner of Police;

(b) a Deputy Commissioner within the meaning of the **Victoria Police Act 2013**;

(c) an Assistant Commissioner within the meaning of the **Victoria Police Act 2013**;

(d) another police officer within the meaning of the **Victoria Police Act 2013**;

(e) a special constable within the meaning of the **Victoria Police Act 2013**;

(f) a police reservist within the meaning of the **Victoria Police Act 2013**;

(g) a protective services officer within the meaning of the **Victoria Police Act 2013**.

119 Fees for access

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

120 Secrecy

S. 120(1) substituted by No. 20/2017 s. 102(1).

(1) This section applies to a person who is or has been—

(a) the Information Commissioner; or

(b) the Privacy and Data Protection Deputy Commissioner; or

(c) an acting Information Commissioner or Privacy and Data Protection Deputy Commissioner; or

(d) a member of staff of the Office of the Victorian Information Commissioner; or

(e) a former Commissioner, acting former Commissioner or an employee of the former Commissioner; or

(f) a person to whom a former secrecy provision applied.

(2) A person to whom this section applies must not, either directly or indirectly, make a record of, disclose or communicate to any person any information about an individual or organisation obtained or received in the course of performing functions or duties or exercising powers under this Act or a former Act except as provided in subsection (3).

S. 120(2) amended by No. 20/2017 s. 102(2).

Penalty: 240 penalty units, or imprisonment for 2 years or both.

(3) A person to whom this section applies may make a record, disclosure or communication referred to in subsection (2) if—

(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 a former Act; or

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

(4) In this section—

former Act means either of the following as in force immediately before its repeal—

S. 120(4) def. of *former Act* amended by No. 20/2017 s. 102(3)(a).

(a) the **Commissioner for Law Enforcement Data Security Act 2005**;

(b) the **Information Privacy Act 2000**;

former Commissioner means a person appointed as Commissioner for Privacy and Data Protection;

S. 120(4) def. of *former Commissioner* inserted by No. 20/2017 s. 102(3)(b).

S. 120(4) def. of *former secrecy provision* inserted by No. 20/2017 s. 102(3)(b).

former secrecy provision means—

(a) section 67 of the **Information Privacy Act 2000**, as in force immediately before its repeal; or

(b) section 15 of the **Commissioner for Law Enforcement Data Security Act 2005** as in force immediately before its repeal.

S. 121 (Heading) amended by No. 20/2017 s. 106(3).

121 Information Commissioner to give notice before certain disclosures

S. 121(1) amended by No. 20/2017 s. 106(21).

(1) Before disclosing or communicating to any person, other than an a member of staff of the Office of the Victorian Information Commissioner, any information given to the Information Commissioner pursuant to a prescribed requirement (including information contained in a document required to be produced to the Information Commissioner), the Information Commissioner must—

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

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

Penalty: 60 penalty units.

(2) In this section, ***prescribed requirement*** means a requirement made under—

(a) Subdivision 3 of Division 8 of Part 3; or

(b) Part 6; or

(c) Division 3 of Part 5 of the **Information Privacy Act 2000** as in force immediately before its repeal.

122 Offence to obstruct, mislead or provide false information

S. 122 substituted by No. 20/2017 s. 103.

(1) A person must not, without reasonable excuse, wilfully obstruct, hinder or resist the Information Commissioner, the Privacy and Data Protection Deputy Commissioner, a delegate of the Information Commissioner or the Privacy and Data Protection Deputy Commissioner or a member of staff of the Office of the Victorian Information Commissioner, in—

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

(b) exercising, or attempting to exercise, a power under this Act.

Penalty: 60 penalty units.

(2) A person must not, without reasonable excuse, provide information or make a statement to the Information Commissioner, the Privacy and Data Protection Deputy Commissioner, a delegate of the Information Commissioner or the Privacy and Data Protection Deputy Commissioner or a member of staff of the Office of the Victorian Information Commissioner knowing that it is false or misleading in a material particular.

Penalty: 60 penalty units.

(3) A person must not, without reasonable excuse, mislead or attempt to mislead the Information Commissioner, the Privacy and Data Protection Deputy Commissioner, a delegate of the Information Commissioner or the Privacy and Data Protection Deputy Commissioner or a member of staff of the Office of the Victorian Information Commissioner.

Penalty: 60 penalty units.

123 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.

124 Prosecutions

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

S. 124(1)(a) substituted by No. 60/2014 s. 136.

(a) a police officer within the meaning of the **Victoria Police Act 2013**; or

S. 124(1)(b) amended by No. 20/2017 s. 106(2).

(b) the Information Commissioner; or

S. 124(1)(c) amended by No. 20/2017 s. 106(2).

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

125 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 subsection (1), the regulations may prescribe fees for providing access to personal information under this Act.

(3) The regulations—

(a) may be of general or limited application; and

(b) may differ according to differences in time, place or circumstances; and

(c) may leave any matter to be determined by the Minister; and

(d) may apply, adopt or incorporate any matter contained in any document, code, standard, rule, specification or method, formulated, issued, prescribed or published by any person whether—

(i) wholly or partially or as amended by the regulations; or

(ii) formulated, issued, prescribed or published at the time the regulations are made or at any time before then; or

(iii) as formulated, issued, prescribed or published from time to time.

Part 8—Repeal of Acts and transitional and savings provisions

126 Repeal of Information Privacy Act 2000

The **Information Privacy Act 2000** is **repealed**.

127 Repeal of Commissioner for Law Enforcement Data Security Act 2005

The **Commissioner for Law Enforcement Data Security Act 2005** is **repealed**.

128 Transitional and savings provisions

Schedule 2 has effect.

New s. 129 inserted by No. 20/2017 s. 104.

129 Transitional provisions—Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017

Schedule 3 has effect.

Pt 9 (Heading and ss 129–141) repealed by No. 60/2014 s. 141.

* * * * *

Schedules

Schedule 1—The Information Privacy Principles

In these Principles—

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

(a) racial or ethnic origin; or

(b) political opinions; or

(c) membership of a political association; or

(d) religious beliefs or affiliations; or

(e) philosophical beliefs; or

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

(g) membership of a trade union; or

(h) sexual preferences or practices; or

(i) criminal record—

that is also personal information;

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 the individual 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 Organisation (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 IPP 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 IPP 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 IPP 2.1(d) to (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 into 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 precontractual measures taken in response to the individual's request; or

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

(e) all of the following apply—

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

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

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

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

Schedule 2—Transitional and savings provisions

1 Definitions

In this Schedule—

commencement day means the day on which Part 8 comes into operation;

Commissioner for Law Enforcement Data Security means the Commissioner for Law Enforcement Data Security appointed under section 5 of the **Commissioner for Law Enforcement Data Security Act 2005** as in force immediately before the commencement day;

former Commissioner means—

(a) the Commissioner for Law Enforcement Data Security; or

(b) the Privacy Commissioner;

old Act means—

(a) the **Commissioner for Law Enforcement Data Security Act 2005**; or

(b) the **Information Privacy Act 2000**;

Privacy Commissioner means the Privacy Commissioner appointed under section 50 of the **Information Privacy Act 2000** as in force immediately before the commencement day.

2 General transitional provisions

(1) This Schedule does not affect or take away from the **Interpretation of Legislation Act 1984**.

(2) If a repealed provision of an old Act continues to apply by force of this Schedule, the following provisions also continue to apply in relation to that provision—

(a) any other repealed provisions of the old Act necessary to give effect to that provision;

(b) any regulations made under the old Act for the purposes of that provision.

(3) Without limiting subclause (1), in declaring that certain provisions of the new Act are to be treated as re-enacting with modifications certain provisions of the **Information Privacy Act 2000**, this Schedule must not be taken to limit the operation of any provision of the **Interpretation of Legislation Act 1984** relating to the re-enactment.

(4) This Schedule applies despite anything to the contrary in any other provision of the new Act.

3 Superseded reference

(1) On and from the commencement day, a reference to an old Act in any Act or in any instrument made under any Act or in any other document of any kind, must be read as a reference to this Act unless the context otherwise requires.

(2) In this clause, a reference to any Act does not include a reference to this Act or a provision of an old Act continued by this Act.

4 Re-enacted provisions—Information Privacy Act 2000

A provision or provisions of the **Information Privacy Act 2000** specified in Column 1 of the Table are taken to be re-enacted (with modifications) by the provision or provisions of this Act appearing opposite in Column 2 of the Table.

Old provision	*New provision*
Section 14(1) and (2)	Section 18
Section 15(2)	Section 19
Section 16(1) and (4)	Section 20
Section 18	Section 21
Section 19	Section 22
Section 20	Section 23
Section 21	Section 24
Section 22	Section 25
Section 23	Section 26
Section 24	Section 27
Section 25	Section 57
Section 26	Section 58
Section 27	Sections 59 and 60
Section 28	Section 61
Section 29 (except subsection (3))	Section 62
Sections 29(3), 34A, 34B, 34C and 34D	Section 63
Section 30	Section 64
Section 31	Section 65
Section 32	Section 66
Section 33	Section 67
Section 34	Section 68

Old provision	*New provision*
Section 35	Section 69
Section 36	Section 70
Section 37	Section 71
Section 38	Section 72
Section 39	Section 73
Section 40	Section 74
Section 41	Section 75
Section 42	Section 76
Section 43	Section 77
Section 44	Section 78
Section 45	Section 79
Section 46	Section 80
Section 47	Section 81
Section 48	Section 82
Section 49	Section 83
Section 64	Section 28
Section 65	Section 122
Section 66	Section 117
Section 68	Section 118
Section 69	Section 119
Schedule 1	Schedule 1

5 Office of Privacy Commissioner abolished

On the commencement day—

(a) the office of the Privacy Commissioner is abolished and the person holding that office and any person acting in that office go out of office; and

(b) all rights, property and assets that, immediately before that day, were vested in the office of the Privacy Commissioner are, by force of this section, vested in the office of the Commissioner; and

(c) all debts, liabilities and obligations of the office of the Privacy Commissioner existing immediately before that day become, by force of this section, debts, liabilities and obligations of the office of the new Commissioner; and

(d) the Commissioner is, by force of this section, substituted as a party to any proceeding pending in any court or tribunal to which the Privacy Commissioner was a party immediately before that day; and

(e) the Commissioner is, by force of this section, substituted as a party to any arrangement or contract entered into by or on behalf of the Privacy Commissioner as a party and in force immediately before that day.

6 Office of Commissioner for Law Enforcement Data Security abolished

On the commencement day—

(a) the office of the Commissioner for Law Enforcement Data Security is abolished and the person holding that office and any person acting in that office go out of office; and

(b) all rights, property and assets that, immediately before that day, were vested in the office of the Commissioner for Law Enforcement Data Security are, by force of this section, vested in the office of the Commissioner; and

(c) all debts, liabilities and obligations of the office of the Commissioner for Law Enforcement Data Security existing immediately before that day become, by force of this section, debts, liabilities and obligations of the office of the Commissioner; and

(d) the Commissioner is, by force of this section, substituted as a party to any proceeding pending in any court or tribunal to which the Commissioner for Law Enforcement Data Security was a party immediately before that day; and

(e) the Commissioner is, by force of this section, substituted as a party to any arrangement or contract entered into by or on behalf of the Commissioner for Law Enforcement Data Security as a party and in force immediately before that day.

7 References to former Commissioner

On the commencement day any reference to a former Commissioner in any Act (other than this Act) or in any rule, regulation, order, agreement, instrument, deed or other document (by whatever named called or however described) must, so far as it relates to any period on or after that day and if not inconsistent with the context or subject-matter, be construed as a reference to the Commissioner.

8 Staff of Privacy Commissioner and Commissioner for Law Enforcement Data Security

On the commencement day, any staff employed under Part 3 of the **Public Administration Act 2004** immediately before the commencement day by a former Commissioner are taken to be

employed by the Commissioner under section 114 of this Act.

9 Offences

On and after the commencement day, the Commissioner may commence or continue a prosecution for an offence committed under the **Information Privacy Act 2000** or the **Commissioner for Law Enforcement Data Security Act 2005**.

10 Annual reports under Information Privacy Act 2000 for reporting periods which end before commencement day

(1) This clause applies if—

(a) a reporting period has ended before the commencement day; and

(b) the Privacy Commissioner has not prepared a report of operations referred to in section 62 of the **Information Privacy Act 2000** for that reporting period before that day.

(2) On and after the commencement day, the Commissioner must, for the reporting period, prepare a report of operations under Part 7 of the **Financial Management Act 1994** which includes the information required by section 62 of the **Information Privacy Act 2000**.

(3) Section 62 of the **Information Privacy Act 2000** applies for the purposes of subclause (2) as if that section had not been repealed.

(4) In this clause—

reporting period means the period commencing on 1 July in any year and ending on 30 June in the following year.

11 Annual reports under Information Privacy Act 2000 for reporting periods that end on or after commencement day

(1) This clause applies if a reporting period ends on or after the commencement day.

(2) On and after the commencement day, the Commissioner must, for the reporting period, prepare a report which includes the information required by section 62 of the **Information Privacy Act 2000** and include that report as part of the Commissioner's first report after the end of the reporting period under section 116.

(3) Section 62 of the **Information Privacy Act 2000** applies for the purposes of subclause (2) as if that section had not been repealed.

(4) In this clause—

reporting period means the period commencing on 1 July in any year and ending on 30 June in the following year.

12 Approved codes of practice

(1) On the commencement day, an approved code of practice under the **Information Privacy Act 2000** that was in operation immediately before that day, is taken to be an approved code of practice under this Act.

(2) On the commencement day, the register of approved codes of practice kept under section 22 of the **Information Privacy Act 2000** is taken to be the register established under section 25 of this Act.

13 Complaints and compliance notices

(1) This Act applies to a complaint made but not declined, referred or finally determined under the **Information Privacy Act 2000** before the commencement day as if the complaint had been made under section 58 of this Act.

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

14 Annual reports under Commissioner for Law Enforcement Data Security Act 2005 for reporting periods which end before commencement day

(1) This clause applies if—

(a) a reporting period has ended before the commencement day; and

(b) the Commissioner for Law Enforcement Data Security has not made a report to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** for that reporting period before that day.

(2) On and after the commencement day, the Commissioner must, for the reporting period, make a report to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005**.

(3) Section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** applies for the purposes of subclause (2) as if that section had not been repealed.

(4) In this clause—

reporting period means the period commencing on 1 July in any year and ending on 30 June in the following year.

15 Annual reports under Commissioner for Law Enforcement Data Security Act 2005 for reporting periods which end on or after commencement day

(1) This clause applies if a reporting period ends on or after the commencement day.

(2) On and after the commencement day, the Commissioner must, for the reporting period, make a report to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** and include that report as part of the Commissioner's first report after the end of the reporting period under section 116.

(3) Section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** applies for the purposes of subclause (2) as if that section had not been repealed.

(4) In this clause—

reporting period means the period commencing on 1 July in any year and ending on 30 June in the following year.

16 Annual reports under Commissioner for Law Enforcement Data Security Act 2005 that have not been laid before Parliament

(1) This clause applies if—

(a) a report has been made to the Minister under section 17 of the **Commissioner for Law Enforcement Data Security Act 2005** before the commencement day; and

(b) that report has not been laid before each House of Parliament in accordance with that section before that day.

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

Schedule 3—Transitional provisions—Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017

Sch. 3 repealed by No. 60/2014 s. 141, new Sch. 3 inserted by No. 20/2017 s. 105.

1 Definition

In this Schedule—

commencement day means the day on which Part 3 of the **Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017** comes into operation.

2 Office of Commissioner for Privacy and Data Protection abolished

On the commencement day—

(a) the office of the Commissioner for Privacy and Data Protection is abolished and the person holding that office and any person acting in that office go out of office; and

(b) all rights, property and assets that, immediately before that day, were vested in the office of the Commissioner for Privacy and Data Protection are, by force of this clause, vested in the Office of the Victorian Information Commissioner; and

(c) all debts, liabilities and obligations of the office of the Commissioner for Privacy and Data Protection existing immediately before that day become, by force of this clause, debts, liabilities and obligations of the Office of the Victorian Information Commissioner; and

(d) the Information Commissioner is, by force of this clause, substituted as a party to any proceeding pending in any court or tribunal

to which the Commissioner for Privacy and Data Protection was a party immediately before that day; and

(e) the Information Commissioner is, by force of this clause, substituted as a party to any arrangement or contract entered into by or on behalf of the Commissioner for Privacy and Data Protection as a party and in force immediately before that day.

3 References to Commissioner for Privacy and Data Protection

On the commencement day any reference to the Commissioner for Privacy and Data Protection in any Act (other than this Act) or in any rule, regulation, order, agreement, instrument, deed or other document (by whatever name called or however described) must, so far as it relates to any period on or after that day and if not inconsistent with the context or subject matter, be construed as a reference to the Information Commissioner, in the Information Commissioner's capacity under this Act.

4 Staff

On the commencement day, any staff employed under Part 3 of the **Public Administration Act 2004** immediately before the commencement day by the Commissioner for Privacy and Data Protection are taken to be employed by the Information Commissioner under section 6Q of the **Freedom of Information Act 1982**.

5 Codes of practice

This Act as in force on and after the commencement day applies to any application to approve a code of practice or amend an approved code of practice that was received but not approved before the commencement day.

6 Public interest determinations

This Act as in force on and after the commencement day applies to any application for a public interest determination or a temporary public interest determination that was received but not determined before the commencement day.

7 Information usage arrangements

This Act as in force on and after the commencement day applies in relation to any application to approve an information usage arrangement or amend an approved information usage arrangement that was received but not approved before the commencement day and anything done under this Act as in force before the commencement day in relation to that application has effect for that purpose.

8 Complaints

This Act as in force immediately before the commencement day continues to apply in relation to any complaint made under Division 8 of Part 3 but not determined before the commencement day as if any reference to the Commissioner for Privacy and Data Protection were a reference to the Information Commissioner.

9 Compliance notices

This Act as in force immediately before the commencement day continues to apply in relation to a written notice given before the commencement day under section 79, as in force immediately before its substitution, as if any reference to the Commissioner for Privacy and Data Protection were a reference to the Information Commissioner.

10 Protective data security standards

The Information Commissioner may amend, revoke or reissue in accordance with section 87 a protective data security standard issued and in force before the commencement day.

11 Law enforcement data security standards

The Information Commissioner may amend, revoke or reissue in accordance with section 92 a law enforcement data security standard issued and in force before the commencement day.

12 Reports for reporting periods which end before commencement day

(1) This clause applies if—

(a) a reporting period has ended before the commencement day; and

(b) the Commissioner for Privacy and Data Protection has not prepared an annual report referred to in section 116 for that reporting period before that day.

(2) On and after the commencement day, the Information Commissioner must prepare an annual report for the reporting period in accordance with section 116.

(3) The annual report may be prepared as a composite report with the report prepared under clause 14 of Schedule 1 to the **Freedom of Information Act 1982**.

(4) In this clause—

reporting period means the period commencing on 1 July in any year and ending on 30 June in the following year.

13 Annual reports for reporting periods which end on or after the commencement day

(1) This clause applies if a reporting period ends on or after the commencement day.

(2) On and after the commencement day, the Information Commissioner must prepare a report in accordance with section 116 for the part of the reporting period occurring before the commencement day and include that report in the Information Commissioner's first report under that section after the end of the reporting period.

(3) In this clause—

reporting period means the period commencing on 1 July in any year and ending on 30 June in the following year.

14 Report to Minister

(1) This clause applies if the Commissioner for Privacy and Data Protection has not prepared a report requested under section 111 before the commencement day.

(2) On and after the commencement day, the Information Commissioner must prepare the report in accordance with section 111 as in force before the commencement day.

Endnotes

1 General information

See www.legislation.vic.gov.au for Victorian Bills, Acts and current authorised versions of legislation and up-to-date legislative information.

Minister's second reading speech—

Legislative Assembly: 12 June 2014

Legislative Council: 7 August 2014

The long title for the Bill for this Act was "A Bill for an Act to provide for responsible collection and handling of personal information in the Victorian public sector, to establish a protective data security regime, to repeal the **Information Privacy Act 2000** and the **Commissioner for Law Enforcement Data Security Act 2005**, to make consequential amendments to other Acts and for other purposes."

The **Privacy and Data Protection Act 2014** was assented to on 2 September 2014 and came into operation as follows:

Sections 129–136 on 3 September 2014: section 2(2); sections 1–128, 138–141 on 17 September 2014: Special Gazette (No. 317) 16 September 2014 page 1; section 137 on 1 July 2015: section 2(3).

INTERPRETATION OF LEGISLATION ACT 1984 (ILA)

Style changes

Section 54A of the ILA authorises the making of the style changes set out in Schedule 1 to that Act.

References to ILA s. 39B

Sidenotes which cite ILA s. 39B refer to section 39B of the ILA which provides that where an undivided section or clause of a Schedule is amended by the insertion of one or more subsections or subclauses, the original section or clause becomes subsection or subclause (1) and is amended by the insertion of the expression "(1)" at the beginning of the original section or clause.

Interpretation

As from 1 January 2001, amendments to section 36 of the ILA have the following effects:

- **Headings**

All headings included in an Act which is passed on or after 1 January 2001 form part of that Act. Any heading inserted in an Act which was passed before 1 January 2001, by an Act passed on or after 1 January 2001, forms part of that Act. This includes headings to Parts, Divisions or Subdivisions in

a Schedule; sections; clauses; items; tables; columns; examples; diagrams; notes or forms. See section 36(1A)(2A).

- **Examples, diagrams or notes**

All examples, diagrams or notes included in an Act which is passed on or after 1 January 2001 form part of that Act. Any examples, diagrams or notes inserted in an Act which was passed before 1 January 2001, by an Act passed on or after 1 January 2001, form part of that Act. See section 36(3A).

- **Punctuation**

All punctuation included in an Act which is passed on or after 1 January 2001 forms part of that Act. Any punctuation inserted in an Act which was passed before 1 January 2001, by an Act passed on or after 1 January 2001, forms part of that Act. See section 36(3B).

- **Provision numbers**

All provision numbers included in an Act form part of that Act, whether inserted in the Act before, on or after 1 January 2001. Provision numbers include section numbers, subsection numbers, paragraphs and subparagraphs. See section 36(3C).

- **Location of "legislative items"**

A "legislative item" is a penalty, an example or a note. As from 13 October 2004, a legislative item relating to a provision of an Act is taken to be at the foot of that provision even if it is preceded or followed by another legislative item that relates to that provision. For example, if a penalty at the foot of a provision is followed by a note, both of these legislative items will be regarded as being at the foot of that provision. See section 36B.

- **Other material**

Any explanatory memorandum, table of provisions, endnotes, index and other material printed after the Endnotes does not form part of an Act. See section 36(3)(3D)(3E).

2 Table of Amendments

This publication incorporates amendments made to the **Privacy and Data Protection Act 2014** by Acts and subordinate instruments.

Privacy and Data Protection Act 2014, No. 60/2014[6]

Assent Date: 2.9.14
Commencement Date: Ss 129–136 on 3.9.14: s. 2(2); s. 137 on 1.7.15: s. 2(3)
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Privacy and Data Protection Act 2014, No. 60/2014

Assent Date: 2.9.14
Commencement Date: S. 141 on 17.9.14: Special Gazette (No. 317) 16.9.14 p. 1
Note: S. 141 repeals Pt 9 (ss 129–141) and Schedule 3 on 9.12.15
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Inquiries Act 2014, No. 67/2014

Assent Date: 23.9.14
Commencement Date: S. 147(Sch. 2 item 28) on 15.10.14: Special Gazette (No. 364) 14.10.14 p. 2
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Statute Law Revision Act 2015, No. 21/2015

Assent Date: 16.6.15
Commencement Date: S. 3(Sch. 1 item 41) on 1.8.15: s. 2(1)
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Health Complaints Act 2016, No. 22/2016

Assent Date: 3.5.16
Commencement Date: S. 240 on 1.2.17: s. 2(2)
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Powers of Attorney Amendment Act 2016, No. 64/2016

Assent Date: 15.11.16
Commencement Date: S. 16 on 1.5.17: s. 2(2)
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017, No. 20/2017

Assent Date: 16.5.17
Commencement Date: Ss 78–106 on 1.9.17: s. 2(3)
Current State: This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

---

3 Amendments Not in Operation

This publication does not include amendments made to the **Privacy and Data Protection Act 2014** by the following Act/s.

Fines Reform and Infringements Acts Amendment Act 2016, No. 29/2016

Assent Date:	31.5.16
Commencement Date:	S. 111 not yet proclaimed
Current State:	This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Medical Treatment Planning and Decisions Act 2016, No. 69/2016

Assent Date:	29.11.16
Commencement Date:	S. 158 not yet proclaimed
Current State:	This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

Family Violence Protection Amendment (Information Sharing) Act 2017, No. 23/2017

Assent Date:	14.6.17
Commencement Date:	Ss 20–22 not yet proclaimed
Current State:	This information relates only to the provision/s amending the **Privacy and Data Protection Act 2014**

At the date of this publication, the following provisions amending the **Privacy and Data Protection Act 2014** were Not in Operation:

Amending Act/s:

Fines Reform and Infringements Acts Amendment Act 2016, No. 29/2016

111 Definitions

In section 3 of the **Privacy and Data Protection Act 2014**, in the definition of ***law enforcement agency*** after paragraph (e) **insert**—

"(ea) the Director, Fines Victoria employed under section 4 of the **Fines Reform Act 2014**;".

___

Medical Treatment Planning and Decisions Act 2016, No. 69/2016

158 Privacy and Data Protection Act 2014

In section 28(6) of the **Privacy and Data Protection Act 2014**, in the definition of ***authorised representative***—

(a) in paragraph (a), for subparagraph (iii) **substitute**—

"(iii) a medical treatment decision maker for the individual within the meaning of the **Medical Treatment Planning and Decisions Act 2016**; or

(iiia) a support person for the individual within the meaning of the **Medical Treatment Planning and Decisions Act 2016**; or";

(b) in paragraph (a)(iv), **omit** "or a person responsible".

——

Family Violence Protection Amendment (Information Sharing) Act 2017, No. 23/2017

20 New section 15A inserted

After section 15 of the **Privacy and Data Protection Act 2014 insert**—

"**15A Exemption—information sharing under the Family Violence Protection Act 2008**

(1) Nothing in IPP 1.4 or 1.5, or any applicable code of practice modifying the application of IPP 1.4 or 1.5 or prescribing how IPP 1.4 or 1.5 is to be applied or complied with, applies to the collection of personal information by an information sharing entity for the purposes of Part 5A of the **Family Violence Protection Act 2008**

about a person of concern, or a person who is alleged to pose a risk of committing family violence.

(2) Nothing in IPP 10.1, or any applicable code of practice modifying the application of IPP 10.1 or prescribing how IPP 10.1 is to be applied or complied with, applies to the collection of sensitive information by an information sharing entity for the purposes of Part 5A of the **Family Violence Protection Act 2008** about a person of concern, or a person who is alleged to pose a risk of committing family violence.

(3) Nothing in IPP 10.1, or any applicable code of practice modifying the application of IPP 10.1 or prescribing how IPP 10.1 is to be applied or complied with, applies to the collection of sensitive information about a primary person or a linked person by an information sharing entity for—

(a) a family violence protection purpose relating to a primary person who is a child; or

(b) a family violence assessment purpose relating to a primary person who is a child.

(4) Nothing in IPP 1.4 or 1.5, or any applicable code of practice modifying the application of IPP 1.4 or 1.5 or prescribing how IPP 1.4 or 1.5 is to be applied or complied with, applies to the collection of personal information about an individual by the Central Information Point for the purposes of Part 5A of the **Family Violence Protection Act 2008**.

(5) 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 personal information about an individual held by the Central Information Point for the purposes of Part 5A of the **Family Violence Protection Act 2008**.

(6) Nothing in IPP 10.1, or any applicable code of practice modifying the application of IPP 10.1 or prescribing how IPP 10.1 is to be applied or complied with, applies to the collection of sensitive information about an individual by the Central Information Point for the purposes of Part 5A of the **Family Violence Protection Act 2008**.

(7) In this section—

Central Information Point has the meaning given in section 144O of the **Family Violence Protection Act 2008**;

family violence has the meaning given in the **Family Violence Protection Act 2008**;

family violence assessment purpose has the meaning given in section 144A of the **Family Violence Protection Act 2008**;

family violence protection purpose has the meaning given in section 144A of the **Family Violence Protection Act 2008**;

information sharing entity has the meaning given in the **Family Violence Protection Act 2008**;

linked person has the meaning given in section 144A of the **Family Violence Protection Act 2008**;

person of concern has the meaning given in section 144B of the **Family Violence Protection Act 2008**;

primary person has the meaning given in section 144E of the **Family Violence Protection Act 2008**.".

21 Information Privacy Principles

In section 18(2) of the **Privacy and Data Protection Act 2014**, for "section 14 or 15" **substitute** "section 14, 15 or 15A".

22 Amendment of Schedule 1—The Information Privacy Principles

(1) In clause 2.1(d)(i) of Schedule 1 to the **Privacy and Data Protection Act 2014 omit** "and imminent".

(2) In clause 6.1(a) of Schedule 1 to the **Privacy and Data Protection Act 2014 omit** "and imminent".

(3) In clause 10.1(c) of Schedule 1 to the **Privacy and Data Protection Act 2014 omit** "and imminent".

4 Explanatory details

[1] S. 31: The amendments proposed by section 106(7)(b) of the **Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017**, No. 20/2017 are not included in this publication because the words "Internet site of the Commissioner" do not appear in sections 31, 39 and 50.

Section 106(7)(b) reads as follows:

> **106 Amendment of references to Commissioner for Privacy and Data Protection**
>
> (7) In sections 31, 39 and 50 of the **Privacy and Data Protection Act 2014**—
>
> (b) for "Internet site of the Commissioner" **substitute** "Internet site of the Office of the Victorian Information Commissioner".

[2] S. 39: See note 1.

[3] S. 50: See note 1.

[4] S. 57(4): The amendment proposed by section 106(12)(b) of the **Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017**, No. 20/2017 is not included in this publication because the words "employees in the office of the Commissioner" do not appear in section 57(4).

Section 106(12)(b) reads as follows:

> **106 Amendment of references to Commissioner for Privacy and Data Protection**
>
> (12) In section 57 of the **Privacy and Data Protection Act 2014**—
>
> (b) in subsection (4), for "employees in the office of the Commissioner" **substitute** "members of staff of the Office of the Victorian Information Commissioner".

[5] S. 62: The amendment proposed by section 106(13)(c) of the **Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017**, No. 20/2017 is not included in this publication because the words "an employee in the office of the Commissioner" do not appear in section 62.

Section 106(13)(c) reads as follows:

106 Amendment of references to Commissioner for Privacy and Data Protection

(13) In section 62 of the **Privacy and Data Protection Act 2014**—

(c) for "an employee in the office of the Commissioner" **substitute** "a member of staff of the Office of the Victorian Information Commissioner".

[6] Table of Amendments: The amendments proposed by sections 130 and 131 of the **Privacy and Data Protection Act 2014**, No. 60/2014 are not included in this publication, as there is no paragraph (i) in section 14(1) and the words "the police force of Victoria" do not appear in section 16(d).

Sections 130 and 131 read as follows:

130 Organisations to which this Part applies

For section 14(1)(i) **substitute**—

"(i) Victoria Police;".

131 Exemption—law enforcement

In section 16(d), for "the police force of Victoria" **substitute** "Victoria Police".