Office of the Information Commissioner

Information Privacy Principles

The *Privacy and Responsible Information Sharing Act 2024* (WA) (**PRIS Act**), outlines 11 Information Privacy Principles **(IPPs**) in Schedule 1 to the PRIS Act. These are reproduced in this document. The official version is found in the Schedule.

The IPPs cover collection, use, disclosure, quality, security, openness and transparency, access and correction, unique identifiers, anonymity, disclosures outside Australia and automated decision-making in the context of personal information. They also regulate de-identified information in relation to security and disclosures outside of Australia.

The IPPs have not yet commenced. **The Government has stated that they will commence on 1 July 2026.**

Contents

PRINCIPLE 1: Collection

1.1. An IPP entity must not collect personal information (other than sensitive personal information) unless the information is necessary for 1 or more of the IPP entity's functions or activities.

1.2. An IPP entity must not collect sensitive personal information that relates to an individual unless the information is necessary for 1 or more of the IPP entity's functions or activities and —

(a) the individual consents to the collection of the information; or

(b) the collection of the information is required or authorised by or under law; or

(c) both of the following apply —

(i) the collection of the information is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual, or a threat to the life, health, safety or welfare of any individual due to family violence;

(ii) the individual to whom the information relates is incapable under section 154(4) of giving consent to the collection;

or

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

(e) the collection of the information is permitted under subclause 1.3.

1.3. or the purposes of subclause 1.2(e), collecting sensitive personal information is permitted 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 IPP entity to seek the individual's consent to the collection.

1.4. An IPP entity must not collect personal information that relates to an individual unless the collection is fair and reasonable in the circumstances, taking into account the following matters —

(a) whether the individual would reasonably expect the information to be collected in the circumstances;

(b) the kind of personal information collected, including whether any of that information is sensitive personal information;

(c) the amount of personal information collected;

(d) whether the collection of the information is necessary for 1 or more of the IPP entity's functions or activities;

(e) whether there is a risk of loss, harm or other detriment to any individual as a result of the collection of the information;

(f) whether the collection of the information for 1 or more of the IPP entity's functions or activities is, on balance, in the public interest;

(g) in the case of personal information that relates to a child — whether the collection of the information is in the best interests of the child;

(h) the objects of this Act.

1.5. Subclause 1.4 does not apply to the collection of personal information if —

(a) the collection is required or authorised by or under law; or

(b) the IPP entity reasonably believes that the collection is necessary to prevent or lessen —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a threat to the life, health, safety or welfare of any individual due to family violence;

or

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

1.6. An IPP entity must not collect personal information in an unreasonably intrusive way.

1.7. Before collecting personal information, an IPP entity must make a written record of the purposes for which the information will be collected and used or disclosed.

1.8. An IPP entity must collect personal information that relates to an individual only from the individual unless —

(a) the individual consents to the collection of the information from someone other than the individual; or

(b) the collection of the information is required or authorised by or under law; or

(c) it is unreasonable or impracticable to do so.

1.9. At or before the time (or, if that is not practicable, as soon as practicable after) an IPP entity collects personal information that relates to an individual from the individual, it must take such steps (if any) as are reasonable in the circumstances

to ensure that the individual is given, or made aware of, the following information —

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

(b) how the individual may access the information (if applicable);

(c) the purposes for which the information is collected and will be used or disclosed;

(d) whether the IPP entity usually discloses information of that kind and, if so, the persons or bodies or kinds of persons or bodies to which the information is usually disclosed;

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

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

1.10. If an IPP entity collects personal information that relates to an individual from someone other than the individual, the IPP entity must take such steps (if any) as are reasonable in the circumstances —

(a) to satisfy itself that the information was not originally collected from the individual in contravention of this clause; and

(b) to ensure that the individual is given, or made aware of, the information referred to in subclause 1.9(a) to (f), except to the extent that giving or making the individual aware of that information would pose —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a threat to the life, health, safety or welfare of any individual due to family violence.

1.11. If an IPP entity collects personal information that relates to an individual from someone other than the individual in connection with a complaint made about the individual, the IPP entity is not required to comply with subclause 1.10 in relation to the collection of the information unless the IPP entity contacts the individual about the complaint.

1.12. An IPP entity must ensure that the information that an individual is given, or made aware of, under subclause 1.9 or 1.10(b) is up-to-date, clear, concise and expressed in plain language.

PRINCIPLE 2: Use and disclosure

2.1 If an IPP entity holds personal information that relates to an individual that was collected to be used or disclosed for a particular purpose (the ***primary purpose***), the IPP entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless —

(a) the individual would reasonably expect the IPP entity to use or disclose the information for the secondary purpose and the secondary purpose is —

(i) if the information is not sensitive personal information — related to the primary purpose; or

(ii) if the information is sensitive personal information — directly related to the primary purpose;

or

(b) the individual consents to the use or disclosure; or

(c) all of the following apply —

(i) the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) the research or statistics are not to be published in a form that identifies any particular individual;

(iii) it is impracticable for the IPP entity to seek the individual's consent before the use or disclosure or, in the case of disclosure, the IPP entity reasonably believes that the recipient of the information will not further disclose the information;

or

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

(i) a serious threat to the life, health, safety or welfare of any individual; or

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

(iii) a threat to the life, health, safety or welfare of any individual due to family violence;

or

(e) the IPP entity 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 the matter to relevant persons or authorities; or

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

(g) the IPP entity reasonably believes that the use or disclosure is necessary for —

(i) a law enforcement function to be performed by a law enforcement agency; or

(ii) proceedings before a court or tribunal.

2.2 An IPP entity must not use or disclose personal information unless the use or disclosure is fair and reasonable in the circumstances, taking into account the following matters —

(a) whether the individual would reasonably expect the information to be used or disclosed in the circumstances;

(b) the kind of personal information used or disclosed, including whether any of that information is sensitive personal information;

(c) the amount of personal information used or disclosed;

(d) whether the use or disclosure is necessary for 1 or more of the IPP entity's functions or activities;

(e) whether there is a risk of loss, harm or other detriment to any individual as a result of the use or disclosure of the information;

(f) whether the disclosure or use of the information for 1 or more of the IPP entity's functions or activities is, on balance, in the public interest;

(g) in the case of personal information that relates to a child — whether the use or disclosure of the information is in the best interests of the child;

(h) the objects of this Act.

2.3 Subclause 2.2 does not apply to the use or disclosure of personal information if —

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

(b) the IPP entity reasonably believes that the use or disclosure is necessary to prevent or lessen —

(i) a serious threat to the life, health, safety or welfare of any individual; or

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

(iii) a threat to the life, health, safety or welfare of any individual due to family violence;

or

(c) the IPP entity 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 the matter to relevant persons or authorities; or

(d) the IPP entity reasonably believes that the use or disclosure is necessary for —

(i) a law enforcement function to be performed by a law enforcement agency; or

(ii) proceedings before a court or tribunal.

2.4 Before using or disclosing personal information for a secondary purpose, the IPP entity must make a written record of the secondary purpose.

2.5 If an IPP entity uses or discloses personal information in a manner permitted by subclause 2.1(g) or 2.3(d), the IPP entity must make a written record of the use or disclosure.

2.6 For the purposes of this clause, a disclosure of information that is covered by an express exception from a secrecy provision in a written law is taken to be authorised by law.

PRINCIPLE 3: Information quality

3 An IPP entity must take such steps (if any) as are reasonable in the circumstances to ensure that personal information it collects, uses or discloses is accurate, complete and up-to-date.

PRINCIPLE 4: Information security

4.1 An IPP entity 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 IPP entity must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which it may be used or disclosed under this Schedule, unless the IPP entity is expressly required or authorised to retain the information by or under another law.

PRINCIPLE 5: Openness and transparency

5.1 An IPP entity must develop a document setting out policies on its handling of personal information and must make the document available to anyone who requests it.

5.2 A document referred to in subclause 5.1 must be up-to-date, clear, concise and expressed in plain language.

5.3 On request by a person, an IPP entity must take reasonable steps to let the person know, generally —

(a) the kinds of personal information that the IPP entity collects and holds; and

(b) how the IPP entity handles personal information; and

(c) the purposes for which the IPP entity handles personal information; and

(d) whether any personal information held by the IPP entity is used for an automated decision-making process.

PRINCIPLE 6: Access and correction

6.1 If an IPP entity holds personal information that relates to an individual, it must provide the individual with access to the information on a request made by the individual in accordance with section 40, except to the extent that —

(a) providing access would endanger the life or physical safety of any person; or

(b) there are reasonable grounds to believe that —

(i) the person requesting access is a perpetrator, or alleged perpetrator of family violence; and

(ii) denying access is necessary to prevent or lessen a threat to the life, health, safety or welfare of any individual due to family violence;

or

(c) providing access would enable the existence, non-existence or identity of any confidential source of information in relation to the enforcement or administration of the law to be discovered; or

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

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

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

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

(h) providing access would be unlawful; or

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

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

(k) providing access would be likely to prejudice any of the law enforcement functions of a law enforcement agency; or

(l) providing access would be likely to reveal evaluative information generated within the IPP entity about a commercially sensitive decision-making process.

6.2 If the IPP entity denies access to the personal information because of subclause 6.1(l), the IPP entity may include in the reasons for the denial of access referred to in subclause 6.7 an explanation for the commercially sensitive decision.

6.3 If an IPP entity is not required to provide an individual with access to information because of any of subclause 6.1(a) to (l), the IPP entity 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 a fee for making a request for access to personal information applies under regulations made for the purposes of section 40(2)(e), the IPP entity may refuse access to the personal information until the fee is paid.

6.5 If an individual makes a request to an IPP entity in accordance with section 41 for the correction of personal information that relates to the individual, and the individual establishes that the information is not accurate, complete and up-to-date, the IPP entity 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 IPP entity disagree about whether the information is accurate, complete and up-to-date, and the individual requests the IPP entity to associate with the information a statement claiming that the information is not

accurate, complete or up-to-date, the IPP entity must take reasonable steps to do so.

6.7 An IPP entity must provide reasons for a denial of access to, or a refusal of a request for the correction of, personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an IPP entity, the IPP entity must, as soon as practicable, but no later than 45 days after the day on which the request is made —

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

(b) correct the information or provide reasons for the refusal of the request for the correction of the information; or

(c) provide reasons for the delay in responding to the request.

PRINCIPLE 7: Unique identifiers

7.1 An IPP entity must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the IPP entity to perform any of its functions or activities efficiently.

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

(a) the adoption of the unique identifier is necessary to enable the IPP entity to perform any of its functions efficiently; or

(b) the individual consents to the use of the unique identifier; or

(c) the IPP entity is an outsourcing entity under a State services contract and is adopting the unique identifier assigned by a contracted service provider in the provision of services under the contract; or

(d) the IPP entity is a contracted service provider under a State services contract and is adopting the unique identifier assigned by the relevant outsourcing entity.

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

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

(b) circumstances referred to in IPP 2.1(c), (e), (f) or (g) apply to the use or disclosure; or

(c) the individual consents to the use or disclosure.

7.4 An IPP entity must not require an individual to provide a unique identifier in order to obtain a service unless —

(a) the provision of the identifier is required or authorised by or under law; or

(b) the provision is in connection with the purpose for which the identifier was assigned or a directly related purpose.

PRINCIPLE 8: Anonymity

8.1 Individuals must have the option of not identifying themselves when dealing with an IPP entity.

8.2 Subclause 8.1 does not apply to an IPP entity in relation to a matter if —

(a) the IPP entity is required or authorised by or under law to deal with individuals who have identified themselves in relation to that matter; or

(b) it is impracticable for the IPP entity to deal with individuals who have not identified themselves in relation to that matter.

PRINCIPLE 9: Disclosures outside Australia

9.1 An IPP entity must not disclose personal information that relates to an individual to a person (other than the individual) outside Australia unless —

(a) the IPP entity reasonably believes that the person to whom the information is disclosed is subject to a law, binding administrative scheme, or contract, that requires the person to comply with principles for handling the information that are substantially similar to the information privacy principles; or

(b) the individual consents to the disclosure; or

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

(d) the disclosure is necessary for the performance of a contract between the individual and the IPP entity or for the implementation of pre-contractual measures taken in response to the individual's request; or

(e) the disclosure is necessary for the conclusion or performance of a contract that is concluded in the interest of the individual between the IPP entity and a third party; or

(f) all of the following apply —

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

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

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

or

(g) the IPP entity has taken reasonable steps to ensure that the information will not be held, used or disclosed by the recipient inconsistently with the information privacy principles.

9.2 An IPP entity must not disclose de-identified information that relates to an individual to a person (other than the individual) outside Australia unless the IPP entity takes reasonable steps to ensure that the person to whom the de-identified information is disclosed —

(a) protects the de-identified information from misuse and loss and from unauthorised re-identification, access, modification or disclosure; and

(b) does not —

(i) re-identify the de-identified information (except in circumstances referred to in IPP 11.2(c) or (d)); or

(ii) further disclose the information in a manner that is likely to undermine the effectiveness of the de-identification of the information.

PRINCIPLE 10: Automated decision-making

10.1 An IPP entity that employs an automated decision-making process involving the use of personal information in making significant decisions about individuals must —

(a) conduct an assessment of the impact of the automated decision-making process on those individuals, having regard to —

(i) the elimination or minimisation of harm, bias and discrimination; and

(ii) whether there is a process by which individuals about whom decisions are made can request human intervention; and

(iii) whether the handling of personal information in the process complies with any applicable requirements under this Act;

and

b) periodically evaluate the operation and effectiveness of the automated decision-making process; and

(c) reassess the matter referred to in paragraph (a) when changes are made to the automated decision-making process.

10.2 If an IPP entity employs an automated decision-making process involving the use of personal information in making a significant decision about an individual, the IPP entity must —

(a) notify the individual that an automated decision-making process has been employed in making the decision; and

(b) on request, give the individual information about how the automated decision-making process is employed in making decisions; and

(c) provide a process by which the individual can request human intervention in relation to the decision.

10.3 A notification under subclause 10.2(a) —

(a) may be given with, or as part of, any notification of the significant decision required to be given under a written law; and

(b) subject to paragraph (a), must be given as soon as practicable.

10.4 Information provided under subclause 10.2(b) must be reasonably comprehensive and provided in a form that is capable of being understood by a person without specialist knowledge.

PRINCIPLE 11: De-identified information

11.1 An IPP entity must take reasonable steps to protect the de-identified information it holds from misuse and loss and from unauthorised re-identification, access, modification or disclosure.

11.2 An IPP entity must not re-identify de-identified information that it holds unless —

(a) the de-identified information was de-identified by the IPP entity itself; or

(b) all of the following apply —

(i) the de-identified information was collected from another IPP entity;

(ii) that other IPP entity has given written authorisation for the IPP entity to re-identify the de-identified information for a specified purpose;

(iii) the re-identification is undertaken for the specified purpose;

or

(c) the re-identification is undertaken to test the effectiveness of de-identification processes or security measures protecting information; or

(d) the re-identification is required or authorised by or under law.