Global Data and Cyber Handbook - Australia

Legal Bases for Processing of Personal Data

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 31 December 2024*

☒ Yes

The following are potential legal bases for processing personal data:

☒         appropriate notice has been provided to or made available to the data subject

☒         the data subject has provided consent to the processing for the identified purposes

☒         other

As a general rule, notice is all that is required to collect personal information other than for sensitive information, where consent is required.

Personal information can only be collected by fair and lawful means and if the information is reasonably necessary for (or, in the case of agencies, directly related to) one or more of its functions or activities.

Personal information must only be used or disclosed for the primary purpose of collection or for a permitted secondary purpose. Permitted secondary purposes include those which are: (a) related (directly, in the case of sensitive information) to the primary purpose of collection; and (b) within the reasonable expectations of the individual. Both of these factors will be influenced by whatever notices that have been given to the individual. Other permitted secondary purposes are limited to specified exceptional circumstances (e.g., permitted health situations, compliance with Australian law or a court/tribunal order, etc.)

The employee records exemption may apply to justify the collection and processing of personal data of employees, but the exception is quite narrow and may change or be removed in the future (see the section on Data Processing in the Employment Context).

Government-related identifiers (including healthcare identifiers and tax file numbers) can only be collected and processed for more limited purposes. Credit-related personal information and CDR Data are also subject to additional restrictions.

There are also consent requirements in relation to direct marketing under the APPs, the Spam Act and the DNCR Act.

The review of the Privacy Act considered the bases on which personal information can be used or disclosed. Among other things, the report on the review recommended – and the government agreed in-principle (subject to further consultation) – to introduce a requirement that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. The review report also proposed – and the government endorsed this in-principle – to require APP entities to undertake a privacy impact assessment prior to undertaking activities with high privacy risks.

# Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 31 December 2024*

☒ Yes

The following are potential legal bases for processing special categories of personal data:

☒         the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data

☒         processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

☒         processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

☒         processing is necessary for the establishment, exercise or defense of legal claims

☒         processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

☒         processing is necessary for reasons of public interest in the area of public health

☒         processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

☒         other

Consent is required to collect sensitive information unless an exception applies. The exceptions are:

Where collection is required or authorized by or under an Australian law or court/tribunal order

Where a permitted general situation exists in relation to the collection of the information by the APP entity. Permitted general situations are certain emergency-type situations defined in section 16A of the Privacy Act, and in summary cover:

Lessening or preventing a serious threat to life, health or safety

Locating a person reported as missing

Where it is reasonably necessary for establishing, exercising or defending a legal or equitable claim or for confidential alternative dispute resolution

Where necessary for diplomatic or consular functions or activities or for Defence Force activities outside Australia

The APP entity is an organization and a permitted health situation exists in relation to the collection of the information by the entity. Permitted health situations are defined in section 16B of the Privacy Act and in summary cover:

Collection in the process of providing a health service, as authorized by law or subject to a professional code of ethics

Collection in the course of medical research that is subject to professional safeguards, where obtaining consent is impracticable, and the research cannot be performed without the information being collected

Use or disclosure for conducting research, compiling or analyzing statistics

Use or disclosure necessary to prevent a serious threat to the life, health or safety or a genetic relative

Disclosures to the responsible person for an individual in certain circumstances

The APP entity is an enforcement body and the entity reasonably believes that:

If the entity is the Immigration Department, the collection of the information is reasonably necessary for, or directly related to, one or more enforcement-related activities conducted by, or on behalf of, the entity

Otherwise, the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities

The APP entity is a non-profit organization and both of the following apply when:

The information relates to the activities of the organization

The information relates solely to the members of the organization, or to individuals who have regular contact with the organization in connection with its activities

Explicit or express consent is not mandated, but the APP Guidelines indicate that consent must be clear, specific, informed, voluntary and given by a person with capacity to be valid. It is best practice to obtain express consent. That said, the guidelines also indicate that use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. Additionally, the OAIC asserts that an APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.

Unless consent is given for an additional purpose of use or disclosure, sensitive information may only be used for the primary purpose of collection or for a permitted secondary purpose (see above).

The circumstances in which health records can be collected and processed will depend on the content of applicable State or Territory health records laws. Collection and processing of My Health Records are generally much more restricted, and access to records is usually limited to individuals themselves (and/or their authorized or nominated representative) and their healthcare provider(s).

The review of the Privacy Act considered the bases on which personal information (including sensitive information) can be used or disclosed. Among other things, the government has agreed in-principle (subject to further consultation) to the following reform proposals made in the review report:

Providing in the legislation that consent must be voluntary, informed, current, specific and unambiguous in order to constitute valid consent, and expressly recognizing the ability for individuals to withdraw consent in an easily accessible manner

Recognizing collection, use, disclosure and storage of precise geolocation tracking data as a practice that requires consent

Prohibiting certain uses and disclosures of personal information of children (e.g., direct marketing)

Applying additional requirements (e.g., for a privacy impact assessment) before certain high-risk activities involving personal information can be undertaken

Allowing for broad consent to be given for certain research purposes

The review report also recommended, and the government agrees in-principle, that OAIC guidance on consent could be further expanded.

# Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 31 December 2024*

☒ No

The Privacy Act does not deal specifically with minors or specify an age after which individuals can make their own privacy decisions. However, the APP Guidelines indicate that:

Where an APP entity is seeking consent from an individual under the age of 18, it will need to determine on a case-by-case basis if the individual has capacity to consent

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise

An individual aged under 15 is presumed not to have capacity to consent

In practice, it is usual to seek a parent's or guardian's consent for the collection of personal information from children, especially where sensitive information is concerned and where a younger child is involved.

The review of the Privacy Act considered whether additional privacy protections in relation to children should apply to all APP entities. The review report endorses existing OAIC guidance on children, young people and capacity, but also suggests codifying the principle that consent must be given by someone with capacity in order to be valid. Other proposals include that notices and privacy policies should be clear and understandable, in particular for information addressed to children and that there should be a Children's Online Privacy Code, which will provide more guidance and regulated online services that are likely to be accessed by children. In response, the government has agreed to define a child as an individual who has not reached 18 years of age and agrees in-principle (subject to further consultation) with the report's other proposals specifically on children. The Tranche 1 Privacy Act reforms also set out a framework for the development of the Children's Online Privacy Code by 11 December 2026.

# In what circumstances do these special requirements apply?

*Last review date: 31 December 2024*

N/A

# What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 31 December 2024*

N/A

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.