Chapter 3:

Australian Privacy Principle 3 —

Collection of solicited personal information

Version 1.2, May 2026

OAIC

Contents

Key points

- APP 3 outlines when an APP entity may collect solicited personal information.
- An APP entity 'solicits' personal information if it explicitly requests an individual or another entity to provide personal information, or it takes active steps to collect personal information. See Chapter 4 (APP 4) for where an entity has taken no active steps to collect the information.
- 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 agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities
    - an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities.
- APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. An APP entity may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection, unless an exception applies.
- 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 (additional exceptions apply to agencies).
- Where personal information is publicly available on the internet, that does not allow it to be collected and used in whatever way the APP entity chooses without regard to the knowledge and reasonable expectations of the person whose information it concerns.[1] Publicly available personal information must still be collected in accordance with APP 3 or APP 4, and once collected is subject to the APPs.
- It is implicit in the requirement that personal information collection be reasonably necessary for an entity's functions and activities that entities ensure proportionality in their collection of personal information.[2] Entities should adopt a data minimisation approach and limit collection of personal information to the minimum amount necessary in the circumstances. Over-collection may contravene the requirements of APP 3, as well as increase risks to the security of personal information and lead to greater potential harm in the event of a data breach.

What does APP 3 say?

3.1 The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4).

3.2 APP 3 deals with two aspects of collecting solicited personal information:

[1] Court Data Australia and Office of the Australian Information Commissioner [2025] ARTA 876 (28 May 2025) at [41].

[2] Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [77]. This position is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that this position reflects the determination subject to that review and will be updated should the outcome of the review change this position.

- when an APP entity can collect personal information — the requirements vary according to whether the personal information is or is not sensitive information, and whether the APP entity is an agency or an organisation
- how an APP entity must collect personal information — the same requirements apply to all APP entities and to all kinds of personal information, with additional exceptions available to agencies.

3.3 In summary, the principles that apply are:

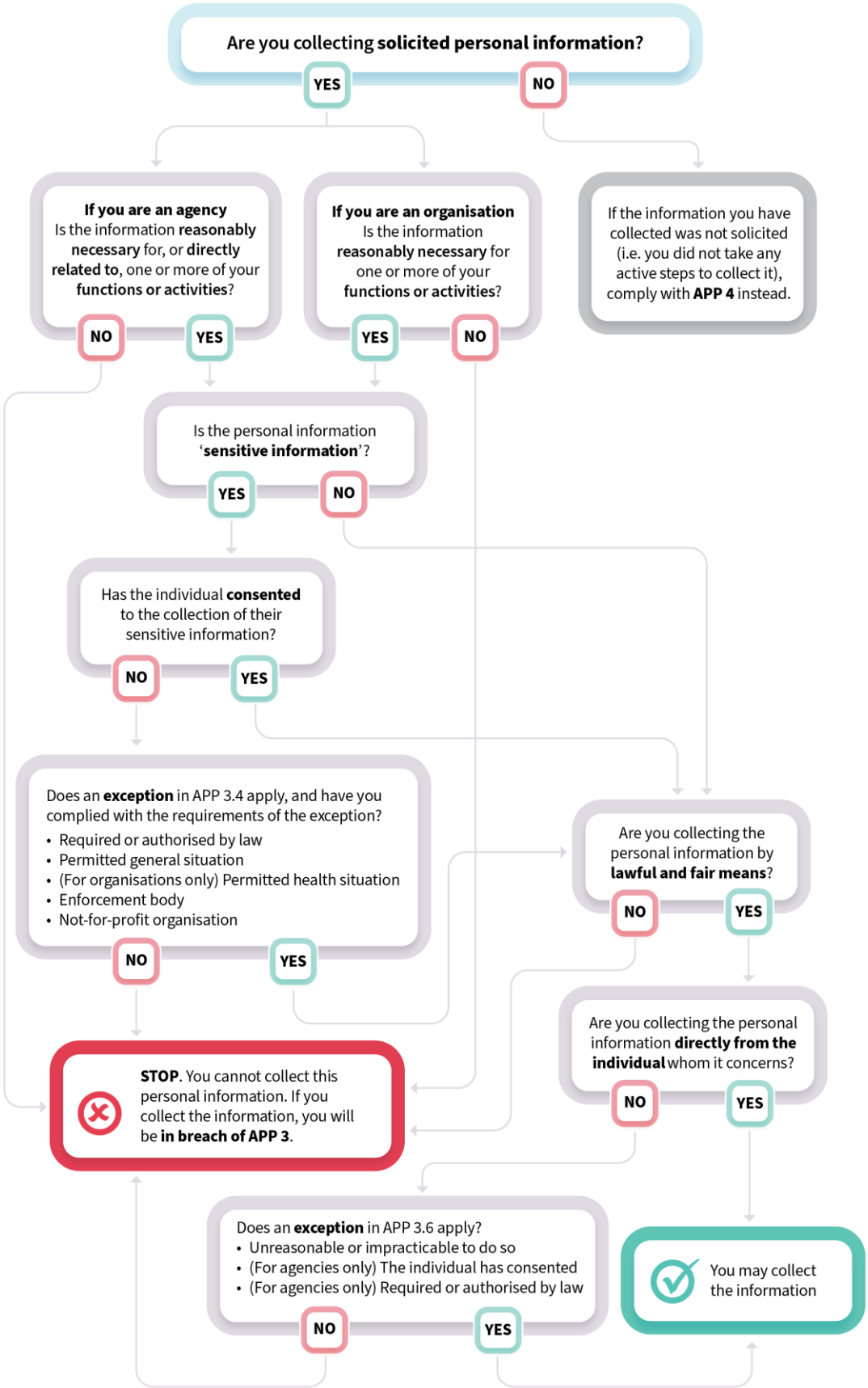
- an **agency** may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1)
- an **organisation** may only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.2)
- in addition to the above requirements, an APP entity may only solicit and collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3)
- an APP entity must solicit and collect personal information:
  - only by lawful and fair means (APP 3.5), and
  - directly from the individual, unless an exception applies (APP 3.6).

3.4 Figure 1 demonstrates at a high level each of these requirements and how they relate to each other. It is to be read in conjunction with these Guidelines. Download the Requirements under APP 3 (Collection of solicited personal information) flow chart.

Requirements under APP 3

(Collection of solicited personal information)

This flow chart is to be read in conjunction with **Chapter 3 (APP 3) of the APP Guidelines**.



'Solicit' and 'collect'

3.5 APP 3 applies when an APP entity 'solicits' and 'collects' personal information, while APP 4 applies when an APP entity receives personal information that it 'did not solicit'. Examples of solicited personal information collected by an entity are given in paragraph 3.11 below; examples of unsolicited personal information received by an entity are given in Chapter 4 (APP 4).

3.6 An APP entity 'collects' personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication' (s 6(1)). This concept applies broadly, and includes gathering, acquiring or obtaining personal information from any source (including publicly available sources on the internet) and by any means.

3.7 Where an APP entity creates personal information with reference to, or generated, inferred or observed from, other information the entity holds, this is a 'collection' of personal information and APP 3 obligations will apply. For example, through artificial intelligence (AI), automated decision making, data analytics, online cookies or 'internet of things' devices.[3]

3.8 In practice, all personal information that is held by an entity will generally be treated as information that was collected by the entity. An APP entity 'collects' personal information even if it only holds the information momentarily (e.g. for milliseconds).[4] 'Collect' is discussed in more detail in Chapter B (Key concepts).

3.9 An APP entity 'solicits' personal information 'if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included' (s 6(1)). The request may be made to an agency, organisation, individual or a small business operator.[5] A 'request' is an active step taken by an entity to collect personal information, and may not involve direct communication between the entity and an individual.

3.10 Two entities may collect the same personal information[6] (just as two entities may 'hold' the same information under the Privacy Act), for example where one entity collects personal information pursuant to a contract with another. Whether or not the entity with 'control' but not possession is taken to collect personal information can depend on the contractual arrangements in place, for example whether the entity has contractual control over the personal information.[7]

Privacy tip: If an entity engages a third party to collect personal information, they should make sure the arrangements (such as a contract) cover how personal information will be

[3] For more information on 'collection' through the use of AI, see OAIC, Guidance on privacy and the use of commercially available AI products, OAIC website <https://www.oaic.gov.au>.

[4] See Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026) at [59] which states 'There is no minimum temporal threshold for collection'. See also discussion at [42]–[59] and [169].

[5] An 'entity' is defined in s 6(1) to mean an agency, organisation or small business operator. 'Organisation' is defined in s 6C to include an individual.

[6] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) at [72], citing Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307 at [184]; and Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34 (30 June 2021) at [71].

[7] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) at [64]-[72].

handled and that the third party is aware of the Privacy Act obligations. This is particularly important if the third party is located offshore as the entity may be held liable for the acts of that third party.

3.11 Examples of solicited personal information collected by an APP entity include the following, where they are collected for inclusion in a record or generally available publication:

- personal information provided by an individual in response to a request, direction or order
- personal information gathered from the internet by the entity, including via automated collection methods such as data scraping, web crawling[8] and third-party tracking pixels
- personal information about an individual provided by another entity in response to a request, direction, order or arrangement for sharing or transferring information between both entities
- personal information that is collected and held by an entity momentarily before being destroyed or disclosed to another entity, for example where an entity is collecting personal information through facial recognition technology[9] or where an entity is functioning as a router or hub for a service or system, such as a digital identity exchange
- personal information purchased from another entity, including from a data broker
- personal information provided at a business meeting, where it relates to the subject matter of the meeting, including personal information from online professional networking platforms, business cards exchanged at the meeting, and, where the meeting is online, recordings and transcripts, including those generated by systems including AI
- personal information provided by an individual to an AI chatbot or agent on the entity's website
- a completed form or application submitted by an individual
- a complaint letter sent in response to a general invitation on an APP entity's website to individuals to complain to the entity
- an employment application sent in response to either a job advertisement published by an entity or an expression of interest register maintained by the entity
- a form completed to enter a competition being conducted by an entity
- personal information provided to a 'fraud hotline' that is designed to capture 'tip-offs' from the public
- an entry in an APP entity's visitors book or self-service kiosk
- a record of a credit card payment
- CCTV footage that identifies individuals.

[8] See for example, Clearview AI Inc and Australian Information Commissioner [2023] AATA 1069 (8 May 2023) and Court Data Australia and Office of the Australian Information Commissioner [2025] ARTA 876 (28 May 2025).

[9] See for example, Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026).

Collecting for an APP entity's 'functions or activities'

3.12 An APP entity must only collect personal information which is reasonably necessary for one or more of the entity's functions or activities (APPs 3.1 and 3.2).[10] Agencies may, in addition, collect personal information that is directly related to one or more of the agency's functions or activities. Regarding sensitive information, there is an additional requirement to seek consent for the collection, unless an exception in APP 3.4 applies. Even where an exception applies, the collection will generally still need to be reasonably necessary for (or, for agencies, directly related to) the entity's functions or activities (APP 3.3).

3.13 Determining whether a particular collection of personal information is permitted involves a two-step process:

- identifying an APP entity's functions or activities — different criteria apply for ascertaining the functions and activities of agencies and organisations
- determining whether the particular collection of personal information is reasonably necessary for (or, for agencies, directly related to) one of those functions or activities.

Identifying the functions or activities of an agency

3.14 An agency's functions will be conferred either by legislation (including a subordinate legislative instrument) or an executive scheme or arrangement established by government. Identifying an agency's functions involves examining the legal instruments that confer or describe the agency's functions. These include:

- Acts and subordinate legislative instruments
- the Administrative Arrangements Order made by the Governor-General
- government decisions or ministerial statements that announce a new government function.[11]

3.15 The activities of an agency will be related to its functions. The activities of an agency include incidental and support activities, such as human resource, corporate administration, property management, analytics and public relations activities.

3.16 One resource that describes an agency's functions is that agency's Information Publication Scheme (IPS) entry.[12] Agencies to which the *Freedom of Information Act 1982* (FOI Act) applies are required to publish on a website 'details of the functions of the agency'. This forms part of the IPS established by the FOI Act (ss 8(2)(c), 8D(3)). The IPS entries of most agencies are readily accessible through a link on the homepage of the agency's website. Another resource that describes agency functions and activities is the annual report of an agency, usually accessible from the agency's website.

[10] See OAIC, Chapter 9 (APP 9) for a discussion of particular issues relating to the lawful collection of government related identifiers by organisations, OAIC website <https://www.oaic.gov.au>.

[11] The source and scope of government functions are discussed at greater length in OAIC, FOI Guidelines at [13.38]–[13.49], OAIC website <https://www.oaic.gov.au>.

[12] An agency's incidental functions (described in paragraph 3.15) are not required to be published in its IPS entry: see OAIC, FOI Guidelines at [13.47]–[13.49], OAIC website <https://www.oaic.gov.au>.

3.17 The functions and activities of an agency are to be determined objectively. By way of example, for something to be considered a function or activity of an agency under APP 3, it would not be sufficient for an agency to simply describe its functions and activities on its website or in its annual report if these are inconsistent with the practical reality or with the agency's legislative mandate.

Identifying the functions or activities of an organisation

3.18 An organisation's functions or activities include:

- current functions or activities of the organisation
- proposed functions or activities the organisation has decided to carry out and for which it has established plans
- activities the organisation carries out in support of its other functions and activities, such as human resource, corporate administration, property management, analytics and public relations activities.

3.19 The functions and activities of an organisation will commonly be described (though not necessarily exhaustively) on a website, in an annual report, and in corporate brochures, advertising, product disclosure statements and client and customer letters and emails.

3.20 The functions and activities of an organisation are to be determined objectively. For example, by examining documents outlined in the above paragraph, constitutive documents, the functions and activities it has focused on in the past, public statements it has issued, and any representations it has made to individuals about its functions and activities in the course of collecting their personal information such as in its privacy policy.

3.21 While an organisation's functions and activities can change over time, they cannot be changed unilaterally or immediately. For example, for something to be considered a function or activity of an agency under APP 3, it would not be sufficient for an organisation to simply describe its functions and activities on its website or in its annual report if these are inconsistent with the practical reality.

3.22 An organisation's ability to collect personal information under APP 3 only extends to functions or activities that are lawful.

Collecting personal information that is 'directly related to' an agency's functions or activities

3.23 An agency may collect personal information that is 'directly related to' one or more of the agency's functions or activities (APP 3.1). An agency may collect sensitive information with consent that is 'directly related to' one or more of the agency's functions or activities (APP 3.3). To be 'directly related to', a clear and direct connection must exist between the personal information being collected and an agency function or activity. For example, collecting personal information for the purposes of handling a complaint about the agency has been considered intrinsic to its functions and activities.[13]

[13] 'ZJ' and Australian Centre for International Agricultural Research (Privacy) [2021] AICmr 92 (17 December 2021) at [56].

Collecting personal information that is 'reasonably necessary' for an APP entity's functions or activities

3.24 An APP entity may collect personal information that is 'reasonably necessary' for a function or activity of the entity (APP 3.1 and APP 3.2).[14] An APP entity may collect sensitive information with consent where the sensitive information is 'reasonably necessary' for a function or activity of the entity (APP 3.3).

3.25 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection is reasonably necessary. In the context of the Privacy Act, it would not be sufficient if the collection is merely helpful, desirable or convenient. 'Reasonably necessary' is discussed further in Chapter B (Key concepts).

3.26 Proportionality is implicit in this 'reasonably necessary' requirement, and requires entities to take a data minimisation approach.[15] Data collected should be relevant, minimal, and not excessive. Data minimisation is an important risk mitigation measure and represents best practice for APP entities.

3.27 Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

- the primary purpose of collection ('purpose' is discussed further in Chapter B (Key concepts))
- how the personal information will be used in undertaking a function or activity of the APP entity (for example, in most circumstances collection on the basis that personal information could become necessary for a function or activity in the future, would not be reasonably necessary. This is distinct from collecting personal information for a foreseeable event that may never occur if that collection is reasonably necessary for a function or activity (see Example B below). It is also distinct from collecting personal information for a proposed function and activity for which there are established plans
- whether the entity could undertake the function or activity without collecting that personal information, or by collecting a lesser amount of personal information
- whether the collection is proportionate, which involves balancing the privacy impacts resulting from the collection against the benefits gained, with reference to the relevant function or activity.

Example A: A delivery company must verify the residency status of its new couriers through the onboarding process. It gives its new couriers two options: to present their identity documents (such as passport or birth certificate) in person at one of their corporate offices ahead of their start date, or to verify their identity document online using a secure identity verification service. Regardless of which option the courier picks, the delivery company never

[14] An APP entity may also collect the personal information of an individual (other than sensitive information) from a related body corporate (s 13B(1)(a)).

[15] Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [77]. This position is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that this position reflects the determination subject to that review and will be updated should the outcome of the review change this position.

collects or retains the identity document itself or any details from the document. It simply has a checkbox which is ticked when the residency status has been verified via either method.

Example B: A child care centre collects emergency contact details and some health information about enrolled children in case this is needed in the event of an accident or emergency. The child care centre collects this to ensure it can prevent and respond to accidents. It may be that an accident or emergency does not occur and the personal information is never needed, but the child care centre may still collect this personal information as it is reasonably necessary for its functions and activities.

3.28 The following are instances in which the OAIC has previously ruled that a collection of personal information was not reasonably necessary for an entity's function or activity:

- a third-party rental technology platform asking rental applicants to provide personal information that did not establish the individual's identity, their ability to pay rent, or the likelihood they will look after the property, such as their gender, citizenship status and visa expiry[16]
- all rental applicants being asked to provide emergency contact and vehicle details, when this information is only required to administer the tenancy of the successful applicant[17]
- a third-party rental technology platform asking all rental applicants to provide identification documents, certain details in identification documents such as passports, number of names listed on Medicare card and card colour, for identity verification, when, at the tenancy application stage, individuals' identity can be sufficiently established by collecting less information[18]
- a job applicant being asked to advise if they had suffered a work-related injury or illness, when this was not relevant to the position being advertised[19]

[16] Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [75]–[85]. The Commissioner found it was not reasonably necessary for the respondent to collect gender, names and ages of dependents, student status, bankruptcy status, retirement status, details of previous living history, details of property ownership, current applications for other properties, bond and rent assistance application status, and citizenship status and visa expiry. This ruling is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that the information in this dot point and footnote reflects the determination subject to that review and will be updated should the outcome of the review change this finding.

[17] Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [86]–[88]. This ruling is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that the information in this dot point reflects the determination subject to that review and will be updated should the outcome of the review change this finding.

[18] In addition, where verification of identity is required prior to offering a tenancy contract, the OAIC has found that there are less privacy intrusive ways to establish the identity of an individual. For example, individuals could be referred to an appropriately secure third-party ID verification service, or physical sighting of the documents: Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [85]. This ruling is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that the information in this dot point and footnote reflects the determination subject to that review and will be updated should the outcome of the review change this finding.

[19] Own Motion Investigation v Australian Government Agency [2007] PrivCmrA 4, Australasian Legal Information Institute website <www.austlii.edu.au>.

- a person applying to open a bank account being asked to complete a standard form application that included a question about marital status, when this had no bearing on the applicant's eligibility to open an account[20]
- a medical practitioner photographing a patient for the patient's medical file, when this was not necessary to provide a health service.[21]

3.29 Other examples of personal information collection that may not be reasonably necessary for an APP entity's functions or activities include:

- collecting personal information about a group of individuals, when information is only required for some of those individuals. For example, collecting personal information about all job applicants, when information is only required for shortlisted candidates
- collecting more personal information than is required for a function or activity. For example, collecting all information entered on an individual's driver licence when the purpose is to establish if the individual is aged 18 years or over
- collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future (this is to be distinguished from the situation where personal information is required for a function or activity, but is not being used immediately)
- an organisation collecting personal information for or on behalf of a related body corporate where the collection of that personal information is not reasonably necessary for the organisation's own functions or activities
- collecting personal information to train an AI model, when this training could be achieved with de-identified information or with a lesser amount of personal information.[22]

3.30 Where a collection of personal information is not 'reasonably necessary', it may also be unfair and/or unlawful in breach of APP 3.5. See 'Collecting by lawful and fair means' below.

Collecting sensitive information

3.31 APP 3.3 imposes an additional requirement of **consent** for collecting sensitive information about an individual. Unless an exception applies, an APP entity must:

- satisfy the criteria above, i.e. the collection of the sensitive information must be reasonably necessary for (or, for agencies, directly related to) one or more of the entity's functions or activities, and
- the individual about whom the sensitive information relates must consent to the collection (APP 3.3(a)).

3.32 'Sensitive information' is defined in s 6(1), and is discussed in more detail in Chapter B (Key concepts). 'Consent' is defined in s 6(1) as 'express consent or implied consent', and is discussed in more detail in Chapter B (Key concepts). The four key elements of consent are:

[20] D v Banking Institution [2006] PrivCmrA 4, Australasian Legal Information Institute website <www.austlii.edu.au>.

[21] M v Health Service Provider [2007] PrivCmrA 15, Australasian Legal Information Institute website <www.austlii.edu.au>.

[22] For a case study on using de-identified information to train an AI model, see OAIC, Report into preliminary inquiries of I-MED, OAIC website <https://www.oaic.gov.au>. For more information on the use of AI, see OAIC, Guidance on developing and training generative AI models and Guidance on privacy and the use of commercially available AI products, OAIC website <https://www.oaic.gov.au>.

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

3.33 An APP entity should generally seek express consent from an individual before collecting the individual's sensitive information, given the greater privacy impact this could have.

3.34 Generally, it should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way. An APP entity cannot infer consent simply because they have provided individuals with notice of a proposed collection of personal information (including sensitive information). This is because all four elements of consent are unlikely to have been satisfied. Further notice is required to ensure informed consent can be provided.

3.35 An APP entity should exercise particular caution when using automated collection methods such as data scraping or third-party tracking pixels, as these could inadvertently be configured to collect sensitive information.

3.36 APP 3.4 lists five exceptions to the requirements outlined in paragraph 3.31. These are considered below.

Collecting sensitive information as required or authorised by law

3.37 An APP entity may collect sensitive information if the collection 'is required or authorised by or under an Australian law or a court/tribunal order' (APP 3.4(a)). The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in more detail in Chapter B (Key concepts).

3.38 An example of where a law or order may require or authorise collection of sensitive information is the collection by an authorised officer under the Migration Act 1958 of personal identifiers (that may include biometric information) from a non-citizen who is in immigration detention.[23]

3.39 Where an APP entity has discretion as to what and/or how they will collect information under the relevant law, they should collect only what sensitive information is reasonably necessary to fulfil their obligation under that law. The entity should, in addition, ensure their handling of the information is proportionate to the aim of fulfilling the legal obligation.

3.40 For example, the Online Safety Act 2021 authorises the collection of personal information through requiring age-restricted social media platforms to take 'reasonable steps' to prevent users under 16 years of age from having an account with the platform.[24] In narrow circumstances and depending on the deployment context, this may extend to the collection of sensitive information inputs that are necessary to achieve the objective of preventing users under 16 years of age from having accounts. The entity should minimise what it collects to fulfil this obligation. The entity should further process information temporarily,

[23] See Migration Act 1958, ss 5A, 261AA.

[24] See Online Safety Act 2021, s 63D.

for example use technology solutions that temporarily process personal information inputs as part of age assurance and do not retain them.[25]

3.41 Where this exception is not engaged, the requirements outlined in paragraph 3.31 including for the collection of personal or sensitive information to be 'reasonably necessary' will apply to collection of any such information. This limits what information may be collected to those steps that would fulfil an APP entity's function to comply with the relevant law.

Collecting sensitive information where a permitted general situation exists

3.42 An APP entity may collect sensitive information if a 'permitted general situation' exists in relation to the collection (APP 3.4(b)).

3.43 Section 16A lists seven permitted general situations (two of which apply only to agencies). The seven situations are set out below, and are discussed further in Chapter C (Permitted general situations), including the meaning of relevant terms.

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

3.44 An APP entity may collect sensitive information if:

- it is unreasonable or impracticable to obtain the individual's consent to the collection, and
- the entity reasonably believes the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A(1), Item 1).

3.45 For guidance on 'unreasonable or impracticable to obtain consent', see Chapter C (Permitted general situations).

3.46 The following factors are relevant to whether an APP entity reasonably believes the collection of sensitive information is necessary: [26]

- the suitability of the proposed collection, including its efficacy in addressing the serious threat
- the alternatives available to lessen or prevent the serious threat, including whether less privacy-intrusive alternatives are available to address the serious threat,
- whether the proposed collection is proportionate. This involves balancing the privacy impacts resulting from the collection of sensitive information against the benefits to be gained from doing so.

3.47 For further guidance on 'reasonably believes the collection is necessary', see Chapter C (Permitted general situations).

3.48 Examples of where this permitted general situation might apply are:

[25] For privacy guidance on this topic, see OAIC, Privacy Guidance on Part 4A (Social Media Minimum Age) of the *Online Safety Act 2021*, OAIC website <https://www.oaic.gov.au>.

[26] See Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026) at [132] and [175], in which these factors were considered in the context of using a facial recognition technology system to collect sensitive information to lessen or prevent a serious threat.

- collecting health information about an individual who is seriously injured, requires treatment and, due to their injuries, cannot give informed consent, on the basis that it is impracticable to obtain the individual's consent
- collecting sensitive information about a parent that is required to provide assistance to a child who may be at risk of physical or sexual abuse by the parent, on the basis that it would be unreasonable to obtain the parent's consent
- collecting sensitive information using a facial recognition system for the limited purpose of combatting very significant retail crime, violence, abuse and intimidation, in a security environment that poses unique challenges such as products on sale that can be readily accessed by individuals and used as a weapon (e.g. axes, screwdrivers).[27]

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

3.49 An APP entity may collect sensitive information if the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being, or may be engaged in, and
- reasonably believes that the collection is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).

3.50 This permitted general situation is intended to apply to an APP entity's internal investigations about activities within or related to the entity.[28] The focus is on the internal investigation with respect to its objective or outcome, for example, to form a view about a breach of an employment contract, or to make a report to police where indicated by the investigation. The nature of the 'appropriate action' is the investigation with a view to its objectives and its outcomes.[29] The 'appropriate action' is not the underlying methodology chosen to undertake this internal investigation.[30]

3.51 For guidance on 'reason to suspect', 'unlawful activity', 'misconduct' and 'serious' misconduct, see Chapter C (Permitted general situations).

---

[27] See Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026) at [161] and [175]. Note that OAIC, Facial recognition technology: a guide to assessing the privacy risks, OAIC website <https://www.oaic.gov.au>, will be updated to include a case study and further guidance on the Bunnings decision.

[28] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 67.

[29] Commissioner Initiated Investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025) ('Kmart') at [73]. This position is not settled given the Kmart determination is under review in the Administrative Review Tribunal. Entities should be aware that the information in this section reflects the determination subject to that review and will be updated should the outcome of the review change this position.

[30] See Commissioner Initiated Investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025) ('Kmart') at [69]–[81], in which the 'appropriate action' was 'to detect and prevent fraudulent returns by ascertaining whether an individual was seeking, or likely to be seeking, to fraudulently return a product they purported to have purchased from the respondent, in circumstances where they had not purchased the product'. The 'appropriate action' was *not* the underpinning methodology that the respondent used to undertake this internal investigation, such as the availability of a particular database and images. This position is not settled given the Kmart determination is under review in the Administrative Review Tribunal. Entities should be aware that the information in this section reflects the determination subject to that review and will be updated should the outcome of the review change this position.

3.52 The following factors are relevant to whether an APP entity reasonably believes the collection of sensitive information is necessary in order for the entity to take appropriate action to address suspected unlawful activity or serious misconduct:[31]

- the suitability of the proposed collection, including its efficacy in allowing the entity to take appropriate action in relation to the suspected unlawful activity or serious misconduct
- the alternatives available to the entity to take appropriate action in relation to the suspected unlawful activity or serious misconduct, including whether less privacy-intrusive alternatives are available
- whether the proposed collection is proportionate. This involves balancing the privacy impacts resulting from the collection of sensitive information against the benefits to be gained from doing so.

3.53 Examples of where this permitted general situation might apply are the collection of sensitive information by:

- an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities
- an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct.

Locating a person reported as missing

3.54 An APP entity may collect sensitive information if:

- the entity reasonably believes that the collection is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the collection complies with rules made by the Information Commissioner under s 16A(2) (s 16A(1), Item 3).

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

3.55 An APP entity may collect sensitive information if the collection is reasonably necessary to establish, exercise or defend a legal or equitable claim (s 16A(1), Item 4).

3.56 An example of where this permitted general situation might apply is an insurer collecting health information about an individual who has made an insurance compensation claim but is suspected of misrepresenting their claim or the extent of their injuries.[32]

[31] See Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026) at [132], in which these factors were considered in the context of using a facial recognition technology system to collect sensitive information to take appropriate action to address suspected unlawful activity or serious misconduct.

[32] N and Law Firm [2011] AICmrCN 8, Australasian Legal Information Institute website <www.austlii.edu.au>. See also B v Law Firm [2011] PrivCmrA 2 (3 May 2011), viewed 6 March 2013, Australasian Legal Information Institute website <www.austlii.edu.au>.

Reasonably necessary for a confidential alternative dispute resolution process

3.57 An APP entity may collect sensitive information if the collection is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

3.58 An example of where this permitted general situation might apply is an alternative dispute resolution practitioner making a record of a party recounting their version of events, where that account includes the disclosure of sensitive information about an individual who is directly or indirectly involved in the dispute. This permitted general situation will only apply where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

Necessary for a diplomatic or consular function or activity

3.59 An agency may collect sensitive information if the agency reasonably believes the collection is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

3.60 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions collects sensitive information about an individual who is overseas and in need of consular assistance because the individual is in distress, for example due to being detained or a victim of crime, going missing, or needing repatriation in the case of death or serious illness.

Necessary for certain Defence Force activities outside Australia

3.61 The Defence Force (as defined in s 6(1)) may collect sensitive information if it reasonably believes the collection to be necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

Collecting sensitive information where a permitted health situation exists

3.62 An organisation may collect sensitive information if a 'permitted health situation' exists in relation to the collection (APP 3.4(c)). This exception applies only to organisations, and not to agencies.

3.63 Section 16B lists two permitted health situations that relate to the collection of health information by an organisation. The two situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

Providing a health service

3.64 An organisation may collect health information about an individual if the health information is necessary to provide a health service to the individual, and either:

- the collection is required or authorised by or under an Australian law (other than the Privacy Act), or

- the health information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1)).

3.65 An example of where this permitted health situation might apply is where a participant in the My Health Record system collects health information included in a consumer's My Health Record as authorised by the My Health Records Act 2012.[33]

3.66 'Health information' is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

3.67 An organisation may collect health information about an individual if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
  - required by or under an Australian law (other than the Privacy Act)
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
  - in accordance with guidelines approved under s 95A (s 16B(2)).[34]

3.68 An example of where this permitted health situation might apply is an organisation conducting longitudinal research into heart disease and requiring health information about a large number of individuals from different data sources for research linkage. In this case, the collection must be required by an Australian law or carried out in accordance with the rules or guidelines referred to in s 16B(2).

3.69 'Health information' is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

Collecting sensitive information for an enforcement related activity

3.70 An enforcement body may collect sensitive information where:

- if the body is the Immigration Department,[35] the Department reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more

[33] See My Health Records Act 2012, ss 63, 64, 65, 66 and 68.

[34] See National Health and Medical Research Council (NHMRC), Guidelines Approved Under Section 95A of the Privacy Act 1988, NHMRC website <https://www.nhmrc.gov.au>.

[35] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958 and is discussed in Chapter B (Key concepts). This is now the Department of Home Affairs.

enforcement related activities conducted by, or on behalf of, the Department (APP 3.4(d)(i))

- for other enforcement bodies, the body reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more of the body's functions or activities (APP 3.4(d)(ii)).

3.71 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission,[36] the Integrity Commissioner,[37] the Immigration Department, Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

3.72 For an enforcement body to collect sensitive information using this exception, it must:

- for the Immigration Department, identify the 'enforcement related activities' it conducts or that are conducted on its behalf, and for other enforcement bodies, identify their 'functions or activities', and
- 'reasonably believe' that the collection is either 'reasonably necessary for' or 'directly related to' one or more of those functions or activities.

3.73 'Reasonably believes' is discussed in more detail in Chapter B (Key concepts). Identifying the 'functions or activities' of an agency is discussed above at paragraphs 3.14-3.17, while 'reasonably necessary for' and 'directly related to' are discussed above at paragraphs 3.23-3.30.

3.74 'Enforcement related activities' are defined in s 6(1) and discussed in Chapter B (Key concepts). Where applied to the Immigration Department, the activities could include assessing and enforcing compliance with visa and citizenship requirements, and detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship laws. Non-enforcement related activities of the Department do not fall within this exception.[38]

3.75 An example of where the Immigration Department may collect sensitive information from an individual using this exception is where it reasonably believes that the sensitive information directly relates to the function of investigating whether a person has breached an immigration law.

Collection of sensitive information by a non-profit organisation

3.76 A non-profit organisation may collect sensitive information if:

- the information relates to the activities of the organisation, and

[36] In July 2016, the former Australian Crime Commission and CrimTrac were merged to form the Australian Criminal Intelligence Commission.

[37] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[38] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 76.

- the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities (APP 3.4(e)).[39]

3.77 'Non-profit organisation' is defined in s 6(1) as an organisation 'that is a non-profit organisation; and that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes'. The term 'cultural purposes' includes both racial and ethnic purposes.

3.78 There are three criteria a non-profit organisation must meet to rely on this exception to collect sensitive information:

- Firstly, the non-profit organisation can rely on this exception only when collecting sensitive information for an activity that is undertaken for one of the specified purposes in the definition of 'non-profit organisation' (s 6(1)). An organisation conducting activities for some other purpose cannot rely on this exception to collect sensitive information for that purpose.
- Secondly, the sensitive information that is collected must 'relate' to the activity that is being conducted for a specified purpose. A clear relationship, assessed objectively, must exist between the information collected and that activity. For example, the information may relate to a fundraising activity undertaken by a non-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose.
- Thirdly, the sensitive information must relate solely to a member of the organisation, or an individual who has regular contact with the organisation in connection with its activities. Collection of sensitive information about a relative of a member of the organisation would not be covered unless the relative was also a member or person in regular contact with the non-profit organisation.

3.79 An example of where a non-profit organisation may be permitted to collect sensitive information is where a religious organisation collects information about the views of its members on religious or moral issues.

Collecting by lawful and fair means

3.80 An APP entity must collect personal information 'only by lawful and fair means' (APP 3.5). This requirement applies to all APP entities.

Collecting by lawful means

3.81 The term 'lawful' is not defined in the Privacy Act. It is lawful for an organisation to destroy or de-identify unsolicited personal information if it is not unlawful to do so. That is, if the destruction or de-identification is not criminal, illegal or prohibited or proscribed by law. Unlawful activity does not include breach of a contract.

3.82 Examples of collection that would not be lawful include:

- collecting in breach of legislation, for example:

[39] For general privacy guidance for not-for-profit organisations, see OAIC, Privacy for not-for-profits, including charities, OAIC website <https://www.oaic.gov.au>.

  - collecting via computer hacking[40]
  - collecting using telephone interception or a listening device except under the authority of a warrant[41]
  - requesting or requiring information in connection with, or for the purpose of, an act of discrimination[42]
- collecting by a means that would constitute a civil wrong, for example, by trespassing on private property or threatening damage to a person unless information is provided
- collecting information contrary to a court or tribunal order, for example, contrary to an injunction issued against the collector.

Collecting by fair means

3.83 The term 'fair' is not defined in the Privacy Act. The standard of what is 'fair' presents an open-textured and evaluative criterion against which collection by an entity is to be assessed.[43] What is 'fair' under APP 3.5 is to be determined having regard to the consideration of the text, context and purpose of the Privacy Act. When assessing whether a collection is by 'unfair' means for the purposes of APP 3.5, all the circumstances must be considered.[44] Consistent with a contextual approach,[45] the meaning of 'fair' is not fixed; the concept of 'fairness' should be adapted to changing circumstances viewed in context and in accordance with community values.[46]

3.84 A 'fair means' of collecting information includes one that does not involve intimidation or deception.[47] For example, collection may be by unfair means (some may also be unlawful) if it involves:

- deception, for example, wrongly claiming to be a police officer, doctor or trusted organisation, or
- misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information.

3.85 A 'fair means' of collection also extends to the obligation not to use means that are unreasonably intrusive.[48] For example, collection may be by unfair means (some may also be unlawful) if it involves:

---

[40] For example, Criminal Code Act 1995, Part 10.7.

[41] For example, Telecommunications (Interception) Act 1979 (Cth) s 7; Surveillance Devices Act 2004 (Cth) s 14.

[42] See for example, the Disability Discrimination Act 1992, s 30 and the Sex Discrimination Act 1984, s 27.

[43] See for example, Commissioner Initiated Investigation into Property Lovers Pty Ltd (Privacy) [2024] AICmr 249 (22 November 2024) at [46].

[44] 'LP' and The Westin Sydney (Privacy) [2017] AICmr 53 (7 June 2017) at [33]. See also Court Data Australia and Office of the Australian Information Commissioner [2025] ARTA 876 (28 May 2025) at [27] which states: 'The context in which the personal information is collected is important in determining whether the collection was by 'fair means''.

[45] The High Court has endorsed a contextual approach to statutory interpretation in *SZTAL v Minister for Immigration and Border Protection*, in which their Honours stated, 'The starting point for the ascertainment of the meaning of a statutory provision is the text of the statute whilst, at the same time, regard is had to its context and purpose. Context should be regarded at this first stage and not at some later stage and it should be regarded in its widest sense': see, e.g., *SZTAL v Minister for Immigration and Border Protection* (2017) 262 CLR 362, [14] (Kiefel CJ, Nettle and Gordon JJ).

[46] *R v Swaffield; Pavic v The Queen* [1998] HCA 1 [53] (Toohey, Gaudron and Gummow JJ), [131] (Kirby J).

[47] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

[48] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

- excessive collection of personal information
- collecting personal information of an unnecessarily sensitive nature
- collecting personal information from too many individuals, or
- collecting in a way that unreasonably interferes with an individual's daily life, such as by telephoning an individual in the middle of the night.

3.86 There may be other means of collection which are not fair, yet do not fit within the meaning of intimidation, deception, or unreasonable intrusion.

3.87 Following are examples of factors that may influence whether a collection is by fair means. It is important to consider a range of factors and all surrounding circumstances when determining whether a collection is by fair means:

- **Whether the individual is aware of their personal information being collected**

  The level of transparency that has been provided to individuals will be relevant here. For example, whether the individual is aware of the collection of their personal information from the entity's APP 1 privacy policy, terms of service and APP 5 collection notices.[49]

  It would usually be unfair to collect personal information covertly without the knowledge of the individual. However, this may be a fair means of collection if undertaken in connection with a fraud investigation.

  By way of further example, it may be unfair to collect from a document discarded by accident on a street, or from an electronic device which is lost or left unattended.

  An APP entity should not consider collection to be fair simply because they have provided individuals with notice of a proposed collection of personal information.

- **Whether the individual would reasonably expect their personal information to be collected and used in this manner/for this purpose**

  This is to be determined objectively, having regard to what a reasonable person, who is properly informed, would expect in the circumstances.[50] Factors that could inform an individual's reasonable expectations include the purpose for which the personal information was originally made available, what was communicated in privacy policies, collection notices, and other information on online platforms such as terms and conditions of service. A reasonable person might not, for example, expect their personal information to be collected for a purpose unrelated to what they have been informed of.

  Where personal information is publicly available on the internet, that does not allow it to be collected and used in whatever way the APP entity chooses without regard to the knowledge and reasonable expectations of the person whose information it concerns.[51]

---

[49] For guidance on the APP 1 privacy policy requirement, see Chapter 1 (APP 1), OAIC website <https://www.oaic.gov.au>.. For guidance on the APP 5 notification of collection requirement, see Chapter 5(APP 5), OAIC website <https://www.oaic.gov.au>.

[50] For further information, see the definition of 'Reasonable, reasonably' in OAIC, Chapter B: Key Concepts, OAIC website <https://www.oaic.gov.au>.

[51] Court Data Australia and Office of the Australian Information Commissioner [2025] ARTA 876 (28 May 2025) at [41]. Collection of personal information from publicly available sources such as on the internet must be done in accordance with APP 3 or APP 4, and once collected is subject to the APPs.

- **Whether the individual's choice is being distorted, manipulated or undermined, for example through poorly designed or misused 'online choice architecture'**[52]

  The way that information is presented and choices are structured ('online choice architecture') plays an important role in shaping individuals' decision-making and behaviour online.[53] Poor online choice architecture practices include 'harmful nudges and sludge', 'confirmshaming', 'biased framing', 'bundled consent' and 'default settings'.[54] Such practices can steer individuals towards making choices that are otherwise misaligned with their preferences or choices they would normally voluntarily make. They may also force individuals to take multiple steps to find a privacy policy, log out or delete their account, or present them with repetitive prompts aimed at frustrating them and ultimately pushing them to give up more of their personal information than they would like.[55]

  An individual's choice can also be undermined due to being provided with limited options. For example, where they cannot choose which platform to use to access a service and are not provided with alternative pathways.[56]

- **What the risk of harm would be to individuals as a result of the collection**

  The risk of harm increases with the sensitivity of the information. Inappropriate collection and handling of personal information, including sensitive information, can have adverse consequences for an individual or those associated with the individual.

  For example, when considering collecting biometric templates and biometric information via facial recognition technology, an APP entity should consider if this would lead to unjustified adverse effects, such as unjust discrimination.[57]

  The risk of harm also increases with the amount of personal information collected. Over-collection can increase risks for the security of personal information.

- **Whether the individual is in, or is perceived to be in, a vulnerable or at-risk situation**

---

[52] In Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [111]-[119], the Commissioner considered the design, structure and way information is conveyed on the relevant online form as a factor in assessing whether collection was by fair means. This factor is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that the information under this heading reflects the determination subject to that review and will be updated should the outcome of the review change this position.

[53] Information Commissioner's Office and Competition & Markets Authority (2024) *Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information* [PDF], United Kingdom Digital Regulation Cooperation Forum, at page 4.

[54] Information Commissioner's Office and Competition & Markets Authority (2024) *Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information* [PDF], United Kingdom Digital Regulation Cooperation Forum, at page 6.

[55] See OAIC, GPEN Sweep finds majority of websites and mobile apps use deceptive design to influence privacy choices, OAIC website <https://www.oaic.gov.au>.

[56] In Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [110], the Commissioner considered as relevant context how an individual wanting to apply for a property cannot choose which rental platform to use – this choice is made by the real estate agent – and at times individuals have been refused any other method of applying. This consideration is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that the example in this footnote reflects the determination subject to that review and will be updated should the outcome of the review change this position.

[57] For further guidance see OAIC, Facial recognition technology: a guide to assessing the privacy risks, OAIC website <https://www.oaic.gov.au>.

This includes whether the collection is seeking to capitalise on the vulnerability, or perceived vulnerability, of an individual.

Vulnerability can be defined as heightened susceptibility to harm. Factors that may put an individual at higher risk of experiencing negative outcomes include age, language barriers, literacy barriers (including digital literacy barriers), cognitive impairment, remote location, financial distress, family or domestic violence, disability and health conditions.[58]

'At-risk' groups could include children, older people, people from culturally and linguistically diverse communities, and people lacking digital resources such as appropriate device and internet access.[59]

For example, it may be unfair to collect from an individual who is traumatised, in a state of shock or intoxicated.

It may further be unfair to collect in a way that disrespects cultural differences.

An individual may also be vulnerable due to inherent and significant power imbalances. For example, the power imbalance in the rental property market results in individuals feeling that they have no choice but to engage with and submit personal information to rental platforms, even if they are not comfortable doing so, for fear that their applications may be rejected.[60]

3.88 Where a collection of personal information is by unfair means, it may also be unlawful and/or in breach of the requirement to only collect personal information (including sensitive information) that is 'reasonably necessary' (APP 3.1, 3.2 and 3.3).

Collecting directly from the individual

3.89 APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual', unless one of the following exceptions apply:

- for all APP entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual
- for agencies, the individual consents to the personal information being collected from someone other than the individual
- for agencies, the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual.

[58] Witzleb N, Paterson M, Wilson-Otto J, Tolkin-Rosen G and Marks M (2020), 'Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioned by the Office of the Australian Information Commissioner (OAIC)', *OAIC*, at 139–149.

[59] Witzleb N, Paterson M, Wilson-Otto J, Tolkin-Rosen G and Marks M (2020), 'Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioned by the Office of the Australian Information Commissioner (OAIC)', *OAIC*, at 139–149.

[60] Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026) at [110], [121] and [122]. See [110] where the Commissioner noted in this investigation that 'there is an inherent and significant power imbalance in the rental property market which favours real estate agents, property managers and landlords'. This position is not settled given the IRE Pty Ltd determination is under review in the Administrative Review Tribunal. Entities should be aware that this paragraph reflects the determination subject to that review and will be updated should the outcome of the review change this position.

Unreasonable or impracticable to collect directly from the individual

3.90 Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case. Considerations that may be relevant include:

- whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
- the sensitivity of the personal information being collected
- whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected
- any privacy risk if the information is collected from another source
- the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.

Example: An APP entity would not be able to rely on this exception where it collects personal information about individuals from third parties such as data brokers for data enrichment purposes, where the APP entity considers it inconvenient to collect directly from those individuals. In this situation, the APP entity must collect the personal information directly from the individual, in accordance with APP 3.1, 3.2, 3.3 and 3.5.

3.91 The following are given as examples of when it may be unreasonable or impracticable to collect personal information only from the individual concerned:

- collection by a law enforcement agency of personal information about an individual who is under investigation, where the collection may jeopardise the investigation if the personal information is collected only from that individual[61]
- if a legal or official document that is mailed to an individual is returned to the sender, the individual's current contact details may need to be obtained from another source.

Consent by the individual — for agencies only

3.92 The term 'consent' is discussed at paragraph 3.32 above and in Chapter B (Key concepts). As noted in those sections, consent can be express or implied, and must be voluntary, informed, current and specific, and the individual must have capacity to consent.

3.93 An example of where an agency might collect personal information from someone other than the individual is where an individual consents to one agency disclosing their personal information (such as contact details) to the other agency.

[61] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

Required or authorised by law or a court or tribunal order — for agencies only

3.94 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts). It is a common feature of legislation that an agency, for the purpose of performing a function or exercising a power, is authorised to require a person or body to provide personal information.

3.95 An example of where collection by an agency from someone other than the individual concerned might be required or authorised by law is s 44 of the Privacy Act, which provides that the Information Commissioner may issue a notice to a person requiring them to provide specified information for the purpose of an investigation under the Act (and that information may include personal information).

Collecting personal information from a related body corporate

3.96 Section 13B(1)(a) provides that the collection of personal information about an individual (other than sensitive information) by a body corporate from a related body corporate is generally not 'an interference with the privacy of an individual' (interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to collection of information from related bodies corporate and not to other corporate relationships such as a franchise or joint-venture relationship.[62]

3.97 The effect of s 13B(1)(a) is that an APP entity may collect personal information (other than sensitive information) from a related body corporate without satisfying the requirements of APP 3.1 or 3.2 (see paragraphs 3.12-3.30 above). However, s 13B(1A) sets out some exceptions to this, including where the related body corporate is not an organisation.

[62] Section 6(8) states 'for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001'.