Global Data and Cyber Handbook - Australia

Regulators, Enforcement Priorities and Penalties

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 31 December 2024*

The [Office of the Australian Information Commissioner](http://www.oaic.gov.au/) (OAIC) is the main privacy regulator for Australia and administers and enforces the Privacy Act. Currently, the OAIC consists of three separate commissioners:  the Australian Information Commissioner (the head of the OAIC), the Privacy Commissioner and the Freedom of Information Commissioner.

States and Territories with public sector privacy laws also have regulatory bodies responsible for those State and Territory laws:

Currently, the OAIC is fulfilling most of the functions of the ACT Information Privacy Commissioner. The ACT Justice and Community Safety Directorate also has a role as agreed in a [Memorandum of Understanding](https://webarchive.nla.gov.au/awa/20190509042614/https:/www.oaic.gov.au/about-us/corporate-information/mous/mou-australian-capital-territory-and-oaic-provision-of-privacy-services) (MoU) between these bodies. See the OAIC's resource on [ACT Privacy](https://www.oaic.gov.au/privacy/privacy-in-your-state/privacy-in-the-act/) for more details.

[Information and Privacy Commission (NSW)](http://www.ipc.nsw.gov.au/)

[Office of the Information Commissioner (NT)](https://infocomm.nt.gov.au/)

[Office of the Information Commissioner (Qld)](http://www.oic.qld.gov.au/)

[Tasmanian Ombudsman (Tas)](http://www.ombudsman.tas.gov.au/)

[Office of the Victorian Information Commissioner (Vic)](https://www.ovic.vic.gov.au/)

States without public sector privacy laws nevertheless have bodies with privacy- or information-related responsibilities ([South Australian privacy committee (SA)](https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa) and [Office of Digital Government (WA)](https://www.wa.gov.au/organisation/office-of-digital-government)).

Where they exist, State and Territory health records laws are enforced by State/Territory-specific regulators:

The [ACT Human Rights Commission](http://hrc.act.gov.au/health/)

The Victorian [Health Complaints Commissioner](https://hcc.vic.gov.au/providers/health-records-providers)

In other States and Territories, the public sector regulators listed above

The [Australian Digital Health Agency](https://www.digitalhealth.gov.au/) (ADHA) is the system operator for the My Health Record system and could be said to play a regulatory role in this respect, although the OAIC also has a role to play. Where a data breach (or, in some cases, another matter notified to ADHA) involves personal information, ADHA will refer it to the OAIC.

The three regulators for the CDR (see above) are:

The Australian Competition and Consumer Commission (ACCC)

The OAIC

The [Data Standards](https://consumerdatastandards.gov.au/) body

However, several important functions relating to CDR previously held by the ACCC (e.g., [rule-making powers](https://treasury.gov.au/consultation/c2021-187223)) were shifted to the [Treasury](https://treasury.gov.au/) with a view to expediting the expansion of the regime.

The [Department of Home Affairs](https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security) is responsible for Australian national security, and within this department, the [Cyber and Infrastructure Security Centre](https://www.cisc.gov.au/) exercises regulatory functions under the [Security of Critical Infrastructure Act 2018 (Cth)](https://www.legislation.gov.au/Series/C2018A00029). The Australian [Attorney-General's Department](https://www.ag.gov.au/) also has a role, particularly under the [Telecommunications (Interception and Access) Act 1979 (Cth)](https://www.legislation.gov.au/Series/C2004A02124).

The [Australian Communications and Media Authority](https://www.acma.gov.au/) (ACMA) is the regulator for telecommunications, radiocommunications, spam and telemarketing legislation.

The [Australian Securities and Investments Commission](https://asic.gov.au/) (ASIC) is the regulator for corporations and financial services in Australia and its regulatory role can be relevant to the extent that privacy and security matters affect the compliance (or otherwise) of regulated entities with financial services and corporations regulation.

The [Office of the National Data Commissioner](https://www.datacommissioner.gov.au/) oversees the DATA Scheme under the DATA Act.

Additionally, while more of a policy-making body than a regulator, the National Cyber Security Coordinator and the National Office of Cyber Security provide strategic direction and oversight for cyber security policy, and oversee responses to consequences arising from cyber security incidents.

# How active is each of the regulator(s)?

*Last review date: 31 December 2024*

☒ Moderately active     ☒ Very active

The Privacy Commissioner is very active, while other regulators are moderately active.

# What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 31 December 2024*

The OAIC's recent enforcement activities have included conducting preliminary inquiries, undertaking investigations, making determinations and bringing legal proceedings in court against APP entities that breach the Privacy Act. The OAIC's approach to enforcement has been largely consistent over the years, generally opting for a conciliatory approach before progressing to formal enforcement. Its [Guide to Privacy Regulatory Action](https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action) describes its approach to privacy regulatory action in a number of spheres, with reference to other key documents such as its [Privacy Regulatory Action Policy](https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy) and joint (with the ACCC) CDR [Compliance and Enforcement Policy](https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/compliance-and-enforcement-policy).

The OAIC [Corporate Plan 2024-25](https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2024-25) indicates that the OAIC's key priorities generally remain consistent with previous Corporate Plans. Key activities for 2024-25 are stated to be:

Influencing and upholding privacy and information access rights frameworks

Advancing online privacy protections for Australians

Encouraging and supporting the proactive release of government-held information

Taking a contemporary approach to regulation

Five areas identified for specific regulatory focus in 2024-25 are:

Aligning emerging technologies, including AI, with community expectations and regulations, while targeting current and emerging harms and guiding compliance

Supporting a privacy-protecting digital economy by regulating compliance and supporting entities under the NDB scheme, Digital ID system, and CDR co-regulation

Promoting open government and enhancing FOI capabilities of the Australian Government for timely access and proactive release of information

Strengthening and enforcing personal information protections and contributing to privacy law reform

Building the OAIC’s internal capability and culture

The Privacy Commissioner has also made public statements that high privacy impact technologies such as facial recognition are also a focus for the OAIC. Together with overseas privacy regulators, the OAIC made a [joint submission](https://www.oaic.gov.au/engage-with-us/submissions/dp-reg-joint-submission-safe-and-responsible-ai-in-australia-discussion-paper) to a 2023 government consultation on [safe and responsible AI](https://consult.industry.gov.au/supporting-responsible-ai), and released a [joint statement](https://www.oaic.gov.au/newsroom/global-expectations-of-social-media-platforms-and-other-sites-to-safeguard-against-unlawful-data-scraping) on data scraping on social media platforms and other publicly accessible sites. Other recent public enforcement and guidance initiatives have related to [facial recognition](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks) and tracking through pixel tagging.

Recent changes to the Privacy Act (in 2022 and 2024) allow the OAIC (among other things) to undertake pre-emptive assessments of compliance with the notifiable data breach scheme, to conduct search and seizure activities, to seek more information and documents from entities, to issue infringement notices and seek lower order civil penalties for failures to comply with certain requirements, power to conduct public inquiries, and to direct complaint respondents to appoint an independent expert to assist with breach remediation efforts. The test for extra-territorial application of the Privacy Act was also simplified in 2022, making enforcement potentially easier. These changes, increased OAIC budget allocations, and the expected wider reform of the Privacy Act mentioned in other responses are resulting in increased enforcement action by the OAIC. This is in the context of a series of high-profile data breaches at large Australian companies impacting a significant proportion of the population.

The ACMA's key recent enforcement activities relating to the privacy space involve the issuance of infringement notices (often with sizeable financial penalties attached) against businesses who send unsolicited commercial electronic messages in breach of the Spam Act (e.g., without sufficient consent and/or without the minimum mandatory content). Other enforcement activities include investigations on misuse of subscriber data or failing to conduct customer authentication.

The ACMA's [compliance priorities](https://www.acma.gov.au/compliance-priorities) for 2024-25 include targeting misleading spam messages and combatting SMS impersonation scams. Additionally, ACMA currently oversees the voluntary [Australian Code of Practice on Disinformation and Misinformation](https://digi.org.au/disinformation-code/) and reports to government on associated matters. A [bill](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7239) was introduced to Federal Parliament which would have increased the ACMA's power to monitor and combat misinformation and disinformation on digital platforms, but did not gather sufficient support so is not proceeding at this time.

The ACCC's key data-related enforcement activities in recent years have involved litigation for alleged misleading and deceptive conduct in relation to data handling practices. The ACCC has examined and criticized the lack of visibility and consumer choice about data collection practices and is advocating for regulatory reforms in this area.

The ACCC's [Compliance and enforcement priorities for 2024-2025](https://www.accc.gov.au/about-us/accc-priorities/compliance-and-enforcement-priorities) are not privacy-specific, but they include consumer and fair trading issues in the digital economy, which (based on the ACCC's approach to date) could extend to looking at data handling practices in a digital context. In any event, we expect the ACCC to continue taking an interest where it perceives that organizations are misleading consumers about privacy matters.

ASIC’s [2024-2025 enforcement priorities](https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-252mr-asic-announces-new-enforcement-priorities-with-a-focus-on-cost-of-living-pressures/) do not specifically mention data privacy or cybersecurity, but its enduring priorities include misconduct carrying a high risk of significant consumer harm, systemic compliance failures by large financial institutions, and governance and directors’ duties failures. In practice, ASIC has in the recent past taken successful enforcement action against a financial services licensee for breach of its license conditions by, among other things, failing to have adequate cybersecurity risk management in place. ASIC has also made [statements](https://asic.gov.au/about-asic/news-centre/articles/what-a-federal-court-ruling-on-cybersecurity-means-for-afs-licensees/) that it may take action against other regulated entities whose cyber security measures are lacking, which may result in significant penalties. ASIC has also used its [research](https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-300mr-asic-calls-for-greater-organisational-vigilance-to-combat-cyber-threats/) to advocate for more organizational vigilance on cyber security.

# What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 31 December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Increasing

Australian regulators have various powers to investigate or take action against entities that fail to meet data or cyber obligations. Some notable examples of regulatory enforcement are:

The ACMA imposed a fine of AUD 1.5 million against a major telecommunications company that suffered a data breach in late 2022 and is following that up with legal proceedings brought in 2024.

The OAIC found that a major Australian retailer interfered with the privacy of the individuals whose personal information and sensitive information it collected through its facial recognition technology system in many of its retail stores by collecting the sensitive information of those individuals in circumstances where the individuals did not consent to the collection of the information and failing to take such steps as were reasonable in the circumstances to notify those individuals about the facts, circumstances and purposes of collection, and the consequences of not collecting that information.

The OAIC found that scraping data to target vulnerable people by a purported property education business was unlawful and interfered with the privacy of individuals, as they failed to collect the personal information by fair means, take reasonable steps to notify individuals whose information was collected, and to ensure that the information it collected was accurate and up to date.

The OAIC also agreed to a AUD 50 million settlement with a major social media company relating to the disclosure of its users’ personal information to an in-platform app for political profiling.

Enforcement under the SOCI Act is confidential due to the associated national security concerns, but it is understood that the Australian Cyber Security Centre has been active in its enforcement.

The powers of Australian regulators to take action in relation to breaches of data and cyber obligations are also increasing. For example, the SOCI Act was recently amended to:

Clarify existing obligations in relation to systems holding "business critical data"

Enhance government assistance measures to better manage the impacts of all hazards incidents on critical infrastructure

Simplify information sharing across industry and Government

Introduce a power for the Government to direct entities to address serious deficiencies within their risk management programs, and

Align telecommunication providers to the same standards as other critical infrastructure entities by moving security regulation of the telecommunications sector from the Telecommunications Sector Security Reforms (TSSR) in the Telecommunications Act 1997 to the SOCI Act.

The Tranche 1 reforms of the Privacy Act also provided the OAIC with additional enforcement powers and investigation powers, including through the adoption of certain aspects of the Regulatory Powers (Standard Provisions) Act 2014 (Cth). In particular, the Tranche 1 reforms provided for additional investigation powers in respect of alleged breaches of the Privacy Act’s civil penalty provisions, in addition to the Commissioner’s pre-existing investigation powers. Additionally, the Commissioner has gained the power to conduct public inquiries into matters relating to privacy, on the direction or approval of the Attorney-General (in respect of systemic or industry-wide issues).

Class actions/group actions under data or cyber regulation are:

☒         Increasing

There is a trend towards class actions in relation to data breaches and cyber failings. Some recent high profile examples are:

In 2023, multiple class action claims were filed against a major Australian health insurer, relating to a mass data breach which occurred in October 2022 and affected millions of customers’ health information.

Also in 2023, class action claims were filed against a major telecommunications company that was affected by a mass data breach resulting from a hack, alleging that the company breached its contract with customers, breached the APPs under the Privacy Act, breached a duty of care owed to customers and engaged in misleading and deceptive conduct contrary to the Australian Consumer Law.

A potential class action is being investigated against a major financial services company relating to security breaches in March 2023, which compromised the personal information (including passports, driver's licenses, and Medicare numbers) of millions of customers in Australia.

# What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 31 December 2024*

There are:

☒         administrative remedies / civil penalties applied by regulators and law enforcement

Under the Privacy Act, the Privacy Commissioner has the power to investigate organizations based on complaints or of the Commissioner's own accord, accept enforceable undertakings, make determinations, apply to the court for injunctions or civil penalties and, in some cases, issue infringement notices.

The maximum penalty for a corporation for serious interferences of privacy is the greater of:

AUD 50,000,000

If a court can determine the value of the benefit obtained from the contravention - three times the value of the benefit, or

If a court cannot determine the value of the benefit obtained from the contravention - 30% of the body corporate's adjusted turnover during the breach turnover period.

A mid-tier civil penalty provision exists for non-serious interferences with privacy, and a new low-level civil penalty provision to address specific administrative breaches of the law, with attached infringement notice powers for the OAIC with set penalties. Also of note, the Privacy Commissioner may issue infringement notices imposing monetary penalties for failure or refusal to provide information, answer questions or produce documents or records.

The Privacy Commissioner's determinations can include requirements for the respondent to a complaint to take specified steps to rectify conduct that led to a breach, which may include a direction to engage an independent and suitably qualified adviser to assist with this process at the respondent's own cost. Additionally, the Privacy Commissioner may also issue a compliance notice requiring an entity it reasonably believes is in breach of certain APPs to remedy that non-compliance.

Under the Healthcare Identifiers Act, knowing or reckless unauthorized use or disclosure of healthcare identifiers can result in a maximum civil penalty of AUD 990,000 for corporations and AUD 198,000 for individuals.

Misuse of a My Health Record or breach of the requirements of the MHR Act is subject to a maximum civil penalty of AUD 2,475,000 for corporations and AUD 495,000 for individuals.

State and Territory public sector privacy, health records laws, surveillance laws, telecommunications laws and critical infrastructure laws also have their own civil penalty regimes which may be triggered by data-related breaches.

☒         criminal penalties from regulators and law enforcement

Use or disclosure of false or misleading credit reporting information, credit information or credit eligibility information is an offence under the Privacy Act subject to a maximum penalty of AUD 66,000.

It is also a criminal offense to fail or refuse to provide information, answer questions or produce documents or records required under the Privacy Act, subject to a penalty of AUD 19,800. If there is a "system of conduct" or a "pattern of behavior" that results in two or more failures or refusals, the penalty increases to AUD 99,000.

Unauthorized use or disclosure of healthcare identifiers is an offense under the Healthcare Identifiers Act subject to a maximum penalty of imprisonment for two years or AUD 39,600.

For criminal breaches of the MHR Act, the maximum penalty is up to five years' imprisonment and/or a fine of AUD 99,000.

State and Territory public sector privacy, health records laws, surveillance laws, telecommunications laws and critical infrastructure laws also have their own criminal penalty regimes, which may be triggered by data-related breaches.

Under the Crimes Act 1914 (Cth), criminal pecuniary penalties can typically be increased five-fold, and penalties for imprisonment can be converted into monetary penalties, for corporations.

☒         private remedies

A range of private remedies are, or are expected to become, available:

A [2024 County Court of Victoria decision](https://bakerxchange.com/rv/ff00dbc90f903f3f32e503fbbc47b53b80ee3bca) suggests the existence of an Australian common law cause of action for invasion of privacy. It remains to be seen whether this position will be endorsed by higher courts.

The report on the review of the Privacy Act proposed – and the government has agreed in-principle – that the legislature should introduce a direct right of action for individuals against organizations that breach their privacy and a tort for serious invasions of privacy. The 2024 Tranche 1 reforms to the Privacy Act, which are scheduled to commence within six months of 11 December 2024, will enable individuals to bring a direct claim in tort for a serious invasion of their privacy. A broader individual right of action for an interference with their privacy is expected to be implemented in Tranche 2 reforms, though the timing is uncertain at this stage.

Breach of the Australian Privacy Principles and certain other provisions in the Privacy Act is an interference with the privacy of an individual. An individual can complain to the OAIC about interferences with their privacy, and the OAIC may assist with conciliation or commence an investigation, and potentially subsequently make a determination in the individual's favor (which may result in compensation being paid to the individual and/or an apology being made)

An individual could potentially bring an action for damages on the basis of breach of statutory duty, on another tortious basis (e.g., negligence), or for breach of contract, depending on the circumstances

☒         other

Failure to comply with the Privacy Act can result in complaint-based or Commissioner-initiated investigations by the OAIC, depending on the particular breach and the surrounding circumstances. The Privacy Commissioner is also empowered with broad information-sharing powers that enable it to share relevant information with other enforcement agencies, including the Australian Federal Police or Commonwealth Department of Public Prosecutions, in order for them to consider further enforcement action. The OAIC may also conduct public enquiries and make certain emergency declarations, and has certain monitoring and investigation powers (e.g., search and seizure powers) under the [Regulatory Powers (Standard Provisions) Act 2014 (Cth)](https://www.legislation.gov.au/C2014A00093/latest/text).

Organizations may also be required to give enforceable undertakings by regulators to avoid further enforcement action being taken.

Under the Privacy Act and some other legislation (e.g., the Spam Act, the Telecommunications Act), regulators may issue infringement notices requiring immediate payment of penalties and/or cessation of alleged contraventions without needing to bring legal proceedings for a civil penalty order.

Notably, since the December 2024 reforms to the Privacy Act, courts have had express powers to make any order they see fit after a civil penalty relating to an interference with privacy has been established. Additionally, the OAIC now has the power to make declarations requiring APP entities to prevent or reduce any reasonably foreseeable loss or damage likely to be suffered by an individual as a result of an eligible data breach.

# If data subjects have private remedies, what form can these remedies take?

*Last review date: 31 December 2024*

☒         representative actions (e.g., brought by a consumer/data privacy body or the supervisory authority)

Individuals do not currently have rights to directly enforce the Privacy Act (or the Spam Act, the DNCR Act, MHR Act or Healthcare Identifiers Act) in court. At present, individuals may complain (on their own behalf and potentially as representatives of other affected individuals) to the OAIC about an alleged interference with their privacy, and the OAIC may take enforcement action in response. Among other things, the OAIC may direct an APP entity that has breached the APPs in respect of an individual's personal information to apologize to the affected individual and/or pay them compensation. In civil penalty proceedings instigated by the OAIC, a court could also make orders aimed at redressing harm to affected individuals. There is one [recent court decision](https://insightplus.bakermckenzie.com/bm/dispute-resolution/australia-the-right-to-privacy-a-new-cause-of-action) that suggests that there might be a common law cause of action for invasion of privacy, but it remains to be seen whether this is followed by other courts.

Looking ahead, as noted in a previous response, the report on the review of the Privacy Act proposed – and the government agreed in-principle – that the law should be changed to give individuals a direct statutory right of action. Recent Tranche 1 reforms to the Privacy Act, which are scheduled to commence within six months of 11 December 2024, will enable individuals to bring a direct claim in tort for a serious invasion of their privacy. Once this cause of action becomes available, class actions for serious invasions of privacy may be possible, in the right circumstances (at present, class actions relating to personal information would typically have to be brought via other avenues, e.g., breach of confidence or contract). Additionally, the Tranche 1 reforms expressly grant the Federal Court power to issue any order it sees fit where it has determined that a civil penalty provision of the Privacy Act has been contravened, and individuals may recover any compensation ordered to be paid to them as a debt. A broader individual right of action for an interference with their privacy is expected to be implemented in Tranche 2 of the reforms to the Privacy Act, though the timing is uncertain at this stage.

State and Territory health privacy/records laws also contain mechanisms for individuals to complain to relevant authorities about interferences with privacy, with escalation to a tribunal expressly contemplated in some States' legislation. The position is typically similar under general State/Territory public sector privacy laws, although notably the Information Privacy Act 2014 (ACT) contemplates that individuals may seek certain orders from courts.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.