

SCHEDULE 2

Section 65(1)

INFORMATION PRIVACY PRINCIPLES

IPP 1 Collection

- 1.1 A public sector organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 A public sector 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) a public sector 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;
 - (b) the fact that the individual is able to have access to the information;
 - (c) the purpose for which the information is collected;
 - (d) the persons or bodies, or classes of persons or bodies, to which the organisation usually discloses information of the same kind;
 - (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, a public sector organisation must collect personal information about an individual only from the individual.
- 1.5 If a public sector organisation collects personal information about an individual from another person, 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 the individual or another individual.

IPP 2 Use and disclosure

- 2.1 A public sector organisation must not use or disclose personal information about an individual for a purpose ("the secondary purpose") other than the primary purpose for collecting it unless one or more of the following apply:
 - (a) if the information is sensitive information –

- (i) the secondary purpose is directly related to the primary purpose; and
 - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
- (b) if the information is not sensitive information –
 - (i) the secondary purpose is related to the primary purpose; and
 - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
- (c) the individual consents to the use or disclosure of the information;
- (d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent –
 - (i) a serious and imminent threat to the individual's or another individual's life, health or safety; or
 - (ii) a serious threat to public health or public safety;
- (e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in and uses or discloses the information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;
- (f) the use or disclosure is required or authorised by law;
- (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) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
 - (ii) enforcing a law relating to the confiscation of proceeds of crime;
 - (iii) protecting public revenue;
 - (iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
 - (v) preparing for or conducting proceedings before a court or tribunal or implementing the orders of a court or tribunal;
- (h) the Australian Security Intelligence Organisation ("ASIO") has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIO authorised by the Director-General of ASIO

to receive the information and an officer or employee of ASIO authorised by the Director-General of ASIO to do so has certified in writing that the information is required in connection with the performance of the functions of ASIO;

- (i) the Australian Secret Intelligence Service ("ASIS") has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIS authorised by the Director-General of ASIS to receive the information and an officer or employee of ASIS authorised by the Director-General of ASIS to do so has certified in writing that the information is required in connection with the performance of the functions of ASIS.

Note 1: It is not intended to deter public sector organisations from lawfully co-operating with law enforcement agencies in the performance of their functions.

Note 2: IPP 2.1 does not override any existing legal obligations not to disclose personal information. IPP 2.1 does not require a public sector organisation to disclose personal information – a public sector organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: A public sector organisation is also liable to the requirements of IPP 9 if it transfers personal information to a person outside the Territory.

- 2.2 If a public sector organisation uses or discloses personal information under IPP 2.1(g), the organisation must make a written note of the use or disclosure.

IPP 3 Data quality

- 3.1 A public sector organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

IPP 4 Data security

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

IPP 5 Openness

- 5.1 A public sector organisation must make available to the public a document in which it clearly expresses its policies for the management of personal information that it holds.
- 5.2 On the request of an individual, a public sector organisation must take reasonable steps to inform the individual of the kind of personal information it holds, why it holds the information and how it collects, holds, uses and discloses the information.

IPP 6 Access and correction

- 6.1 If an individual requests a public sector organisation holding personal information about the individual for access to the personal information, the organisation must provide the individual with access to the information except to the extent that –
- (a) providing access would pose a serious threat to the life or health of the individual or another individual;
 - (b) providing access would prejudice measures for the protection of the health or safety of the public;
 - (c) providing access would unreasonably interfere with the privacy of another individual;
 - (d) the request for access is frivolous or vexatious;
 - (e) the information relates to existing or anticipated 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;
 - (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way that would prejudice the negotiations;
 - (g) providing access would be unlawful;
 - (h) denying access is required or authorised by law;
 - (i) providing access would be likely to prejudice an investigation of possible unlawful activity;

- (j) providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:
 - (i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
 - (ii) enforcing a law relating to the confiscation of proceeds of crime;
 - (iii) protecting public revenue;
 - (iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
 - (v) preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or
- (k) providing access would prejudice –
 - (i) the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or
 - (ii) the maintenance of law and order in the Territory.

6.2 However, where providing access under IPP 6.1 would reveal evaluative information generated within a public sector 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 access to the decision.

6.3 If a public sector organisation holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.4 If –

- (a) an individual and a public sector organisation disagree about whether personal information about the individual held by the organisation is accurate, complete or up to date; and
- (b) the individual requests the organisation to associate with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date,

the organisation must take reasonable steps to comply with that request.

6.5 A public sector organisation must provide reasons for refusing to provide access to or correct personal information.

- 6.6 If a public sector organisation charges a fee for providing access to personal information, the fee is not to be excessive.
- 6.7 If an individual requests a public sector organisation for access to or to correct personal information held by the organisation, the organisation must –
- (a) provide access or reasons for refusing access;
 - (b) make the correction or provide reasons for refusing to make it; or
 - (c) provide reasons for the delay in responding to the request,
- within a reasonable time.

IPP 7 Identifiers

- 7.1 A public sector organisation must not assign unique identifiers to individuals unless it is necessary to enable the organisation to perform its functions efficiently.
- 7.2 A public sector organisation must not adopt a unique identifier of an individual that has been assigned by another public sector organisation unless –
- (a) it is necessary to enable the organisation to perform its functions efficiently;
 - (b) it has obtained the consent of the individual to do so; or
 - (c) it is an outsourcing organisation adopting the unique identifier created by a contract service provider in the performance of its obligations to the outsourcing organisation under a service contract.
- 7.3 A public sector organisation must not use or disclose a unique identifier assigned to an individual by another public sector organisation unless –
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to that other organisation;
 - (b) IPP 2.1(d), (e), (f) or (g) applies to the use or disclosure; or
 - (c) it has obtained the consent of the individual to the use or disclosure.

- 7.4 A public sector organisation must not require an individual to provide a unique identifier in order to obtain a service unless its provision –
- (a) is required or authorised by law; or
 - (b) is in connection with the purpose for which the unique identifier was assigned or for a directly related purpose.

IPP 8 Anonymity

- 8.1 A public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.

IPP 9 Transborder data flows

- 9.1 A public sector organisation must not transfer personal information about an individual to a person (other than the individual) outside the Territory unless –
- (a) the transfer is required or authorised under a law of the Territory or the Commonwealth;
 - (b) the organisation reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to these IPPs;
 - (c) the individual consents to the transfer;
 - (d) the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request;
 - (e) the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual;
 - (f) 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 the transfer;
 - (iii) it is likely that the individual would consent to the transfer; or
 - (g) the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred in a manner that is inconsistent with these IPPs.

IPP 10 Sensitive information

10.1 A public sector organisation must not collect sensitive information about an individual unless –

- (a) the individual consents to the collection;
- (b) the organisation is required by law to collect the information;
- (c) the individual is –
 - (i) physically or legally incapable of giving consent to the collection;
or
 - (ii) physically unable to communicate his or her consent to the collection,

and collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or

- (d) collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

10.2 Despite IPP 10.1, a public sector 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 for the purpose of providing government funded targeted welfare or educational services;
- (b) there is no other 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.