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.