Chapter C — Permitted general situations

Version 1.0, February 2014

What are permitted general situations?

C.1 The information handling requirements imposed by some APPs do not apply if a 'permitted general situation' exists. This exception applies in relation to the collection of sensitive information (APP 3), the use or disclosure of personal information (APPs 6 and 8) and the use or disclosure of a government related identifier (APP 9). It is nevertheless open to an APP entity to comply with the APP requirements even though an exception applies.

C.2 There are seven permitted general situations listed in s 16A:

- lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d))
- taking appropriate action in relation to suspected unlawful activity or serious misconduct (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d))
- locating a person reported as missing (see APPs 3.4(c), 6.2(c) and 8.2(d))
- asserting a legal or equitable claim (see APPs 3.4(c) and 6.2(c))
- conducting an alternative dispute resolution process (see APPs 3.4(b) and 6.2(c))
- performing diplomatic or consular functions – this permitted general situation only applies to agencies (see APP 3.4(b), 6.2(c) and 8.2(d))
- conducting specified Defence Force activities – this permitted general situation only applies to the Defence Force (see APP 3.4(b), 6.2(c) and 8.2(d))

C.3 These permitted general situations are discussed generally below. Specific examples relevant to each APP are also given in the chapter relating to that APP.

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

C.4 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and:

- it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and
- the entity reasonably believes that the collection, use or disclosure 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, Item 1).

Unreasonable or impracticable to obtain consent

C.5 Consent is defined as 'express consent or implied consent' (s 6(1)) and is discussed in Chapter B (Key concepts). The main criteria for establishing consent are:

- 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.

C.6 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 nature of, and potential consequences associated with, the serious threat. For example, the urgency of a situation and level of threatened harm may require collection, 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 collection, 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 source of the threat. For example, it may be unreasonable to seek consent from the individual posing the threat where that individual could reasonably be anticipated to withhold consent, or where the act of seeking that individual's consent could increase the threat
- 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 capacity of the individual to give consent. For example, it may be unreasonable or impracticable to obtain consent where an individual is incapable of communicating consent because of their physical or psychological state or their age (capacity is discussed as part of 'consent' in Chapter B (Key concepts))
- the number of individuals whose personal information is to be collected, used or disclosed. For example, it may be impracticable to obtain consent from a very large number of individuals (though see below as to the relevance of inconvenience, time and costs)
- the inconvenience, time and cost involved in obtaining consent. 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.

Reasonably believes collection, use or disclosure is necessary

C.7 Where it is unreasonable or impracticable to obtain consent, an APP entity must reasonably believe the collection, use or disclosure is necessary to lessen or prevent a serious threat. The terms 'reasonably believes' and 'necessary' are discussed in Chapter B (Key concepts).

C.8 In summary, there must be a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of an APP entity to be able to justify its

reasonable belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient.

Lessen or prevent a serious threat

C.9 This permitted general situation applies to a serious threat to the life, health or safety of any individual, or to public health or safety. The permitted general situation would not apply after the threat has passed. 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, such as a threatened outbreak of infectious disease. This allows an APP entity to take preventative action to stop a serious threat from escalating before it materialises.

C.10 The permitted general situation applies to a threat to life, health or safety. This can include a threat to a person'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.

C.11 The threat may be to an individual the APP entity is dealing with 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.

C.12 A 'serious threat to public health or safety' relates to broader safety concerns affecting a number of people. Examples include:

- the potential spread of a communicable disease
- harm, or threatened harm, to a group of people due to a terrorist incident
- harm caused by an environmental disaster.

C.13 If time permits, attempts could be made to seek the consent from the relevant individuals for the collection, use or disclosure, before relying on this permitted general situation.

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

C.14 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and 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, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A, Item 2).

C.15 This permitted general situation is intended to apply to an APP entity's internal investigations about activities within or related to the entity.[1] It applies when the entity has reason to suspect unlawful activity, as well as misconduct of a serious nature that does not necessarily amount to unlawful activity.

C.16 'Unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass. The unlawful activity must relate to the APP entity's functions or activities. For example, harassment or discrimination within an entity would be an unlawful activity.

C.17 'Misconduct' is defined in s 6(1) to include 'fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty'. 'Serious' misconduct does not cover minor breaches and transgressions. The serious misconduct must relate to the APP entity's functions or activities. For example, a serious breach by a staff member of the Australian Public Service Code of Conduct, or fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities.

C.18 An APP entity must have 'reason to suspect' that unlawful activity or serious misconduct is being, or may be engaged in. Though only a reasonable suspicion is required, it is the responsibility of the entity to be able to justify the suspicion.

C.19 An APP entity must 'reasonably believe' that the collection, use or disclosure of personal information is 'necessary' for the entity to take 'appropriate action'. 'Reasonably believes' and 'necessary' are discussed further in Chapter B (Key concepts). In summary, there must be a reasonable basis for the belief that the collection, use or disclosure is necessary, and not merely a genuine or subjective belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of an entity to be able to justify its reasonable belief.

C.20 Whether action is 'appropriate' will depend on the nature of the suspected unlawful activity or misconduct and the nature of the action that the APP entity proposes to take. Appropriate action may include investigating an unlawful activity or serious misconduct and reporting these matters to the police or another relevant person or authority.[2] For example, if an entity reasonably believes that it cannot effectively investigate serious misconduct without collecting, using or disclosing personal information, this permitted general situation may apply.

Locating a person reported as missing

C.21 This permitted general situation applies when an APP entity reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to

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

[2] Where an APP entity seeks to disclose personal information to an 'enforcement body', such as the Australian Federal Policy or the police force or service of a State or Territory, it may be able to rely on the exception at APP 6.2(e). APP 6.2(e) permits the use or disclosure of personal information where an APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (see Chapter 6).

assist any APP entity, body or person to locate a person who has been reported as missing. The collection, use or disclosure must comply with the rules made by the Information Commissioner under s 16A(2) (s 16A, Item 3).

C.22 The terms 'reasonably believes' and 'reasonably necessary' are discussed further in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief that the collection, use or disclosure is reasonably necessary, and not merely a genuine or subjective belief. 'Reasonably necessary' has regard to whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an entity to be able to justify that the entity reasonably believes that the collection, use or disclosure is reasonably necessary.

C.23 The rules made by the Commissioner under s 16A(2) are a legislative instrument that are available on the Comlaw website.[3]

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

C.24 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A, Item 4).

C.25 The term 'reasonably necessary' is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.26 This permitted general situation applies to the collection, use or disclosure of personal information in relation to existing or anticipated legal proceedings in a court or tribunal. Where legal proceedings have not yet commenced, this situation will usually only apply to a collection, use or disclosure involving a real possibility of legal proceedings, for example where professional legal advice is sought about commencing legal proceedings. By contrast, this permitted general situation does not compel an APP entity to disclose personal information in response to a request from a third party, and it may be difficult for an entity to be satisfied that it is reasonably necessary to do so solely on the basis that a third party has requested the information in connection with existing or anticipated legal proceedings.

C.27 An APP should not rely on this permitted general situation to disclose personal information if doing so would be contrary to an Australian law (for example, a statutory secrecy provision) or a legal order or principle (for example, if disclosure would be a breach of legal professional privilege).

[3] See Comlaw website <www.comlaw.gov.au>.

Reasonably necessary for a confidential alternative dispute resolution process

C.28 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the purposes of a confidential alternative dispute resolution process (s 16A, Item 5).

C.29 The term 'reasonably necessary' is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.30 The phrase 'alternative dispute resolution process' (or ADR) is not defined in the Privacy Act. ADR covers processes, other than judicial determinations, in which an impartial person assists those in a dispute to resolve the issues between them. That person may, but is not required to, have any particular form of accreditation. Examples of ADR processes include mediation, conciliation, facilitation, expert assessment, determination, or neutral evaluation.[4]

C.31 For the exception to apply, the parties to the dispute and the ADR provider must be bound by confidentiality obligations such that any personal information collected, used or disclosed for the purpose of that ADR process will not be used or disclosed for any purpose outside the ADR process, including use or disclosure in subsequent proceedings. The confidentiality obligations may be imposed through contractual agreements or legislative provisions.

C.32 This permitted general situation extends to a disclosure of personal information by an APP entity to an ADR provider, a collection, use or disclosure by an entity for the purpose of participating in the ADR, and the collection, use or disclosure by an entity in relation to a complaint of professional misconduct against an ADR practitioner.

Necessary for a diplomatic or consular function or activity

C.33 This permitted general situation applies when an agency reasonably believes that the collection, use or disclosure of personal information is necessary for the agency's diplomatic or consular functions or activities (s 16A, Item 6). This permitted general situation applies only to agencies, and not to organisations. The terms 'reasonably believes' and 'necessary' are discussed further in Chapter B (Key concepts).

C.34 The terms 'diplomatic' and 'consular' are not defined in the Privacy Act. An agency can rely on this permitted general situation only if it has diplomatic or consular functions or powers, conferred either by legislation or an executive instrument (such as the

[4] Attorney-General's Department and National Alternative Dispute Resolution Advisory Council (NADRAC), *Your Guide to Dispute Resolution*, viewed 6 February 2014, Attorney-General's Department website <www.ag.gov.au>.

Administrative Arrangements Order). The following are given as examples of when this permitted general situation might apply:

- Diplomatic functions or activities: where an agency collects, uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.
- Consular functions or activities: where an agency collects, uses or discloses personal information to:
    - assist Australian citizens who are in distress overseas, including where an Australian individual is detained or is the victim of crime, or where assistance is required with repatriation in the case of death or serious illness, or to provide assistance in response to a crisis or emergency overseas
    - provide information to the next of kin of an Australian individual who is overseas where, for example, the individual is seriously injured or is suffering serious physical or mental illness, and the agency considers that there are likely to be significant, serious or undesirable consequences for the individual or their next of kin if it does not disclose the personal information.

Necessary for certain Defence Force activities outside Australia

C.35 This permitted general situation applies to the collection, use or disclosure of personal information by the Defence Force, where it reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories:

- war or warlike operations
- peacekeeping or peace enforcement
- civil aid, humanitarian assistance, medical or civil emergency or disaster relief (s 16A, Item 7).

C.36 For a discussion of 'reasonably believes' and 'necessary', see Chapter B (Key concepts).

C.37 The following are given as examples of when this permitted general situation might apply:

- War or warlike operations/peacekeeping or peace enforcement: where the Defence Force collects sensitive information, such as biometric information, about an enemy or other hostile adversary and uses and discloses this and other personal information in order to support Defence Force military operations.
- Civil aid, humanitarian assistance, medical or civil emergency or disaster relief: where the Defence Force collects sensitive information about an individual in the immediate aftermath of a natural or man-made disaster outside Australia and the

external Territories, and uses or discloses this and other personal information in order to trace the individual or relatives of the individual, or assist in the provision of proper medical care.