Office of the Information Commissioner

# Information Privacy Principles – Summary

The Information Privacy Principles (**IPPs**) outline how IPP entities must handle personal information and in some instances, de-identified information. This summary provides an overview of the IPPs and the exceptions to the IPPs. The full IPPs are in Schedule 1 of the *Privacy and Responsible Information Sharing Act 2024* (WA) (**PRIS Act**). The IPPs are reproduced in our Information Privacy Principles PDF.

## Key terms:

IPP entities

IPP entities are Western Australian government agencies, departments, statutory authorities, Local Governments, Ministers, Parliamentary Secretaries, government trading enterprises, and some contracted service providers to government.

Personal information

Personal information includes name, date of birth, address, contact information, location information, unique identifiers (e.g. drivers licence number or IP address), information that relates to someone's features or behaviour. It can include personal information about a deceased person and inferences made about people. This list is not exhaustive.

Sensitive personal information

Sensitive personal information includes information that relates to an individual's racial or ethnic origin, gender identity, sexual orientation, political opinions, religious beliefs, trade union membership, or criminal record. It also includes health, genetic or genomic and biometric information. This list is not exhaustive.

De-identified information

De-identified information is information that has been changed or had information removed so that an individual can no longer be identified from it.

Disclosure

Disclosure is sharing personal information outside the IPP entity.

# Information Privacy Principles

**1. Collection**

An IPP entity must not collect unnecessary personal information. Any personal information collected must be necessary for the functions or activities of the IPP entity.

An IPP entity must collect personal information fairly and reasonably. This includes considering the amount of information collected, its sensitivity, whether an individual would expect it to be collected and any harm or loss to any individual because of the collection.

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

An IPP entity must only collect sensitive personal information in certain circumstances, for example when required by law or if an individual consents to the collection.

Before personal information is collected, an IPP entity must document why it is being collected and how it will be used or disclosed.

When an IPP entity collects personal information from an individual, it must tell them the reason for its collection, and its use or disclosure, how the IPP entity can be contacted, amongst other details. This information must be clear, concise and up to date.

**2. Use and disclosure**

An IPP entity must only use and disclose personal information for the reason it was collected. This is called the primary purpose.

An IPP entity may only use or disclose personal information for another purpose in certain circumstances. This is called the secondary purpose.

The circumstances where an IPP entity may use or disclose personal information for a secondary purpose include if an individual consents, the law allows it, to prevent a serious threat of harm to an individual or the public, or if it is necessary for law enforcement or court proceedings.

An IPP entity must use or disclose personal information fairly and reasonably. This includes considering the amount of information used or disclosed, its sensitivity, whether an individual would expect it to be used or disclosed, and any harm or loss to any individual because of the use or disclosure.

Before personal information is used or disclosed for a secondary purpose, an IPP entity must document that purpose.

**3. Information quality**

An IPP entity must take reasonable steps to make sure the personal information collected, used or disclosed is correct, complete, and up to date.

**4. Information security**

An IPP entity must take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, modification, or disclosure.

An IPP entity must take reasonable steps to destroy, or permanently de-identify personal information when it is no longer needed, unless a law requires the IPP entity to keep it.

**5. Openness and transparency**

An IPP entity must have a publicly available privacy policy that sets out what personal information it collects and holds, and how and why it handles personal information. The privacy policy must also include whether any personal information is used in automated decision-making.

Importantly, the policy must be up-to-date, clear, concise and expressed in plain language.

**6. Access and correction**

An individual can request access to personal information that an IPP entity holds about them. An individual can also request an IPP entity correct the personal information it holds about them if it is not accurate, complete or up to date.

An IPP entity must make a decision about the request for access or correction as soon as practicable, but no later than 45 days after the request was made. If the IPP entity refuses to give access or correct the personal information, it must give an individual valid reasons.

Note: IPP 6 applies only to IPP entities who are contracted service providers to government. Refer to the information below about the exceptions to the IPPs.

The right to access or correct personal information in government documents held by IPP entities that are not contracted service providers is under the *Freedom of Information Act 1992* (WA).

No wrong door: If an individual applies to an IPP entity for access or correction of their personal information under the PRIS Act when their right of access is under the FOI Act, or an individual applies under the FOI Act when their right of access is under the PRIS Act, both the FOI Act and the PRIS Act provide that the application should be taken as an application under the correct legislation.

**7. Unique identifiers**

An IPP entity must not assign a unique identifier to an individual unless it is necessary to perform its functions or activities efficiently.

An IPP entity can only adopt, use or disclose a unique identifier used by another IPP entity for an individual in limited circumstances.

An IPP entity can only require an individual to provide a unique identifier to obtain a service in limited circumstances.

**8. Anonymity**

An IPP entity must give an individual the opportunity to not identify themself.

An IPP entity can only require an individual to identify themself if the law or circumstances make it necessary.

**9. Disclosures outside Australia**

An IPP entity must not send personal information overseas unless certain requirements are met. This includes, for example, that the overseas recipient of the information is subject to similar requirements as the IPP entity under the IPPs.

Further, an IPP entity must not send de-identified information overseas unless the recipient has appropriate security in place to protect the information and does not try to re-identify it.

**10. Automated decision-making**

If an IPP entity makes important decisions about individuals using automated decision-making processes (that is a process without much human input), it must assess the risks to ensure harm, bias and discrimination is minimised and that the requirements of the PRIS Act are complied with. This should be done periodically and when changes are made to the automated decision-making.

An IPP entity must let individuals know it is using automated decision-making and there must be a process where people can request human involvement in the decision.

**11. De-identified information**

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

An IPP entity must not re-identify de-identified information unless certain circumstances apply.

# Exceptions

There are some exceptions to the IPPs that set out when the IPPs do not apply. A summary of the exceptions is set out below.

**Personal, family or household affairs exception -** section 21

The IPPs do not apply to the handling of personal information by an individual or to personal information held by an individual in connection with the individual's personal, family or household affairs.

**Publicly available information -** section 22

The IPPs (other than IPP 6) do not apply to information contained in documents that are generally available to the public.

**Law enforcement functions -** section 23

Some of the IPPs will not apply to a law enforcement agency if it reasonably believes that non-compliance is necessary for its law enforcement functions.

**Emergency response functions -** section 24

Some of the IPPs will not apply to an IPP entity if it reasonably believes that non-compliance is necessary for its emergency response functions.

**Child protection functions -** section 25

Some of IPP 1 will not apply to an IPP entity if it reasonably believes that non-compliance is necessary for its child protection functions.

**Family violence -** section 26

Some of IPP 1 will not apply to the collection of personal information of a perpetrator or alleged perpetrator which relates to family violence or alleged family violence.

**IPP 6 does not apply to all IPP entities -** section 27

IPP 6 does not apply to an IPP entity that is an agency under the FOI Act or to a Parliamentary Secretary.

This means that IPP 6 only applies to contracted services providers to government.