Chapter 8: Directing a privacy impact assessment

Contents

Legislative framework

8.1 Section 33D of the Privacy Act empowers the Commissioner to direct an agency to give the Commissioner a privacy impact assessment (PIA).

8.2 The Act provides that where an agency proposes to engage in an activity or function involving the handling of personal information about individuals, and the Commissioner considers that the activity or function might have a significant impact on the privacy of individuals, the Commissioner may direct the agency to give the Commissioner a PIA about the activity or function.

Purpose and key features of the PIA direction power

8.3 A PIA is a written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact (s 33D(3)). The OAIC will use the PIA direction power to ensure that, for proposed activities or functions that involve the handling of personal information and which the Commissioner considers might have a significant impact on privacy, the privacy risks inherent in that activity or function are identified and managed, minimised or eliminated before they materialise.

8.4 Typically, a PIA should be conducted when a particular activity or program is at the proposal stage. The findings of a PIA conducted at this stage can then be taken into account when designing the proposal before proceeding to implementation.

8.5 The OAIC expects an entity to consider conducting a PIA and publishing the final report whenever an entity proposes to engage in an activity or function involving the handling of personal information. Where the OAIC becomes aware of a proposal which may have a significant impact on the privacy of individuals, the OAIC will generally recommend that an entity undertake a PIA. Considering and conducting a PIA are intrinsically linked to an entity's obligations under APP 1.[1] Entities can obtain guidance on determining whether a PIA is necessary and on conducting PIAs from the *Guide to undertaking privacy impact assessments*.[2]

8.6 An agency should not wait for a recommendation or direction from the OAIC to conduct a PIA. The OAIC expects agencies will recognise the benefits of conducting a PIA and a PIA direction should not generally be required. A PIA direction should be a last resort, where the OAIC considers that a PIA is necessary to ensure that a proposed activity or function is appropriately balanced against the protection of the privacy of individuals and the agency is not already conducting a PIA.

8.7 This is consistent with the OAIC's preferred regulatory approach of working with entities to facilitate legal and best practice compliance. To assist with this approach in relation to agencies, the OAIC will use the Information Contact Officer Network to ensure agencies maintain an open dialogue with the OAIC so that the OAIC is aware of major projects or policies that are being proposed and that may require a PIA.

Proposed activities and functions for which the PIA direction power may be used

8.8 The PIA direction power may be used when an agency proposes to engage in an activity or function that the Commissioner considers might have a significant impact on the privacy of individuals. This includes when the agency proposes to:

- engage in a new activity or function, or
- substantively change an existing activity or function. This includes a substantive change to the system that delivers an existing function or activity.

8.9 The Commissioner must also be satisfied that the proposed activity or function might have a significant impact on the privacy of individuals. In considering whether a proposed activity or function might have a significant impact on the privacy of individuals, the OAIC will take the following matters into account:

- the number of individuals whose personal information will be handled as a result of the proposed activity or function
- the amount and sensitivity of the personal information handled as a result of the proposed activity or function

[1] See the Australian Privacy Principles Guidelines, Chapter 1.

[2] See *Guide to undertaking privacy impact assessments*

- whether the proposed activity or function will be subject to the Privacy Act, or whether all or any part will be exempt
- whether the proposed activity or function involves a technology or the convergence of existing technologies
- whether the proposed activity or function involves the use of a technology in a new way
- any steps already taken by the agency to manage, minimise or eliminate the privacy impacts of the proposed activity or function
- any other matter the Commissioner considers relevant.

8.10 The PIA direction power only applies to the proposed functions or activities of an agency. Whether this power should be extended to apply to organisations subject to the Privacy Act is due to be reviewed by the Minister with responsibility for administering the Privacy Act by 12 March 2019 (s 33D(7)).

Circumstances in which the PIA direction power might be used

8.11 There are two main circumstances in which consideration is likely to be given to exercising this power:

- when the OAIC, in the course of providing guidance to an agency on a proposed agency activity or function, considers that the proposed activity or function might have a significant impact on the privacy of individuals and recommends a PIA be conducted, and the agency does not conduct one
- when the OAIC otherwise becomes aware of an agency's proposed activity or function (for example, through a media report) and considers that it might have a significant impact on the privacy of individuals and the agency has not conducted a PIA.

Procedural steps in issuing a PIA direction

8.12 Where the OAIC becomes aware of a proposed activity or function of an agency it may seek further information about the impact of the proposal on the privacy of individuals. The OAIC will generally use the following procedure:

- The OAIC may seek information from the agency in relation to the proposed activity or function to find out whether it involves the handling of personal information, and whether it might have a significant impact on the privacy of individuals.
- If so, the OAIC will generally suggest to the agency that it consider conducting a PIA, if it is not already doing so, to assist it in identifying and managing, minimising or eliminating privacy impacts. The suggestion to consider undertaking a PIA may be made by the OAIC in a public submission.
- If the agency does not plan to conduct a PIA and the OAIC continues to consider that the proposed activity or function might have a significant impact on the privacy of individuals, the OAIC will make a written recommendation that the agency undertake a PIA and give the PIA to the Commissioner.[3] The recommendation generally will note that

[3] A recommendation would be made in written correspondence to the agency and not in a public submission.

if the agency does not adopt the recommendation, the OAIC will consider whether a PIA direction should be issued.

- The OAIC will seek confirmation from the agency whether or not it intends to adopt the recommendation and conduct a PIA.
- Where the agency indicates it intends to conduct a PIA, the OAIC will maintain contact with the agency.
    - If it appears that the PIA is not being conducted in a timely manner, or is not conducted to a sufficient standard, the OAIC will notify the agency that it may consider issuing a PIA direction.
    - Where the agency does not progress the PIA in a timely manner following that notification, the OAIC will consider whether a PIA direction should be issued.
- If the agency does not intend to conduct a PIA, the OAIC will consider whether a PIA direction should be issued.
- The factors identified in paragraph 38 of the OAIC's *Privacy regulatory action policy* will be used to inform the decision. The OAIC may seek information from the agency to assist in making this decision.
- Where the decision is to issue a PIA direction, the direction to be issued will be prepared. The direction will generally:
    - include an explanation of PIAs
    - refer the agency to the *Guide to undertaking privacy impact assessments*
    - provide the timeframe in which the agency must give the Commissioner the PIA
    - outline how the PIA is to be provided to the Commissioner, and
    - outline the consequences of failing to comply with the direction.

  The direction will be issued by the Commissioner.
- An agency may seek an extension of time in which to give the PIA to the Commissioner. The OAIC would generally grant an extension where:
    - the proposed function or activity will not be implemented during the time period of the extension
    - the extension will not otherwise impact the ability of the agency to adopt the recommendations in the PIA
    - it is satisfied that the agency's need for additional time in which to complete the PIA is reasonable in the circumstances.
- When the agency gives the Commissioner the PIA, the OAIC will review the PIA to ensure that:
    - it identifies impacts that the proposed activity or function might have on the privacy of individuals in accordance with the *Guide to undertaking privacy impact assessments*
    - it sets out recommendations for managing, minimising or eliminating that impact in accordance with the *Guide to undertaking privacy impact assessments*
    - the agency has responded to each recommendation in the PIA. In responding to each recommendation the agency should indicate whether it intends to implement (or has

already implemented) the recommendation or not, and the rationale for this decision.

- The OAIC may also provide comments to the agency on the PIA's adequacy and the agency's response to the recommendations. The OAIC expects the agency to review, and where necessary address, the OAIC's comments.
- The OAIC will seek confirmation from the agency that the agency has implemented the recommendations in the PIA in accordance with the agency's responses to those recommendations prior to the implementation of the activity or function. Where the OAIC continues to hold concerns about the impact of a proposed activity or function on the privacy of individuals, the OAIC will generally inform the Minister of the matter.

When is an agency considered to have complied with the PIA direction?

8.13 The OAIC will consider that an agency has complied with a PIA direction when the agency has given the PIA to the Commissioner in accordance with the direction and any extensions granted.

Steps the OAIC will take where an agency does not comply with a direction

8.14 Where an agency does not comply with a PIA direction, the OAIC will use the following procedure:

- If an agency has not complied with the PIA direction the OAIC will first contact the agency to determine the agency's progress and whether and when they intend to comply with the PIA direction.
- If the agency does not intend to comply with the PIA direction within a reasonable timeframe, the OAIC will consider this a failure to comply with the direction.
- Where an agency has failed to comply with a PIA direction, the OAIC will advise both the Minister responsible for administering the Privacy Act, and the Minister responsible for the non-compliant agency (as required by s 33D(6)).

Publication

8.15 The OAIC will generally publish all PIA directions issued, and will require the agency to publish all final PIAs prepared in response to a PIA direction. To the extent possible, the OAIC will publish PIA directions in full or in an abridged version on its website: <www.oaic.gov.au>. It is sometimes inappropriate to publish all or part of a PIA direction or PIA because of statutory secrecy provisions or for reasons including privacy, confidentiality, commercial sensitivity, security or privilege. The OAIC will take those considerations into account when deciding whether to publish a PIA direction, and whether to require an agency to publish their PIA.

8.16 Publication of PIA directions on the OAIC website may be accompanied by other communication such as a media release, media interview or social media. These communications will be made in accordance with the approach set out in the *Privacy regulatory action policy*.

8.17 The OAIC may refer to PIA directions in speeches and at other events such as Information Contact Officer Network meetings, Privacy Connections events and conferences.

Additional resources

8.18 The OAIC has published the *Guide to undertaking privacy impact assessments* which provides key guidance on conducting a PIA.