Australian Government

Office of the Australian Information Commissioner

Guide to the *Privacy (Persons Reported as Missing) Rule 2014*

March 2014

Contents

Background

The Australian Privacy Principles (APPs)[1] are legally binding principles that set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. They apply to most Australian Government agencies[2] and some private sector organisations — collectively referred to as APP entities. Further guidance about the APPs is contained in the OAIC's *Australian Privacy Principle guidelines*.[3]

The information handling requirements imposed by some APPs do not apply if a 'permitted general situation' (PGS) exists. The PGSs are set out in subsection 16A(1) of the Privacy Act.[4]

The existence of a permitted general situation (PGS) provides an exception to the general prohibition against an APP entity collecting sensitive information about an individual (APP 3.4(b)), and the use and disclosure of personal information for a secondary purpose (APP 6.2(c)).

Item 3 of the table in subsection 16A(1) details a PGS which relates to the collection, use or disclosure of personal information to locate a person who has been reported as missing (PGS 3). It states:

> An APP entity is permitted to collect, use or disclose personal information if:
>
> (a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and
>
> (b) the collection, use or disclosure complies with the rules made under subsection (2).

Subsection 16A(2) states:

> The Commissioner may, by legislative instrument, make rules relating to the collection, use or disclosure of personal information that apply for the purposes of item 3 of the table in subsection (1).

The *Privacy (Persons Reported as Missing) Rule 2014* is a legislative instrument made under subsection 16A(2) of the Privacy Act and applies for the purposes of PGS 3.

Outline of this guide

This guide is to assist APP entities and others to understand and use the Privacy (Persons reported as Missing) Rule 2014 (the Rule). In particular, the guide outlines:

- the mandatory requirements in PGS 3 and the Rule — generally indicated by 'must' or 'is required to'

[1] See the *Privacy Act 1988*, Schedule 1, Comlaw website <www.comlaw.gov.au>, or the OAIC's *Privacy Fact Sheet 17: Australian Privacy Principles*, OAIC website <www.oaic.gov.au>.
[2] The APPs also apply to Norfolk Island agencies.
[3] See OAIC website <www.oaic.gov.au>.
[4] Guidance about the Permitted General Situations is in Chapter C, APP guidelines.

- the Information Commissioner's interpretation of PGS 3 and the Rule, including the matters that the Commissioner may take into account when exercising functions and powers relating to the APPs — generally indicated by 'should' or 'is expected to'
- examples that explain how PGS 3 and the Rule may apply — generally indicated by 'for example' or 'examples include'. Any examples given are not intended to be definitive or exhaustive of how an entity may comply with the mandatory requirements, and an entity's compliance will depend on the particular circumstances
- good privacy practice to supplement minimum compliance with the mandatory requirements in PGS 3 and the Rule — generally indicated by 'could'.

This guide is not legally binding and does not constitute legal advice about how an APP entity must or should comply with PGS 3 and the Rule in particular circumstances. An entity may wish to seek independent legal advice where appropriate.

Who should use this guide?

The Rule and this guide may be relevant to three types of bodies:

- an APP entity[5] that seeks to use or disclose personal information (including sensitive information) about a person reported as missing, in response to a request from a locating body (see Key concepts for more information about 'locating bodies')
- a locating body that is an APP entity and seeks to collect sensitive information about a person reported as missing
- a locating body that is not an APP entity and seeks to collect sensitive information about a person reported as missing. Locating bodies that are not APP entities are not covered by the Rule or the APPs. However, being aware of the requirements of the Rule will ensure that locating bodies frame their requests for information in a way that assists APP entities to comply with the Rule in responding to the request.

Requirements and scope of PGS 3 and the Rule

Requirements of PGS 3 and the Rule

PGS 3 applies in relation to the collection of sensitive information (APP 3) and the use or disclosure of personal information for a secondary purpose (APP 6). The Rule sets out when, under PGS 3:

- an APP entity may collect sensitive information about a person reported as missing
- an APP entity may use or disclose personal information about a person reported as missing.

[5] 'APP entity' is defined in s 6(1) of the Privacy Act as an 'agency or organisation'. 'Agency' is defined in s 6(1) and 'organisation' is defined in s 6C.

Importantly:

- only an APP entity that is a locating body may collect sensitive information about a person reported as missing
- an APP entity may only use or disclose personal information about a person reported as missing in response to a request from a locating body
- personal information (including sensitive information) may only be collected, used or disclosed if the APP entity reasonable believes that the collection, use or disclosure:
    - is reasonably necessary to assist the locating body to locate the person reported as missing, and
    - would not pose a serious threat to the life, health or safety of any individual
- the personal information that is collected, used or disclosed must be limited to that which is reasonably necessary to make contact with, or offer proof of life of, the person reported as missing
- personal information may only be used or disclosed where:
    - it is unreasonable or impracticable to obtain the consent of the person reported as missing
    - the use or disclosure is not contrary to any wish expressed by the person reported as missing of which the APP entity is aware.

Scope of PGS 3 and the Rule

Although PGS 3 and the Rule permit the collection of sensitive information, and the use or disclosure of personal information in certain circumstances (see above), it is important to be aware of the limited scope of PGS 3 and the Rule. Under PGS 3 and the Rule, an APP entity:

- may only collect sensitive information, or use or disclose personal information, to locate the person reported as missing. PGS 3 and the Rule do not permit sensitive information to be collected, or personal information to be used or disclosed, after the person reported as missing has been found. An APP entity would need to rely on another exception to APP 3.3 to collect sensitive information, or APP 6.1 to use or disclose personal information about an individual who has been located[6]
- is permitted, but not required, to collect the sensitive information, and use or disclose the personal information, of a person reported as missing. The Rule does not affect the operation of other laws that deal with the collection, use and disclosure of the personal information of a person reported as missing, for example, secrecy or confidentiality provisions which may prohibit the disclosure of certain types of personal information
- is not permitted to use or disclose a government related identifier

[6] See OAIC, *APP guidelines*, OAIC website <www.oaic.gov.au>.

- is only permitted to collect sensitive information or use or disclose personal information about the person reported as missing. Where an APP entity wishes to collect, use or disclose another individual's personal information (including sensitive information) to locate a person reported as missing, it should seek the consent of that individual, or consider whether another exception to APPs 3 or 6 applies to the proposed collection, use or disclosure
- must comply with the APPs in handling any personal information collected, used or disclosed. For example, APP 10 (quality of personal information) and APP 11 (security of personal information).

The Rule only applies to the collection of sensitive information, and the use or disclosure of personal information (including sensitive information) under the exception in PGS 3. The APP guidelines contain guidance on when an APP entity (including an APP entity that is a locating body) may collect, use or disclose personal information (including sensitive information) in other circumstances.

The Rule only applies to APP entities. Where an entity (other than an APP entity) collects sensitive information, or uses or discloses personal information in circumstances covered by PGS 3 and the Rule, the Commissioner encourages compliance with the Rule and the APPs more generally as a best practice approach to privacy, subject to any specific privacy requirements the entity may already be subject to.

Guidance for a locating body

Making requests to an APP entity for personal information about a person reported as missing

An APP entity may only use or disclose personal information under the Rule if the use or disclosure is in response to a request from a locating body.

Processing requests from locating bodies may be resource intensive for an APP entity. A locating body could endeavour to make requests in a way that meets the needs of the APP entity.

For example, a locating body could consider making requests for personal information using a template form, which could include information to assist an APP entity to decide whether it can use or disclose the personal information as requested by the locating body under the Rule. For example, the locating body could provide information about:

- the type of proof of life or contact information that the locating body reasonably believes would assist it to locate the person reported as missing, where practicable
- why the locating body reasonably believes that the personal information is reasonably necessary to assist it to locate the person reported as missing
- any factors relevant to the APP entity deciding whether it is unreasonable or impracticable for the APP entity to obtain consent, such as where the request is urgent.

Where a locating body makes regular requests for personal information to an APP entity, it may be useful for both parties to discuss the particular needs of that APP entity in relation to the form in which requests are made.

Although a locating body may need to provide some personal information as part of its request (for example, to allow the APP entity to locate relevant information in its records about the individual), the locating body should ensure that it minimises the amount of personal information that it discloses as part of its request.

Collecting sensitive information under the Rule

The Rule permits a locating body that is an APP entity to collect sensitive information to assist it to locate a person reported as missing in certain circumstances.[7] A locating body that is not an APP entity is not required to comply with the APPs and the Rule (see above). However, where a non-APP entity locating body collects personal information (including sensitive information), the Commissioner encourages compliance with the Rule and the APPs more generally, as a best practice approach to privacy , subject to any specific privacy requirements the entity may already be subject to.

An APP entity must satisfy a four-step test to determine whether it is permitted to collect sensitive information under the Rule.

- Is it a locating body? (s 5(1)(a) of the Rule. See Key concepts for a discussion of 'locating body')
- If so, does it reasonably believe that the collection of the particular sensitive information is reasonably necessary to assist it to locate the person reported as missing? (s 5(1)(b) of the Rule. See Key concepts for a discussion of 'reasonably believe' and 'reasonably necessary')
- Is the sensitive information reasonably necessary to make contact with, or offer proof of life of, the person reported as missing? (s 5(1)(c) of the Rule. See Key concepts for a discussion of 'contact or proof of life information')
- Would the collection of the sensitive information pose a serious threat to the life, health or safety of any individual? (s 5(1)(d) of the Rule. See Key concepts for a discussion of 'serious threat to the life, health or safety of any individual')

Handling sensitive information after collection

A locating body that is an APP entity must handle the personal information (including sensitive information) that it holds in accordance with the APPs. Two important obligations are discussed below.

Disclosing the sensitive information of the person reported as missing

APP 6 requires an APP entity to only use or disclose personal information (including sensitive information) it holds for the purpose for which it was collected, unless the

[7] APP 3 sets out when an APP entity may collect personal information (including sensitive information) in other circumstances.

individual whose personal information has been collected has consented to the use or disclosure, or where an exception under APP 6.2 or 6.3 applies. Where a locating body that is an APP entity collects sensitive information under the Rule, it must only use or disclose it for the purpose of locating the person reported as missing, or a directly related purpose, unless another exception applies.

Generally, this would not include disclosure to the individual who reported the person as missing to the locating body, unless the person reported as missing has been located and consents to such disclosure (APP 6.1(a)). The locating body should allow the person reported as missing to indicate to the locating body how much personal information (if any) they wish to be disclosed to the individual that reported them as missing.

Where the person reported as missing has not been located, the locating body should not disclose any personal information collected from an APP entity to the individual that reported the person as missing, unless an exception in APP 6.2 or 6.3 applies.

The existence of an exception does not compel the locating body to use or disclose the personal information. Before using or disclosing the personal information of a person reported as missing, the locating body could consider the known wishes of the individual.

Retaining the sensitive information of the person reported as missing

APP 11.2 requires that where an APP entity holds personal information (including sensitive information) that it no longer needs for any purpose permitted by the APPs, it should take reasonable steps to destroy or de-identify the information, unless the information is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain the information. See APP 11 and Chapter 11 (APP 11) of the OAIC's APP guidelines for further information.[8]

Guidance for an APP entity

Receiving a request from a locating body for personal information of a person reported as missing

Processing requests for personal information under the Rule may be resource intensive for an APP entity. An APP entity that anticipates receiving a large number of requests could consider setting up processes to handle the processing of requests. Where an APP entity receives regular requests for personal information from a locating body, it may be useful for both parties to discuss the particular needs of the entity in relation to the form in which requests are made.

When processing requests for personal information under the Rule, an APP entity could also take account of the timelines that the locating body is working to, and whether the locating body has requested acknowledgement of receipt of the request.

[8] OAIC, *APP guidelines: Chapter 11 (APP 11)*, OAIC website <www.oaic.gov.au>.

Collecting personal information from a locating body under the APPs

Where an APP entity receives a request from a locating body about a person reported as missing, it is likely that the APP entity will have to collect personal information about that person, in order to identify the person in its records and respond to the locating body's request.[9]

An APP entity may collect personal information (other than sensitive information) where it is reasonably necessary for (or for agencies, directly related to) one or more of the entity's functions or activities. One of the lawful functions or activities of an APP entity is assisting a locating body to locate a person reported as missing under PGS 3. Personal information that is reasonably necessary for (or directly related to) that function or activity is likely to be limited to information that enables the APP entity to identify the individual in its records.

APP entities will still need to comply with other APPs in relation to the personal information it collects from a locating body of the person reported as missing. For example, APP 11.2 requires that where an APP entity holds personal information (including sensitive information) that it no longer needs for any purpose permitted by the APPs, it should take reasonable steps to destroy or de-identify the information, unless the information is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain the information. See APP 11 and Chapter 11 (APP 11) of the OAIC's APP guidelines for further information.[10]

Using or disclosing personal information in response to a request from a locating body

When an APP entity has received a request for personal information from a locating body, it must satisfy a five-step test to determine whether a particular use or disclosure of personal information is permitted under the Rule. This includes personal information collected from the locating body as part of the request, and additional personal information it holds about the person reported as missing.

- Does the APP entity reasonably believe that the use or disclosure of the particular personal information is reasonably necessary to assist the locating body to locate the person reported as missing? (s 6(1)(b) of the Rule. See Key concepts for a discussion of 'reasonably believe' and 'reasonably necessary')
- Is it unreasonable or impracticable to obtain of the consent of the person reported as missing to the use or disclosure of the information? (s 6(1)(d) of the Rule. See discussion of 'consent', below)
- Is the personal information reasonably necessary to make contact with, or offer proof of life of, the person reported as missing? (s 6(1)(e) of the Rule. See Key concepts for a discussion of contact or proof of life information)

[9] The Rule only relates to the collection of sensitive information by a locating body.
[10] OAIC, *APP guidelines: Chapter 11 (APP 11)*, OAIC website <www.oaic.gov.au>.

- Is the use or disclosure contrary to any wish expressed by the person reported as missing of which the APP entity is aware? (s 6(1)(f) of the Rule. See discussion of the known wishes of the individual, below)
- Would the use or disclosure of the personal information pose a serious threat to the life, health or safety of any individual? (s 6(1)(g) of the Rule. See Key concepts for a discussion of 'serious threat to the life, health or safety of any individual').

The Rule only permits the APP entity to disclose personal information to the requesting locating body (s 6(1)(c)). If the APP entity wishes to disclose the personal information to another individual or entity, it may only do so in accordance with APP 6.1.

Consent

The Rule requires an APP entity to only use or disclose the personal information of a person reported as missing where:

- it is not reasonable or practicable to seek the consent of the person reported as missing to the use or disclosure of their personal information, and
- the use or disclosure is not contrary to any known wishes of that individual.

The requirement to consider whether obtaining consent is reasonable or practicable recognises that:

- the whereabouts of an individual only needs to be unknown to the locating body in order for that individual to be considered a 'person reported as missing' under the Rule.[11] If the APP entity knows the whereabouts of the person reported as missing, it may be reasonable and practicable to obtain their consent
- the person reported as missing may have exercised their free choice to disassociate themselves from friends and family for legitimate reasons, including removing themselves from harmful environments.

This approach is consistent with the emphasis of the Privacy Act of the importance of an individual's control over how their personal information is handled.

Consent is defined in the Privacy Act as 'express consent or implied consent' (s 6(1)). An APP entity may use or disclose personal information if the individual consents to that use or disclosure (APP 6.1(a)). Further guidance about the elements of consent, including assessing an individual's capacity to consent, can be found in the OAIC's APP guidelines (Chapter B (Key concepts) and Chapter 6 (APP 6)).

[11] 'Person reported as missing' is defined in s 4(2) of the Rule as an individual:
(a) who has been reported as missing to a locating body
(b) whose whereabouts are unknown to the locating body, and
(c) who is being sought by the locating body because there are serious concerns for their safety and/or welfare or for the purpose of re-uniting them with their family

but does not include an individual who is being sought:
(d) in relation to legal matters, including but not limited to, debt, maintenance, support proceedings, wills, child custody, divorce or investigations into suspected criminal activity of the individual, or
(e) for the purpose of genealogical research.

Unreasonable or impracticable to obtain consent

An APP entity should be able to point to one or more clear reasons that make it unreasonable or impracticable to obtain an individual's consent. Relevant considerations may include:

- the ability to contact the individual to obtain consent. For example, it may be impracticable to obtain consent if the individual's location is unknown after reasonable enquiries have been made, or if they cannot be contacted for another reason
- the potential consequences for the individual associated with any delay to the disclosure of the information to the locating body. For example, where there is concern for the safety and welfare of the person reported as missing, the urgency of the situation and level of potential threat may require use or disclosure before it is possible to seek consent
- the possible adverse consequences for an individual if their consent is not obtained before the use or disclosure — it may be more difficult for an entity to establish that it was unreasonable or impracticable to obtain the individual's consent as the risk of adversity increases
- the capacity of the person reported as missing to give consent. For example, it may be unreasonable or impracticable to obtain consent where the person reported as missing is incapable of communicating consent because of their physical state, their psychological state, or their age. Capacity is discussed as part of 'consent' in Chapter B (Key concepts) of the OAIC's APP guidelines.
- the inconvenience, time and cost involved — however, an entity is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Known wishes of the individual

An APP entity must not use or disclose the personal information of a person reported as missing if the use or disclosure is contrary to any wish expressed by the person reported as missing of which the APP entity is aware. The wishes of the person reported as missing need not have been communicated in writing.

Examples of when an APP entity may be aware of an individual's wishes will depend on the circumstances, but will include where the individual has specifically requested that the APP entity does not use or disclose their personal information.

Written note of disclosure

If an APP entity discloses personal information in accordance with the Rule, the entity must make a written note of the disclosure (subsection 6(2)). On each occasion that an APP entity discloses the personal information of a person reported as missing, a note

(either electronic or hard copy) of the disclosure must be included on that individual's record.

The APP entity could include the following details in that note:

- the date of the disclosure
- details of the personal information that was disclosed
- which locating body the information was disclosed to
- the basis for the entity's 'reasonable belief' that the information was reasonably necessary to assist to locate the person reported as missing. This will help the entity assure itself that the disclosure is in accordance with the Rule, and it may be a useful reference if the entity later needs to justify its reasonable belief.

This requirement does not apply where a law prohibits the APP entity from making such a record.

Key concepts

This section outlines some key words and phrases that are defined or used in PGS 3 and the Rule.

Contact or proof of life information

The Rule specifies that the sensitive information that is collected, or the personal information that is used or disclosed must be limited to the extent reasonably necessary to make contact with, or to offer proof of life of, the person reported as missing.

This limitation recognises that the purpose of the collection, use or disclosure under the exception in PGS 3 and the Rule is to assist a locating body to locate a person reported as missing. The personal information that is handled under PGS 3 and the Rule should be limited to that which is necessary to achieve this purpose. An APP entity should be mindful of this purpose when assessing whether the personal information is reasonably necessary to make contact with, or to offer proof of life of, the individual. In particular, an APP entity and/or locating body should consider whether the personal information is likely to practically assist a locating body to locate the person reported as missing. The information may not, on its own, lead to the location of the individual, however it may provide the locating body with valuable knowledge, for example, the State or Territory that the individual is believed to be currently or recently resident in, or whether there is a record of the individual's entry to or exit from Australia.

Examples of personal information that is likely to be reasonably necessary to make contact with, or to offer proof of life, of the person reported as missing will depend on the circumstances, but may include:

- the last known address or contact details of the individual, including a telephone number or email address

- photographic identification (however, an APP entity is not permitted to use or disclose a government related identifier under the Rule. Any copy of the photographic identification of a person reported as missing must not contain a government related identifier of that individual, such as a driver licence number or passport number, unless permitted under APP 9)
- bank or utility bills
- record of entry to or exit from Australia
- evidence of recent contact with an APP entity
- the presence of the individual on a list of survivors from a particular disaster or incident.

Locating body

Only an APP entity that is a locating body may collect sensitive information under the Rule. An APP entity may only use or disclose personal information under the Rule if it is in response to a request from a locating body.

The term 'locating body' is defined in the Rule. A 'locating body' means:

- the Australian Federal Police
- a police force or service of a State or Territory
- the Salvation Army Family Tracing Service
- the Australian Red Cross Tracing Service
- International Social Service Australia
- a Link-Up Service of a State or Territory
- Department of Foreign Affairs and Trade.

The locating bodies are the key entities involved in locating persons reported as missing in Australia, or Australians reported as missing overseas. By listing these entities in the Rule, the OAIC does not endorse the information handling practices or searching processes undertaken by these entities, but seeks to provide clarity to APP entities that wish to collect sensitive information or use or disclose personal information in accordance with this Rule.

In general terms, these locating bodies have the following characteristics in common:

- They have acceptance as an authority for investigating or searching for persons reported as missing by the community of search bodies and support groups for family and friends of missing persons.
- Their investigations into or searches for a person reported as missing are triggered by a concern for the person's safety and wellbeing, or for the purpose of reuniting the person with their family.

- They have information handling policies that require that the locating body does not disclose information about the whereabouts of a person reported as missing to another individual or entity, without the consent of the person reported as missing.

It is open to the OAIC to reconsider an entity's status as a locating body under the Rules.

Person reported as missing

The Rule regulates how an APP entity may collect sensitive information, or use or disclose personal information, where the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist a locating body to locate a 'person reported as missing'.

A person reported as missing is defined in the Rule to mean an individual:

(a) who has been reported as missing to a locating body, and
(b) whose whereabouts are unknown to the locating body
(c) who is being sought by the locating body because there are serious concerns for their safety and/or welfare or for the purpose of re-uniting them with their the family

but does not include an individual who is being sought:

(d) in relation to legal matters, including but not limited to, debt, maintenance, support proceedings, wills, child custody, divorce or investigations into suspected criminal activity of the individual, or
(e) for the purpose of genealogical research.

There are a number of elements to this definition that must be satisfied for an individual to be considered as a 'person reported as missing' for the purposes of the Rule:

- the individual must have been reported as missing to a locating body. The report may be made to any locating body. An official missing person report to a police force of a State or Territory is not required for the purposes of the Rule (although, as a locating body, the existence of a report to a police force of a State or Territory may satisfy the definition of 'person reported as missing')
- the individual's whereabouts must be unknown to the locating body who receives the report. Another individual or entity may know the whereabouts of the individual, however this does not mean that the individual is not a 'person reported as missing'
- the individual must be sought because there are serious concerns for their safety and welfare or for the purpose of re-uniting them with their family. The terms 'family' and 'child' (used in the definition of 'family') are defined in the Rule
- the individual must not be sought in relation to a legal matter or for the purpose of genealogical research. These matters are excluded because the Commissioner considers them to be outside of the scope of PGS 3. An APP entity may be able to rely on other exceptions to APP 3 and APP 6 to collect, use or disclose personal information for these purposes.

Reasonable, Reasonably[12]

A 'reasonableness' test is included in several sections of the Rule. An APP entity must form a 'reasonable belief' that the collection, use or disclosure is 'reasonably necessary'. 'Reasonable belief' and 'reasonably necessary' are discussed further below.

'Reasonable' and 'reasonably' are not defined in the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.[13] It is the responsibility of an APP entity to be able to justify that its conduct was reasonable. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person';[14] it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[15] As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

Reasonably believes[16]

The Rule requires an APP entity to have a 'reasonable belief' that the collection, use or disclosure is reasonably necessary to assist a locating body to locate a person reported as missing.

The phrase 'reasonable belief' is to be applied in the same manner as 'reasonable' and 'reasonably'. That is, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. The requirement for a reasonable belief precludes arbitrary action, but may still leave something to surmise or conjecture.[17] It is the responsibility of an entity to be able to justify its reasonable belief.

Reasonably necessary[18]

An APP entity may only use or disclose personal information about a person reported as missing if it is 'reasonably necessary' to assist a locating body to locate the individual. The type of personal information that may be collected, used or disclosed under the Rule is

[12] Discussion of the terms 'reasonable' and 'reasonably' in this guide comes from the OAIC's *APP guidelines: Chapter B (Key concepts)*, OAIC website <www.oaic.gov.au>.
[13] For example, *Jones v Bartlett* [2000] HCA 56 [57] – [58] (Gleeson CJ); *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20 [12] (Mason, Wilson and Dawson JJ).
[14] *George v Rockett* (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ).
[15] *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).
[16] Discussion of the term 'reasonable belief' in this Guide comes from the OAIC's *APP guidelines: Chapter B (Key concepts)*, OAIC website <www.oaic.gov.au>.
[17] *George v Rockett* (1990) 170 CLR 104 at 112, 116.
[18] Discussion of the term 'reasonably necessary' in this guide comes from the OAIC's *APP guidelines: Chapter B (Key concepts)*, OAIC website <www.oaic.gov.au>.

limited to information that is 'reasonably necessary' to make contact with, or offer proof of life of, the person reported as missing.

The term 'reasonable' is discussed above. 'Necessary' is not defined in the Privacy Act. The High Court of Australia has noted that 'there is, in Australia, a long history of judicial and legislative use of the term 'necessary', not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[19] However, in the context of the Rule, it would not be sufficient if the collection, use or disclosure is merely helpful, desirable or convenient.

The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

The test must be applied in a practical sense. For example, if an APP entity cannot in practice effectively assist a locating body to locate the person reported as missing without using or disclosing the individual's personal information, the use or disclosure would usually be considered reasonably necessary. However, a collection, use or disclosure of personal information will not usually be considered reasonably necessary if there are reasonable alternatives available.

Serious threat to the life, health or safety of any individual[20]

An APP entity must not collect, use or disclose personal information about an individual if the APP entity reasonably believes that the collection, use or disclosure would pose a serious threat to the life, health or safety of any individual.

The threat may be to the person reported as missing or to another person. It may also be a threat of serious harm to an unspecified individual, such as a threat to inflict harm randomly.

A 'serious' threat is one that poses a significant danger to an individual or individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant. A threat that may have dire consequences but is highly unlikely to occur would not normally constitute a serious threat. On the other hand, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat.

A serious threat to life, health or safety can include a threat to an individual's physical or mental health and safety. It could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The permitted general situation would not ordinarily extend to a threat to an individual's finances or reputation.

[19] *Mulholland v Australian Electoral Commissioner* [2004] HCA 41 [39] (Gleeson CJ).

[20] Discussion of 'serious threat to the life, health or safety of any individual' in this guide comes from the OAIC's *APP guidelines: Chapter C (Permitted general situations)*, OAIC website <www.oaic.gov.au>.