Australian Government
Office of the Australian Information Commissioner

Office of the Australian Information Commissioner

Consumer Data Right regulatory strategy

OAIC

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

ISSN 2202–7262

Creative commons

Contact

Enquiries regarding the licence and any use of this strategy are welcome.

Online: Submit an Enquiry form
Website: www.oaic.gov.au
Phone: 1300 363 992
Monday to Thursday
10 am to 4 pm (AEST/AEDT)

Mail: Office of the Australian Information Commissioner
GPO Box 5288
Sydney NSW 2001

Non-English speakers

If you speak a language other than English and need help, please call the Translating and Interpreting Service on 131 450 and ask for the Office of the Australian Information Commissioner on 1300 363 992.

Accessible formats

All our publications can be made available in a range of accessible formats. If you would like this report in an accessible format, please contact us.

Last modified: 20 Jan 2026

Contents

CDR regulatory strategy

The OAIC is the independent national regulator for privacy and freedom of information. Our purpose is to promote and uphold individuals' rights to access government-held information and have their personal information protected.

The OAIC regulates the privacy aspects of the CDR system.

As the privacy regulator of this system, and of consumer data sharing activities under the Privacy Act more broadly, the OAIC is responsible for ensuring that regulated entities are supported to understand their compliance obligations and that consumers' privacy is protected when sharing their data.

The OAIC acknowledges the privacy benefits consumers can gain through using the CDR system to share data and aims to use its powers to encourage trust and confidence in the CDR system.

This strategy is informed by the OAIC's overarching focus, as outlined in its Statement of regulatory approach, on directing its regulatory powers to address conduct that presents the greatest risks of harm to individuals. It outlines the regulatory activities we undertake and how these will contribute to our vision as privacy regulator of the CDR system. This strategy is informed by the OAIC's overarching focus on directing its regulatory powers to address conduct that presents the greatest risks of harm to individuals.

Vision and objectives

The OAIC's vision as privacy regulator of the CDR system and other data sharing activities by APP entities aims to ensure the following objectives:

Objective 1

Consumers recognise and avoid unsafe data sharing and choose safer alternatives (such as CDR)

Objective 2

Entities shift to more secure and privacy protecting methods of consumer data sharing

Objective 3

Consumers trust their privacy is protected when using the CDR system

Having a safe and secure way for consumers to share and unlock the value of their data will enhance Australia's productivity.

Regulatory focus areas

To achieve these vision objectives, the OAIC will:

- maintain its focus on CDR framework compliance to actively identify emerging CDR risks and privacy compliance issues and deploy its full regulatory toolkit across education, compliance and enforcement to promote trust in the CDR system.
- include a focus on using the Privacy Act framework to target the harms arising from CDR-alternative activities (other consumer data sharing activities) such as screen scraping.
- progress complementary regulatory activities to protect consumers' privacy in CDR sectors, including in relation to the use of automated decision-making.

As outlined in its Statement of regulatory approach, the OAIC applies a proactive and harm-focused approach, taking regulatory action to encourage and support compliance and to address high risk matters with the greatest potential for harm.

As part of using the Privacy Act framework to target harms arising from CDR-alternative activities, the OAIC is currently undertaking an assessment of screen scraping practices which is assessing the risks and potential harms of screen scraping.

OAIC regulatory activities

To achieve our objectives the OAIC will adopt a whole of system approach to regulation:

Educate

Issue guidance, encourage compliance with the law and encourage consumers and businesses to shift to more secure data sharing.

Monitor

Actively identify emerging CDR risks and privacy compliance issues and continue compliance assessment programs targeted at CDR entities.

Enforce

Enforce privacy safeguards under the CDR including resolution of possible breaches through complaints management, investigation, determination, litigation and other formal enforcement outcomes.

Deter/Encourage

Ensure visibility of our regulatory action to highlight and communicate risks of CDR alternatives to encourage more entities to adopt the CDR.

Collaborate

Build relationships with the regulated community, industry and across Government.

Indicative activities

Through a range of activities, we will target actions and initiatives that reflect our regulatory strategy and focus areas. Below are some indicative activities that may be undertaken over the three years of this strategy.

		Year 1	Year 2	Year 3+
Activity 1	Continuing to provide (and update) guidance and education to: • consumers on the benefits of the CDR versus higher risk data sharing alternatives • accredited entities on CDR privacy obligations, and • APP entities on privacy obligations when engaging in data sharing activities			
Activity 2	Handling enquiries and complaints and notifiable data breaches			
Activity 3	Engaging with recognised EDR schemes in relation to handling of complaints			
Activity 4	Integrating data sharing practices into Privacy Attitudes Survey			
Activity 5	Undertaking assessments of entities operating within the CDR-framework, including: • assessing ADR use of outsourcing arrangements (completed) • assessing data quality obligations for a data holder (completed)			
Activity 6	Undertaking assessments of CDR-alternative data sharing activities, including: • assessing the risks and potential harms of screen scraping			
Activity 7	Engaging with other agencies in the CDR system to ensure privacy is appropriately protected as the regulatory framework evolves			
Activity 8	Proactively applying enforcement powers to issue determinations, injunctions and civil penalty provisions, including: • issuing a determination against Regional Australia Bank Ltd for breach of Privacy Safeguards 1 and 11 (completed) • enforcement actions where identified in accordance with this regulatory strategy			
Activity 9	Proactively communicating guidance and outcomes from complaints, assessments, investigations and determinations			

Expected outcomes

Privacy laws actively enforced to address harms linked to data sharing

Compliance and enforcement activity will ensure accountability, address harms, and provide a deterrent against negligent or malicious data practices.

Consumer adoption is driven up due to increased understanding of the CDR

By gaining a comprehensive understanding of the benefits of the CDR program and the privacy safeguards protecting it, consumers are empowered to make informed decisions about their data sharing practices and how their personal data is handled. Consumers are informed about the dangers of alternative practices such as screen scraping.

Entities are encouraged to use more secure data sharing practices

Entities will be motivated to adopt and promote more secure data sharing practices.

Entities develop skills, education and awareness on privacy practices and obligations

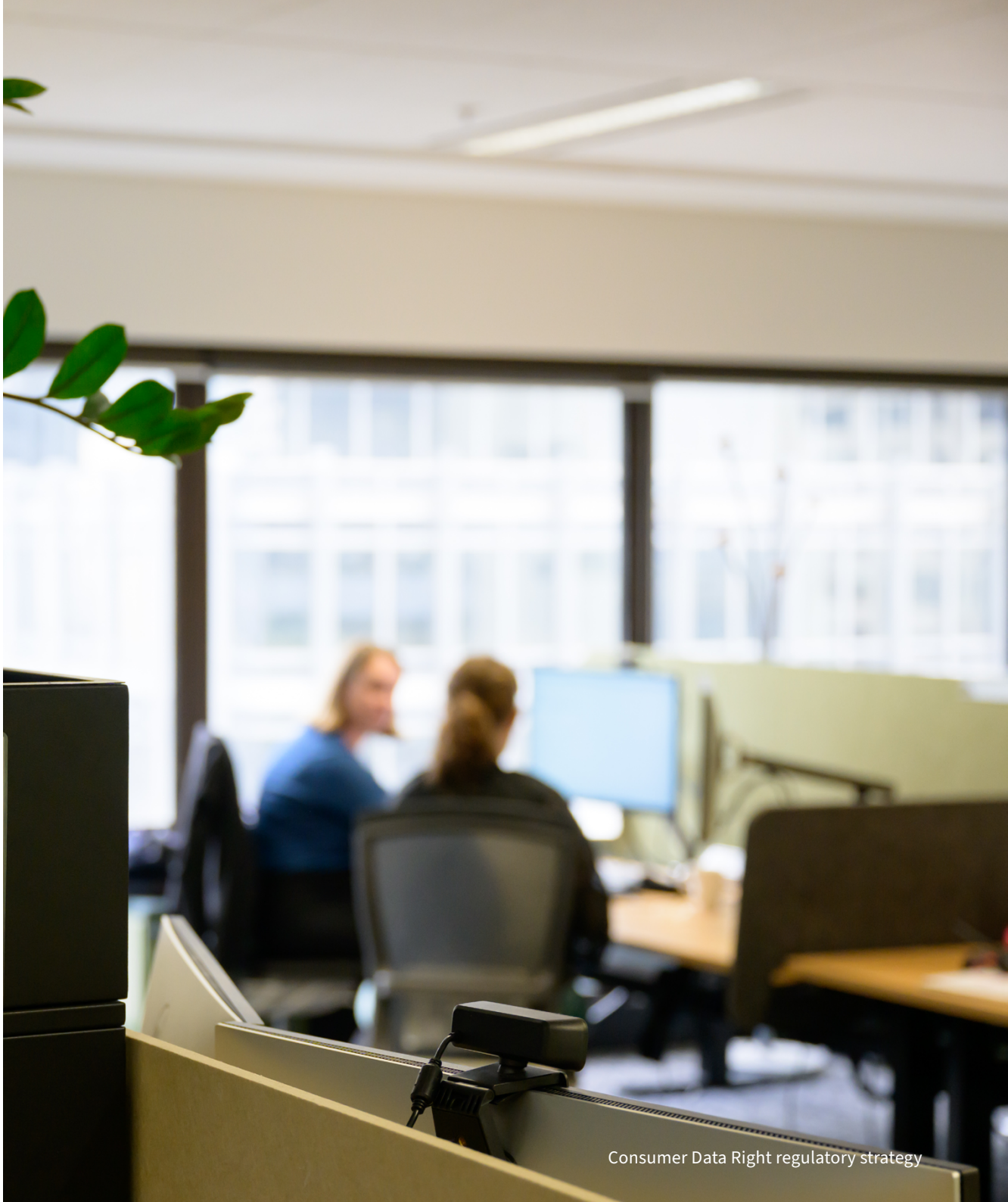
Entities invest in the necessary skills, education and awareness among staff regarding their privacy obligations. This commitment to training and knowledge will ensure that employees are well-equipped to handle data responsibly and in compliance with regulatory requirements and industry best practice.

Impacts

The OAIC aims to realise the following impacts through its activities and as a result of the above outcomes:

- Consumers make informed and safer choices about when and how to share their data
- Entities are confident they have the information they require to comply with legislation
- Entities consistently uphold quality privacy practices and demonstrate compliance with all relevant legislation
- Improved privacy practices amongst organisations that engage in data sharing
- A reduction in higher-risk data sharing activities

The impact of the regulatory initiatives contained within this strategy will be monitored and reported upon in accordance with the OAIC performance reporting framework.



www.oaic.gov.au