



Requests for correction of personal information: Guide for decision makers

Application of Australian Privacy Principle 13

1. Australian Privacy Principle 13 (APP 13) (Schedule 1 to the [Privacy Act 1988](#) (Privacy Act)) came into force on 12 March 2014 and provides individuals with a right to request correction of personal information held about them. This requires decision makers to apply APP 13 when responding to requests.

Example: A Defence member moves house and requests that PMKeyS is updated to reflect their new address.

Note: Processing of requests to correct information, other than personal information, remains the same.

What does APP 13 require?

2. APP 13 provides individuals with a right to request correction of personal information about them that is held by Defence.
3. Defence must take reasonable steps to correct personal information if it is satisfied that, having regard to the purpose for which it is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. This supports our obligations under APP 10 to only use or disclose accurate, up-to-date and complete information.
4. Defence must respond to requests for correction of personal information within 30 calendar days. If a request to correct personal information is denied written reasons must be provided.
5. If an individual requests a statement be included with their personal information, Defence must take steps that are reasonable in the circumstances to include that statement with that information.
6. On request from an individual, Defence must notify third parties of any changes to personal information it has previously disclosed to another entity.

What is personal information?

7. The Privacy Act defines 'personal information' as:
information or an opinion about an identified individual, or an individual who is reasonably identifiable:
 - a. whether the information or opinion is true or not; and
 - b. whether the information or opinion is recorded in a material form or not.
8. This includes information from which an individual can be 'reasonably identified' using other sources, even if the individual is not named. For example, a PMKeyS number alone could be considered personal information in the Defence context because any Defence staff member who has access to PMKeyS could reasonably identify the staff member to whom the PMKeyS number is attached.

Note: The [Important terms](#) page on the Privacy Knowledge Site contains more information on important privacy terms.



What does a request under APP 13 look like?

9. There is no prescribed format for making a request and it does not have to state that it is a request under APP 13. A request can be submitted on a standard form or made orally. You are able to ask a person to put an oral request in writing.

Example: A person ringing the Defence Service Centre to update their super fund.

10. To fall within the scope of APP 13, the request, or part of the request, must relate to the personal information about the individual making the request. APP 13 does not apply to non-personal information, or personal information about other people. These can be dealt with on an administrative basis outside of APP 13 but similar considerations may apply.

Who is responsible for making a decision on a request?

11. In other circumstances, who should decide whether a correction to personal information should be made will depend on the nature of the information and the circumstances in which the information is to be changed. If the information is to be changed is an update of current details, these changes may be made in accordance with local operating procedures.

Example: A Defence member submits an AD 150—*ADF Personal Data* requiring changes to PMKeyS. This could be changed by orderly room staff.

12. For more complex matters, decisions to correct personal information should be made by an O5/EL1 or higher in the business area that has responsibility for the official record.

Example: For complex matters involving the weighing up of information.

13. If the area that received the request on behalf of Defence does not hold or is not responsible for the information, the request should be forwarded without delay to the relevant business area to action.

How long does Defence have to respond to a request?

14. Defence must respond to a request for correction of personal information within 30 days. The 30 day period commences the day after Defence receives the request even if the request has been made to a part of Defence that does not hold the information, or the request has been made orally.

15. This means Defence must do one of the following within 30 days:

- a. correct the personal information as requested;
- b. notify the individual of its refusal to correct the information and the reasons for refusing the request.

16. If it is impracticable to response to the individual within 30 days, decision makers must contact the individual to explain the delay and provide an expected timeframe for finalising the request.

Example: If there is a justifiable need to clarify the individual's request, or to locate information to be corrected, or to consult a third party.

Before correcting personal information

17. Depending on the circumstances, it may be necessary to take additional steps to verify the identity of the individual making the request to correct their personal information. The individual may need to produce documents to enable Defence to positively verify their identity.

Example: Defence ID card.

18. In some cases, a request may be made by a legal representative of an individual, such as a power of attorney, or legal practitioner. In these circumstances, evidence of the authority to act should be requested and retained, such as a completed power of attorney document.

19. Additional steps may need to be taken to verify the accuracy of the information provided by the applicant before a correction is made.

When can information be changed?

20. Any personal information that Defence considers inaccurate, out-of-date, incomplete, irrelevant or misleading may be corrected either on request of an individual or when Defence becomes aware of any of the above. However, decision makers should note that personal information is not necessarily incorrect just because an individual disagrees with information Defence holds about them.

Example: An individual's disagreement with a finding made in an inquiry, or medical or psychological assessment does not mean the finding or assessment is incorrect and needs to be changed.

21. Personal information may be held for multiple purposes and may require correction for one purpose but not for another purpose. When assessing a request, the decision maker should consider whether the information is held for multiple purposes and if so, which of these will require correction.

Example: A Defence member's name may be correct in PMKeyS but may be misspelt on their Defence ID card.

Taking reasonable steps to correct personal information

22. Defence must take reasonable steps to correct personal information if requested. What this means in practice depends on a range of factors, including:

- a. the sensitivity of the information;
- b. the possible adverse consequences for the individual if the information is not corrected;
- c. the practicability of making the correction;
- d. the likelihood Defence will use or disclose the information;
- e. the purpose for which the information is held;
- f. record keeping requirements that may apply to the information under an Australian court or tribunal order;
- g. whether the personal information is in the possession of Defence or a third party.

23. More information on what constitutes reasonable steps is contained in the Office of the Australian Information Commissioner's [APP Guidelines](#) (paragraphs 13.47 and 13.48).

24. In some circumstances it may be appropriate to retain a copy of the original information. This is particularly important where the original information informed a business decision or action. It may be appropriate to mark the retained original information in some way to indicate that it is inaccurate, out-of-date, incomplete, irrelevant or misleading and should not be relied on for other purposes. It may also be appropriate to include the correct personal information or cross reference to where the corrected information is held.

Example: When updating a document in Objective, each edit of a document is saved as a new version of that document to ensure previous versions are not lost.

25. Under the [Archives Act 1983](#) (Archives Act), records more than 15 years old cannot be altered unless required or authorised by law. APP 13 provides authority to amend a record more than 15 years old where it is required under this principle.

Refusing to make corrections

26. A request by a person to correct personal information may be refused if Defence does not consider the personal information to be:

- a. inaccurate;
- b. out-of-date;
- c. incomplete;
- d. irrelevant; or
- e. misleading.

27. If Defence decides not to make the corrections requested, either in full or in part, written reasons for the decision must be provided. The reason must state the basis for the refusal and how the decision maker came to the conclusion that the request should be refused. The decision maker must also advise the person requesting the correction that they can seek review of the decision through the Defence Privacy Office.

Additional responsibilities

28. If personal information has been corrected, Defence must take steps that are reasonable in the circumstances to notify other agencies or organisations to which Defence has given the information of the corrections made.

Example: Changing personal information that forms part of a work health and safety incident report may require the change to be reported to Comcare.

29. If the request has been refused, and the individual requests Defence to include a statement with the information that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, Defence must take steps that are reasonable in the circumstances to include the statement with the information. This must be done in a way that will make the statement apparent to users of the information, for example, in a Defence context, by 'linking' documents in Objective, or using the 'notes' function in Objective.

Access charges

30. No fee is payable by the person making the request for either submitting the request or to cover the costs of correcting personal information.

Further advice

31. For further advice regarding a request for correction of personal information, contact the Defence Privacy Office:

Email: defence.privacy@defence.gov.au

32. The Complaints and Resolution [Privacy Knowledge Site](#) on the DRN contains information on the APPs and their application in a Defence context.

33. The Office of the Australian Information Commissioner's [APP Guidelines](#), Chapter 13, provides detailed advice on how to interpret APP 13.