

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Information Privacy Individual Action Plan**

Australia (2020)

|  | APEC Principle /Commentary | **Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [[1]](#footnote-1)** | **Provision[[2]](#footnote-2)** | **Sanction[[3]](#footnote-3)** | **Results/ Status[[4]](#footnote-4)** |
| --- | --- | --- | --- | --- | --- |
| A | Is privacy a constitutionally protected right in your economy? | No  | n/a | n/a | n/a |
| B | If not, what other available legislation deals with privacy or confidentiality of personal information. | There is separate privacy legislation in most State and Territory jurisdictions which applies to State and Territory government agencies only. This table will focus only on Australia’s Privacy Act. The *Privacy Act 1988* (Privacy Act) gives effect to Australia’s agreement to implement Guidelines adopted in 1980 by the Organisation for Economic Cooperation and Development for the protection of Privacy and Transborder Flows of Personal Data, as well as obligations under Article 17 of the International Covenant on Civil and Political Rights.The Privacy Act sets out safeguards for the handling of personal information by federal government agencies and certain private sector organisations (referred to collectively as APP entities). The Office of the Australian Information Commissioner (the OAIC) is responsible for Privacy and Freedom of Information regulation and the government agency information publication scheme. The OAIC also has oversight functions in relation to credit reporting, data matching, spent convictions, health information and telecommunications legislation.  | *Privacy Act 1988* (Cth) An electronic version can be found at: [Privacy Act 1988 (legislation.gov.au)](https://www.legislation.gov.au/Details/C2021C00242/Download)For various State and Territory privacy laws, see: <https://www.oaic.gov.au/privacy/privacy-in-your-state/>The Office of the Australian Information Commissioner Act 2010 (legislation.gov.au) | The Office of the Australian Information Commissioner (OAIC), is an independent regulator charged with enforcement of the Privacy Act at the federal level. Most States and Territories also provide for enforcement compliance under their own legislation. The OAIC assists government agencies and relevant private sector organisations to comply with the Act, provides assistance to individuals about their rights under the Act and related legislation, and promotes best practice in privacy standards.The Information Commissioner has the power to:* Investigate a complaint that an individual has made to the Information Commissioner.
* Make a determination of a complaint either dismissing the compliant or finding the complaint substantiated, declare that the respondent cease the conduct/not repeat the conduct; redress the person’s loss; declare the complainant is entitled to compensation; or not take further action.
* Seek an enforcement order from a court.
* Apply to the court for a civil penalty order for a breach of a civil penalty provision.
* Commence an Information Commissioner initiated investigation.
* Conduct a privacy assessment in relation to a particular entity or act or practice, including to audit compliance with the Privacy Act.
* Ask an entity to develop an enforceable code, and register codes.
* Direct an agency to undertake a privacy impact assessment.
* Recognise external dispute resolution schemes to handle particular privacy related complaints.
 | n/a |
| 1 | ***I Preventing Harm*****(Ref. Para. 14)**Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information. | *Privacy Act 1988* (Cth)  | The Privacy Actprovides for 13 Australian Privacy Principles (APPs) guiding how a data controller/processor is required to handle personal information in a way that prevents harm to individuals. The APPs cover open and transparent management of personal information, notification, collection, use and disclosure, quality and security of personal information. APP 11 provides that an APP entity must take such steps as are reasonable to protect personal information from misuse, interference and loss and from unauthorized access, modification or disclosure.The APPs also provides individuals with rights to access and correct personal information (APP 12 and APP 13).  | The Privacy Act gives individuals the right to make a complaint if they believe that their personal information, including health information, has been mishandled by a Commonwealth government agency or certain private sector organisations. After investigating a complaint, the Information Commissioner may: * Make a determination dismissing the complaint.
* Find a complaint is substantiated and make a determination.
* Accept an enforceable undertaking.
* Bring proceedings to enforce a determination or enforceable undertaking.
* Seek an injunction including before, during or after an investigation or the exercise of another regulatory power.
* Apply to the court for a civil penalty order for a breach of a civil penalty provision.
 | n/a |
| 2 | ***II Notice*****(Ref. Para. 15-17)**Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that shouldinclude:a) the fact that personal information is being collected;b) the purposes for which personal information is collected;c) the types of persons or organizations to whom personal information might be disclosed;d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. | *Privacy Act 1988* (Cth)APPs 1 and 5 | **APP 1**APP 1 requires an APP entity to: * Take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.
* Have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information.
* Take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form and, upon request, in a particular form.

**APP 5**APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include:* the APP entity’s identity and contact details
* facts and circumstances of collection
* if collection is required or authorised by law
* the purpose of collection
* consequences for the individual if personal information is not collected
* other APP entities, bodies or persons to which the personal information is usually disclosed
* information about the entity’s Privacy Policy
* likely cross-border disclosure of personal information, and
* when notification is to occur.

The requirement to notify applies to all personal information ‘collected’ about an individual, either directly from the individual or from a third party.  | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the OAIC. |   |
| 3 | ***III Collection Limitation*****(Ref. Para. 18)**The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. | *Privacy Act 1988* (Cth)APPs 1, 3 and 5  | **APP 1**APP 1 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. It contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy:* the kinds of personal information collected and held by the entity
* how personal information is collected and held
* the purposes for which personal information is collected, held, used and disclosed
* how an individual may access their personal information and seek its correction
* how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled and
* whether the entity is likely to disclose personal information to overseas recipients and if so, the relevant countries.

**APP 3**The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4). APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information. For personal information (other than sensitive information), an APP entity that is an organisation (not a government agency), may only collect this information where it is reasonably necessary for the organisation’s functions or activities.APP 3 contains more stringent requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the individual concerned consents to the collection and the information is reasonably necessary for one or more of the entity’s functions or activities. APP 3 requires that personal information must only be collected by lawful and fair means.Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable.**APP 5**APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include:* the APP entity’s identity and contact details
* facts and circumstances of collection
* if collection is required or authorised by law
* the purpose of collection
* consequences for the individual if personal information is not collected
* other APP entities, bodies or persons to which the personal information is usually disclosed
* information about the entity’s Privacy Policy
* likely cross-border disclosure of personal information, and
* when notification is to occur.
 | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the OAIC. | n/a |
| 4 | ***IV Use of Personal Information*****(Ref. Para. 19)**Personal information collected should be used only to fulfill the purposes ofcollection and other compatible or related purposes except:a) with the consent of the individual whose personal information is collected;b) when necessary to provide a service or product requested by the individual; or,c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. | *Privacy Act 1988* (Cth)APP 6 | **APP 6** APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the ‘primary purpose’), or for a secondary purpose if an exception applies. The exceptions include where: * the individual has consented to a secondary use or disclosure
* the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
* the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
* a permitted general situation exists in relation to the secondary use or disclosure
* the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure
* the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body or
* the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.

APP 6 does not apply to the use or disclosure of personal information for the purpose of direct marketing (this is covered by APP 7), or specific government related identifiers (this is covered by APP 9).  | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the OAIC. | n/a |
| 5 | ***V Choice*****(Ref. Para. 20)**Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not beappropriate for personal information controllers to provide these mechanisms when collecting publicly available information. | *Privacy Act 1988* (Cth) | The APPs are not written using the language of ‘choice’, but rather require entities to seek consent or fall within specified exceptions if they wish to use or disclose personal information for secondary purposes. |  | n/a |
| 6 | ***VI Integrity of Personal Information*****(Ref. Para. 21)**Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. | *Privacy Act 1988* (Cth)APPs 10, 11 and 13 | **APP 10**APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses. APP10 requires an entity must take reasonable steps to ensure the personal information the entity collects is accurate, up-to-date and complete. If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction (under APP 13).**APP 11**An APP entity must take reasonable steps to protect the personal information it holds, including from misuse, interference, loss and unauthorised access, modification or disclosure. If reasonable steps are taken to comply with APP 11, this reduces the likelihood that personal information will need correction (under APP 13).**APP 13**APP 13 relates to correction of personal information. It operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including informal arrangements and, for government agencies, the *Freedom of Information Act 1982* (Cth). APP 13 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. The requirement to take reasonable steps applies in two circumstances: where an APP entity is satisfied, independently of any request, that personal information it holds is incorrect, or where an individual requests an APP entity to correct their personal information. APP 13 also sets out other minimum procedural requirements in relation to correcting personal information. An APP entity must: * Upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity
* Give a written notice to an individual when a correction request is refused, including the reasons for the refusal and the complaint mechanisms available to the individual
* Upon request by an individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be incorrect.
* Respond in a timely manner to an individual’s request to correct personal information or to associate a statement with the personal information (APP 13.5(a)).
* Not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement.

When taking steps to identify and correct incorrect personal information under APP 13, an entity should consider whether it still needs the personal information for a permitted purpose, or whether reasonable steps must be taken to destroy or de-identify the information under APP 11.  | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the OAIC. | n/a |
| 7 | ***VII Security Safeguards*****(Ref. Para. 22)**Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. | *Privacy Act 1988* (Cth)APPs 8 and 11Section 16CPart IIIC – Notifiable Data Breaches Scheme | **APP 8 and Section 16C**APP 8 and section 16C of the Privacy Act create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual’s personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.This reflects a central object of the Privacy Act of facilitating the free flow of information across borders while ensuring that the privacy of individuals is respected.APP 8 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C). The exceptions to the requirement in APP 8 and to the accountability provision in s 16C are:* Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme and a readily accessible dispute resolution scheme
* Disclosing personal information to an overseas recipient with the individual’s consent after the individual is expressly informed
* Disclosing personal information to an overseas recipient as required or authorised by law
* Disclosing personal information to an overseas recipient where a permitted particular situation exists
* Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing
* Disclosing personal information to an overseas recipient for an enforcement related activity of an Australian enforcement body.

When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6. That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies. **APP 11**An APP entity must take reasonable steps to protect the personal information it holds, including from misuse, interference, loss and unauthorised access, modification or disclosure. The Information Commissioner administers the Notifiable Data Breaches scheme and has powers to investigate and regulate non-compliance. **Notifiable Data Breaches Scheme**Under Part IIIC of the Privacy Act, the Notifiable Data Breaches scheme requires an APP entity to notify individuals and the Australian Information Commissioner where there has been an unauthorised access, disclosure or loss of personal information that a reasonable person would conclude is likely to result in serious harm to an individual (some limited exceptions apply).  | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the OAIC.In relation to cross border transfers, the OAIC works cooperatively with overseas Privacy Enforcement Authorities/regulators and is an active participant on a number of international regulator networks.The OAIC is a participant in the APEC Cross Border Enforcement Arrangement (CPEA).Under the Notifiable Data Breaches Scheme, the OAIC has a role in encouraging compliance, including handling complaints, conducting investigations, and taking other regulatory action to instances of non-compliance.  | n/a |
| 8 | ***VIII Access and Correction*****(Ref. Para. 23-25)**Individuals should be able to:a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;i. within a reasonable time;ii. at a charge, if any, that is not excessive;iii. in a reasonable manner;iv. in a form that is generally understandable; and,c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.Such access and opportunity for correction should be provided except where:(i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question;(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or(iii) the information privacy of persons other than the individual would be violated.If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.  | *Privacy Act 1988* (Cth)APPs 1, 5, 10, 12 and 13 | **APP 1** APP 1 requires an entity to have a clearly expressed and up-to-date policy that includes: * the kinds of personal information that the entity collects and holds; and
* how an individual may access personal information about the individual that is held by the entity and seek the correction of such information.

**APP 5** Requires an APP entity that collects personal information to take such steps (if any) as are reasonable in the circumstances to notify the individual of certain matters, which include:* the identity and contact details of the APP entity
* the purpose for which the APP entity collects the personal information, and
* information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information (as contained within the entity’s privacy policy, required by APP 1).

**APP 10**APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (APP 10). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction (under APP 13)**APP 12**If an APP entity holds personal information about an individual, APP 12 requires the entity, on request by the individual, to give the individual access to the information. An APP entity may refuse to give access if required or authorised to refuse access under an Australian law. An organisation may refuse to give access if any of the criteria listed in APP 12 are made out. These exceptions relate to protecting the safety of the public, the privacy of individuals, and the integrity of law enforcement related activities or legal proceedings. The access may also be refused if the request is frivolous or vexatious or giving access would reveal commercially sensitive information about the organisation. **APP 13**APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. This requirement applies where: * the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
* the individual requests the entity to correct the personal information

In accordance with APP 13, the APP entity must: * respond to the request within 30 days if the entity is a government agency or within a reasonable period if the entity is an organization, and
* not charge the individual for making the request, for correcting the personal information or for associating the statement with the personal information.

If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out the reasons for the refusal (unless it would be unreasonable to do so), and the mechanisms available to complain about the refusal. In particular, the individual should be advised that: * a complaint should first be made in writing to the APP entity (s 40(1A))
* the entity should be given a reasonable time (usually 30 days) to respond
* a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any), and
* lastly, that a complaint may be made to the Australian Information Commissioner (s 36).

If an APP entity refuses a request to correct personal information, the individual can request the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. The entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.  | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the OAIC. | n/a |
| 9 | ***IX Accountability*****(Ref. Para. 26)**A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. | *Privacy Act 1988* (Cth)APPs 1 and 8Section 16C*Privacy (Australian Government Agencies – Governance) APP Code 2017* | **APP 1**APP 1 requires an entity to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:* will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity, and
* will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.

**APP 8**APP 8 deals with overseas disclosure of personal information held in Australia. APP 8 generally requires an APP entity, before disclosing personal information to an overseas recipient, such as a subcontractor, to take reasonable steps to ensure that overseas recipient will handle the personal information in accordance with the APPs. Importantly, the APPs include a requirement for businesses to take reasonable steps to protect personal information from unauthorised access or disclosure (APP 11).**Section 16C**Section 16C of the Privacy Act makes the Australian APP entity responsible for personal information disclosed to an overseas recipient, unless an exception applies. This means the Australian APP entity will be accountable if the overseas entity mishandles the information.The *Privacy (Australian Government Agencies – Governance) APP Code 2017* commenced on 1 July 2018. It requires Australian Government agencies subject to the Privacy Actto appoint a Privacy Officer and a Privacy Champion to undertake particular functions and roles (sections 10 and 11). | Breaches of the Privacy Act (including the APPs) are regulated and enforceable by the(OAIC).The Information Commissioner has a range of powers under the Privacy Act relating to the conduct of investigations including powers: * to conciliate complaints
* to make preliminary inquiries of any person
* to require a person to give information or documents, or to attend a compulsory conference, and
* to transfer matters to an alternative complaint body in certain circumstances (s 49).

As a result of an investigation, the Information Commissioner can:* Make a determination dismissing the complaint.
* Find a complaint is substantiated and make a determination.
* Accept and enforceable undertaking.
* Bring proceedings to enforce a determination or enforceable undertaking
* Seek an injunction including before, during or after an investigation or the exercise of another regulatory power.
* Apply to the court for a civil penalty order for a breach of a civil penalty provision.
 | n/a |
| C | Network point of contact arrangements[[5]](#footnote-5) |  | Contact details will be made available to APEC members through the APEC Secretariat. |  |  |

1. *Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.* [↑](#footnote-ref-1)
2. *Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled “APEC Principle/ Commentary”.* [↑](#footnote-ref-2)
3. *Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).*  [↑](#footnote-ref-3)
4. *Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies’ practice, for example enacted, introduced, draft.  If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."* [↑](#footnote-ref-4)
5. *Please provide contact details such as name and/or title, address, telephone and email contacts. This information will not be published but will be made available to economies.* [↑](#footnote-ref-5)