



Australian Government

Office of the Australian Information Commissioner

Guide to privacy regulatory action



Updated June 2020

OAIC

Contents

A comprehensive contents page appears at the beginning of each chapter.

Introduction

Chapter 1: Privacy complaint handling process

Chapter 2: Commissioner initiated investigations and referrals

Chapter 3: Enforceable undertakings

Chapter 4: Determinations

Chapter 5: Injunctions

Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions

Chapter 7: Privacy assessments

Chapter 8: Directing a privacy impact assessment

Chapter 9: Data breach incidents

Introduction

Contents

Purpose of the Guide to privacy regulatory action	1
Other documents relating to regulatory powers	1
Regulatory powers available	2
Regulatory action principles	3
Approach to using regulatory powers and selecting appropriate action	4

Purpose of the Guide to privacy regulatory action

The *Guide to privacy regulatory action* consists of different chapters, each relating to a regulatory power under the *Privacy Act 1988* (Cth) (Privacy Act), the *My Health Records Act 2012* (Cth) (My Health Records Act), the Consumer Data Right (CDR) scheme set out in Part IVD of the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act), and other legislation that confers functions relating to privacy on the Commissioner.¹ Each chapter includes information about the legislative framework, purpose and procedural steps for exercising the regulatory power.

The purpose of this guide is to:

- be a source of information for entities about the Office of the Australian Information Commissioner's (OAIC's) exercise of particular regulatory powers
- provide OAIC staff with practical guidance about exercising a particular regulatory power
- promote consistency and transparency in the OAIC's exercise of its regulatory powers
- facilitate efficient and effective regulatory action.

Other documents relating to regulatory powers

The *Guide to privacy regulatory action* is one of a suite of documents that relate to the OAIC's use of its regulatory powers:

- The *Privacy regulatory action policy* explains the OAIC's approach to using its regulatory powers under the Privacy Act and other legislation, and communicating information publicly. This includes the considerations the OAIC will take into account in deciding when to take privacy regulatory action and what action to take. This document also explains the principles which will guide the OAIC when taking regulatory action, and the circumstances in which information

¹ For example, Part VIIC Division 5 of the *Crimes Act 1914* (Cth) confers on the Commissioner regulatory powers in relation to spent convictions.

about regulatory activity may be communicated publicly. The chapters in this guide should be read in conjunction with the policy.

- The *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (My Health Records Enforcement Guidelines) is a registered legislative instrument which explains the OAIC's approach to using its enforcement powers in its role as regulator of the My Health Record system. These guidelines are made by the Commissioner under s 111 of the My Health Records Act.
- The *CDR regulatory action policy* explains the OAIC's approach to using its regulatory powers in relation to the CDR scheme. Like the *Privacy regulatory action policy*, the *CDR regulatory action policy* outlines the matters the OAIC will consider when deciding to take regulatory action, the principles it is guided by, and the circumstances in which information about regulatory activity may be communicated publicly. The *CDR regulatory action policy* can also be read in conjunction with the joint *Australian Competition and Consumer Commission (ACCC) and OAIC Compliance and Enforcement Policy for the Consumer Data Right (ACCC and OAIC Compliance and Enforcement Policy)*.
- Some of the OAIC's guidance material relates to the OAIC's regulatory powers. This is designed to provide targeted information about specific regulatory powers to the OAIC's various stakeholders, including complainants and regulated entities.

Regulatory powers available

As outlined in the *Privacy regulatory action policy* and the My Health Records Enforcement Guidelines, the Privacy Act, My Health Records Act and Part IVD of the Competition and Consumer Act confer a range of enforcement and other regulatory powers on the Commissioner, which are based on an escalation model. These include the following powers:

- directing an agency (but not an organisation) to give the Commissioner a privacy impact assessment (Privacy Act s 33D)
- monitoring, or conducting an assessment of, whether personal information or CDR data is being maintained and handled by an entity as required by law (Privacy Act ss 28A and 33C; Competition and Consumer Act s 56ER)
- conciliating a complaint (Privacy Act s 40A)
- investigating a matter (either in response to a complaint (Privacy Act s 40(1)) or on the Commissioner's own initiative (Privacy Act s 40(2)), and various related powers including to decline to investigate a complaint (s 41), to refer the matter and discontinue an investigation where certain offences may have been committed (s 49), and to refer a complaint to a specified alternative complaint body (s 50) (see generally Privacy Act Part V)
- reporting to the Minister in certain circumstances such as following an investigation, monitoring activity or assessment (Privacy Act ss 30 and 32), or report to the Minister, the ACCC or the Data Standards Chair in relation to assessments conducted under the CDR scheme (Competition and Consumer Act s 56ER(3))
- accepting an enforceable undertaking (Privacy Act s 80V; My Health Records Act s 80; Competition and Consumer Act s 56EW)
- bringing proceedings to enforce an enforceable undertaking (Privacy Act s 80V; My Health Records Act s 80; Competition and Consumer Act s 56EW)

- making a determination (Privacy Act s 52)
- bringing proceedings to enforce a determination (Privacy Act ss 55A and 62)
- seeking an injunction (Privacy Act s 80W; My Health Records Act s 81; Competition and Consumer Act s 56EX)
- applying to the court for a civil penalty order (Privacy Act s 80U; My Health Records Act s 79; Competition and Consumer Act s 56EU)
- directing an entity to make a notification under the Notifiable Data Breaches scheme (NDB scheme) (Privacy Act s 26WR) or CDR scheme (Competition and Consumer Act s 56ES), or declaring the notification is not required or can be delayed (Privacy Act s 26WQ).

Contraventions of certain provisions of the My Health Records Act are ‘interferences with privacy’ for the purposes of the Privacy Act and the OAIC may investigate those contraventions either under the Privacy Act (using the investigative provisions in Part V of the Privacy Act) or under the My Health Records Act. The My Health Records Enforcement Guidelines provide guidance about the OAIC’s approach to investigating these My Health Records Act contraventions.

Section 56ET(3) of the Competition and Consumer Act extends the application of the OAIC’s regulatory powers under Part V of the Privacy Act to include the enforcement of privacy safeguards and privacy or confidentiality related CDR Rules under the CDR scheme. Therefore, the Commissioner can investigate an act or practice that may be a breach the privacy safeguards and privacy or confidentiality related CDR Rules under the CDR scheme.

It is open to the OAIC to use a combination of privacy regulatory powers to address a particular matter.

Regulatory action principles

The *Privacy regulatory action policy* sets out the principles which will guide the OAIC when it takes privacy regulatory action. These principles are independence, accountability, proportionality, consistency, timeliness and transparency.

Similarly, the *CDR regulatory action policy* and the *ACCC and OAIC Compliance and Enforcement Policy* set out the principles which will guide the OAIC when it takes regulatory action in relation to the CDR scheme. These principles are accountability, efficiency, fairness, proportionality and transparency.

The OAIC will take regulatory action in accordance with the principles set out in the *Privacy regulatory action policy* and, where relevant, the *CDR regulatory action policy* and the My Health Records Enforcement Guidelines.

Importantly, when taking privacy regulatory action, the OAIC will act consistently with general principles of good decision making, as explained in the *Best Practice Guides* published by the Administrative Review Council in 2007.² In particular, the OAIC will act fairly and in accordance with principles of natural justice (or procedural fairness).

In addition, in any litigation, the OAIC will act in accordance with its obligations to act as a model litigant in accordance with the *Legal Services Directions 2017*.

² The Administrative Review Council *Best Practice Guides* are published at [Other ARC publications](#).

Approach to using regulatory powers and selecting appropriate action

An investigation may be commenced by the OAIC into a suspected or alleged interference with privacy, either on receipt of a complaint or as a Commissioner initiated investigation (CII).

Following a complaint investigation or CII, the Commissioner may decide to take enforcement action against an entity. The available enforcement powers escalate from less serious to more serious options.

The *Privacy regulatory action policy*, the *CDR regulatory action policy* and My Health Records Enforcement Guidelines provide further guidance about how the OAIC decides whether to take privacy or CDR regulatory action and what action to take, including:

- the steps the OAIC can use to facilitate legal and best practice compliance
- the factors taken into account in deciding when to take privacy or CDR regulatory action, and what action to take
- the sources of information the OAIC will consider in seeking to identify both systemic issues and serious issues that can be targeted for privacy or CDR regulatory action.

When making a decision as to whether or not to exercise a regulatory power, the OAIC will be guided by the *Privacy regulatory action policy*, the *CDR regulatory action policy* or My Health Records Enforcement Guidelines as appropriate.

Chapter 1: Privacy complaint handling process

Contents

Legislative framework	1
General approach to handling privacy complaints	3
How the OAIC handles privacy complaints	4
Representative complaints	5
Confidentiality	5
Investigating privacy complaints	6
Conciliating a complaint	7
Types of outcomes in conciliated matters	7
How the OAIC tries to conciliate matters	8
Compulsory conciliation conference	8
Use of conciliation information	9
Deciding not to investigate a complaint	9
Referral of matters	10
Purpose of the OAIC's complaint referral powers	10

Legislative framework

- 1.1 Section 36(1) of the Privacy Act provides for an individual (the complainant) to complain to the Commissioner about an interference with their privacy by certain Australian Government agencies or private sector organisations (the respondent).¹
- 1.2 A complaint about an act or practice that may be an interference with privacy can be made by an individual on their own behalf, and on behalf of other individuals with their consent.
- 1.3 The Privacy Act also provides for representative complaints to be made on behalf of a class of people where all the class members are affected by an interference with privacy (s 38(1)).
- 1.4 Section 13 of the Privacy Act sets out the acts and practices that may be an interference with the privacy of an individual. These include:

¹ The Privacy Act also covers the Norfolk Island public sector. For information about what agencies and organisations are covered by the Privacy Act see [Rights and responsibilities](#).

- a breach of an Australian Privacy Principle (APP) or a registered APP privacy code²
 - a breach of rules under s 17 in relation to tax file number information
 - a breach of a provision of Part IIIA or the registered CR code,³ and
 - a breach of prescribed NDB scheme requirements.⁴
- 1.5 Other legislation can also provide that an act or practice is an interference with privacy and therefore can be investigated by the Commissioner:
- s 73 of the *My Health Records Act 2012* (Cth)
 - s 29 of the *Healthcare Identifiers Act 2010* (Cth)
 - s 35L of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
 - s 135AB of the *National Health Act 1953* (Cth)
 - s 173 of the *Personal Property Securities Act 2009* (Cth), and
 - s 22A of the *National Cancer Screening Register Act 2016* (Cth).
- 1.6 Section 56ET(3) of the Competition and Consumer Act extends the Commissioner’s investigative powers under Part V of the Privacy Act to apply to the handling of CDR data for CDR consumers, which includes individuals and small businesses.⁵ This means the Commissioner can investigate an act or practice that may be a breach of a Privacy Safeguard and privacy or confidentiality related CDR Rules under the CDR scheme.
- 1.7 The Commissioner also has power to investigate complaints made under Part VIIC of the *Crimes Act 1914* (Cth) concerning the Commonwealth spent convictions scheme and s 13 of the *Data-Matching Program (Assistance and Tax) Act 1990*, and exercises some of the functions of the ACT Information Privacy Commissioner under the *Information Privacy Act 2014* (ACT).
- 1.8 Further information on the OAIC's role in investigating breaches of privacy provisions contained in other legislation is available at [Other legislation](#).⁶
- 1.9 Part V of the Privacy Act outlines the processes by which privacy complaints can be handled. This may include one or more of the following steps — conducting preliminary inquiries, opening an investigation, attempting to conciliate a complaint, and making a determination.
- 1.10 The Commissioner has a wide range of powers relating to the privacy complaint handling process including to:
- assist a person to formulate and make a complaint (s 36(4))
 - make preliminary inquiries of any person (s 42)

² For acts that occurred on or after 12 March 2014. For events that occurred prior to 12 March 2014 the relevant principles are, for government agencies, the Information Privacy Principles and, for organisations, the National Privacy Principles.

³ For acts that occurred on or after 12 March 2014. For events that occurred prior to 12 March 2014 the law as it was at 11 March 2014 applies.

⁴ Contained in s 26WH(2), s 26WK(2), s 26WL(3), and s 26WR(10).

⁵ Note that this only applies in relation to CDR complaints, and that small businesses cannot make complaints about any other act or practice that may be an interference with privacy as defined in s 13 of the Privacy Act, as individuals can under s 36 of the Privacy Act. “Individual” is defined in s 6 of the Privacy Act to mean a natural person.

⁶ How a complaint is handled under legislation other than the Privacy Act may vary according to any specific handling requirements of that legislation.

- transfer matters to an alternative complaint body in certain circumstances (s 50)
 - attempt to conciliate the complaint (s 40A)
 - conduct an investigation into the complaint (s 40)
 - at any stage, not investigate, or cease to investigate or not investigate further, the complaint on various grounds (generally referred to as a ‘decline’) (ss 41, 49, 49A)
 - require a person to give information or documents, or to attend a compulsory conference (ss 44, 45, 46, 47)
 - enter premises to inspect documents (s 68)
 - accept an enforceable undertaking (s 80V)
 - make a determination about the complaint (s 52)
 - seek to enforce a determination in a court (s 55A).
- 1.11 Not all of these powers will be used in resolving any particular complaint. These powers are explained further throughout this Chapter or elsewhere in this Guide.
- 1.12 To facilitate the complaint handling process the Commissioner delegates complaint handling functions to OAIC staff, other than the s 52 power to determine a matter. Throughout the rest of this Chapter we have used ‘the OAIC’ unless the power or function can only be performed by the Commissioner.
- 1.13 The Commissioner also has an agreement with the ACT Government to handle complaints under the *Information Privacy Act 2014* (ACT) about breaches of the Territory Privacy Principles by ACT public sector agencies. The powers in relation to handling those complaints are outlined in the ACT legislation and, in some respects differ from the Privacy Act powers. For more information see [Privacy in the ACT](#).

General approach to handling privacy complaints

- 1.14 The OAIC provides a free, informal and accessible complaint process. Parties do not require legal representation to participate in the complaint handling process or the determination process.⁷ Parties generally bear their own costs in the complaint handling process, including any legal expenses.
- 1.15 Where appropriate, the OAIC endeavours to resolve complaints through conciliation. Generally, where a complaint is not declined for some reason, or it cannot be resolved through conciliation, the complaint may be determined by the Commissioner under s 52.
- 1.16 The OAIC has an impartial role so does not advocate for any party in handling a privacy complaint.
- 1.17 In carrying out the OAIC 's functions to investigate and, if appropriate, to attempt to resolve privacy complaints through conciliation, the OAIC will:
- use a process that is accessible, flexible and timely, and done in accordance with the principles of natural justice and procedural fairness

⁷ For more information about the determination process see Chapter 4.

- focus on providing an opportunity for the parties to resolve complaints through conciliation.

How the OAIC handles privacy complaints

- 1.18 Complaints must be in writing and must identify the person making the complaint, the respondent and the alleged act or practice that is an interference with privacy. The OAIC cannot accept anonymous complaints.
- 1.19 Complaints are assessed on receipt. If the complaint does not reach the threshold required because it does not identify an interference with privacy the OAIC will contact the complainant and advise them why their matter cannot be dealt with as a complaint. The OAIC may provide appropriate assistance to the complainant to help formulate the complaint. Where appropriate the OAIC may refer the complainant to another agency or organisation that may be able to assist them.⁸
- 1.20 Where a matter reaches the required threshold to be a complaint under s 36 the OAIC will consider how best to deal with it. The OAIC can, at any stage of the process, attempt to conciliate the complaint or decline to investigate the complaint based on the information available to the OAIC.
- 1.21 Generally a complainant must have complained to the respondent⁹ and given them a chance to respond to the complaint before the OAIC can investigate (s 40(1A)).¹⁰ In limited circumstances the OAIC may decide to investigate the complaint if it is considered that it is not appropriate for the complainant to first complain to the respondent, for example:
- where there is a significant power differential between the complainant and respondent and the complainant may be disadvantaged in a direct approach to the respondent to resolve the issues in the complaint
 - where there is a history of similar issues associated with the respondent
 - where the complaint identifies a systemic issue.¹¹
- 1.22 Section 40(1B) of the Privacy Act also provides for additional circumstances in which the OAIC can investigate a complaint without requiring a complainant to first complain to the respondent. This relates to complaints about access to and correction of credit reporting information.
- 1.23 Where a complaint raises an issue that could be an interference with privacy the OAIC may conduct preliminary inquiries to obtain relevant information of any person to assist with the handling of the complaint.¹² These inquiries may be made, for example, to clarify the allegations in the complaint or to confirm that the OAIC has jurisdiction.

⁸ See the 'Referral of matters' section towards the end of this Chapter.

⁹ Organisations and agencies may find our resource [Handling privacy complaints](#) useful in dealing with privacy complaints.

¹⁰ In addition, complainants are encouraged to use the services of a [recognised EDR scheme](#), of which the respondent is a member, before approaching the OAIC, but this is not mandatory. The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 stated (on page 4) that (*relevant*) amendments proposed to the Privacy Act (*and now enacted*) were intended to recognise and encourage the use of external dispute resolution services.

¹¹ See definition of systemic privacy issues in the *Privacy regulatory action policy* (paras 12–13).

¹² Section 42 of the Privacy Act.

- 1.24 Where the OAIC is unlikely to open an investigation for a reason provided for by s 41 of the Privacy Act¹³ the OAIC will contact the complainant and advise them of our view. The OAIC will generally write to the complainant outlining our reasons for that view and ask if they have any further relevant information that they wish to provide. In these cases the OAIC does not generally advise the respondent of the complaint unless a decision to proceed to investigation is made.
- 1.25 The Privacy Act obliges the OAIC to make a reasonable attempt to conciliate the complaint where the OAIC is of the view it is reasonably possible that a complaint could be successfully conciliated (s 40A). Conciliation can be attempted at any stage of the complaint handling process.
- 1.26 When the OAIC has opened an investigation into the complaint, under s 40, the OAIC can compel the production of relevant documents and information or require witnesses to attend and answer questions (s 44), if that will assist the investigation. Where a complaint is not declined or finalised on some other basis, and cannot be resolved through conciliation, and an investigation has been opened, the Commissioner may determine the complaint under s 52 of the Privacy Act.
- 1.27 A complainant can withdraw a complaint at any time without penalty.

Representative complaints

- 1.28 The Privacy Act allows for representative complaints to be made where an act or practice may be an interference with the privacy of a number of individuals. Particular conditions apply to a representative complaint and these are outlined in ss 38 to 39 of the Act. A representative complaint does not need to identify the class members by name or specify how many class members there are, however, an individual who is part of a class where a representative complaint has been lodged cannot bring an individual complaint unless they withdraw from the representative complaint.
- 1.29 Conditions for making a representative complaint include:
- that the class members have a complaint against the same respondent
 - the complaints all arise out of the same or similar circumstances, and
 - the complaints give rise to a substantial common issue of law or fact.
- 1.30 A representative complaint must address each of these conditions in the complaint and also identify the remedy or relief sought. A representative complaint may be lodged by a complainant who is a class member or a person or organisation who is not a class member.
- 1.31 The OAIC may not accept or continue with a representative complaint where the OAIC is not satisfied the complainant can adequately represent the interests of the class members.

Confidentiality

- 1.32 The OAIC is bound by the APPs when handling complaint related personal information, and manages complaints confidentially. As such, the OAIC does not disclose the particulars of a complaint during the complaint handling process to persons other than the parties to a

¹³ For more information about the OAIC's power to decline a complaint see 'Deciding not to investigate a complaint' later in this Chapter.

complaint or third parties with information relevant to the inquiry that can assist the inquiry. This is to ensure that parties will participate fully and frankly in the complaint process.

- 1.33 The Privacy Act does not impose an obligation of confidentiality on the parties to a complaint. However, APP obligations do apply to APP entities and information they obtain during the course of a complaint. If the parties have settled the matter with an agreement that includes a confidentiality clause they may be bound by that agreement.
- 1.34 In addition, conciliation, where that is occurring, works best in an atmosphere where parties can raise issues in a frank way without fear of the information being disseminated further and the OAIC encourages parties not to disseminate information while involved in the conciliation process.

Investigating privacy complaints

- 1.35 Where possible the OAIC tries to handle privacy complaints informally and flexibly. In some cases, before commencing an investigation under s 40 of the Privacy Act, the OAIC may conduct preliminary inquiries and obtain information that will assist the OAIC to explain an issue to a complainant that may resolve an issue or lead the complainant to withdraw the complaint on the basis they are satisfied with the explanation that has been provided.
- 1.36 Where the OAIC has established jurisdiction to investigate it will generally notify a respondent of the complaint under the investigation power (s 40). The respondent will be provided with a copy of the complaint, asked to respond to the specific issues in the complaint and to tell the OAIC whether they are willing to try to resolve the complaint through conciliation.
- 1.37 In many cases a complaint can be quickly resolved prior to a detailed written response being provided. This occurs in circumstances where a respondent is willing to try to resolve the complaint on the terms the complainant has identified, or is willing to negotiate terms of resolution with the complainant.
- 1.38 For procedural fairness and transparency, generally any substantive information provided by a party to a complaint will be provided to the other party to facilitate the handling of the complaint. This includes the complaint, the respondent's response, offers of resolution and other relevant information.
- 1.39 Generally the OAIC does not accept confidential submissions. If information that is commercially sensitive or is sensitive for some other reason has to be provided to assist the OAIC with its investigation the OAIC will usually ask that the information be provided in a form that can be provided to the other party.¹⁴
- 1.40 At each stage of the complaint process the officer handling the matter will assess the available information and keep the parties advised of the OAIC's views on the matter. Where an investigation has been commenced the OAIC may decline to continue to investigate a matter, or attempt to conciliate a matter, at any stage during the investigation where that appears to be the appropriate course of action.
- 1.41 Where the OAIC's investigation indicates that it is likely that an interference with privacy has occurred and conciliation is not considered appropriate or conciliation has been attempted without resolution, then the OAIC may investigate the matter and will consider what

¹⁴ See Chapter 4 as well in relation to confidential information, in the context of making a determination.

enforcement action to take. The OAIC will review the matter against either the *Privacy regulatory action policy* or the *CDR regulatory action policy* or the *My Health Records Enforcement Guidelines 2016* as applicable to assess the appropriate enforcement response.

- 1.42 Generally the appropriate enforcement response for a complaint, where an investigation has been opened, conciliation has not resolved the matter and the complaint has not been declined, will be a determination under s 52. However other enforcement action may also be considered appropriate, in addition to a determination, for example seeking a civil penalty for a serious or repeated interference with privacy.
- 1.43 Where the OAIC considers that there is a likelihood that it will decide to seek a civil penalty for a serious or repeated interference with privacy, the complaint investigation will be conducted with a view to ensuring that sufficient admissible evidence will be available to allow that case to be pursued in court if necessary. For more information see Chapter 6 on civil penalties.

Conciliating a complaint

- 1.44 Where the OAIC considers it is reasonably possible a complaint may be conciliated successfully there must be a reasonable attempt to conciliate (s 40A(1)).
- 1.45 The OAIC is not required to attempt to resolve the complaint through conciliation where the OAIC has decided not to investigate, or not to further investigate, a complaint.
- 1.46 Factors the OAIC may take into account in assessing whether it is possible to successfully conciliate a complaint may include:
- the approach taken by the parties to conciliation i.e. willingness to discuss conciliation, whether resolution proposals are generally appropriate and proportionate to the nature of the complaint and outcomes generally applicable to privacy complaints
 - previous resolution attempts and any outcomes achieved or actions taken by either party regarding the complaint
 - the responsiveness of the parties to the OAIC's attempts to assist the parties to resolve a complaint, and
 - the length of time the OAIC and the parties have taken to try to resolve a complaint.
- 1.47 The OAIC will generally ask the complainant to outline what they are seeking to resolve the complaint and ask the respondent to consider that proposal or propose an alternative basis for resolution.

Types of outcomes in conciliated matters

- 1.48 Outcomes that may be achieved in privacy complaints may include:
- change in practice, procedure or policy
 - access to information
 - staff training
 - review of privacy policies and procedures
 - statement of regret or a private or public apology

- financial compensation.
- 1.49 Parties will be advised of resources and information to help them develop or respond to a proposal for resolution, for example, determinations by the Commissioner, information about conciliated matters the OAIC has published in annual reports or on its website, and complaint outcomes in similar jurisdictions, for example, New Zealand and New South Wales privacy jurisdictions and the Commonwealth discrimination jurisdiction.

How the OAIC tries to conciliate matters

- 1.50 The OAIC generally tries to resolve privacy complaints through conciliation by:
- phone and email based shuttle negotiations - where the parties are separately communicated with
 - teleconferences involving all parties
 - face to face meetings with the parties (where practicable and appropriate).
- 1.51 In each case the officer handling the matter will contact the parties to discuss the issues in the complaint and the outcome being sought. The officer will try to assist the parties to negotiate a satisfactory resolution to the complaint.
- 1.52 Where a matter is resolved the parties may enter into a conciliation agreement or deed of release prepared by one of the parties to the complaint or the OAIC. In limited situations the Commissioner may accept an enforceable undertaking from the respondent as part of the resolution of a complaint (for more information see Chapter 3 Enforceable undertakings).
- 1.53 Sometimes a party to a complaint may be legally represented. To ensure fairness in the process the OAIC may recommend to the parties that they get legal or other professional advice if they are entering into a legal deed or agreement.
- 1.54 Where conciliation is successful the file will be closed on the basis the matter has been adequately dealt with.
- 1.55 Where a complaint is not able to be resolved through conciliation the matter will generally move to determination under s 52 or be declined under the powers available in s 41. Although the matter could be finalised under s 40A on the basis there is no reasonable likelihood that the matter will be resolved by conciliation, this discretionary power would only be used in limited circumstances.

Compulsory conciliation conference

- 1.56 The OAIC can require a complainant or respondent or other relevant party to attend a conciliation conference (s 46). A person who has been directed to attend and fails to attend is guilty of an offence.
- 1.57 Generally, the OAIC relies on voluntary participation in a conciliation process as resolution generally relies on the understanding that parties are participating in good faith to genuinely resolve the matter.
- 1.58 In some cases where a matter is not able to be resolved through voluntary participation the OAIC may consider compelling a person to attend a conciliation conference where the OAIC is of the view the matter may be able to be resolved if the parties were to deal directly with each other over the complaint. Factors that may contribute to this view are where:

- the proposals for resolution are appropriate to the interference with privacy raised by the complaint
 - a party indicates they are willing to resolve a complaint but are unwilling to commit to a resolution process or outcome
 - the parties have been involved in extended negotiations and it is likely the matter may resolve if the parties are required to deal with the remaining issues at hand.
- 1.59 The OAIC may advise the parties of the intention to issue a notice compelling their attendance at a conciliation conference where the matter has been unable to be resolved through usual conciliation processes.
- 1.60 The OAIC may take into account the parties' circumstances in issuing a notice to compel attendance at a conciliation conference, for example, whether the parties are legally represented, geographic considerations, and constraints on time to ensure the parties are able to comply with the notice to attend.

Use of conciliation information

- 1.61 Anything said or done in the course of conciliation cannot be used in any legal proceedings or in any hearing before the Commissioner (including where the Commissioner decides to determine the matter under s 52 of the Privacy Act), except where the parties otherwise consent. Conciliation information may also be used in circumstances where something was said or done to advance the commission of a fraud or an offence, or renders a person liable to a civil penalty.
- 1.62 Generally this will mean that the Commissioner will not consider anything said or done in conciliation in any determination hearing or determination decision. If a party seeks a review, by the AAT or Federal Court, of a decision in a determination the Commissioner cannot refer to information about the conciliation process in those proceedings.

Deciding not to investigate a complaint

- 1.63 The OAIC may at any time during the complaint process exercise the discretion not to investigate a complaint or not to investigate a complaint further for a reason provided for in s 41 of the Act. This is commonly referred to as 'declining a complaint'.
- 1.64 The OAIC will consider all the information provided by the parties and any other relevant information in deciding whether to decline to investigate or further investigate a complaint.
- 1.65 The Commissioner or delegate may decide not to investigate or investigate further for a range of reasons provided for by s 41 which include where he or she is satisfied that:
- the act or practice is not an interference with privacy
 - the complaint was made more than 12 months after the complainant became aware of the act or practice
 - the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith
 - a recognised external dispute resolution scheme has dealt with, or would more effectively deal with, the act or practice, for example, the Telecommunications Industry

Ombudsman, Financial Ombudsman Service, Credit & Investments Ombudsman or a state or territory based energy, water or transport related Ombudsman

- the act or practice is subject to an application, or would be more appropriately dealt with, under another Commonwealth, state or territory law, for example, this might include discrimination law or other court proceedings, or
- the respondent has dealt with, or is adequately dealing with the complaint, for example, where a deed of release about the same subject matter has previously been entered into.

- 1.66 A decision to decline a complaint for one of the reasons in s 41 is a discretion exercised by the Commissioner or the Commissioner's delegate and consequently subject to review under the *Administrative Decisions (Judicial Review) Act 1977 (Cth)*. Given this, there is a requirement that a decision to decline a complaint is subject to due care and based on information that can withstand rigorous review.
- 1.67 Where the OAIC is intending to decline a complaint the OAIC will advise the complainant, in writing, of that view and the reasons for it and provide an opportunity for the complainant to provide any further information they think is relevant. The OAIC will consider any additional information before making a final decision on how to proceed with the complaint.

Referral of matters

- 1.68 Section 50 of the Privacy Act allows the OAIC to not investigate, or not investigate further, a matter and to transfer it to an 'alternative complaint body' where the OAIC forms the opinion that:
- a complaint (or application where applicable) relating to that matter has been, or could have been, made by the complainant to the alternative complaint body, and
 - the matter could be more conveniently or effectively dealt with by that alternative complaint body.
- 1.69 The 'alternative complaint bodies' to which the OAIC can transfer matters include the Australian Human Rights Commission, the Commonwealth Ombudsman, and an external dispute resolution scheme recognised by the Commissioner under s 35A of the Privacy Act.

Purpose of the OAIC's complaint referral powers

- 1.70 Referral of a complaint to an alternative complaint body is likely to arise in very limited cases where the OAIC's jurisdiction overlaps with that of an alternative complaint body, and the complaint (or application) may be made about the act or practice to either the OAIC or the other body and the referral will ensure that the complaint is dealt with in the most convenient and effective manner.
- 1.71 The OAIC will generally only use the referral power where:
- it considers that a complaint or application relating to the matter has been, or could have been made, to an alternative complaint body which provides a better or more effective remedy for the subject matter of the complaint, and
 - there is no relevant ground on which the OAIC should decline to investigate the complaint, and

- the complainant does not accept the OAIC's advice to withdraw their complaint and make a complaint or application to the alternative complaint body.
- 1.72 Affording an individual the opportunity to first withdraw their complaint and make a complaint or application to the alternative complaint body themselves is intended to allow an individual to, as much as possible, retain responsibility and control over how their matter is dealt with.
- 1.73 From 1 July 2020, the OAIC may transfer CDR complaints to the ACCC, or to a recognised EDR scheme, if it considers the matter is best dealt with by such entities. The transfer of complaints to the ACCC is permitted by s 29(2)(aa)(iv) of the *Australian Information Commissioner Act 2010*, and to EDRs under s 50 of the Privacy Act as outlined above. This is also in line with the 'no wrong door' policy of the CDR scheme, whereby if the OAIC or ACCC, as co-regulators of the scheme, receive a matter that is best dealt with by the other, or by an EDR scheme, the matter is transferred across to that body.

Chapter 2: Commissioner initiated investigations and referrals

Contents

Legislative framework	1
Referral of allegations to the OAIC	2
OAIC framework for considering referrals	3
Considerations in opening a CII	4
Procedural steps in conducting a CII	4
1. Notification to respondent	4
2. Information gathering	4
3. Decision making	4
4. Conclusion and publication	5

Legislative framework

- 2.1 Section 40 of the Privacy Act gives the Commissioner the power to conduct investigations.
- 2.2 Section 40(2) of the Privacy Act enables the Commissioner to commence an investigation on the Commissioner's own initiative, where:
- a. an act or practice may be an interference with the privacy of an individual or a breach of Australian Privacy Principle (APP) 1; and
 - b. the Commissioner thinks it is desirable to do so.
- 2.3 The Commissioner can also commence investigations into the privacy aspects of the CDR scheme. This is because s 56ET of the Competition and Consumer Act provides that s 40(2) of the Privacy Act extends to a possible breach of a privacy safeguard, or a privacy or confidentiality related CDR Rule, and a data breach made under Part IIIC of the Privacy Act relating to the CDR scheme.
- 2.4 Investigations conducted under s 40(2) are known as 'Commissioner initiated investigations' (CIIs).
- 2.5 Prior to commencing an investigation, the Commissioner may conduct preliminary inquiries under s 42(2) of the Privacy Act, to determine whether to commence a CII. Once a CII has been commenced, the OAIC will conduct its investigation in accordance with Part V of the Privacy Act.
- 2.6 Where the Commissioner has identified an interference with privacy, there are a number of enforcement powers available to the Commissioner.



- 2.7 The Commissioner endorses a focus on engagement, advice and support in preference to deterrence and punishment where appropriate.
- The Commissioner’s powers, ranging from less serious to more serious regulatory action, include the ability to:
 - conduct an assessment of an entity’s privacy practices (s 33C of the Privacy Act; s 56ER of the Competition and Consumer Act) and provide non-binding recommendations
 - accept an enforceable undertaking (s 80V of the Privacy Act; s 56EW of the Competition and Consumer Act)
 - make a determination (s 52 of the Privacy Act) directing an entity to take certain steps
 - bring proceedings to enforce an enforceable undertaking (s 80V of the Privacy Act; s 56EW of the Competition and Consumer Act)
 - bring proceedings to enforce a determination (ss 55A and 62 of the Privacy Act)
 - seek an injunction to prevent conduct that would constitute a contravention of the Privacy Act (s 80W of the Privacy Act), and against CDR participants to enforce the privacy safeguards (s 56EX of the Competition and Consumer Act)
 - apply to a court for a civil penalty order for a breach of a civil penalty provision (s 80 U of the Privacy Act), and seek civil penalties for certain contraventions of the privacy safeguards (s 56EU of the Competition and Consumer Act), which includes serious or repeated interferences with privacy.
- 2.8 The Commissioner may, at any time, also decide to discontinue an investigation where the Commissioner is satisfied that no further regulatory action is warranted in the circumstances. This may occur where the Commissioner decides that the entity has not breached the Privacy Act or the requirements of the privacy safeguards and CDR Rules, or if the Commissioner considers there has been a breach that is immaterial or has been adequately dealt with.

Referral of allegations to the OAIC

- 2.9 The OAIC becomes aware of matters that may warrant the commencement of a CII through a number of channels, including:
- a complaint by an individual, or a representative complaint (under the Privacy Act), or a CDR consumer (under the Competition and Consumer Act)
 - a referral from another regulator or external dispute resolution (EDR) scheme
 - media reports and social media commentary
 - a referral from a member of the community or information provided by an informant
 - information gathered in the course of other regulatory activity of the OAIC (for example, privacy assessments, data breach notifications, and engagement with the ACCC in relation to the CDR scheme).

OAIC framework for considering referrals

- 2.10 The OAIC has a range of options available to respond to referrals, including no action, provision of general guidance or preliminary inquiries for the purpose of deciding whether to commence a CII. The OAIC will consider each referral it receives against its strategic regulatory priorities.
- 2.11 In deciding how to respond to a referral, the key considerations are the likelihood that the allegation referred to the OAIC is accurate, and the seriousness of the alleged breach. The OAIC may also consider the other matters outlined in the *Privacy regulatory action policy*, or the *CDR regulatory action policy* for CDR matters. In deciding whether to take any action in response to an alleged breach of the Privacy Act, the OAIC will consider the likelihood of an allegation, and its seriousness. The OAIC's response will be based on an evaluation of each allegation with reference to its potential seriousness, as summarised in the table below.

 Seriousness	No action	Commence CII (or preliminary inquiries)	Commence CII (or preliminary inquiries)
	No action	Advise respondent of allegation and provide general guidance	Advise respondent of allegation and provide general guidance
	No action	No action	Advise respondent of allegation and provide general guidance
	 Likelihood		

- 2.12 If an allegation is both serious and likely, the OAIC will commence preliminary inquiries and may recommend the Commissioner conduct a CII.
- 2.13 If an allegation appears likely to be accurate, but is less serious, the OAIC will typically write to the respondent to advise that an allegation has been made, and provide general guidance to allow the respondent to address the issue itself.
- 2.14 In other cases the OAIC will not take action in response to a referral. However, the OAIC will keep a record of the referral and may refer to it in future.
- 2.15 The OAIC will not usually reveal the name of the person who made the referral to the respondent.
- 2.16 Where referrals relate to allegations about compliance with the CDR scheme, the OAIC may provide the ACCC with details of the allegation and any action the OAIC has taken in response.

Considerations in opening a CII

- 2.17 The Commissioner's primary objective when undertaking a CII is improving the privacy practices of investigated entities and the regulated community generally.
- 2.18 When deciding whether to commence a CII, the OAIC will consider the factors identified in the OAIC's *Privacy regulatory action policy*, and where appropriate, the *CDR regulatory action policy* and its strategic regulatory priorities.
- 2.19 The Commissioner will also consider the specific and general educational, deterrent or precedential value of commencing a CII, and whether it presents an opportunity to provide guidance to industry, Government or the public on better privacy practice and acceptable privacy standards.

Procedural steps in conducting a CII

- 2.20 Where the OAIC decides to commence a CII, the following four steps will be taken.

1. Notification to respondent

- 2.21 The OAIC will notify the respondent in writing about its decision to commence a CII, and the initial scope of the investigation. If during the course of the investigation other issues arise in relation to the respondent's compliance with the APPs or the privacy safeguards and CDR Rules, these may be considered as part of the investigation. After notifying the respondent of the investigation, the OAIC will typically place a notice on its website stating that it is commencing an investigation. However, the OAIC will not comment further until the investigation is complete.

2. Information gathering

- 2.22 The OAIC will correspond with the respondent to gather information. The OAIC will seek the cooperation of the respondent in the provision of necessary information, and the respondent is typically the OAIC's primary source of relevant information.
- 2.23 The OAIC may gather information from other sources as required, such as the ACCC for CDR matters.
- 2.24 The Commissioner may issue a notice under s 44 of the Privacy Act requiring a person to provide information or produce documents, or to give evidence to the Commissioner in person.

3. Decision making

- 2.25 The Commissioner will consider the information provided to the OAIC and form a preliminary view in relation to the matter.
- 2.26 The Commissioner may decide to exercise a discretionary power under s 41 of the Privacy Act to discontinue an investigation, including where the Commissioner is satisfied that no breach has occurred or that the breach has been adequately dealt with by the respondent and no further regulatory action is warranted in the circumstances.

- 2.27 Where the Commissioner forms a preliminary view that the respondent has failed to meet the requirements of the Privacy Act or the requirements of the privacy safeguards or CDR Rules, the Commissioner may take further regulatory action, including the following:
- The Commissioner may seek an enforceable undertaking from the respondent under s 33E of the Privacy Act and s 56EW of the Competition and Consumer Act. More information about enforceable undertakings is available in Chapter 3 of this guide.
 - The Commissioner may make a determination under s 52(1A) of the Privacy Act. The determination, including the Commissioner's reasons for the determination, will be published on the OAIC's website. More information about determinations is available in Chapter 4 of this guide.
 - The Commissioner may seek an injunction against a person to enforce the Privacy Act (s 80W of the Privacy Act) and against CDR participants to enforce the privacy safeguards (s 56EX of the Competition and Consumer Act). More information about injunctions is available in Chapter 5 of this guide.
 - Where a civil penalty provision has been breached, the Commissioner may apply to the court for a civil penalty order under s 80U of the Privacy Act and s 56EU of the Competition and Consumer Act. More information about civil penalties is available in Chapter 6 of this guide.
 - The Commissioner may report to the Minister about a CII under s 30 of the Privacy Act. In certain circumstances, the Commissioner is required to report to the Minister.
- 2.28 The Commissioner may decide that although the entity has breached the Privacy Act or the requirements of the privacy safeguards and CDR Rules, no further action is required. This will depend on the specific circumstances of the matter, and if the Commissioner forms this view, the Commissioner may send a warning letter to the entity which sets out the OAIC's awareness of acts or practices of the entity that may not be compliant with its privacy obligations, and warns the entity that the OAIC may take future privacy regulatory action if it does not improve its compliance.

4. Conclusion and publication

- 2.29 At the conclusion of a CII, the OAIC will typically place a notice on its website advising of the conclusion of the investigation.
- 2.30 Where the Commissioner considers there is sufficient public interest in an incident, the Commissioner may publish a report of the investigation, which would be published alongside or as part of any enforceable undertaking or determination.
- 2.31 The OAIC will make decisions about communications in connection with CIIs in accordance with the considerations set out in the 'Public communication as part of regulatory action' sections of the *Privacy regulatory action policy*, and where appropriate, the *CDR regulatory action policy*.

Chapter 3: Enforceable undertakings

Contents

Legislative framework	1
Enforceable undertaking under the Privacy Act	1
Enforceable undertaking under the My Health Records Act	2
Enforceable undertaking under the Competition and Consumer Act	2
Purpose and key features of an enforceable undertaking	4
Who can give an enforceable undertaking?	4
At what point can an enforceable undertaking be accepted?	4
Enforceable undertaking terms and requirements	5
Procedural steps	6
Raising the possibility of an enforceable undertaking	6
Negotiating the terms of the enforceable undertaking	7
Commissioner considers whether to accept the enforceable undertaking	7
Approval of the Independent Expert	8
Decision communicated to the respondent	8
Undertaking published	9
Ongoing monitoring	9
Varying, withdrawing and cancelling an enforceable undertaking	9
Breach of an enforceable undertaking	10
Enforcement through the Court	10
Publication	11

Legislative framework

- 3.1 An enforceable undertaking is a written agreement between an entity or person (the respondent) and the Commissioner, which is provided under either the Privacy Act, the My Health Records Act or the Competition and Consumer Act, and is enforceable against the respondent in the courts.

Enforceable undertaking under the Privacy Act

- 3.2 Section 114 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) empowers the Commissioner to accept a written undertaking given by an entity that it will either:

- take specified action in order to comply with the Privacy Act
 - refrain from taking specified action in order to comply with the Privacy Act
 - take specified action directed towards ensuring that the entity does not contravene a provision under the Privacy Act, or is unlikely to contravene such a provision in the future.
- 3.3 An enforceable undertaking may be varied or withdrawn with the consent of the Commissioner (s 114 (3) of the Regulatory Powers Act), or cancelled by the Commissioner (s 114 (5) of the Regulatory Powers Act).
- 3.4 If the Commissioner considers that an entity has breached an undertaking, the Commissioner may apply to the Federal Court or Federal Circuit Court to enforce the undertaking (ss 113 and 115 of the Regulatory Powers Act, s 80V of the Privacy Act).

Enforceable undertaking under the My Health Records Act

- 3.5 Under s 114 of the Regulatory Powers Act, the Commissioner may accept a written undertaking in relation to the My Health Records Act given by a person that the person will:
- take specified action in order to comply with the My Health Records Act
 - refrain from taking specified action, in order to comply with the My Health Records Act
 - take specified action directed towards ensuring that the person does not contravene the My Health Records Act, or is unlikely to contravene the My Health Records Act, in the future.
- 3.6 Section 80 of the My Health Records Act triggers the provisions of Part 6 of the Regulatory Powers Act which provides a framework for accepting and enforcing undertakings relating to compliance with legislative provisions. This means that the Commissioner may accept an undertaking relating to compliance with a My Health Records Act provision that is enforceable under Part 6 of the Regulatory Powers Act.
- 3.7 An enforceable undertaking may be varied or withdrawn with the consent of the Commissioner, or cancelled by the Commissioner.
- 3.8 If the Commissioner considers that a person has breached an undertaking accepted under s 80 of the My Health Records Act and that undertaking has not been withdrawn or cancelled, the Information Commissioner may apply to the relevant court for an order directing the person to comply with the undertaking (or one or more of the orders listed in Part 6 of the Regulatory Powers Act).

Enforceable undertaking under the Competition and Consumer Act

- 3.9 Under s 114 of the Regulatory Powers Act, the Commissioner may accept a written undertaking in relation to the CDR scheme as set out in the Competition and Consumer Act, given that the person will:
- take specified action in order to comply with the privacy safeguards
 - refrain from taking specified action, in order to comply with the privacy safeguards

- take specified action directed towards ensuring that the person does not contravene the privacy safeguards, or is unlikely to contravene the privacy safeguards, in the future.
- 3.10 Section 56EW of the Competition and Consumer Act triggers the provisions of Part 6 of the Regulatory Powers Act which provides a framework for accepting and enforcing undertakings relating to compliance with legislative provisions. This means that the Commissioner may accept an undertaking relating to compliance with a privacy safeguard provision that is enforceable under Part 6 of the Regulatory Powers Act.
- 3.11 An enforceable undertaking may be varied or withdrawn with the consent of the Commissioner, or cancelled by the Commissioner.
- 3.12 If the Commissioner considers that a person has breached an undertaking accepted under s 56EW of the Competition and Consumer Act and that undertaking has not been withdrawn or cancelled, the Commissioner may apply to the relevant court for an order directing the person to comply with the undertaking (or one or more of the orders listed in Part 6 of the Regulatory Powers Act).

Which Act to use?

- 3.13 Acts or practices that interfere with an individual's privacy but do not relate to a contravention of the My Health Records Act, or to a privacy safeguard set out in Part IVD of the Competition and Consumer Act, are governed by the Privacy Act and an enforceable undertaking that relates to those acts or practices will be accepted by the Commissioner under the Privacy Act.
- 3.14 Acts or practices that contravene certain provisions of the My Health Records Act are deemed by s 73 of that Act to be an interference with an individual's privacy for the purposes of the Privacy Act. Depending on the circumstances, an enforceable undertaking in relation to these contraventions may be able to be accepted under the My Health Records Act or the Privacy Act.
- 3.15 Sub-section 80(2) of the My Health Records Act also empowers the My Health Record System Operator¹ to accept enforceable undertakings. The Commissioner may consult with the System Operator when investigating a complaint and considering accepting an undertaking, in line with the *Agreement for information sharing and complaint referral relating to the personally controlled electronic health (eHealth) record system between the OAIC and the System Operator*.²
- 3.16 For conduct that is a breach of a privacy safeguard, the Commissioner may accept an enforceable undertaking under the Competition and Consumer Act.

¹ 'System Operator' is defined in s 14 of the My Health Records Act.

² The [agreement](#) can be viewed on the OAIC's website.

Purpose and key features of an enforceable undertaking

- 3.17 An enforceable undertaking is an important enforcement tool for use in situations where there has been or appears to have been an interference with the privacy of an individual³ and the Commissioner considers an agreed change to future behaviour offers the most appropriate regulatory outcome in the particular circumstances.
- 3.18 Generally, an enforceable undertaking seeks to have a respondent voluntarily agree to:
- modify its acts, practices, procedures or behaviour to ensure it complies with the law (for example, ceasing the practice that led to the breach or implementing new policies for handling personal information)
 - remedy the damage any breach has caused (for example making an apology or making a payment to an individual or individuals to rectify damage)
 - commit to certain future compliance measures (for example conducting reviews and audits, providing training for managers and staff and implementing a compliance monitoring and reporting framework).

Who can give an enforceable undertaking?

- 3.19 An enforceable undertaking for conduct under the Privacy Act can only be given by ‘an entity’. The term ‘entity’ means an agency, an organisation or a small business operator (these terms are further defined in s 6(1) of the Privacy Act). The term ‘organisation’ can include an individual (including a sole trader).
- 3.20 An enforceable undertaking for conduct under the My Health Records Act and the Competition and Consumer Act can be given by ‘a person’.⁴ This term captures both individuals and participants in the My Health Record system, such as registered repository operators, portal operators and healthcare provider organisations.
- 3.21 For each undertaking, the individual giving and executing the undertaking must have the authority to negotiate on behalf of, and bind, the respondent entity or person.

At what point can an enforceable undertaking be accepted?

- 3.22 The Commissioner may accept an enforceable undertaking given by an entity or person where the Commissioner considers there is a reasonable basis to suggest that the entity or person has interfered with the privacy of an individual. For example, an enforceable undertaking may be accepted during a complaint investigation, an enquiry into a data breach incident, or a Commissioner initiated investigation.

³ The *Privacy regulatory action policy* and the My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 outline the range of avenues through which the OAIC may become aware of alleged interferences with privacy or other privacy concerns.

⁴ The term ‘person’ is not defined in the My Health Records Act and the Competition and Consumer Act, so the meaning is drawn from the *Acts Interpretation Act 1901* (Cth). That Act states that expressions used to denote persons generally, such as ‘person’, include a body politic or body corporate as well as an individual (s 2C).

- 3.23 An enforceable undertaking may form part of a conciliated outcome following a complaint. Section 40A of the Privacy Act requires the Commissioner to make a reasonable attempt to conciliate a complaint where the Commissioner considers there is a reasonable possibility that the complaint can be conciliated successfully.

Enforceable undertaking terms and requirements

- 3.24 The Privacy Act, the My Health Records Act and Part IVD of the Competition and Consumer Act do not impose a particular structure for an enforceable undertaking. However, an undertaking must be written and must be expressed to be an undertaking under s 114 of the Regulatory Powers Act.
- 3.25 In addition, the OAIC expects that the terms of any undertaking will usually (at a minimum):
- state the name of the respondent, the date the undertaking was accepted by the Commissioner and the date when the undertaking comes into effect
 - be signed by the CEO or other senior executive of the respondent and the Commissioner (or approved delegate) – without the signature of both parties, the undertaking has no effect
 - describe and acknowledge the act(s) or practice(s) about which the OAIC is concerned
 - outline specified steps the respondent will take to rectify the act or practice, and ensure that it is not repeated or continued. This will usually include a requirement for the respondent to complete reviews and establish a monitoring and reporting framework. Specifically, the respondent will usually be required to:
 - nominate in writing a representative responsible for overseeing compliance with the undertaking and reporting to the OAIC
 - engage, in consultation with the OAIC, an appropriately experienced and qualified third party to review the act or practice and make recommendations to improve the respondent's compliance with the Privacy Act (the Independent Expert)
 - ensure that the OAIC receives a copy of the Independent Expert's report, including a copy of the Independent Expert's draft report prior to engagement with the respondent
 - implement the recommendations in that report
 - provide a certification by the Independent Expert to the OAIC that the respondent has implemented the recommendations and rectified the deficiencies identified by the review
 - outline what, if any, steps the respondent will take to notify individuals affected by the act or practice, where it has not already done so
 - contain dates by which the respondent must complete each step
 - be readily understood; for example, an undertaking that deals with complex and technical issues may have a glossary to define the terms used
 - be capable of implementation and include action which is capable of being measured or tested objectively
 - be certain and capable of enforcement; for example, each step that the respondent is required to complete must be clear and unambiguous

- contain the respondent's agreement to material that arose in conciliation (if conciliation occurred) being submitted in any proceeding to enforce the undertaking.⁵ Where an undertaking forms parts of a conciliated outcome, this could be achieved by a statement of agreed facts being attached to the undertaking with the consent of both the respondent and complainant
- outline what, if any, steps the respondent will take to resolve the matter with individuals affected by the act or practice; for example, payment the respondent will make by way of compensation for any loss or damage suffered by reason of the act or practice of concern
- contain the respondent's acknowledgement that the OAIC may publish the undertaking in full (see 'Publication' below for further information). Any concerns the respondent has about publication should be raised and resolved as the terms of the undertaking are being negotiated.

3.26 For undertakings relating to the My Health Record system, reference should also be made to ss 8 and 9 of the My Health Records Enforcement Guidelines when considering the terms of an undertaking.

3.27 The Commissioner will not accept an undertaking that:

- denies responsibility for the act or practice of concern⁶
- merely undertakes to comply with the law without explaining how compliance will be achieved
- seeks to impose terms or conditions on the OAIC or Commissioner (however, the undertaking may include an acknowledgement that certain information provided to the OAIC pursuant to the undertaking is communicated in confidence).

Procedural steps

3.28 When the acceptance of an enforceable undertaking is a possible regulatory outcome in a matter, the OAIC will generally follow the process set out below.

Raising the possibility of an enforceable undertaking

3.29 The possibility of an enforceable undertaking may arise where either:

- the respondent suggests to the OAIC that it gives an undertaking in relation to a matter
- the OAIC raises the possibility of an undertaking with the respondent as a potential option in relation to a matter.

3.30 Before the OAIC raises the possibility of an undertaking, or when the respondent suggests giving an undertaking, the OAIC must assess whether an undertaking offers an appropriate

⁵ This is necessary because s 40A(5) of the Privacy Act limits the circumstances in which evidence of anything said or done in the course of the conciliation can be relied upon in legal proceedings. Such material can be used for this purpose where both the respondent and complainant agree. The OAIC would also need to obtain the complainant's agreement before material from a conciliation can be used in enforcement proceedings.

⁶ This does not preclude the possibility of an enforceable undertaking being accepted on a 'without prejudice' basis in circumstances where the OAIC considers that it would provide an effective regulatory outcome.

regulatory outcome in a matter, or whether an alternative regulatory outcome would be more appropriate. In making this assessment, the OAIC will refer to the factors set out in the [Privacy regulatory action policy](#), the [CDR regulatory action policy](#) or the [My Health Records Enforcement Guidelines](#) as applicable.

Negotiating the terms of the enforceable undertaking

- 3.31 Where the Commissioner considers that an undertaking may be an appropriate regulatory outcome in the matter and the respondent will consider giving an undertaking in relation to the matter, the OAIC and respondent can commence negotiation of the terms of that undertaking.
- 3.32 When negotiating the terms of the enforceable undertaking, the Commissioner (through the OAIC) will have regard to:
- the requirements for the terms of an undertaking set out above in this chapter or, if the undertaking is related to the My Health Records Act, ss 8.4 and 8.5 and ss 9.3 and 9.4 of the My Health Records Enforcement Guidelines
 - the interests of individuals who have been the subject of an interference with privacy
 - the OAIC's goal of taking enforcement action and how an undertaking will contribute to fulfilling the OAIC's regulatory role in the particular matter (see the [Privacy regulatory action policy](#) and [CDR regulatory action policy](#))
 - the principles guiding regulatory decisions and action outlined in the [Privacy regulatory action policy](#) or the [CDR regulatory action policy](#) if applicable, or if the undertaking is related to the My Health Records Act, the My Health Records Enforcement Guidelines.
- 3.33 Until an undertaking is accepted and signed by the Commissioner, the Commissioner retains the discretion to accept or not accept the undertaking when it is submitted for final approval. Any agreement on terms between OAIC staff and the respondent is 'in principle' agreement only and subject to final acceptance by the Commissioner.
- 3.34 At the outset of negotiations, the OAIC will identify a reasonable time frame within which any undertaking should be negotiated. If an agreed undertaking cannot be negotiated within that time, the OAIC will consider pursuing alternative enforcement mechanisms such as potential for the Commissioner to make a determination in respect of the matter.

Commissioner considers whether to accept the enforceable undertaking

- 3.35 Where OAIC staff and the respondent have agreed on terms, the proposed undertaking to be given by the respondent will be submitted to the Commissioner for consideration.
- 3.36 The decision to accept an undertaking in the terms given by the respondent will be made by the Commissioner.
- 3.37 Whether the Commissioner accepts an undertaking will be determined on a case by case basis, with reference to the [Privacy regulatory action policy](#), the [CDR regulatory action policy](#) or the My Health Records Enforcement Guidelines (as applicable), and whether the Commissioner believes that the respondent has the ability to, and genuinely intends to, comply with the terms of the undertaking.

Approval of the Independent Expert

- 3.38 The Independent Expert is expected to provide assurance to the Commissioner that the steps planned or taken by the respondent satisfy the terms of the undertaking. The Independent Expert must be competent to undertake the role and independent from the respondent, such that he or she can bring objective and impartial judgment to the role. It is important that the Independent Expert is, and is seen to be, independent.
- 3.39 It is the responsibility of the respondent and the proposed Independent Expert to demonstrate competence and independence. The Commissioner may make any inquiries considered necessary in order to be satisfied that the proposed Independent Expert brings the requisite competence and independence to the role.
- 3.40 Factors the Commissioner may consider when determining whether a proposed Independent Expert is competent to undertake the role:
- the qualifications, experience and technical expertise of the proposed Independent Expert, or the senior staff within the relevant entity who will be engaged in the work
 - whether the Independent Expert has adequate resources to perform the necessary work
 - where appropriate, references from entities regarding the proposed Independent Expert's demonstrated experience in related work.
- 3.41 Factors the Commissioner may consider when determining whether a proposed Independent Expert is sufficiently independent to undertake the role:
- whether the fees and remuneration received by the proposed Independent Expert from the respondent in the previous two years are material (materiality should be considered in the context of the Independent Expert's Australian-based revenue)
 - what other work senior staff proposed to conduct the work of the Independent Expert, have been engaged in for or on behalf of the respondent in the previous two years
 - whether there are any staff from the Independent Expert's entity embedded in the respondent's organisation, or otherwise operating under a co-sourcing arrangement
 - whether the senior staff proposed to conduct the work of the Independent Expert have ever previously worked for the respondent
 - whether the senior staff proposed to conduct the work of the Independent Expert have a financial or other interest in the respondent's business, such as shares
 - whether the senior staff proposed to conduct the work of the Independent Expert have previously audited, reviewed, planned, advised or implemented any systems and processes of the respondent, and if so, whether there is a nexus between those systems and processes and the undertaking
 - any joint ventures between the proposed Independent Expert and the respondent
 - whether the Independent Expert has satisfactory policies and processes in place to ensure that any conflict of interest that arises during the course of the undertaking is managed appropriately and reported to the Commissioner.

Decision communicated to the respondent

- 3.42 The OAIC will communicate the Commissioner's decision in writing to the respondent.

- 3.43 Where the Commissioner has agreed to accept the undertaking, this written correspondence will request the respondent to arrange signing of the undertaking by the CEO or other senior executive of the respondent, before returning the signed copy to the OAIC for execution by the Commissioner.
- 3.44 Where the Commissioner has not agreed to accept the undertaking, the written correspondence will advise the respondent of the OAIC's next steps in the matter. This may involve further negotiations in relation to the proposed undertaking, or consideration of alternative enforcement action.

Undertaking published

- 3.45 Once the undertaking has been executed by both the respondent and the Commissioner, the OAIC will generally publish the undertaking (see the 'Publication' heading below).

Ongoing monitoring

- 3.46 It is the respondent's responsibility to ensure it complies with the terms of the undertaking. The OAIC will maintain contact with the respondent and monitor the respondent's compliance, including by ensuring that required reports and notifications are provided in accordance with the timeframes outlined in the enforceable undertaking. If the respondent breaches the undertaking, the OAIC may take further action (see below).

Varying, withdrawing and cancelling an enforceable undertaking

- 3.47 A respondent can vary or withdraw an enforceable undertaking, but must have the consent of the Commissioner in order to do so.⁷
- 3.48 The decision as to whether or not to allow a respondent to vary or withdraw an undertaking will be made by the Commissioner on a case-by-case basis.
- 3.49 The Commissioner generally will only consent to the variation or withdrawal of an undertaking if:
- compliance with the enforceable undertaking is subsequently found to be impractical, or
 - there has been a material change in the circumstances which led to the undertaking being given, meaning that variation or withdrawal are appropriate in the circumstances.
- 3.50 In addition, the Commissioner will only consent to variation or withdrawal where satisfied that an appropriate regulatory outcome will still be achieved in the circumstances. In the case of the withdrawal of an undertaking, the OAIC may decide to take alternative enforcement action.
- 3.51 A respondent wishing to seek consent to varying or withdrawing an undertaking should make a request in writing to the OAIC. Where the Commissioner consents to the variation or

⁷ Privacy Act s 80V, My Health Records Act s80, which trigger Part 6 of the Regulatory Powers Act.

withdrawal of an undertaking, the OAIC will communicate this decision to the respondent in writing.⁸

- 3.52 In addition, the Commissioner may, by written notice given to the respondent, cancel an undertaking accepted under either the Privacy Act, the My Health Records Act or the Competition and Consumer Act.⁹ A decision to cancel an undertaking would normally only be made where subsequent information or conduct by the respondent leads the OAIC to consider that the undertaking is not an effective regulatory outcome in the circumstances. This is only expected to occur in exceptional circumstances, for example, if the Commissioner was misled about the extent of a particular breach.

Breach of an enforceable undertaking

- 3.53 Where the OAIC believes that a respondent has breached the terms of an enforceable undertaking, the OAIC will generally use the following procedure.
- 3.54 The OAIC will first bring the issue of suspected or actual non-compliance with the terms of the undertaking to the attention of the respondent and seek a response. This notification and response may be sufficient to resolve the breach.
- 3.55 The OAIC may decide to address non-compliance through the court enforcement mechanisms in Part 6 of the Regulatory Powers Act. This process is outlined below.
- 3.56 The factors which the Commissioner will take into account when deciding whether to seek an order from a court to enforce an undertaking are set out in the *Privacy regulatory action policy* and, where applicable, the *CDR regulatory action policy* or the My Health Records Enforcement Guidelines. In addition, the Commissioner will also consider the following factors:
- the nature and length of non-compliance
 - the reason for non-compliance
 - whether the non-compliance was inadvertent
 - whether the respondent had previously not complied with the terms.
- 3.57 In limited circumstances, the OAIC may initiate further negotiations with the respondent to expand or otherwise vary the terms of the undertaking.
- 3.58 For an undertaking relating to compliance with the My Health Records Act, the OAIC may also refer the issue to the My Health Record System Operator who has the power to take administrative action against the respondent.

Enforcement through the Court

- 3.59 Where the OAIC decides to address non-compliance through the court enforcement mechanisms in Part 6 of the Regulatory Powers Act, the Commissioner may apply to a relevant court for one of a number of orders.

⁸ See s 114(3) of the Regulatory Powers Act.

⁹ See s 80V of the Privacy Act, s 80 of the My Health Records Act and s 56EW of the Competition and Consumer Act, which trigger Part 6 of the Regulatory Powers Act; also see s 8.8 of the My Health Records Enforcement Guidelines.

3.60 In general terms, a court may make any or all of the following orders:

- directing the respondent to comply with the undertaking
- directing the respondent to pay compensation
- any other kind that the court thinks appropriate.

Publication

3.61 The OAIC may publish an enforceable undertaking on the OAIC's website (s 80V (4) of the Privacy Act and s 80 (4) of the My Health Records Act).

3.62 Generally, the OAIC will publish an undertaking on its website <www.oaic.gov.au>. An undertaking will usually contain an acknowledgement from the respondent that the undertaking may be published, unless the OAIC has agreed otherwise with the respondent when the undertaking terms were being negotiated (see above). The OAIC may agree otherwise where it is inappropriate to publish all or part of an undertaking because of statutory secrecy provisions or for reasons of privacy, confidentiality, commercial sensitivity, security or privilege.

3.63 The publication of an undertaking may be accompanied by other communications such as a media release, media interview or social media posts. The OAIC generally will also publicly communicate:

- a decision by the Commissioner to vary, withdraw or cancel a published undertaking
- the initiation of court proceedings to enforce an undertaking.

3.64 In addition, before court proceedings are initiated, the OAIC may publicly communicate the fact that a respondent has breached the terms of an undertaking and that the OAIC is making inquiries with the respondent.

Chapter 4: Determinations

Contents

Legislative framework	1
When will a determination be made?	2
Following an investigation of a complaint	2
Following an investigation on the Commissioner's own initiative	2
Procedural steps in making a determination	3
Content of determinations	4
Compensation	5
Following an investigation of a complaint	5
Following an investigation on the Commissioner's own initiative	6
Publication of determinations	6
Review rights	6
Enforcement of determinations	7

Legislative framework

- 4.1 After investigating a complaint,¹ the Commissioner may make a determination which either dismisses the complaint or finds that the complaint is substantiated (s 52(1)).
- 4.2 The complaint handling process under the Privacy Act is free and informal. Parties do not require legal representation to participate in the complaint handling process or the determination process. Parties generally bear their own costs in the complaint handling process.²
- 4.3 The Commissioner can also make a determination after conducting an investigation on his or her own initiative (s 52(1A)).³

¹ Information about our complaint handling process can be found in Chapter 1.

² Where a matter is determined s 52(3) provides for the Commissioner to award an amount to reimburse a complainant for expenses reasonably incurred by the complainant in connection with the making of the complaint and the investigation of the complaint.

³ Information about Commissioner initiated investigations can be found in Chapter 2.

When will a determination be made?

Following an investigation of a complaint

- 4.4 The Commissioner generally tries to resolve complaints through conciliation as provided for by the Privacy Act (s 40A). Sometimes where a matter cannot be resolved through conciliation, and where the complaint is not able to be finalised on some other basis (for example, because the complaint is declined under s 41(1)), the Commissioner may make a determination under s 52.
- 4.5 When deciding whether to make a determination in response to a complaint under s 36, the Commissioner will take into account a number of factors. Factors that would weigh in favour of a determination include that:
- it appears there is a prima facie interference with privacy,⁴ the parties are unable to resolve the matter through conciliation, and the matter cannot otherwise be finalised
 - one or both parties has requested that the matter be finalised by way of a determination and the Commissioner considers that making a determination would be the appropriate resolution in the particular circumstances
 - the issues raised by the complaint are complex and/or systemic⁵
 - the investigation process has not been able to resolve whether an interference with privacy has occurred, and it is likely that the determination process would resolve that question.
- 4.6 The OAIC will also review the matter against either the *Privacy regulatory action policy*, the *CDR regulatory action policy* or the My Health Records Enforcement Guidelines as applicable when considering whether to make a determination.

Following an investigation on the Commissioner's own initiative

- 4.7 Following an investigation on the Commissioner's own initiative, the Commissioner may make a determination under s 40(1A).
- 4.8 A determination is one of several possible outcomes of a Commissioner initiated investigation where a breach appears likely to have occurred. Rather than finalising an investigation by determination, the Commissioner might, for example, accept an enforceable undertaking offered by the respondent. The possible outcomes are discussed in Chapter 2 – Commissioner initiated investigations.
- 4.9 When deciding whether to make a determination, the Commissioner will take into account a number of factors. Factors that would weigh in favour of a determination include that:
- it appears there is a prima facie interference with privacy
 - the respondent has not cooperated with the Commissioner's inquiries or investigation, and the Commissioner believes that it is necessary to make formally binding

⁴ As explained in the Introduction, an 'interference with privacy' includes contraventions of certain provisions of the My Health Records Act.

⁵ See definition of systemic privacy issues in the *Privacy regulatory action policy* (paras 12-13).

declarations that the respondent must take certain steps to address the interference with privacy

- there is a disagreement between the Commissioner and the respondent about whether an interference with privacy has occurred, and the determination would allow that question to be resolved, and
- there is a public interest in the Commissioner making a declaration setting out his or her reasons for finding that an interference with privacy has occurred, and the appropriate response by the respondent.

4.10 The OAIC will also review the matter against either the *Privacy regulatory action policy*, the *CDR regulatory action policy* or the My Health Records Enforcement Guidelines as applicable when considering whether to make a determination.

Procedural steps in making a determination

4.11 In making a determination, the Commissioner may conduct further investigation, and consider additional submissions and information provided by the parties.

4.12 The procedural steps below relate to a determination following investigation of a complaint, but will generally apply in the case of a determination following a Commissioner initiated investigation. However, some steps may not be relevant to a Commissioner initiated investigation, given there is no ‘complainant’ or conciliation process.

4.13 Where a matter is to proceed to determination the OAIC will generally take these steps:

- The OAIC will notify the parties in writing about its decision to make a determination and the basis for that decision. The notice will state how to make submissions, if the parties wish to do so, and the timeframe for making any submissions. In limited cases oral submissions may be sought. The Commissioner may also seek specific information about the remedies sought by the complainant.
- The Commissioner cannot consider any action done or information provided during the course of conciliation unless the complainant and respondent both agree (s 40A).
- If the Commissioner requires further information, and it is not voluntarily forthcoming on request, the Commissioner may, under s 44 of the Privacy Act, require the production of that information from the complainant, the respondent or a third party. The Commissioner may also, under s 45, require a witness to attend and answer questions.
- The Commissioner will adhere to the principles of natural justice and procedural fairness in determining a matter. Those principles include the parties having the opportunity to examine and comment on the information the Commissioner relies on in making the determination. On this basis, the OAIC will provide each party with the submissions and information received from the other party.
- Submissions will generally not be accepted on a confidential basis. This is because any determination made by the Commissioner would not be able to explicitly refer to the contents of such a submission and, in addition, a determination based on material in the submission would generally not satisfy the ‘procedural fairness’ principle unless the other party has been given a chance to respond to it.
- In exceptional circumstances where confidential or commercially sensitive information is essential to the determination process, the Commissioner will accept that information

on a confidential basis and provide access to a summary of that material to ensure the other party is not disadvantaged.

- Parties may request that the Commissioner hold a hearing before making a determination under s 43A of the Act. However, whether a hearing is held is at the discretion of the Commissioner (s 43A(2)(c)). Where a party has requested a hearing, the Commissioner will give all interested parties a reasonable opportunity to make a submission about the request (s 43A(2)(b)).
- Where the Commissioner has allowed an oral submission to be made or a hearing to be held, both parties will generally be invited to participate. The format of a hearing generally comprises the parties providing their oral submissions and responding to questions that the Commissioner may have. The format will also depend on a range of matters including whether the hearing is held by phone, by video conference or at the OAIC's, or another, premise.
- The Commissioner may seek external expert opinion, independent of the parties and at no cost to them, where a matter arising from the determination process raises issues that would benefit from specific technical or other expertise. In those cases, the parties will be advised of the name and qualifications of the external expert and their role in the proceedings.
- In making the determination, the Commissioner will determine whether, on the balance of probabilities, an interference with privacy occurred, having regard to all information available to the Commissioner.

Content of determinations

4.14 A determination will generally contain the following information:

- the relevant parties, including, where relevant, the class members who are to be affected by the determination in relation to a representative complaint (s 53)
- the background to and summary of the complaint or Commissioner initiated investigation, which may include a chronology of events
- the OAIC's investigation process
- the legislative framework
- a summary of the parties' submissions
- any findings of fact (s 52(2))
- whether the complaint is substantiated (s 52(1)(b)) or is dismissed (s 52(1)(a)) following an investigation of a complaint
- any relevant declarations or orders which may include:
 - a declaration that the respondent has engaged in conduct that interfered with the privacy of an individual and that the respondent should not repeat or continue the conduct (s 52(1)(b)(i); s 52(1A)(a))
 - a declaration that respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued (s 52(1)(b)(ia); s 52(1A)(b))

- a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant (s 52(1)(b)(ii)), or with a Commissioner initiated investigation, any loss or damage suffered by one or more individuals whose privacy has been interfered with (s 52(1A)(c))
- a declaration that the complainant (or a Commissioner initiated investigation, one or more individuals whose privacy has been interfered with) is entitled to compensation (s 52(1)(b)(iii); s 52(1A)(d))
- a declaration that it would be inappropriate for any further action to be taken in the matter (52(1)(b)(iv); s 52(1A)(e))
- for determination following a complaint, a declaration that the complainant is entitled to a specified amount to reimburse the complainant for expenses reasonably incurred by the complainant in connection with making the complaint and the investigation of the complaint (s 52(3))
- in relation to representative complaints, the Commissioner may specify amounts or a way to work out amounts for payment to the complainants concerned (s 52 (4)) and may make directions in relation to the manner in which a class member is to establish his or her entitlement to the payment of an amount under the determination; and the manner for determining any dispute regarding the entitlement of a class member to the payment (s 52(5))
- the relevant review and enforcement mechanisms (discussed below).

Compensation

Following an investigation of a complaint

4.15 Where the Commissioner makes a declaration that a complainant is entitled to an amount of compensation, the Commissioner is guided by the following principles on awarding compensation, drawn from a Federal Court decision:

- where a complaint is substantiated and loss or damage is suffered, the legislation contemplates some form of redress in the ordinary course
- awards should be restrained but not minimal
- in measuring compensation the principles of damages applied in tort law will assist, although the ultimate guide is the words of the statute
- in an appropriate case, aggravated damages may be awarded
- compensation should be assessed having regard to the complainant's reaction and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances.⁶

4.16 In addition, the Commissioner is also guided by the principle that once loss is proved, there would need to be good reason why compensation for that loss should not be awarded.⁷ Loss

⁶ *Hall v A & A Sheiban Pty Ltd* (1989) 20 FCR 217 as referred to in *Rummery and Federal Privacy Commissioner* [2004] AATA 1221, [32]-[35].

⁷ *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 [34].

or damage in this context can include hurt feelings and/or humiliation suffered by the complainant. The Commissioner may also award an amount to reimburse the complainant for expenses reasonably incurred in connection with the making of the complaint and the investigation of the complaint.

- 4.17 In deciding whether to award compensation and in assessing the appropriate amount of compensation, the Commissioner will consider the information submitted by the parties and previous privacy determinations.
- 4.18 The Commissioner can also award aggravated damages as well as general damages where he or she is of the view it is warranted.⁸ The principles for awarding aggravated damages, drawn from Federal Court decisions, include:
- aggravated damages may be awarded where the respondent behaved ‘high-handedly, maliciously, insultingly or oppressively in committing the act’ complained about⁹
 - the ‘manner in which a defendant conducts his or her case may exacerbate the hurt and injury suffered by the plaintiff so as to warrant the award of additional compensation in the form of aggravated damages’.¹⁰

Following an investigation on the Commissioner’s own initiative

- 4.19 The Commissioner also has power to award compensation following a determination made after an investigation conducted on the Commissioner’s own initiative.
- 4.20 However, a Commissioner initiated investigation is less likely to determine the quantum of loss or damage suffered by individuals affected by an interference with privacy. Rather than awarding compensation by determination, the OAIC would typically inform affected individuals to make a complaint about the act or practice if the individual believes he or she has suffered compensable loss or damage.

Publication of determinations

- 4.21 Once made, and sent to the parties, determinations will be published on the OAIC’s website and on the AustLII website.¹¹
- 4.22 The Commissioner will generally publish the name of the respondent. However, the Commissioner will generally not publish the names of complainants, respondent individuals or any third party individuals.

Review rights

- 4.23 A party may apply under s 96 of the Privacy Act to have a decision under subsection 52(1) or (1A) to make a determination reviewed by the AAT. The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy

⁸ *Rummery* [2004] AATA 1221 [32].

⁹ *Hall v A & A Sheiban Pty Ltd* [1989] FCA 72 [75].

¹⁰ *Elliott v Nanda & Commonwealth* [2001] FCA 418 [180].

¹¹ [Australian Information Commissioner on AustLII](#).

determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the *Administrative Appeals Tribunal Act 1975* (Cth)). An application fee may be payable when lodging an application for review to the AAT.

- 4.24 A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) to have the determination reviewed by the Federal Circuit Court or the Federal Court of Australia. The Court may refer the matter back to the Commissioner for further consideration if it finds the decision was wrong in law or the Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court.

Enforcement of determinations

- 4.25 Under s 55 of the Privacy Act, where a determination applies to a respondent that is not a government agency, the respondent must comply with any declarations made in the determination within the period specified in the determination.
- 4.26 Under s 58 of the Privacy Act, where a determination applies to a government agency it must comply with any declarations made by the Commissioner in that determination.
- 4.27 Either the complainant or Commissioner may commence proceedings in the Federal Court or the Federal Circuit Court for an order to enforce a determination. However different rules apply depending on who the respondent is, for example, if the respondent is not a government agency the Court will re-examine whether there has been an interference with privacy.

Chapter 5: Injunctions

Contents

Legislative framework	1
Injunctions under the Privacy Act	1
Injunctions under the My Health Records Act	2
Injunctions under the Competition and Consumer Act	3
Purpose and key features of an injunction	4
Interim injunctions	4
Permanent injunctions	5
Injunctions restraining a person from engaging in conduct	5
Injunctions requiring a person to do a thing	6
The content of injunctions	6
Procedural steps in seeking an injunction	6
After an injunction has been granted	8
Publication	8

Legislative framework

- 5.1 An injunction is a Court order directing a person to do a specific thing or, more commonly, to not do a specific thing.
- 5.2 The Privacy Act, the My Health Records Act and the Competition and Consumer Act empower the Commissioner to apply to a federal Court for an injunction against a person. This chapter relates to an injunction application made by the Commissioner.

Injunctions under the Privacy Act

- 5.3 Section 80W of the Privacy Act with Part 7 of the Regulatory Powers Act empowers the Commissioner (or any other person) to apply to the Federal Court or Federal Circuit Court for an injunction.
- 5.4 Where a person has engaged, is engaging, or is proposing to engage, in any conduct that constituted or would constitute a contravention of the Privacy Act, the Court may grant an injunction:
 - restraining a person from engaging in the conduct; and
 - if in the Court’s opinion it is desirable to do so, requiring the person to do an act or thing (s 121(1) of the Regulatory Powers Act).

- 5.5 The Court may also grant an injunction requiring a person to do an act or thing where the person has refused or failed, is refusing or failing, or is proposing to refuse or fail, to do that act or thing where that refusal or failure was, is, or would be a contravention of the Privacy Act (s 121(2) of the Regulatory Powers Act).
- 5.6 Where an application is made to a Court for an injunction under s 80W, the Court may, if in the Court's opinion it is desirable to do so, grant an interim injunction restraining a person from engaging in conduct pending the determination of the application (s 122 of the Regulatory Powers Act).
- 5.7 'Person' in Part 7 of the Regulatory Powers Act includes natural persons, bodies politic, corporations, companies and bodies corporate.¹

Injunctions under the My Health Records Act

- 5.8 Under s 81 of the My Health Records Act, the Commissioner (or the My Health Record System Operator²) may apply to a Court for an injunction. Section 81 of the My Health Records Act triggers the provisions of Part 7 of the Regulatory Powers Act which deals with obtaining, imposing and discharging injunctions to enforce legislative provisions.
- 5.9 If a person has engaged, is engaging or is proposing to engage in any conduct that constituted, constitutes or would constitute a contravention of the My Health Records Act, a Court may grant an injunction:
- restraining the person from engaging in the conduct; and
 - if in the Court's opinion it is desirable to do so, requiring the person to do any act or thing.
- 5.10 The Court may also grant an injunction requiring a person to do an act or thing if the person has refused or failed, is refusing or failing, or is proposing to refuse or fail, to do that act or thing and that refusal or failure was, is, or would be a contravention of the My Health Records Act.
- 5.11 Under the My Health Records Act, a 'Court' means the Federal Court of Australia, the Federal Circuit Court, or a court of a State or Territory that has jurisdiction in relation to matters arising under the My Health Records Act (s 81(3)).
- 5.12 If an application is made to a Court for an injunction under s 81 of the My Health Records Act (see also Part 7 of the Regulatory Powers Act), the Court may grant an interim injunction restraining a person from engaging in conduct or requiring a person to do a thing, before considering the application and pending the determination of the application. See below for further information about interim injunctions.
- 5.13 'Person', for the purpose of s 81 of the My Health Records Act, includes natural persons, bodies politic, corporations, companies and bodies corporate.³

¹ Section 2C of the *Acts Interpretation Act 1901* and s 6(4) of the Privacy Act.

² 'System Operator' is defined in s 14 of the My Health Records Act.

³ Section 2C of the *Acts Interpretation Act 1901*.

Injunctions under the Competition and Consumer Act

- 5.14 Under s 56EX of the Competition and Consumer Act, the Commissioner may apply to a Court for an injunction. Section 56EX of the Competition and Consumer Act triggers the provisions of Part 7 of the Regulatory Powers Act.
- 5.15 If a person has engaged, is engaging or is proposing to engage in any conduct that constituted, constitutes or would constitute a contravention of a privacy safeguard, a Court may grant an injunction:
- restraining the person from engaging in the conduct; and
 - if in the Court’s opinion it is desirable to do so, requiring the person to do any act or thing.
- 5.16 The Court may also grant an injunction requiring a person to do an act or thing if the person has refused or failed, is refusing or failing, or is proposing to refuse or fail, to do that act or thing and that refusal or failure was, is, or would be a contravention of a privacy safeguard.
- 5.17 Under the Competition and Consumer Act, a ‘relevant court’ means the Federal Court of Australia, the Federal Circuit Court, or a court of a State or Territory that has jurisdiction in relation to the matter (s 56EX(3)).
- 5.18 If an application is made to a Court for an injunction under s 56EX of the Competition and Consumer Act (see also Part 7 of the Regulatory Powers Act), the Court may grant an interim injunction restraining a person from engaging in conduct or requiring a person to do a thing, before considering the application and pending the determination of the application. See below for further information about interim injunctions.
- 5.19 ‘Person’, for the purpose of s 56EX of the Competition and Consumer Act, includes natural persons, bodies politic, corporations, companies and bodies corporate.⁴

Which Act to use?

- 5.20 Conduct that interferes, or would interfere, with an individual’s privacy, but does not relate to a contravention of the My Health Records Act or to a privacy safeguard set out in Part IVD of the Competition and Consumer Act, is governed by the Privacy Act, and the Commissioner may apply to a Court for an injunction under that Act.
- 5.21 Conduct that contravenes certain provisions of the My Health Records Act are deemed by s 73 of that Act to be an interference with an individual’s privacy for the purposes of the Privacy Act. Depending on the circumstances, the Commissioner may apply to a Court in relation to conduct that contravenes or would contravene certain provisions of the My Health Records Act, for an injunction under the My Health Records Act or the Privacy Act.
- 5.22 Section 81 of the My Health Records Act also empowers the My Health Record System Operator to make an application for an injunction. The OAIC may consult with the System Operator when investigating a complaint and considering whether to apply for an injunction, in line with the *Agreement for information sharing and complaint referral relating to the personally controlled electronic health (eHealth) system between the OAIC and the System Operator*.⁵

⁴ Section 2C of the *Acts Interpretation Act 1901*.

⁵ The agreement can be viewed on the [OAIC’s website](#).

- 5.23 For conduct that is a breach of a privacy safeguard, the Commissioner may apply to a Court for an injunction under the Competition and Consumer Act.

Purpose and key features of an injunction

- 5.24 Injunctions are an important enforcement tool for compelling a person to modify their behaviour in order to prevent them from contravening, or from continuing to contravene, the Privacy Act, the My Health Records Act, or a privacy safeguard set out in Part IVD of the Competition and Consumer Act.
- 5.25 Generally, an injunction may be appropriate if the conduct:
- is serious or has had, or is likely to have, serious or extensive adverse consequences
 - is systemic or poses ongoing compliance or enforcement issues
 - is deliberate or reckless or where the entity involved is not being cooperative, or
 - raises significant concerns of public interest.
- 5.26 The Commissioner may seek an injunction on its own or with civil penalty proceedings, or other enforcement action.

Interim injunctions

- 5.27 The OAIC may seek and obtain a temporary injunction (known as an ‘interim injunction’) on an urgent basis pending the Court’s determination of an application for a permanent injunction under s 80W of the Privacy Act, s 81 of the My Health Records Act or s 56EX of the Competition and Consumer Act (see also Part 7 of the Regulatory Powers Act). An interim injunction may prevent further harm or maintain the status quo. The interim injunction will be effective from the time the interim injunction is granted to the time that the Court’s final decision is made.
- 5.28 The OAIC may seek an interim injunction on an ‘ex parte’ basis, meaning that the Court may consider whether to make the order without the respondent participating. Ex parte interim injunctions will generally be sought by the OAIC at the start of Court proceedings and in urgent circumstances, where an injunction is required as soon as possible and it is not practicable for the OAIC to first contact the respondent. This type of injunction will usually only be effective for a short period – typically no more than one week. After this period, the OAIC will have to participate in a further Court hearing with the respondent present.
- 5.29 Under s 122(1) of the Regulatory Powers Act, the Court has a general power to grant interim injunctions — meaning that an interim injunction restraining a person from engaging in conduct or an interim injunction compelling a person to do a particular act or thing may be possible depending upon the circumstances.
- 5.30 To obtain an interim injunction under s 80W of the Privacy Act, s 81 of the My Health Records Act or s 56EX of the Competition and Consumer Act, the Commissioner must establish that:
- there is a serious question to be tried in relation to the facts asserted to support the injunction application
 - the balance of convenience favours granting an injunction, in that the harm or inconvenience caused by the refusal of an injunction outweighs the harm or inconvenience that the respondent would suffer if the injunction were granted, and

- it is desirable in all the circumstances to grant the interim injunction.

5.31 Factors relevant to the balance of convenience include:

- the strength of the Commissioner's case
- the purpose served by the interim injunction (for example, is it designed to prevent the respondent from taking an action that would render granting a final injunction futile)
- the effect of the injunction on the respondent and any third parties
- the availability of alternative remedies
- any delay in making the application, and
- any undertakings offered by the respondent to cease (or not to commence) the relevant conduct.⁶

5.32 Where the Commissioner is applying for an ex parte interim injunction, the Commissioner will also be subject to a special ethical obligation usually described as the 'duty of utmost disclosure'. This means that the Commissioner must disclose all factors relevant to a consideration of whether to grant an interim injunction – especially those factors which go against granting an injunction.

5.33 This duty is treated most seriously by the Court, and a failure to comply will normally result in a discharge of the injunction, with costs ordered against the applicant. A failure by the Commissioner to disclose relevant factors would also be a breach of the Commonwealth's obligation to act as a model litigant under the Legal Services Directions.

Permanent injunctions

5.34 For a permanent injunction, the Commissioner must establish on the balance of probabilities that the facts asserted to support the injunction are made out.

5.35 The power to grant an injunction is a discretionary power and the Court will also consider whether it is desirable in all the circumstances to exercise that power having regard to the scope and purpose of the relevant Act.

Injunctions restraining a person from engaging in conduct

5.36 To grant an injunction restraining a person from engaging in conduct, the Court must be satisfied that:

- a person has engaged, is engaging in or is proposing to engage in conduct in contravention of either the Privacy Act, the My Health Records Act or a privacy safeguard set out in Part IVD of the Competition and Consumer Act.

5.37 The Court may grant an injunction restraining a person from engaging in conduct whether or not:

- it appears to the court that the person intends to engage again in conduct of that kind,
- the person has previously engaged in conduct of that kind, and

⁶ See *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57; *Castlemaine Tooheys Ltd v South Australia* (1986) 161 CLR 148.

- there is an imminent danger of substantial damage to any person if the first mentioned person were to engage in conduct of that kind (s 124(1) of the Regulatory Powers Act).
- 5.38 Where the Court grants an injunction restraining a person from engaging in conduct that is, or would be, a contravention of the Privacy Act, or the My Health Records Act or a privacy safeguard as set out in Part IVD of the Competition and Consumer Act, the Court may also make an order requiring the person to do any act or thing, if it is in the Court's opinion desirable to do so (s 80W of the Privacy Act, and s 81 of the My Health Records Act and s 56EX of the Competition and Consumer Act (see also Part 7 of the Regulatory Powers Act)).
- 5.39 For example, a Court may grant a permanent injunction restraining a person from collecting certain information about consumers and requiring them to put in place specified risk management practices to prevent similar breaches from occurring again.

Injunctions requiring a person to do a thing

- 5.40 To grant an injunction requiring a person to do a thing, the Court must be satisfied that:
- a person has refused or failed, or is proposing to refuse or fail, to do a thing; and
 - the refusal or failure was, is, or would be a contravention of either the Privacy Act, the My Health Records Act or a privacy safeguard set out in Part IVD of the Competition and Consumer Act.
- 5.41 The Court may grant an injunction requiring a person to do a thing whether or not:
- it appears to the Court that the person intends to refuse or fail again to do the thing,
 - the person has previously refused or failed to do that thing, and
 - there is an imminent danger of substantial damage to any person if the first mentioned person were to refuse or fail to do that thing (s 124(2) of the Regulatory Powers Act).
- 5.42 For example, a Court may grant a mandatory injunction requiring a person to correct personal information it holds about individuals.

The content of injunctions

- 5.43 The form of any injunction sought must be certain and capable of enforcement. It must be clear and unambiguous to the affected person, and to the Court, what it is that they must do or not do.
- 5.44 The Court will not grant an injunction that simply requires a person to 'comply with the Act'. An injunction must set out the specific acts that the person must do or not do.
- 5.45 An injunction should not prohibit conduct falling outside the boundaries of s 80W of the Privacy Act, s 81 of the My Health Records Act or s 56EX of the Competition and Consumer Act. That is, an injunction cannot operate on conduct that is not related to ensuring compliance with the Privacy Act, My Health Records Act, or a privacy safeguard set out in Part IVD of the Competition and Consumer Act.

Procedural steps in seeking an injunction

- 5.46 When seeking an injunction, the OAIC will generally use the following steps:

- Where the OAIC becomes aware that an entity might have engaged, be engaging, or proposes to engage in conduct that would contravene the Privacy Act, My Health Records Act or a privacy safeguard set out in Part IVD of the Competition and Consumer Act, the OAIC will make preliminary inquiries about the matter.
- The OAIC will review the matter against the *Privacy regulatory action policy* (including the factors set out in paragraph 38) or s 7.1 of the My Health Records Enforcement Guidelines or the *CDR regulatory action policy* as applicable, as well as the additional factors outlined above, in paragraph 25, to assess whether seeking an injunction is an appropriate regulatory response, either by itself or in conjunction with other remedies.
- Where an injunction is identified as an appropriate regulatory response in the circumstances, the OAIC will assess the matter to determine whether enough admissible evidence and arguments exist to satisfy the Court of the matters it must consider in determining whether to grant an injunction. The amount and type of evidence required to support an application for an injunction will depend on the type of injunction being sought (see above). External legal counsel may be briefed at this time.
- Where the available evidence and arguments are considered sufficient, the Commissioner will consider and decide whether to commence proceedings. To make this decision, the Commissioner will refer to either the *Privacy regulatory action policy* (including the factors set out in paragraph 38) or s 11.3 of the My Health Records Enforcement Guidelines or the *CDR regulatory action policy* as applicable. Where proceedings are to be commenced, external legal counsel will usually be engaged to run the matter.
- The appropriate Court documents to initiate proceedings will be prepared and lodged with the Court, and served on the respondent entity.
 - Generally, only persons who are parties to the legal proceedings in which an injunction is granted will be bound by the injunction. It is important to ensure that all persons the Commissioner seeks to bind by an injunction are joined as respondents in the proceedings.
 - This application must generally be accompanied by a supporting affidavit of the Commissioner, setting out:
 - the conduct, refusals or failures the Commissioner considers is, or would be, a breach of the Privacy Act, the My Health Records Act or a privacy safeguard set out in Part IVD of the Competition and Consumer Act
 - the evidence on which the Commissioner bases this view, and
 - the specific orders that the Commissioner is seeking from the Court.
 - In very urgent circumstances, including where a matter is heard on an *ex parte* basis, (such as where the need for an injunction becomes apparent a matter of hours before the conduct is likely to occur), the Commissioner may provide the above information orally at hearing.
- Following receipt of the Commissioner's application, the Court will set down a time to hear the application for an injunction.
- The OAIC will pursue the application in accordance with its model litigant obligations, any relevant Court rules and procedures, and any directions or orders issued by the Court.

- Following judgment in the matter, the OAIC will generally publicly communicate the outcome of the proceedings.
- If the OAIC is dissatisfied with the Court's decision (for example, if the Court refused to grant an injunction), the OAIC may consider the possible grounds for appeal and whether or not to institute appeal proceedings. In making this decision, the OAIC will act in accordance with its model litigant obligations.
- If the respondent appeals the decision, the OAIC will participate in the appeal proceedings and will act in accordance with its model litigant obligations.

After an injunction has been granted

- 5.47 The Court may discharge or vary an injunction granted under s 80W of the Privacy Act, s 81 of the My Health Records Act or s 56EX of the Competition and Consumer Act (see also Part 7 of the Regulatory Powers Act).
- 5.48 If a person who is the subject of an injunction breaches the injunction, they may be held in contempt of Court, which is punishable by fines and/or imprisonment.
- 5.49 Where the OAIC believes that a respondent has breached an injunction, the OAIC will generally first bring suspected or actual non-compliance to the attention of the respondent and seek a response. This notification and response may resolve the breach.
- 5.50 If the breach remains unresolved, the OAIC may then consider whether it would be appropriate to bring proceedings for contempt of Court. This process requires the OAIC to apply to the Court, supported by evidence and submissions. The burden of proof for contempt proceedings is the criminal standard: the breach must be proven beyond reasonable doubt. Legal advice should be sought before any decision is made to bring contempt proceedings.

Publication

- 5.51 Generally, the OAIC will publicly communicate the following information in connection with an injunction application:
- that proceedings seeking an injunction against a particular respondent have been initiated⁷
 - the outcome of the injunction proceedings
 - where an injunction is granted, the orders made by the Court (subject to any limitations placed on the publication of the orders by the Court)
 - the lodgement of appeal proceedings by either the OAIC or the respondent, and
 - the outcome of any appeal proceedings.
- 5.52 Where an interim injunction has been granted, the OAIC will take care in its communications to avoid any suggestion that a finding has been made that a person has breached the relevant Act or privacy safeguard. By their nature interim injunctions are granted without the

⁷ The initiation of proceedings will not be publicly communicated in the event an ex parte injunction is being sought (an injunction granted by a Court without notice to the respondent who will be bound by the injunction).

Court having yet decided about whether there has been a breach of the relevant Act or privacy safeguard.

- 5.53 Where a Court grants an injunction, the OAIC will, on its website <www.oaic.gov.au>, either publish, or provide a link to, the orders made by the Court. Where the Court has placed limitations on the publication of the orders, the OAIC may publish a redacted version of the orders, or a summary of the orders.
- 5.54 In addition, the OAIC may publicly communicate the fact that the respondent has breached the injunction, and any fine or other punishment meted to the respondent in connection with that breach.

Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions

Contents

Legislative framework	1
Purpose and key features of seeking a civil penalty order	4
Who can be liable for a civil penalty?	4
Applicable mental elements	5
Determining the penalty to impose	5
Serious or repeated interference with privacy	5
Serious interference with privacy	6
Repeated interference with privacy	7
Serious or repeated privacy interference and pre-12 March 2014 conduct	8
Procedural steps	8
Publication	9
Additional resources	9

Legislative framework

- 6.1 Section 80W of the Privacy Act empowers the Commissioner to apply to the Federal Court or Federal Circuit Court for an order that an entity, that is alleged to have contravened a civil penalty provision in that Act, pay the Commonwealth a penalty.
- 6.2 Each civil penalty provision specifies a maximum penalty for contravention of that provision. The penalty is expressed in ‘penalty units’. The value of a penalty unit is contained in s 4AA of the *Crimes Act 1914* (Cth).¹
- 6.3 The ‘civil penalty provisions’ in the Privacy Act include:
- a serious or repeated interference with privacy (s 13G) – 2000 penalty units

¹ The value of a penalty unit as at July 2017 is \$210 — see <https://www.legislation.gov.au/Series/C1914A00012>

- various civil penalty provisions set out in Part IIIA – Credit reporting, with penalties of either 500, 1000 or 2000 penalty units.²
- 6.4 Under s 79 of the My Health Records Act, the Commissioner may apply to a court for an order that a person who is alleged to have contravened a civil penalty provision in that Act pay the Commonwealth a civil penalty. Section 79 triggers the provisions of Part 4 of the Regulatory Powers Act which deals with seeking and obtaining a civil penalty order for contraventions of civil penalty provisions.
- 6.5 The ‘civil penalty provisions’ in the My Health Records Act include:
- unauthorised collection, use or disclosure by a person of health information included in a healthcare recipient’s My Health Record, where the person knows or is reckless as to the fact the collection, use or disclosure is not authorised (s 59(1) and (2)) – criminal offence penalty is 120 penalty units or imprisonment for 2 years, or both. The civil penalty is 600 penalty units.
 - use or disclosure by a person of health information included in a healthcare recipient’s My Health Record where the information was disclosed to the person in contravention of s 59(2) and the person knows or is reckless as to that fact (s 60(1)) – criminal offence penalty is 120 penalty units or imprisonment for 2 years, or both. The civil penalty is 600 penalty units.
 - five other civil penalty provisions set out in Part 5 that relate to:
 - failing to provide required information to the My Health Record System Operator – 100 penalty units
 - failure by a registered healthcare provider organisation, registered repository operator, registered portal operator or a registered contracted service provider to notify a data breach, including a potential data breach, to the OAIC and/or My Health Record System Operator as soon as practicable after becoming aware of the breach – 100 penalty units.
 - failure by a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider to notify the System Operator of ceasing to be eligible to be registered – 80 penalty units.
 - holding or taking records outside Australia – criminal offence penalty of 2 years imprisonment or 120 penalty units, or both, civil penalty of 600 penalty units.
 - certain contraventions of the My Health Records Rules – 100 penalty units
- 6.6 Similarly, under s 56EU of the Competition and Consumer Act, the Commissioner may apply to a court for an order that a person who is alleged to have contravened a civil penalty provision in that Act pay the Commonwealth a civil penalty. Section 56EU triggers the provisions of Part 4 of the Regulatory Powers Act which deals with seeking and obtaining a civil penalty order for contraventions of civil penalty provisions.
- 6.7 The ‘civil penalty provisions’ under s 56EU of the Competition and Consumer Act are subsections:
- 56ED(3)

² Some credit reporting civil penalty provisions have analogous ‘offence’ provisions. Sections 80ZD-80ZF of the Privacy Act outline when civil proceedings can be commenced and continued where criminal proceedings may also be initiated.

- 56EF(1)
 - 56EG(1)
 - 56EH
 - 56EI(1) or (2)
 - 56J(1) or (2)
 - 56EK(1)
 - 56EL(1) or (2)
 - 56EM(1) or (2)
 - 56EN(1), (2), (3) or (4)
 - 56EO(1) or (2)
 - 56EP(1) or (2).
- 6.8 The maximum amounts of penalties, as outlined in s 56EV of the Competition and Consumer Act, are:
- For a body corporate, the greater of either: \$10,000,000; the value of any benefit the relevant court has determined of the body corporate, or any body corporate related to it, obtained directly or indirectly that is reasonably attributable to the contravention, multiplied by three; or if the court cannot determine the value of that benefit, 10% of the annual turnover of the body corporate during the 12-month period ending at the end of the month in which the contravention happened or began.
 - For a person other than a body corporate, the maximum penalty amount is \$500,000.
- 6.9 Particular conduct may contravene both a civil penalty provision in the My Health Records Act and the ‘serious or repeated interference with privacy’ civil penalty provision in the Privacy Act (s 13G). This is because contraventions of the My Health Records Act are interferences with privacy for the purposes of the Privacy Act, and so the OAIC may be able to seek a civil penalty for contravention of s 13G of the Privacy Act where the interference with privacy arises from a breach of the My Health Records Act.
- 6.10 An entity (or person) will also contravene a civil penalty provision, and be liable to pay a penalty, if it:
- attempts to contravene a civil penalty provision
 - aids, abets, counsels or procures a contravention of a civil penalty provision
 - induces a contravention of a civil penalty provision
 - is knowingly concerned in or a party to a contravention of a civil penalty provision, or
 - conspires with others to effect a contravention of a civil penalty provision.³
- 6.11 Under s 80U(2) of the Privacy Act, the Commissioner’s application to the court for a civil penalty order must be made within six years of the alleged contravention.

³ Section 80U of the Privacy Act and s 79 of the My Health Records Act (see also Part 4 of the Regulatory Powers Act, s 92).

- 6.12 If the court is satisfied that the entity (or person) has contravened the civil penalty provision (taking into account the relevant matters set out in the applicable legislation), it may order the entity (or person) to pay such penalty as the court determines appropriate.
- 6.13 For civil penalties of the Privacy Act and My Health Records Act, the maximum penalty that the court can order is the amount listed in the civil penalty provision or, for a body corporate, five times that amount (Privacy Act s 80U, Regulatory Powers Act s 82(5), and My Health Records s 79 (see also Part 4 of the Regulatory Powers Act)).
- 6.14 Where conduct contravenes more than one civil penalty provision, proceedings may be commenced in relation to each contravention; however, the entity (or person) cannot be liable for more than one penalty in relation to that conduct (Privacy Act s 80U; My Health Records Act s 79 and s 56EU(6) of the Competition and Consumer Act (see also Part 4 of the Regulatory Powers Act)).
- 6.15 Where an entity (or person) contravenes a single civil penalty provision multiple times, the court may award a single civil penalty order. However, the amount of that penalty cannot exceed the sum of the maximum penalties that could be ordered if a separate civil penalty order was made for each contravention (Privacy Act s 80U; My Health Records Act s 79 and s 56EV(1) of the Competition and Consumer Act (see also s 85 of the Regulatory Powers Act)).

Purpose and key features of seeking a civil penalty order

- 6.16 By requiring the payment of a penalty to the Commonwealth, a civil penalty order financially penalises an entity or person. A civil penalty order does not compensate individuals adversely affected by the contravention.⁴
- 6.17 The OAIC will not seek a civil penalty order for all contraventions of a civil penalty provision in the Privacy Act, My Health Records Act or the privacy safeguards. The OAIC is unlikely to seek a civil penalty order for minor or inadvertent contraventions, where the entity or person responsible for the contravention has cooperated with the investigation and taken steps to avoid future contraventions.

Who can be liable for a civil penalty?

- 6.18 A civil penalty order under the Privacy Act can only be made against ‘an entity’. The term ‘entity’ means an agency, an organisation or a small business operator (these terms are further defined in s 6(1)). The term ‘organisation’ can include an individual (including a sole trader).

⁴ While a civil penalty order does not compensate individuals, sections 25 and 25A of the Privacy Act do permit an individual to recover compensation or other remedies where a civil penalty order is made against an entity for a contravention of a civil penalty provision contained in Part IIIA (Credit reporting) of the Privacy Act.

- 6.19 A civil penalty order under the My Health Records Act can only be made against ‘a person’.⁵ This term includes both individuals and participants in the My Health Record system, such as registered repository operators, portal operators and healthcare provider organisations
- 6.20 A civil penalty order under s 56EU of the Competition and Consumer Act can be made against a body corporate, and a person other than a body corporate.

Applicable mental elements

- 6.21 For certain civil penalty provisions under the My Health Records Act,⁶ a person can only be liable for a penalty where a particular mental element (knowledge or recklessness) is made out.
- 6.22 There are no applicable mental elements for civil penalty provisions in the Privacy Act.

Determining the penalty to impose

- 6.23 In determining the penalty to be imposed, s 80U of the Privacy Act, s 79 of the My Health Records Act and 56EU of the Competition and Consumer Act (see also s 82(6) of the Regulatory Powers Act) provide that the court must take into account all relevant matters, including:
- the nature and extent of the contravention
 - the nature and extent of any loss or damage suffered because of the contravention
 - the circumstances in which the contravention took place
 - whether the person has previously been found by a court to have engaged in any similar conduct.

Serious or repeated interference with privacy

- 6.24 Section 13G of the Privacy Act is a civil penalty provision for cases of serious or repeated interference with privacy by an entity.
- 6.25 An ‘interference with privacy’ is defined in s 13 of the Act, and is a breach of the Privacy Act or of a privacy-related provision in certain other legislation.⁷
- 6.26 The phrases ‘serious interference with privacy’ and ‘repeated interference with privacy’ are not defined in the Privacy Act. The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*⁸ which introduced these terms into the Privacy Act states that the ordinary meaning of the terms ‘serious’ and ‘repeated’ will apply.

⁵ The term ‘person’ is not defined in the My Health Records Act, so the meaning is drawn from the *Acts Interpretation Act 1901* (Cth). That Act states that expressions used to denote persons generally, such as ‘person’, include a body politic or body corporate as well as an individual (s 2C).

⁶ My Health Records Act ss 59 and 60.

⁷ For example, the *Data-matching Program (Assistance and Tax) Act 1990*, the s 135AA guidelines issued under the *National Health Act 1953*, the *Healthcare Identifiers Act 2010*, the *Personally Controlled Electronic Health Records Act 2012*, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, and the *Personal Property Securities Act 2009*.

⁸ See <https://www.legislation.gov.au/Series/C2012A00197>

6.27 ‘Serious interference with privacy’ and ‘repeated interference with privacy’ are two distinct concepts, either of which may lead the OAIC to seek a civil penalty against an entity. However, in some cases, acts or practices may meet the requirements for both concepts, for example where a single incident that forms part of a repeated interference with privacy is also a serious interference with privacy.

Serious interference with privacy

6.28 Whether an interference with privacy is ‘serious’ is an objective question that will reflect what a reasonable person would consider serious. This means that what is considered a serious interference with privacy may vary and evolve over time as technology and community expectations regarding privacy protections change.

6.29 The following factors are relevant in considering whether a particular interference with privacy is serious:

- the number of individuals potentially affected
- whether it involved ‘sensitive information’ or other information of a sensitive nature
- whether significant adverse consequences were caused or are likely to be caused to one or more individuals from the interference
- whether vulnerable or disadvantaged people may have been or may be particularly adversely affected or targeted
- whether it involved deliberate or reckless conduct
- whether senior or experienced personnel were responsible for the conduct.

6.30 The OAIC will not seek a civil penalty order in all matters involving a ‘serious’ interference with privacy. The OAIC is more likely to seek a civil penalty in a particular matter where one of the following factors is present:

- the serious interference with privacy is particularly serious or egregious in nature. This may arise because a number of different indicators of seriousness are present (for example, the breach involved the health information of a large number of individuals and significant adverse consequences have arisen or are likely to arise), or because one particular indicator of seriousness is present to a significant extent, such as a very large number of individuals being affected, or very substantial detriment having occurred
- the entity has a history of serious interferences with privacy
- the OAIC reasonably considers the serious interference with privacy arose because of a failure by the entity to take its privacy obligations seriously, or a blatant disregard by the entity for its privacy obligations.

6.31 In addition, when deciding whether to commence proceedings against an entity seeking a civil penalty for serious interference with privacy, the OAIC will take into account the factors outlined in the *Privacy regulatory action policy* and where appropriate, the *CDR regulatory action policy*.

6.32 While a history of serious contraventions can be a relevant factor, it is not a prerequisite to the OAIC seeking a civil penalty for serious interference with privacy, and it is possible for a single breach by an entity to be the catalyst for the commencement of proceedings.

Repeated interference with privacy

- 6.33 ‘Repeated interference with privacy’ means that an entity has interfered with the privacy of an individual or individuals on two or more separate occasions. These repeated interferences with privacy could arise from:
- the same act or practice done on two or more occasions
 - different acts or practices done on two or more occasions.
- 6.34 The relevant acts or practices must have occurred on separate occasions. This means that an act or practice that simultaneously results in the interference with privacy of several individuals – such as a mail merge error leading to the personal information of multiple individuals being disclosed to third parties – will not in itself constitute a ‘repeated’ interference with privacy. Similarly, a single act which results in the breach of multiple APPs will not in itself be a ‘repeated’ privacy interference.⁹
- 6.35 The OAIC will not seek a civil penalty order in all matters involving repeated interference with privacy. The cases in which the OAIC is more likely to seek a civil penalty for repeated interference with privacy are those where:
- the entity failed to take reasonable steps to correct and improve its privacy practices following earlier interferences with privacy. The reasonable steps in a particular circumstance will depend on the nature and causes of the earlier interferences with privacy, but may include having conducted an audit of privacy practices and implementing audit findings, conducting staff privacy training, updating entity policies and procedures relating to personal information handling, and improving information security measures
 - the repeated privacy interferences demonstrate a failure by the entity to take its privacy obligations seriously, or a blatant disregard by the entity for its privacy obligations
 - the contraventions comprising the repeated privacy interferences are more serious in nature (whether or not a penalty for serious interference with privacy has previously been imposed)
 - interferences with privacy have occurred on a greater number of occasions
 - the repeated privacy interferences occur within a short period of time.
- 6.36 In addition, when deciding whether to commence proceedings against an entity seeking a civil penalty for repeated interference with privacy, the OAIC will take into account the factors outlined in the *Privacy regulatory action policy* and where appropriate, the *CDR regulatory action policy*.
- 6.37 While the seriousness of the contraventions comprising the repeated interference with privacy will be taken into account, the separate contraventions comprising the sequence of repeated interferences with privacy do not need to be serious for the OAIC to seek a civil penalty. If the OAIC is satisfied that another aspect of the contraventions justifies the seeking of a civil penalty order (such as an apparent blatant disregard by the entity for its privacy obligations) then the OAIC may decide to seek a civil penalty order.

⁹ While these examples would not in themselves constitute repeated interferences with privacy, depending on the circumstances the incidents could still constitute a serious interference with privacy or, if it is one incident in a series of other contraventions committed by the same entity, it could constitute repeated privacy interference together with those other contraventions.

Serious or repeated privacy interference and pre-12 March 2014 conduct

- 6.38 Item 6 of Schedule 6 to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* provides that s 13G applies in relation to an act done, or a practice engaged in, after 12 March 2014.
- 6.39 This means that where the OAIC applies to a court for a civil penalty order against an entity for serious or repeated interference with privacy, the OAIC can only lead evidence relating to interferences with privacy that have occurred since 12 March 2014 to establish its case.

Procedural steps

- 6.40 When seeking a civil penalty order from the courts is a possible regulatory outcome in a matter, the OAIC will generally use the following process:
- The OAIC will first investigate the matter, either in response to a complaint or on the Commissioner's own initiative. Information on complaint investigations is contained in Chapter 1 of this guide, while information on Commissioner initiated investigations is contained in Chapter 2.
 - Where the OAIC's investigation indicates that it is likely that an interference with privacy has occurred, the OAIC will consider whether to take enforcement action and, if so, what enforcement action to take. The OAIC will review the matter against either the *Privacy regulatory action policy*, the *My Health Records Enforcement Guidelines* or the *CDR regulatory action policy* as applicable to assess the appropriate enforcement response.
 - Where seeking a civil penalty order is identified as the appropriate regulatory response in the circumstances, the OAIC will assess the matter to determine whether or not sufficient evidence exists to take successful court action. External legal counsel may be briefed. This includes evaluating:
 - whether there is sufficient admissible evidence for each element of the alleged contravention to successfully establish the case on the balance of probabilities
 - the availability, competence and credibility of witnesses
 - any mitigating factors that might reasonably be raised before the court by the respondent
 - the possibility that any evidence might be excluded by a court.
 - Where the available evidence is sufficient, the Commissioner will consider and decide whether to commence proceedings. To make this decision, the Commissioner will use the *Privacy regulatory action policy*, the *My Health Records Enforcement Guidelines* or the *CDR regulatory action policy* as applicable. Where proceedings are to be commenced, external legal counsel will usually be engaged to run the matter.
 - The court documents to initiate proceedings will be prepared and lodged with the court, and served on the respondent entity.
 - The OAIC will pursue the court proceedings in accordance with its model litigant obligations, any relevant court rules and procedures, and any directions or orders issued by the court.

- Following judgment, the OAIC will generally publicly communicate the outcome of the proceedings.
- If the OAIC is dissatisfied with the court's decision (for example, if the court refused to impose a penalty, or the OAIC considers the imposed penalty inadequate), the OAIC may consider the possible grounds for appeal and whether or not to institute appeal proceedings. In making this decision, the OAIC will act in accordance with its model litigant obligations.
- If the respondent appeals the decision, the OAIC will participate in the appeal proceedings and will act in accordance with its model litigant obligations.

Publication

6.41 The OAIC will publicly communicate the following information in connection with civil penalty proceedings:

- civil penalty proceedings against a particular respondent have been initiated
- the outcome of civil penalty proceedings
- the lodgement of appeal proceedings by either the OAIC or the respondent
- the outcome of any appeal proceedings.

6.42 Where it is appropriate for the OAIC to comment on civil penalty proceedings prior to their resolution, such comment will generally be restricted to the history of the proceedings and any earlier findings by the OAIC or an alternative complaint body.

6.43 Any publications relating to civil penalty proceedings will comply with any relevant court orders.

Additional resources

- Chapter 1 of this guide for information relating to the OAIC's complaint investigation procedures
- Chapter 2 of this guide for information relating to the OAIC's Commissioner initiated investigation procedures.

Chapter 7: Privacy assessments

Contents

Legislative framework	1
Entry and inspection powers	2
Reporting to the Minister	2
Requirement to give information or produce a document	3
Purpose and key features of privacy assessments	3
Types of privacy assessments	3
When will the OAIC conduct a privacy assessment?	5
Assessment outcomes	6
Procedural steps	8
Targeting	9
Planning	9
Fieldwork	10
Reporting	11
Publication	12
Appendix A: Risk based assessments — privacy risk guidance	13

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), entities, including State and Territory health authorities, handling COVID app data 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
 - ensuring that COVID app data is being managed in accordance with Part VIIIA of the Privacy Act
- 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.
- 7.6 In relation to the CDR scheme, the Commissioner may conduct an assessment under s 56ER of the Competition and Consumer Act, in a manner he or she sees fit, of whether a CDR participant is managing and handling CDR data in accordance with the privacy safeguards and privacy or confidentiality related CDR Rules. This is further discussed in the 'Consumer Data Right assessments and audits' section of this chapter.

Entry and inspection powers

- 7.7 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.
- 7.8 Section 68 (2) of the Privacy Act provides that the occupier must provide reasonable facilities and assistance to the Commissioner or authorised delegates.
- 7.9 Under s 68A of the Privacy Act, 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

- 7.10 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.
- 7.11 Similarly, s 56ER(3) of the Competition and Consumer Act provides that the Commissioner may report to the Minister, the Commission [the ACCC] or the Data Standards Chair about an assessment conducted under s 56ER.

Requirement to give information or produce a document

- 7.12 Section 94T of the Privacy Act provides that , in relation to an assessment into the matters in s 94T(1) (relating to Part VIIIA), if the Commissioner has reason to believe that either an entity or a State or Territory authority being assessed has information or a document relevant to the assessment, the Commissioner may, by written notice, require the entity to give the information or produce the document within the period specified in the notice (which must be at least 14 days after the notice is issued).
- 7.13 This power only applies to assessments being conducted into matters under s 94T(1) (relating to the COVIDSafe app and COVID app data).
- 7.14 Unlike s 44 of the Privacy Act, a notice under s 94T(2) can only be given to the entity or authority that is the subject of the assessment, not a third party who may be able to provide relevant information.

Purpose and key features of privacy assessments

- 7.15 As outlined in the *Privacy regulatory action policy* and *CDR 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

- 7.16 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.
- 7.17 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

- 7.18 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, privacy safeguards or privacy or confidentiality related CDR Rules, Part VIIIA). The privacy risks identified should directly relate to the entity's general compliance obligations.
- 7.19 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.
- 7.20 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

- 7.21 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
 - whether a CDR participant is handling CDR data in accordance with the privacy safeguards or the privacy or confidentiality related CDR Rules
 - whether an entity is managing COVID app data in accordance with the requirements of Part VIIIA.
- 7.22 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

- 7.23 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.
- 7.24 The OAIC has an agreement with the Department of Human Services (DHS)¹ 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.

Consumer Data Right (CDR) assessments and audits

- 7.25 As stated earlier in this chapter, s 56ER of the Competition and Consumer Act provides the Commissioner may conduct an assessment, in a manner he or she sees fit, of whether a CDR participant is managing and handling CDR data in accordance with the privacy safeguards and privacy or confidentiality related CDR Rules.

¹ The Department of Human Services (DHS) was renamed to Services Australia in May 2019. However, this guide refers to DHS where relevant, as it continues to be known in the DMP Act.

- 7.26 As the Commissioner can conduct an assessment of compliance with a privacy safeguard in any manner he or she sees fit, the Commissioner may be guided by the processes for privacy assessments completed under the Privacy Act, that are set out in this chapter.
- 7.27 In addition, CDR Rule 9.6(2) provides the Commissioner may, at any time, audit the compliance of any CDR participant with the privacy safeguards in Division 5 of Part IVD of the Competition and Consumer Act² and the CDR Rules to the extent that they relate to the privacy safeguards or the privacy and confidentiality of CDR data.
- 7.28 The Commissioner may also give a CDR participant a written notice that requests the CDR participant to produce copies of records or information from those records for audits that are conducted under CDR Rule 9.6.
- 7.29 The OAIC will work collaboratively with the ACCC in relation to its assessments and audits function. This is to ensure both agencies utilise the range of regulatory powers with a coordinated preventative and proactive approach to CDR compliance, ensuring efficient consideration of the risks while not over-burdening regulated entities with overlapping audit requirements.
- 7.30 More information on the OAIC and ACCC's joint approach to encouraging compliance and preventing breaches of the CDR regulatory framework can be found in the [ACCC and OAIC Compliance and Enforcement Policy](#).

When will the OAIC conduct a privacy assessment?

- 7.31 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*, or the 'Compliance and enforcement approach' section of the *CDR regulatory action policy*, including the 'factors taken into account' and the 'sources of information' sections.
- 7.32 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.

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

² Including Division 5 of Part IVD to the extent that it relates to the CDR Rules, see CDR Rule 9.6(1)(a).

Assessment outcomes

Recommendations

- 7.34 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.
- 7.35 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.
- 7.36 Generally, recommendations will align with the terminology used in the APP guidelines or the Privacy Safeguards Guidelines when assessing compliance under the CDR scheme. The guidelines set out the mandatory requirements of the Privacy Act and the privacy safeguards and CDR Rules under the Competition and Consumer Act, where relevant, and are described by the words ‘must’ or ‘is required to’. Aspects of privacy practice that the Commissioner may take into account when considering entities’ compliance with the Privacy Act or the Competition and Consumer 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 or the privacy safeguards and CDR Rules are generally indicated by ‘could’ in the APP guidelines³ and the Privacy Safeguard Guidelines.⁴
- 7.37 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.
- 7.38 The OAIC will only make recommendations on issues of particular significance or concern to the OAIC, and recommendations will be clear, targeted and actionable.
- 7.39 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.

³ Office of the Australian Information Commissioner, [Australian Privacy Principles guidelines](#), Chapter A, paragraph A.2

⁴ Office of the Australian Information Commissioner, Consumer Data Right Privacy Safeguard Guidelines, Chapter A, paragraph A.4

The content of the assessment report

7.40 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.

7.41 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

7.42 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.

7.43 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

7.44 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.

7.45 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.

7.46 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.

7.47 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

- 7.48 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).
- 7.49 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.
- 7.50 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.
- 7.51 When deciding whether to take further regulatory action as a result of an assessment, the OAIC will refer to the factors set out in the *Privacy regulatory action policy* or the *CDR regulatory action policy*, where appropriate.

Reporting to the Minister

- 7.52 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.
- 7.53 Where the Commissioner does report to the Minister about an assessment, the Commissioner will notify the assessed entity.

Procedural steps

- 7.54 There are four main stages commonly involved in assessments:
1. Targeting
 2. Planning
 3. Fieldwork
 4. Reporting.
- 7.55 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

7.56 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 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.

7.57 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 or privacy safeguards or CDR Rules. 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

7.58 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

7.59 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.

7.60 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 or Privacy Safeguard 1 CDR 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

- 7.61 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.
- 7.62 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

7.63 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
<p>High risks</p> <p>Entity must, as a high priority, take steps to address mandatory requirements of Privacy and related legislation</p>	<p>Immediate management attention is required.</p> <p>This is an internal control or risk management issue that if not mitigated is likely to lead to the following effects</p>	<ul style="list-style-type: none"> • Likely breach of relevant legislative obligations (for example, APP, TFN, Credit, privacy safeguard, Part VIII A) or not likely to meet significant requirements of a specific obligation (for example, an enforceable undertaking) • Likely adverse or negative impact upon the handling of individuals' personal information • Likely violation of entity policies or procedures • Likely reputational damage to the entity, such as negative publicity in national or international media. • Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines • Likely ministerial involvement or censure (for agencies)
<p>Medium risk</p> <p>Entity should, as a medium priority, take steps to address OAIC expectations around requirements of Privacy and related legislation</p>	<p>Timely management attention is expected.</p> <p>This is an internal control or risk management issue that may lead to the following effects</p>	<ul style="list-style-type: none"> • Possible breach of relevant legislative obligations (for example, APP, TFN, Credit, privacy safeguard, Part VIII A) or meets some (but not all) requirements of a specific obligation • Possible adverse or negative impact upon the handling of individuals' personal information • Possible violation of entity policies or procedures • Possible reputational damage to the entity, such as negative publicity in local or regional media • Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities • Possible ministerial involvement or censure (for agencies)
<p>Low risk</p> <p>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</p>	<p>Management attention is suggested.</p> <p>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.</p>	<ul style="list-style-type: none"> • Risks are limited, and may be within acceptable entity risk tolerance levels • Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit, privacy safeguard, Part VIII A) • Minimum compliance obligations are being met

Chapter 8: Directing a privacy impact assessment

Contents

Legislative framework	1
Purpose and key features of the PIA direction power	1
Proposed activities and functions for which the PIA direction power may be used	2
Circumstances in which the PIA direction power might be used	3
Procedural steps in issuing a PIA direction	3
When is an agency considered to have complied with the PIA direction?	5
Steps the OAIC will take where an agency does not comply with a direction	5
Publication	5
Additional resources	6

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.

Chapter 9: Data breach incidents

Contents

Notifiable Data Breaches (NDB) scheme	1
Promoting compliance with the scheme	2
Receipt of notifications	2
Declaration of Commissioner — exception to notification (s 26WQ)	3
Direction of Commissioner — requiring notification (s 26WR)	5
Publication and disclosure of information	7
Reporting under the My Health Records Act	7
Responding to data breach notifications under the My Health Records Act	7
Reporting under the National Cancer Screening Register Act	8
Responding to data breach notifications under the NCSR Act	8
Reporting under Part VIII A of the Privacy Act	9

Notifiable Data Breaches (NDB) scheme

- 9.1 The OAIC administers a Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act.
- 9.2 Under Parts IIIC and VIII A, entities that have information security obligations under the Privacy Act¹ must generally notify individuals or consumers in relation to CDR data, whose information was involved and the Australian Information Commissioner (the Commissioner), about eligible data breaches (ss 26WK and 26WL and s 94S).
- 9.3 The Commissioner has the following functions under the scheme:
- offering advice and guidance to regulated entities, and providing information to the community about the operation of the scheme.
 - promoting compliance with the scheme
 - receiving notifications from entities
 - directing an entity to notify under s 26WR
 - declaring that notification need not be made, or that notification be delayed under s 26WQ
- 9.4 Section 56ES(1) and (2) of the Competition and Consumer Act provides that Part IIIC of the Privacy Act applies to accredited data recipients or designated gateways in relation to their

¹ For more information see [Entities covered by the NDB scheme](#)

handling of CDR data, within the CDR scheme. This means data breaches within the CDR scheme, that relate to the handling of CDR consumers (including individuals and small businesses), must be reported to the OAIC and are subject to the same requirements of Part IIIC of the Privacy Act.

- 9.5 There are specific requirements relating to the COVIDSafe app and COVID app data under Part VIIIA of the Privacy Act. Those specific requirements are outlined separately below.

Promoting compliance with the scheme

- 9.6 Section 13(4A) of the Privacy Act provides that if an entity contravenes any of the following requirements of the NDB scheme, the contravention is taken to be an act that is an interference with the privacy of an individual, subject to possible enforcement action:
- carry out an assessment of a suspected eligible data breach (s 26WH(2))
 - prepare a statement about the eligible data breach, and give a copy to the Commissioner as soon as practicable (s 26WK(2))
 - notify the contents of the statement to individuals whose personal information was involved in the eligible data breach (or, in certain circumstances, publish the statement) as soon as practicable (s 26WL(3))
 - comply with a direction from the Commissioner to notify the eligible data breach (s 26WR(10)).
- 9.7 The OAIC has developed guidance about the NDB scheme to assist entities.
- 9.8 The Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with privacy where the Commissioner thinks it is desirable to do so (s 40(2)). The Commissioner must also investigate complaints made by individuals where an act or practice may be an interference with the privacy of the individual (s 40(1)).
- 9.9 Where the Commissioner has identified an interference with privacy, there are a number of enforcement powers available to the Commissioner, ranging from less serious to more serious regulatory action depending on the relevant factors. These include powers to:
- accept an enforceable undertaking (s 80V of the Privacy Act and s 114 of the Regulatory Powers Act) and bring proceedings to enforce an enforceable undertaking (s 115 of the Regulatory Powers Act)
 - make a determination (s 52) and bring proceedings to enforce a determination (ss 55A and 62)
 - seek an injunction to prevent ongoing activity or a recurrence (s 80W)
 - apply to a court for a civil penalty order for a breach of a civil penalty provision (s 80U), which includes serious or repeated interferences with privacy.
- 9.10 In deciding whether an investigation or enforcement action is appropriate in the circumstances, the Commissioner will act in accordance with the OAIC's *Privacy regulatory action policy*, and the *CDR regulatory action policy* where applicable.

Receipt of notifications

- 9.11 The Commissioner will acknowledge receipt of all data breach notifications.

- 9.12 The Commissioner may or may not take any action in response to a data breach notification. The Commissioner will decide which notifications to respond to depending on available resources, and the Commissioner's evaluation of the extent to which taking action in response to the notification will further the objects of the Privacy Act and the objects of Part IVD of the Competition and Consumer Act for the CDR scheme where appropriate.
- 9.13 Some notifications may point to a possible interference with privacy. Under s 42, the Commissioner may make preliminary inquiries to determine whether to investigate an act or practice that may be an interference with privacy, or in relation to the CDR scheme, that may be a breach of a privacy safeguard or a privacy or confidentiality related Rule, where there has been a complaint or on the Commissioner's own initiative. In deciding whether to make preliminary inquiries or offer advice and guidance in response to a notification, the Commissioner may consider:
- the type and sensitivity of the personal information involved
 - the numbers of individuals or CDR consumers potentially at risk of serious harm
 - whether the data breach has been contained or is in the process of being contained where feasible
 - steps the notifying entity has taken, or is taking, to mitigate the impact on individuals or CDR consumers at risk of serious harm
 - measures that the entity has taken, or is taking, to minimise the likelihood of a similar breach occurring again.
- 9.14 The Commissioner may also inquire about the incident to determine whether the OAIC can provide assistance to the entity, such as best practice advice on data breach responses and the prevention of similar incidents in the future.

Declaration of Commissioner — exception to notification (s 26WQ)

- 9.15 The Commissioner may declare that an entity does not need to comply with the notification requirements in the NDB scheme in relation to an eligible data breach. Under s 26WQ the Commissioner may give written notice declaring that a statement to the Commissioner (under s 26WK) and notification to individuals or CDR consumers (under s 26WL) is not required,² or that notification to individuals or CDR consumers is delayed for a specified period.³
- 9.16 The Commissioner must not make a declaration unless satisfied that it is reasonable in the circumstances to do so, having regard to:
- the public interest (s 26WQ(3)(a))
 - any relevant advice given to the Commissioner by an enforcement body or the Australian Signals Directorate (ASD) (s 26WQ(3)(b)),⁴ and
 - such other matters (if any) as the Commissioner considers relevant (s 26WQ(3)(c)).

² Under s 26WQ(1)(c).

³ Under s 26WQ(1)(d).

⁴ The Commissioner may be given such advice or the Commissioner may or may not request such advice.

- 9.17 An entity that is considering applying to the Commissioner for a s 26WQ declaration should do so as soon as practicable after the entity is aware that there are reasonable grounds to believe an eligible data breach has occurred.
- 9.18 In deciding whether to make a declaration, and on what terms, the Commissioner will have regard to the objects of the Privacy Act and other relevant matters. The Commissioner will consider whether the risks associated with notifying of a particular data breach outweigh the benefits of notification to individuals or CDR consumers at risk of serious harm.
- 9.19 Given the clear objective of the scheme to promote notification of eligible data breaches, and the inclusion of exceptions in the scheme that remove the need to notify in a wide range of circumstances, the Commissioner expects that declarations under s 26WQ will only be made in exceptional cases and only after a compelling case has been put forward by the entity seeking the declaration.

Applying for a s 26WQ declaration

- 9.20 An entity considering making an application under s 26WQ should contact the OAIC in the first instance to discuss its intention.
- 9.21 If the entity decides to make an application, it should provide the following information and documents to the OAIC:
- a detailed description of the data breach
 - a statement outlining the entity's reasons for seeking a s 26WQ notice
 - a draft notice setting out the terms that it believes should be included in the notice issued by the Commissioner
 - relevant supporting documents and evidence (including, if applicable, relevant advice from an enforcement body or the ASD)
 - contact details of an employee or representative of the entity.
- 9.22 The onus is on the entity to demonstrate to the Commissioner that it is appropriate for the Commissioner to make a declaration. As such, the entity applying for a declaration will be expected to make a well-reasoned and compelling case detailing how the data breach is an eligible data breach, why any relevant exceptions do not apply, and why notification should not occur or should be delayed. The entity should provide detailed evidence or information in support of its application.
- 9.23 The Commissioner may seek further information from the entity or third parties. However, given the time critical nature of data breach notifications, the entity may not have a further opportunity to provide evidence or submissions to the OAIC before the Commissioner makes a decision on the application. As such, the entity should include all relevant information in its written application.
- 9.24 In considering whether to make a declaration, the Commissioner will have regard to relevant factors which may include:
- the objects in s 2A of the Privacy Act and the objects of the CDR scheme in Part IVD of the Competition and Consumer Act (set out in s 56AA) if applicable
 - the purposes of the NDB scheme, which include enabling individuals (and in the case of the CDR scheme, CDR consumers) to take steps to protect themselves from serious harm arising from a data breach

- the circumstances of the eligible data breach
- the extent to which notification will cause harm to particular groups or to the community at large
- the extent to which benefits of notification will be lost or diminished if notification does not occur or is delayed
- whether advice from an enforcement body or the ASD indicates that notification would be contrary to the public interest in the effective conduct of enforcement related activities or national security matters
- whether the entity responsible for the eligible data breach has been the subject of prior compliance or regulatory enforcement action by the OAIC, and the outcome of that action
- whether the eligible data breach is an isolated instance, or whether it indicates a potential systemic issue (either within the entity concerned or within an industry) or a potential issue which may pose ongoing compliance or enforcement issues
- such other matters as the Commissioner considers relevant.

9.25 After considering the application, the Commissioner will make one of the following decisions:

- a declaration that notification does not need to occur
- a declaration that notification can be delayed (either for the period proposed by the applicant, or another period selected by the Commissioner)
- a refusal of the application.

9.26 Where the Commissioner refuses a declaration, the Commissioner will give written notice of the refusal (s 26WQ(7)).

9.27 Decisions by the Commissioner under s 26WQ are reviewable by the Administrative Appeals Tribunal (AAT).⁵ An application for review by the AAT may be made by the entity that made the application for the declaration, or another entity whose obligations under the NDB scheme are affected by the declaration.⁶

Direction of Commissioner — requiring notification (s 26WR)

9.28 The Commissioner may direct an entity to:

- prepare a statement about the eligible data breach
- give a copy of the statement to the Commissioner, and
- notify individuals or CDR consumers about the eligible data breach.

9.29 In deciding whether to give a direction to an entity under s 26WR(1), the Commissioner must consider:

- any relevant advice given to the Commissioner by an enforcement body or the ASD (s 26WR(6)(a))

⁵ Privacy Act, ss 96(1)(ba) and 96(bb).

⁶ Privacy Act, ss 96(2A) and 96(2B).

- any relevant submission made by the entity (s 26WR(6)(b))
 - such other matters (if any) as the Commissioner considers relevant (s 26WR(6)(c)).
- 9.30 Under s 26WR(5), a direction by the Commissioner may require an entity to include specified information about the eligible data breach, in addition to the information required in a statement prepared for the Commissioner under s 26WR(4).
- 9.31 The specified information that relates to an eligible data breach is likely to be information that the Commissioner considers would assist individuals or CDR consumers to take appropriate action in response to the eligible data breach. Examples could include:
- information about the risk of harm to individuals that the Commissioner considers exists as a result of the eligible data breach
 - recommendations about steps the Commissioner considers individuals should take in response to the eligible data breach
 - information about complaint mechanisms available under the Privacy Act to individuals and under the Competition and Consumer Act to CDR consumers who are affected by the eligible data breach
 - other specified information relating to the eligible data breach that the Commissioner considers reasonable and appropriate in the circumstances to include in the statement.

Process for making a s 26WR direction

- 9.32 Before directing an entity to notify, the Commissioner will usually ask the entity to agree to notify voluntarily.
- 9.33 If the Commissioner and the entity cannot agree about whether notification should occur, the Commissioner will formally invite the entity to make a submission about the direction under consideration, within a specified period (s 26WR(3)). The form of the invitation, and the period of time specified in the invitation for the entity to respond, will be for the Commissioner to determine depending on the particular circumstances. In deciding the form and period of time to respond, the Commissioner will have regard to the impact on the entity and the nature and imminence of the risk of harm to individuals or CDR consumers who would receive notification of the eligible data breach the Commissioner has reasonable grounds to believe has happened.
- 9.34 The Commissioner will consider submissions and any other relevant information provided by the entity within the period specified before deciding whether to direct the entity to notify under s 26WR.
- 9.35 The Commissioner's decision will be communicated to the entity in writing. Entities can apply to the AAT for review of a decision by the Commissioner under s 26WR(1) to make a direction.⁷
- 9.36 An entity must comply with a direction made under s 26WR(1) as soon as practicable (s 26WR(10)). Contravention of s 26WR(10) is an interference with the privacy of an individual (s 13(4A)).

⁷ Privacy Act, s 96(1)(bc).

Publication and disclosure of information

- 9.37 The OAIC will publish statistics in connection with the NDB scheme, with a view to reviewing this approach 12 months after the scheme's commencement.
- 9.38 The OAIC will respect the confidence of commercially or operationally sensitive information that is provided voluntarily in support of a data breach notification.
- 9.39 As a matter of course, the Commissioner will consult with entities following a request for information made under FOI law. For FOI requests relating to agencies, the Commissioner will offer to transfer requests to the agency in question.
- 9.40 Decisions about public communications will be made in accordance with the considerations set out in the '[Public communication as part of privacy regulatory action](#)' section of the *Privacy regulatory action policy*, and where appropriate, the *CDR regulatory action policy*.

Reporting under the My Health Records Act

- 9.41 Under s 75 of the My Health Records Act, some entities have a mandatory obligation to provide notification of certain data breaches, including potential breaches, in connection with the My Health Record system. The mandatory notification obligation applies to entities that are, or have at any time been, the System Operator,⁸ a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider (as defined in the My Health Records Act). Depending on the entity involved, notification must be made to either the OAIC or the System Operator or both.
- 9.42 A failure by a registered healthcare provider organisation, a registered repository operator, a portal operator or a registered contracted service provider to notify in accordance with s 75 is a breach of a civil penalty provision and may result in that entity being liable to pay a penalty.
- 9.43 The My Health Records Act also outlines in s 75(5) and (6) the steps an entity must take to contain and respond to the breach, or potential breach. The OAIC has developed the *Guide to mandatory data breach notification in the My Health Record system* to assist entities to comply with their mandatory data breach obligations.
- 9.44 Data breaches that are notified under s 75 of the My Health Records Act, do not need to be notified under the NDB scheme.

Responding to data breach notifications under the My Health Records Act

- 9.45 In assessing and responding to mandatory notifications, the OAIC will consider compliance with the My Health Records Act in addition to compliance with the APPs where relevant. The OAIC may also consider whether the breach was reported 'as soon as practicable', as required under s 75(2).

⁸ 'System Operator' is defined in s 14 of the My Health Records Act.

- 9.46 Section 75(5) of the My Health Records Act requires entities to take certain steps in responding to a data breach that may have occurred or arisen. These steps include containing the breach, evaluating the risks arising from the breach, notifying affected healthcare recipients (if the entity is the System Operator) or asking the System Operator to notify affected healthcare recipients (as applicable). The OAIC will consider these steps when assessing the severity of the breach and the entity's response. Section 75(6) of the My Health Records Act also requires entities to take steps in responding to a data breach that has occurred (rather than to a potential data breach). These steps include containing the breach (and to undertake a preliminary assessment of the causes), evaluating the risks related to or arising from the breach, notifying affected healthcare recipients (if the entity is the System Operator) or asking the System Operator to notify affected healthcare recipients (as applicable) and taking steps to prevent or mitigate the effects of further breaches.
- 9.47 The Commissioner has investigative powers under s 73(3) of the My Health Records Act, and may use these powers instead of the investigative powers under the Privacy Act if an investigation is warranted following a mandatory notification. However, the Commissioner will generally conduct investigations under the Privacy Act rather than the My Health Records Act unless there is a reason to conduct the investigation under the latter Act.
- 9.48 When entities are required to notify both the OAIC and the My Health Record System Operator of data breaches, the OAIC may consult with the System Operator when responding to the notification.

Reporting under the National Cancer Screening Register Act

- 9.49 Under s 22A of the National Cancer Screening Register Act 2016 (NCSR Act), the Secretary of the Department of Health (the Secretary), contracted service providers and former contracted service providers have a mandatory obligation to notify the Information Commissioner of certain data breaches, including potential breaches, in connection with the National Cancer Screening Register.
- 9.50 A failure by the Secretary, contracted service providers or former contracted service providers to notify in accordance with s 22A is a breach of a civil penalty provision and may result in that entity being liable to pay a penalty.
- 9.51 The NCSR Act also outlines in ss 22A(4) and (5) the steps the Secretary, contracted service providers or former contracted service providers must take to contain and respond to the breach, or potential breach.
- 9.52 Data breaches that are notified under s 22A of the NCSR Act, may also need to be notified under the NDB scheme, depending on the circumstances.
- 9.53 For more information on reporting under the NDB scheme, see paragraph 9.2.

Responding to data breach notifications under the NCSR Act

- 9.54 The OAIC will generally follow similar steps to the process outlined in relation to the My Health Records Act above [see paragraphs 9.45 to 9.48] when responding to mandatory data breach notifications under s 22A of the NCSR Act.

Reporting under Part VIIIA of the Privacy Act

- 9.55 Subsection 94S(1) provides that a breach of a requirement under Part VIIIA by the data store administrator (being the administrator, an officer or employee of the administrator, or a contracted service provider under a government contract with the administrator) **is taken to be an eligible data breach** by the data store administrator and the individual to whom the data relates is taken to be at risk from the eligible data breach.
- 9.56 Subsection 94S(2) provides that a breach of a requirement under Part VIIIA by a State or Territory health authority (being the authority, an employee of the authority or person in the service of the authority) **is taken to be an eligible data breach** by the State or Territory health authority and the individual to whom the data relates is taken to be at risk from the eligible data breach.
- 9.57 Subsection 94S(3)(a) provides that the breach is an eligible data breach as if the following provisions did not apply:
- S 26WE(3) – this provides that s 26WE(2) (which defines an eligible data breach as an unauthorised access to or disclosure of information that a reasonable person would conclude would be likely to result in serious harm to affected individuals; or that information is lost where unauthorised access is likely to occur and that access would likely result in serious harm to affected individuals) is subject to s 26WF
 - S 26WF – a breach is not an eligible data breach if the entity has taken action in relation to the disclosure before any serious harm results and, as a result, the likelihood of serious harm resulting is mitigated
 - S 26WH – requirement for an entity to carry out an assessment of whether a breach amounts to an eligible data breach
 - S 26WJ – no requirement to conduct an assessment in relation to a breach if another entity has conducted an assessment in relation to the same breach.
- 9.58 Subsection 94S(3)(c) provides that the breach is an eligible data breach as if the following provisions did not apply:
- S 26WN – exemption from notification of eligible data breach under ss 26WL and 26WK(3)(d) where the chief executive officer of a law enforcement body considers that notification will prejudice enforcement related activities
 - S 26WP – exemption from notification of eligible data breach under ss 26WL and 26WK(2)(a)(ii) where compliance would be inconsistent with a secrecy provision
 - S 26WQ – exemption from notification of eligible data breach under ss 26WL and 26WK where the Commissioner makes a declaration those provisions do not apply
 - S 26WS – exemption from the requirement to comply with a s 26WR(1) direction if the chief executive officer of an enforcement body believes that compliance with the direction is likely to prejudice an enforcement related activity
 - S 26WT – exemption from compliance with ss 26WR(1)(b) or 26WR(2) where compliance would be inconsistent with a secrecy provision.
- 9.59 The effect of these provisions is that any data breach by the data store administrator or a State or Territory health authority **is an eligible data breach, and the entity must comply with the requirements of Part IIIC, regardless of:**

- whether the entity has conducted an assessment and the outcome of that assessment
 - whether the entity considers that serious harm is likely to result for affected individuals
 - whether the entity has, or has attempted to, mitigate the risk of harm to affected individuals
 - whether the entity is an enforcement body and the chief executive officer of that body believes that notification of the eligible data breach would be likely to prejudice one of more enforcement activities they are conducting
 - whether there is a secrecy provision (including a prescribed secrecy provision in the regulations) that applies to the information disclosed in the breach
 - whether the Commissioner has made a declaration that ss 26WL and 26WK do not apply
 - whether the chief executive officer of an enforcement body believes that compliance with a direction of the Commissioner is likely to prejudice an enforcement related activity
 - whether compliance with ss 26WR(1)(b) or 26 WR(2) would be inconsistent with a secrecy provision (including a prescribed secrecy provision).
- 9.60 Further, s 94S(3)(b) requires the data store administrator or State or Territory health authority to:
- notify the Commissioner of the eligible data breach (s 94S(3)(b)(i)) and
 - only comply with the following provisions if the Commissioner so requires them to comply:
 - s 26WK – prepare a statement about the eligible data breach and give it to the Commissioner; and
 - s 26 WL – notify affected individuals of the eligible data breach.
- 9.61 Subsection 94S(4) provides that the Commissioner may consider a range of circumstances when considering whether to require either the data store administrator or State or Territory health authority to prepare a statement about the breach and notify affected individuals (s 94S(3)(b)(ii)), the Commissioner **must** require them to comply with those provisions if both of the following apply:
- the Commissioner is satisfied that the breach may be likely to result in serious harm to any of the individuals to whom the information relates and
 - s 94S(5) does not apply.
- 9.62 Note: the test of ‘likely to result in serious harm to any of the individuals’ is the same as exists in relation to NDBs notifiable under Part IIIC of the Privacy Act. However, in Part IIIC this assessment is conducted by the notifying entity and is one of the threshold tests for determining whether a data breach is an eligible data breach under those provisions. In relation to COVID app data, this assessment is undertaken by the Commissioner, who must have regard to the outcome of this assessment to comply with s 94S(4).
- 9.63 Subsection 94S(5) provides guidance for the Commissioner’s decision not to require compliance, or extend the period for compliance, with ss 26WK and 26WL. Satisfaction of s 94S(5) also overrides the mandatory requirement for the Commissioner to direct the data store administrator or State or Territory health authority to comply with s 26WK and 26WL

where the Commissioner is satisfied that a breach is likely to result in serious harm to affected individuals.

- 9.64 Under s 94S(5) the Commissioner may decide not to require compliance, or to extend the period for compliance, if the Commissioner is satisfied on reasonable grounds that it would not be reasonable in the circumstances. In reaching that satisfaction, the Commissioner **must** have regard to:
- the public interest
 - relevant advice provided by an enforcement body or the Australian Signals Directorate.
- 9.65 The Commissioner may take into consideration any other matters as the Commissioner considers relevant or any other advice: s 94S(5)(c) and 95S(6).
- 9.66 Other than the changes outlined above, the requirements of Part IIIC of the Privacy Act apply.