Chapter 7: Privacy assessments

Contents

Legislative framework

7.1 Section 33C of the Privacy Act provides the Commissioner with the power to conduct assessments of APP entities about whether personal information they hold is being maintained and handled in accordance with the Australian Privacy Principles (APPs).

7.2 This section also empowers the Commissioner to conduct assessments of entities covered by the provisions of Part IIIA of the Privacy Act and the registered credit reporting (CR) code, tax file number (TFN) recipients, agencies conducting data matching programs under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and entities that handle information to which s 135AA of the *National Health Act 1953* (Cth) applies.

7.3 Additionally, s 28A of the Privacy Act states that the Commissioner's monitoring functions include:

- monitoring the security and accuracy of information held by an entity that is information to which Part IIIA of the Privacy Act applies and examining entities' records to ensure information is not being used for unauthorised purposes and is protected adequately against unlawful disclosure
- examining the records of the Commissioner of Taxation to ensure TFN information is being used for authorised purposes and adequately protected against unlawful disclosure
- evaluating compliance with the TFN rules issued under s 17 of the Privacy Act and monitoring the security and accuracy of TFN information kept by file number recipients.

7.4 Section 33C(2) of the Privacy Act specifically states the Commissioner may conduct an assessment in a manner the Commissioner considers appropriate.

7.5 In addition to these functions and powers under the Privacy Act, s 309 of the *Telecommunications Act 1997* (Cth) (Telecommunications Act) provides the Commissioner with the power to monitor telecommunications carriers, carriage service providers and number-database operators compliance with Part 13, Division 5 of the Telecommunications

Act or Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). Specifically, this relates to these entities' obligations to record disclosures of personal information made under relevant sections of the Telecommunications Act and TIA Act.

Entry and inspection powers

7.6 Section 68 of the Privacy Act provides wide entry and inspection powers to the Commissioner (or delegates authorised by the Commissioner) to enter an agency, organisation, credit reporting body or credit provider premises and inspect any documents that are kept on the premises that are relevant to the performance of the Commissioner's functions.

7.7 Section 68 (2) provides that the occupier must provide reasonable facilities and assistance to the Commissioner or authorised delegates.

7.8 Under s 68A, the Commissioner must issue a person authorised for the purposes of s 68 with an identity card containing a recent photograph of the authorised person.

Reporting to the Minister

7.9 Section 32 of the Privacy Act provides that after conducting an assessment the Commissioner may report to the Minister about the assessment, and must do so if directed by the Minister. Further, if the Commissioner believes it is in the public interest to provide a further report about the assessment to the Minister to be tabled in Parliament, the Commissioner may do so.

Purpose and key features of privacy assessments

7.10 As outlined in the *Privacy regulatory action policy,* the OAIC will use assessments to facilitate legal and best practice compliance by identifying and making recommendations to address privacy risks and areas of non-compliance. However, there may also be situations where assessments are used strictly to assess an entity's compliance with its legislative obligations.

Types of privacy assessments

7.11 The OAIC needs some flexibility in its approach to privacy assessments. To assist with this, the OAIC undertakes two types of assessments depending upon the circumstances:

- risk based assessments
- compliance based assessments.

7.12 The OAIC expects the majority of privacy assessments it undertakes to be risk based assessments. However, the assessment type will be determined on a case by case basis.

Risk based assessments

7.13 A risk based assessment is an assessment that focuses on identifying privacy risks to the effective handling of personal information by an entity in accordance with relevant legislation (for example, APPs, credit provisions or code, TFN guidelines). The privacy risks identified should directly relate to the entity's general compliance obligations.

7.14 Recommendations may be made based on the OAIC's estimates of the relative privacy risk against the relevant legislative requirements, with the aim of assisting entities to improve their observed privacy practices and procedures.

7.15 The primary outcome of a risk based assessment will be the identification and discussion of individual risks in relation to the entity's compliance with the specific legislation, with an acknowledgement (if appropriate) of any observed strengths of the entity in relation to its privacy practices. A risk based assessment will not provide an overall assessment of the entity's compliance with its legislative obligations (for example, no overall assessment of 'compliant' or 'non-compliant' will be provided in relation to the entity).

Compliance based assessments

7.16 A compliance based assessment is a more specific assessment that focuses on identifying whether an entity has complied with an identified legislative obligation or explicit direction from the OAIC. Instead of identifying privacy risks to an entity's general compliance obligations, the compliance based assessment aims to provide an assessment of an entity's explicit compliance with specific requirements, which could include, for example:

- whether the Commissioner for Taxation meets obligations under s 28A of the Privacy Act in relation to use and disclosure of TFN information
- an entity's compliance with an enforceable undertaking accepted by, or a determination made by, the Commissioner
- the appropriateness of an entity's response to significant risk recommendations previously identified by the OAIC under a risk based assessment
- whether telecommunications carriers, carriage service providers and number-database operators meet obligations under the Telecommunications Act in relation to any disclosures of the personal information held.

7.17 The primary outcome of a compliance based assessment will be an assessment of whether the entity is 'compliant' or 'non-compliant' with the specific identified obligation under the relevant legislation, or the explicit requirement that has been previously provided by the OAIC to the entity.

Assessments for data-matching activities

7.18 Under s 13(5)(a) of the Privacy Act, breaches of Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) (DMP Act) or the rules issued under s 12 of DMP Act are also considered to be interferences with the privacy of an individual.

7.19 The OAIC has an agreement with the Department of Human Services (DHS) to undertake assessments of DHS's compliance with its DMP Act obligations. The OAIC tailors its assessment steps and criteria for these assessments consistent with the requirements of the DMP Act.

When will the OAIC conduct a privacy assessment?

7.20 The OAIC will undertake privacy assessments where it will contribute to achieving its goal of promoting and ensuring the protection of personal information. When deciding whether it is appropriate to undertake a privacy assessment in a particular situation, the OAIC will refer to

the 'Selecting appropriate privacy regulatory action' section of the *Privacy regulatory action policy*, including the 'factors taken into account' and the 'sources of information' sections.

7.21 Generally, the OAIC will undertake a risk assessment targeting exercise each financial year to identify possible industry sectors and/or entities that should be subject to a privacy assessment. An outline of the OAIC's risk assessment targeting process is provided below under the heading 'Targeting'.

Examples of when the OAIC may undertake privacy assessments could include where:

- existing legislation is impacting on sensitive privacy related issues
- new legislation is implemented, which raise significant privacy issues
- industries implement new technology or processes, which raise significant privacy issues
- high risks to individuals' privacy are identified, through factors including the number and nature of privacy complaints to the OAIC and information from media sources or other privacy regulators.

7.22 The OAIC will also undertake privacy assessments where it is specifically funded to do so.

Assessment outcomes

Recommendations

7.23 A recommendation is a suggested course of action or control measure that, if put in place by the assessed entity, will minimise the risks identified in relation to how personal information is handled against the relevant criterion.

7.24 Not all assessment findings will need to be reflected in a recommendation in an assessment report. Many findings, such as those that note good privacy acts or practices, may simply be noted in the assessment report. Conversely each recommendation needs to be supported by at least one finding.

7.25 Generally, recommendations will align with the terminology used in the APP guidelines. The APP guidelines set out that the mandatory requirements of the Privacy Act and are described by the words 'must' or 'is required to'. Aspects of privacy practice that the Commissioner may take into account when considering an entities' compliance with the Privacy Act are indicated by the use of the words 'should' or 'is expected to', when handling personal information. And good privacy practices that may supplement compliance with the mandatory requirements in the APPs are generally indicated by 'could' in the APP guidelines.[1]

7.26 The OAIC will generally only make recommendations with regard to privacy practices that it considers entities 'must' or 'should' do. 'Good privacy practice' considerations will be detailed in the text of the report only.

[1] Office of the Australian Information Commissioner, *APP guidelines*, page 2, available at <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>

7.27 The OAIC will only make recommendations on issues of particular significance or concern to the OAIC, and recommendations will be clear, targeted and actionable.

7.28 Specifically, for risk based assessments:

- the OAIC will not make recommendations against all privacy risks it observes but will do so where considered appropriate in the circumstances. Generally, the OAIC will make recommendations where it identifies medium to high level privacy risks. Further detail about this approach is provided in Appendix A which sets out the OAIC's view of how it determines what constitutes a high, medium or low privacy risk and the action it considers needs to be taken by an entity to address the particular levels of risk.
- for each observation the OAIC will consider:
  - relevant privacy risks, if any
  - the level of the risk; that is, what is the likely outcome for the entity if the identified risk is not addressed
  - the entity's operational context and whether it is reasonable to require the entity to take steps to address the privacy risk.

The content of the assessment report

7.29 Generally the OAIC will provide a report to an assessed entity. The report will detail the extent to which the relevant assessment criteria have been met, taking into account the information and background material collected, and the OAIC's observations.

7.30 The report will also:

- provide a fair and balanced assessment of the assessed areas of the entity, by clearly and concisely setting out the observations and information, privacy risks or findings and recommendations from the assessment
- lead logically to the identification of any privacy risks or areas of non-compliance from which specific recommendations may be developed
- identify and acknowledge any areas where the entity is performing well, and also acknowledge where actions have been taken to identify and address privacy concerns.

Assessment opinion limitations

7.31 The OAIC notes that any assessment opinions it expresses in its privacy assessment reports are limited by:

- the assessment scope and objectives
- the time period in which the assessment fieldwork was undertaken; that is, it is an opinion only applicable to the point-in-time of the fieldwork period
- the areas of the entity that were assessed; that is, the risks for risk based assessment, or findings for compliance based assessments, may not apply to areas of the entity that were not assessed.

7.32 There are limitations on how widely the risks or findings of an assessment can be extrapolated across the wider entity. The assessment report is not a definitive account of an

entity's personal information handling acts or practices and does not fetter the Commissioner's discretion, if for example, a complaint is made.

Resolving a disagreement between the OAIC and an entity about the assessment report

7.33 The OAIC aims to achieve agreement with the assessed entity around the text of the report, and any identified risks from a risk based assessment or findings from a compliance based assessment and any recommendations from the assessment. The OAIC will therefore provide the entity with a draft report on which to comment. However, agreement between the OAIC and the assessed entity about the text of the report may not always be possible.

7.34 The OAIC will amend any factual inaccuracies clearly identified by the entity. However, disagreements may arise in relation to the findings (which may be based on disputed information and/or observations), the risks associated with these findings or any recommendations made in relation to the risks.

7.35 The OAIC will consider, in a balanced and fair manner, whether the information provided by the entity in relation to any disputed part of the report is sufficient to require a reassessment of a risk, finding or recommendation in the draft report. Any change to a risk, finding or recommendation in the report will only be made where supported by objective information.

7.36 The Commissioner or appropriate delegate has the ultimate discretion in determining the content of the report. Any outstanding disagreement between the OAIC and an entity in relation to an assessment finding, recommendation or opinion will generally be brought to the Commissioner's attention before the report is published.

Further regulatory action

7.37 While the primary purpose of conducting a risk based assessment is to assist entities with their privacy practices, there may be circumstances where the OAIC considers it appropriate to take further regulatory action as a result of an assessment. For example, during a risk based assessment if the OAIC identifies significant issues of concern and the entity does not appear willing or capable of taking steps to address these concerns it may be appropriate for the OAIC to open a Commissioner initiated investigation (CII).

7.38 While the primary purpose of a compliance based assessment is to assess an entity's compliance with its legislative obligations, the OAIC will still aim to work co-operatively with an entity to rectify any non-compliance with the entity's legal obligations identified as a result of the assessment. However, there may be circumstances where further regulatory action is required from the OAIC to ensure an entity takes steps to address any issues associated with non-compliance.

7.39 Generally, the OAIC does not expect to take enforcement action directly or only as a result of an assessment outcome or finding. However, in limited circumstances, additional regulatory action may occur.

7.40 When deciding whether to take further regulatory action as a result of an assessment, the OAIC will refer to the factors set out in paragraph 38 of the *Privacy regulatory action policy*.

Reporting to the Minister

7.41 The Commissioner will not routinely report assessment outcomes to the Minister but would do so if directed to by the Minister or where the Commissioner believes a report to be in the public interest. However, assessment reports will generally be made public so will be available to the Minister in that form.

7.42 Where the Commissioner does report to the Minister about an assessment, the Commissioner will notify the assessed entity.

Procedural steps

7.43 There are four main stages commonly involved in assessments:

1. Targeting
2. Planning
3. Fieldwork
4. Reporting.

7.44 This staged process is flexible and there may be situations that warrant the OAIC taking a different approach. For example, a compliance based assessment is unlikely to require as detailed a targeting process as a risk based assessment, given both the entity and the identified legislative obligation will already be established. As such, this stage may not be undertaken for a compliance based assessment.

Targeting

7.45 The OAIC will generally use the following procedure to identify assessment targets:

- Every year the OAIC will conduct initial background research using internally and externally available information from the preceding 12 months (including OAIC complaint and enquiries data, CII or data breach notification data, significant media coverage or information about new technologies, processes or legislation), as well as internal consultation across the OAIC, to identify a list of industry sectors and/or entities that pose the greatest risks to individuals' privacy.

  More in depth background research and risk assessments of an agreed number of identified risk targets will subsequently be undertaken to determine in detail which targets either pose greatest risks to, or present the greatest opportunities for, assessment action.

- In some circumstances, it may be appropriate or necessary to conduct limited external consultation around possible risk targets (for example, with other regulators). The OAIC notes that any external discussion of potential risk targets could have commercially sensitive implications for some APP entities. For these reasons, it is not expected that external consultation would generally be required in determining risk targets, and would only be undertaken in very limited circumstances.

- Selecting assessment targets for funded assessments will involve undertaking targeting in the context of the agreement and involve consultation with the other party to the agreement.

7.46 Once the OAIC decides to assess a particular entity, the OAIC will also determine the initial scope and objective of the assessment:

- The **scope** of the assessment states which of the entity's functions, programs, activities, processes or systems are being considered in the assessment. The scope can also be limited to particular aspects of the entity's obligations such as one or more APPs. Just as importantly, the scope should also clearly identify what will not be considered as a part of the assessment.
- The **objective** of the assessment is the purpose of the assessment — the reason why the assessment is being undertaken. An objective is usually phrased as a question that needs to be answered and may be broad, specific or a combination of those.
- The preliminary scope and objective/s may be further developed during the next stage of the assessment, after initial contact and consultation has occurred with the target entity.

Planning

7.47 Once the likely target entity has been determined, the OAIC will generally use the following procedure for the planning stage of privacy assessments:

- The OAIC will aim to make contact with an appropriate entity employee to discuss:
  - the OAIC's intention to undertake an assessment
  - the appropriateness of the proposed scope, objectives and methodology for the assessment
  - the entity's current and near term operational and business environments, to identify when an assessment could best be undertaken and when relevant staff are likely to be available
  - administrative detail relating to the proposed assessment, such as key contact officers, the proposed timing and length of the assessment, entity facilities or resources required for the OAIC on-site and the relevant location(s) or venue for the assessment.
- The OAIC will then determine in greater detail the assessment methodology including:
  - **assessment criteria** for the assessment. The assessment criteria clearly set out the standards of performance that are expected to exist. This is the standard against which the entity's performance is to be assessed. The assessment criteria will usually be drawn directly from the relevant legislative obligations for the entity.
  - **assessment techniques** available for the assessment and appropriate to collect sufficient information to allow the OAIC to make an assessment of the entity's performance against the identified objectives and assessment criteria. These techniques may include document review, interviews, direct observation/physical

inspection, testing/checking of records/procedures and/or polls and survey research.

- The OAIC will then formally notify the entity by letter of the intention to undertake a privacy assessment. The notification letter will request the entity provide documentation to assist the OAIC prior to the assessment fieldwork.
- The OAIC aims to complete privacy assessments in a timely manner, within a six month period. As such, the OAIC requires entities to provide requested information, comments and responses within specified timeframes. However, the OAIC is willing to be flexible and discuss timeframes to take into account an entity's operational and resourcing considerations.

Fieldwork

7.48 The principal activity in the fieldwork stage is to collect, in a systematic and ordered way, sufficient information to enable the OAIC to identify how an entity is maintaining personal information in accordance with its obligations, in line with the scope, objectives and assessment criteria.

7.49 The OAIC will generally use the following procedure for the fieldwork stage of privacy assessments:

- The OAIC will review all of the information and documentation the entity provides in response to the formal notification letter. Generally, this material should enable the OAIC to understand:
  - what types of personal information the entity handles
  - how the personal information is collected
  - how the entity uses the personal information
  - what the internal flows of personal information within the entity look like
  - what disclosures of the personal information (if any) the entity makes, and to whom
  - what security measures are in place to protect the personal information
  - any other relevant issues in relation to the entities handling of the personal information (including information specifically requested in relation to the agreed scope and objectives of the assessment).
- Staff from the OAIC will usually attend the entity's premises during the fieldwork stage over a set period of time (usually between one to three days) to undertake the assessment. There may be assessments where the OAIC does not need to attend the entity's premises during the fieldwork stage. For example, an assessment may only involve a desktop review of an entity's policies and procedures which are already publicly available (for example, the entity's APP 1 privacy policy).
- Where the OAIC is visiting the entity's premises to conduct assessment fieldwork the OAIC will make the necessary administrative arrangements with the entity such as establishing a time and attendees for the opening and closing conferences and developing an interview schedule for key staff.

- Generally the OAIC will conduct the fieldwork by:
  - holding a brief opening conference with key executive and/or senior staff to provide an overview of the assessment process including the scope, objectives, assessment criteria, assessment techniques and the general timeframe for reporting of assessment results
  - gathering information needed to assess the entity against each of the assessment criterion. Information usually collected includes documents (for example, the entity's process documents), interview responses and observations (for example, observing the acts and practices of the entity's staff undertaking normal business operations)
  - holding a brief closing conference with key executive and/or senior staff and other relevant staff, to discuss preliminary risks/findings and issues likely to be raised in the draft assessment report. The preliminary feedback provided at the closing conference may be subject to change after the OAIC reviews and considers all of the gathered information in the analysis stage. It is intended only to provide an early indication to the entity of any issues that may be identified in the draft assessment report.
- During the fieldwork stage, the OAIC will:
  - notify the entity of any areas of potential concern. By providing continuous and open feedback to the entity, the entity will have the opportunity to correct, amend or provide further explanatory information around the issues or concerns identified
  - consider whether it has collected and recorded a sufficient amount of reliable and valid information during the assessment process to allow it to make an adequate assessment against each of the assessment criterion.

Reporting

7.50 The final stage of a privacy assessment is reporting the results of the assessment formally to the Commissioner and providing the privacy assessment report to the entity.

7.51 The OAIC will generally use the following procedure for the reporting stage of privacy assessments:

- Develop and provide the entity with a draft assessment report for review (aiming to do this within eight weeks from the end of the fieldwork period).
- The entity will usually be requested to provide any comments, clarifications and/or a written response to the draft report including any recommendations within 3 weeks.
- The written response from the assessed entity may also:
  - include information on management initiated improvements since fieldwork
  - seek omissions from the report for privileged or confidential information
  - seek exclusions from the report under s 33 of the Privacy Act.
- The OAIC will review the entity's comments and response to the draft report and make any changes as appropriate. In some cases it may be necessary to hold further

discussions between the OAIC and the entity to reach an agreed position on any outstanding matters.

- A final version of the assessment report will be issued to the entity, and the report will generally be published on the OAIC's website shortly afterwards.

Publication

7.52 Generally, the OAIC will publish all assessment reports. There may be circumstances when it would be inappropriate to publish all or part of an assessment report due to statutory secrecy provisions or reasons of privacy, confidentiality, commercial sensitivity, security or privilege. The OAIC will take these factors into account when deciding whether to publish an assessment report in full or in an abridged version. This will be determined upon a case by case basis.

Appendix A: Risk based assessments — privacy risk guidance

Privacy risk rating	Entity action required	Likely outcome if risk is not addressed
High risks Entity ***must***, as a high priority, take steps to address mandatory requirements of Privacy and related legislation	**Immediate management attention is required.** This is an internal control or risk management issue that if not mitigated is likely to lead to the following effects	o Likely breach of relevant legislative obligations (for example, APP, TFN, Credit) or not likely to meet significant requirements of a specific obligation (for example, an enforceable undertaking) o Likely adverse or negative impact upon the handling of individuals' personal information o Likely violation of entity policies or procedures o Likely reputational damage to the entity, such as negative publicity in national or international media. o Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines o Likely ministerial involvement or censure (for agencies)
Medium risk Entity ***should,*** as a medium priority, take steps to address OAIC expectations around requirements of Privacy and related legislation	**Timely management attention is expected.** This is an internal control or risk management issue that may lead to the following effects	o Possible breach of relevant legislative obligations (for example, APP, TFN, Credit) or meets some (but not all) requirements of a specific obligation o Possible adverse or negative impact upon the handling of individuals' personal information o Possible violation of entity policies or procedures o Possible reputational damage to the entity, such as negative publicity in local or regional media o Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities o Possible ministerial involvement or censure (for agencies)

Low risk Entity ***could***, as a lower priority than for high and medium risks, take steps to better address compliance with requirements of Privacy and related legislation	**Management attention is suggested.** This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the entity or process being assessed.	o Risks are limited, and may be within acceptable entity risk tolerance levels o Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit) o Minimum compliance obligations are being met