
Key compliance trends and predictions for 2025

Key Compliance trends and predictions for 2025

Australia's complex regulatory systems at a State and national level continue to give rise to compliance challenges for organisations across Australia, particularly those with cross-border operations. Further, with the growth in innovative technologies such as AI and as broader developments arise, organisations need to stay ahead of regulatory compliance issues before and as they develop.

In the first half of 2025, Australia will face a Federal election and while the exact date is not yet known (at the time of writing), it must be held on or before 17 May 2025. Once the caretaker period commences, there will not be any significant decisions made and be no new legislative reform. However, in 2024, the Commonwealth Parliament passed a total of 140 Acts. In addition, there were 2833 regulations and other subordinate legislation passed. From a Commonwealth legislative perspective alone, that means that there will be much for organisations and businesses to do.

The numbers of Bills introduced, Acts, Regulations and subordinate legislation passed throughout 2024 in each Australian jurisdiction is shown in the following Table:

Data for 2024:

Jurisdiction	Bills introduced in 2024	Acts passed in 2024	Regulations and other subordinate legislation passed in 2024
Commonwealth	167	140	2833
ACT	45	51	37
New South Wales	134	96	371
Northern Territory	26	23	28
Queensland	53	54	253
South Australia	135	68	127
Tasmania	53	32	103
Victoria	57	51	141
Western Australia	49	53	305

Law Compliance provides legislative compliance services and tools to assist Australian organisations manage their legal compliance obligations – simply and efficiently.

Hundreds of organisations across Australia rely on Law Compliance to identify all of the legislation relevant to them and to monitor changes to those laws. Law Compliance is currently monitoring all Bills introduced throughout the country and in particular is following the Bills which are relevant to our clients' compliance obligations across industries such as the health sector, aged care, statutory bodies, disability care, childcare, education, retail, transport (land, air and sea), utilities, and not-for-profit organisations. Ongoing regulatory developments necessitate timely and actionable information on legal obligations and changes, and resources and tools to support an organisation-wide compliance culture.

Key Compliance trends and predictions for 2025

Through our analysis of passed legislation which is already in force or will take effect during 2025 across Australia, the following key national compliance trends will be relevant for 2025:

1. Aged Care

Following the Royal Commission into Aged Care Quality and Safety, there have been a number of priority areas for reform of the aged care sector. In November 2024, a new Aged Care Act passed Parliament and will commence operation on 1 July 2025. The new *Aged Care Act 2024* (Cth) replaces the *Aged Care Act 1997* (Cth) (**the Old Act**).

One of the key changes between the Old Act and the new, is the introduction of a 'rights-based framework', including a Statement of Rights, aimed at improving the way aged care services are delivered to older people. The framework places particular emphasis on the rights of individuals and ensuring services are of a high quality and are person-centred.



For aged care providers, the most operationally significant changes introduced by the *Aged Care Act 2024* include:

- as mentioned, the introduction of a new Statement of Rights and Statement of Principles;
- new registration requirements, including general and category-specific conditions on provider registration;
- new statutory duties for registered aged care providers and 'responsible persons';
- a change in terminology from 'key personnel' under the Old Act to 'responsible persons';
- strengthened Aged Care Quality Standards;
- new complaints management framework, including greater protections for whistleblowers who call out issues.

The new registration requirements will apply to any organisation that seeks to deliver funded aged care services. Registration will be based on the services delivered and the obligations that follow will be determined by the registration categories in which the provider operates. Aged care providers who deliver services across a number of program areas e.g. home care and residential aged care, will now have a single, universal provider registration. "Deeming" provisions will apply for existing providers linked to their current funding agreements.

The change in focus to a rights-based framework demonstrates the ongoing need for organisations to build strong cultures of compliance in relation to vulnerable clients. All service providers operating in the aged care system must make decisions and take actions from the perspective of a person-centred aged care system and follow the principles of an aged care system that:

- values workers and carers;
- is transparent and sustainable and represents value for money;
- continues to improve.

The Commonwealth Department of Health and Aged Care has released a 'roadmap' of the reforms, including the activities and dates from January to December 2025. A link to the 'roadmap' can be accessed here:

<https://www.health.gov.au/our-work/aged-care-reforms/roadmap>

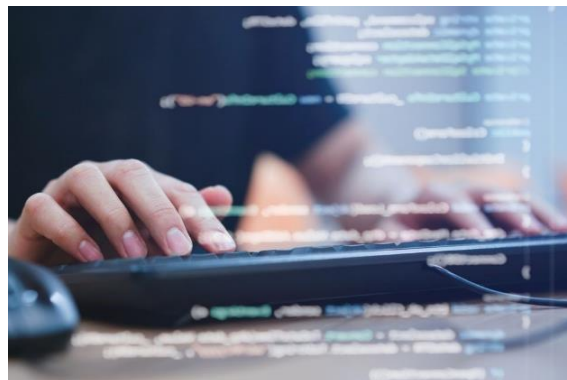
Key Compliance trends and predictions for 2025

2. Privacy and data security

Another area of major reform leading to compliance obligations for 2025, is privacy and data security. Amendments to a number of Acts, most notably the *Privacy Act 1988* (Cth) (the **Privacy Act**) were passed by the Federal Parliament on 29 November 2024.

For organisations to which the Privacy Act applies (**APP Entities**), the most significant changes include:

- creation of a new statutory cause of action to provide redress for serious invasions of privacy;
- amendments to the *Criminal Code Act 1995* (Cth) to include new 'doxxing' offences;
- new provisions requiring organisations to include information in privacy policies about automated decisions that significantly affect the rights or interests of an individual; and
- new provisions requiring the Information Commissioner to develop a Children's Online Privacy Code (**COP Code**) relating to online privacy for children which will result in certain entities being bound by the new provisions.



While many of the amendments came into effect immediately following Royal Assent (i.e. 10 December 2024), commencement of other provisions has been deferred. A summary of the most significant changes is set out below and where the dates the provisions commence have been notified, these are included.

[New statutory cause of action for serious invasions of privacy \(commences on or by 10 June 2025\)](#)

A person may take legal action against an organisation or an individual where the person alleges that they have suffered a serious invasion of their privacy through an intrusion into the person's seclusion or a misuse of their information, and they had a reasonable expectation of privacy in the circumstances. When determining if the invasion of privacy is serious, the courts may have regard to, among other things:

- the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the person bringing the claim;
- whether the other party knew or ought to have known that the invasion of privacy was likely to offend, distress or harm the dignity of the person;
- if the invasion of privacy was intentional – whether the organisation or individual was motivated by malice.

Before the cause of action will be made out, Courts must also determine whether the public interest in the person's privacy outweighs any countervailing public interest, for example, freedom of the media, open justice, freedom of expression, public health and safety, national security and prevention and detection of crime.

It may be a defence to a cause of action where the invasion of privacy was:

- required or authorised by, or under, an Australian law or court or tribunal order;
- reasonably believed to be necessary to prevent or lessen a serious threat to the life, health or safety of a person.

If the cause of action is made out, the remedies may include damages, an apology, a declaration that the organisation or individual has seriously invaded the person's privacy.

Key Compliance trends and predictions for 2025

'Doxxing' offences

'Doxxing', or the release, publication or distribution of personal information via a carriage service in a manner that would be regarded as menacing or harassing, is now illegal under the reforms introduced, and there are two new offences which are punishable by up to 7 years imprisonment.

The provisions target 'doxxing' that is directed at individuals in a menacing or harassing way (up to 6 years imprisonment) and doxing directed at individuals by reason of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin (up to 7 years imprisonment).

The Act provides the following example of 'doxxing':

- publishing the names, images and residential addresses of members of a private online religious discussion group across multiple websites and encouraging others to attend those addresses and block entryways or otherwise harass the members of that group.

The 'doxxing' offences commenced on 11 December 2024.

Updating privacy policies to include 'automated decision-making'

An organisation's privacy policy will need to be updated if it uses computer programs, including artificial intelligence (**AI**), which use an individual's personal information to make decisions, or do a thing that is substantially and directly related to making a decision, that could reasonably be expected to significantly affect the rights or interests of the individual. In such circumstances, the organisation's privacy policy will need to reflect the kinds of personal information used in the operation of the computer program, and the kinds of decisions that are made.

The date by which organisations to which the Privacy Act applies must update their privacy policies has been deferred to 10 December 2026 to allow the changes to be made. However, once the provisions come into effect, they will apply to all 'automated decisions' regardless of whether:

- the personal information was collected or created before or after 10 December 2026;
- the use of the personal information by the computer program occurred before or after 10 December 2026; and
- the arrangement for a computer program to make the decision was made before or after 10 December 2026.

Making a decision includes refusing or failing to make a decision.

Recent OAIC Determination—Commissioner initiated investigation into Bunnings Group Limited

In October 2024, an investigation initiated by the Australian Privacy Commissioner, Carly Kind, found that facial recognition systems operating in Bunnings stores had breached the Privacy Act.

The facial recognition technology (**FRT**) via CCTV, captured the faces of every person who entered 63 Bunnings stores across Victoria and NSW between January 2019 and November 2021, with the likely number of individuals in the hundreds of thousands. The Commissioner determined under section 52 (1A) of the Privacy Act that Bunnings had breached the Australian Privacy Principles through its use of the FRT by collecting personal and sensitive information without consent.

The Commissioner determined that the use of FRT was the "...most intrusive option, disproportionately interfering with the privacy of everyone who entered its stores, not just high-risk individuals."

Bunnings had also failed to take reasonable steps to notify individuals that their personal information was being collected, and did not include the required information in its privacy policy.

Key Compliance trends and predictions for 2025

If an organisation is considering implementing any FRT system, a primary consideration should be whether there is a less intrusive approach that can be taken and ensure that it has sufficiently transparent processes, including compliance with APPs. Before implementing an FRT system, a detailed privacy impact assessment must be carried out.

The OAIC has produced a guide to assessing the privacy risks of FRT and a link to the guide can be found here:

<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks>

3. Cyber Security and Protection of Information

The *Cyber Security Act 2024* (Cth) was enacted within a suite of cyber security legislative reforms (Cyber Security Legislative Package), in response to the Australian Government's 2023-2030 Cyber Security Strategy.

The *Cyber Security Act* commenced on 30 November 2024, but a number of key reforms have been deferred and will not come into effect for up to 12 months after that date.

The key reforms with impact for businesses are the introduction of mandatory reporting of ransomware payments, voluntary information sharing and updated security standards for 'relevant connectable products'.



Mandatory ransomware reporting

An organisation carrying on business in Australia with an annual turnover of more than \$3 million will be a 'reporting business entity' for the purposes of mandatory ransomware reporting. Commonwealth, State and Territory Ministers, departments and bodies established under laws of the Commonwealth, States or Territories for a public purpose are not captured by these obligations.

If a cyber security incident has occurred or is imminent which impacts a 'reporting business entity' and following a demand for payment the 'reporting business entity' or another entity on behalf of the entity impacted by the provides a payment or benefit – known as a ransomware payment, then the 'reporting business entity' must notify the Department of Home Affairs and the Australian Signals Directorate within 72 hours of having made the payment or becoming aware of the payment being made. Failing to notify the Australian Signals Directorate may result in a civil penalty of 60 Penalty units (currently \$19,800).

Mandatory ransomware reporting obligations will commence on 28 May 2025.

Updated security standards for 'relevant connectable products'

New provisions provide for the Minister for Cyber Security to introduce rules relating to mandatory security standards for products that can directly or indirectly connect to the internet, called 'relevant connectable products', that will be acquired in Australia.

'Relevant connectable product' is broadly defined and captures any product that is either capable of connecting to the internet (internet-connectable) or that is capable of sending and receiving data by means of an electrical or electromagnetic transmission (network-connectable).

Key Compliance trends and predictions for 2025

Manufacturers and suppliers of ‘relevant connectable products’ will be subject to the new security standards for classes of relevant specified products prescribed by the rules and may be subject to compliance notices if they do not comply.

The rules made under the *Cyber Security Act 2024* (Cth) will be known as the *Cyber Security (Security Standards for Smart Devices) Rules 2024* (**the Rules**). An exposure draft of the Rules has been released, and submissions are currently being sought.

The Rules will commence on 28 November 2025.

Voluntary information sharing and ‘limited use’ obligations

Changes to the *Cyber Security Act* now allow for a voluntary flow of information for incident coordination where there has been a significant cyber security incident. Organisations may voluntarily give the National Cyber Security Coordinator (**NCSC**) and the Australian Signals Directorate (**ASD**) information about cyber incidents where previously they were constrained in sharing information. The reforms also grant the NCSC the right to use the information, but limits that use for the purpose of responding to and resolving the cyber incident.

It is important to note that where information is provided voluntarily, it cannot be used against the organisation for regulatory purposes. However, these provisions do not create a ‘safe harbour’ against prosecution for a criminal offence or the *Cyber Security Act*.

4. Security of Critical Infrastructure

In addition to cyber security reforms and as part of 2023-2030 *Cyber Security Strategy*, amendments to the *Security of Critical Infrastructure Act 2019* (Cth) (**the SOCI Act**) have also been introduced to improve preparedness and resilience of critical infrastructure assets in Australia. The SOCI Act applies to 11 sectors, including: healthcare and medical, communications, higher education and research, data storage and processing, transport, water and sewerage, energy, defence, food and grocery and financial services and markets.

The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*

(Cth) passed Federal Parliament on 25 November 2024 and commencement dates have been deferred (see below).



Data storage systems

The key operational impacts include expanding what is captured under the ‘critical infrastructure’ obligations to include related data storage systems that store or process business critical data. That means that the data storage system of an entity captured by the SOCI Act will now be deemed to be a part of the critical infrastructure asset and obligations applying to the critical infrastructure asset will also need to take into account the data storage system. However, to be subject to the obligations, the data storage system must:

- be owned or operated by the SOCI entity which is responsible for the critical infrastructure asset;
- be used in connection with the critical infrastructure asset and if vulnerable would impact the critical infrastructure asset;
- store or process ‘business critical data’.

Key Compliance trends and predictions for 2025

The amendments will commence operation on 24 May 2025 and relevant SOCI entities will have until then to ensure that data storage systems are subject to the obligations.

Use and disclosure of protected information

The amendments to these provisions are aimed at appropriately protecting information relating to the operation, structure and location of critical infrastructure assets where disclosure could harm Australia's national interests, but at the same time enabling Government and industry to share information. The implementation period within which of the changes must occur is 6 months, so organisations will need to have considered the reforms by 24 May 2025.

'Protected information' has been amended and is defined to include documents or information obtained or generated in the course of exercising powers or performing duties or functions under, or adopted for the purposes of complying with, the SOCI Act where the disclosure would or could reasonably be expected to prejudice national security, defence or the social or economic stability of Australia, or to prejudice the availability, integrity, reliability or security of a critical infrastructure asset. Disclosure of 'protected information' is limited to these circumstances. However, while disclosure is limited in certain circumstances, the amendments have also clarified when disclosure is permitted and has

Organisations subject to these new provisions will need to ensure they understand the meaning of 'protected information' and what can and cannot be shared.

5. Trends in employment law

We anticipate that there may be trends in employment law which are likely to arise around the 'return to office vs work from home' model. While there have been well-publicised attempts to mandate returns to the office at a business level here and in other jurisdictions, there has not been an attempt to legislate a return to office working in Australia. On the contrary, the *Fair Work Legislation Amendment (Secure Jobs Better Pay) Act 2022 (Secure Jobs Better Pay)* amendments in 2023 provided greater scope for employees to request flexible work.

It is expected that employee well-being will be a continuing theme with various measures to support workers' physical, mental, and emotional health likely, including through the 'Right to Disconnect' laws and managing psychosocial hazards in the workplace. The latter is supported through a new code of practice whereby persons conducting a business or undertaking can obtain practical guidance on how to manage psychosocial health and safety risks at work. The *Work Health and Safety (Managing Psychosocial Hazards at Work) Code of Practice 2024* can be accessed at:

[Work Health and Safety \(Managing Psychosocial Hazards at Work\) Code of Practice 2024](#)

From 1 January 2025, intentional underpayment of wages by employers became a criminal offence. Regulators will continue to focus on exploitation of vulnerable workers and these new criminal offences now also apply together with significant monetary penalties. These penalties were evidenced in August 2024 in a case before the Federal Court which awarded record penalties of a total of \$13.7 million against a company and a further amount of \$1.6 million in penalties personally against the CEO and director of the company. The company, Sushi Bay Pty Ltd was found to have underpaid 163 employees over several years as well as keeping false and misleading



Key Compliance trends and predictions for 2025

records, failing to pay annual leave, knowingly providing false or misleading information to the Fair Work Ombudsman, among other things¹.

The changes to the *Fair Work Act 2009* (Cth) mean that an employer, who can be an individual or a company, will commit an offence if they engage in intentional conduct to fail to pay an amount in full on or before it is due, to an employee. The “amount due” includes wages, superannuation, leave entitlements and allowances.

Some exceptions to the criminal offences’ provisions do apply to certain employers, namely:

- employers in NSW, Queensland, South Australia, Tasmania and Victoria who are sole traders, partnerships other unincorporated entities or non-trading corporations;
- in relation to most Victorian State Government employees;
- in relation to certain types of underpayments regarding Tasmanian local Government employees.

If an employer has made an underpayment as a result of a genuine mistake, an accident or a miscalculation, they will not be liable to the criminal penalties, provided that once they become aware, they correct the underpayment.

There have been a number of class actions in the public health sector which stress the need for employers to ensure all entitlements are paid, and the significance of diligently applying the provisions of each instrument. We are expecting employers to be subjected to further scrutiny through proceedings seeking redress for underpayments, even if not as a prosecution for intentional underpayments.

As a result of earlier amendments to the Fair Work Act, certain fixed term employees will be treated as on-going employees and contractors may be considered employees, depending on the nature of their engagement. This means that the pool of people able to access certain employment entitlements and unfair dismissal remedies will be larger.

6. Social media age restrictions

The *Online Safety Act 2021* (Cth) was amended by the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) in November 2024 with the introduction of age restrictions related to certain social media platforms, such as Snapchat, TikTok, Facebook, Instagram and X.

The changes mean that the providers of certain kinds of social media platforms must take steps to prevent young people who are under 16 years from having accounts. For the purposes of the changes, ‘age-restricted social media platform’ means an electronic service:

- the sole or a significant purpose, of which is to enable online social interaction between 2 or more end-users;
- which allows end-users to link to, or interact with, some or all of the other end-users;
- which allows end-users to post material on the service.

The changes also allow for the Minister to make legislative rules which may prescribe other electronic services to be captured or other conditions.



¹ *Fair Work Ombudsman v Sushi Bay Pty Ltd (in liq) (No 3)* [2024] FCA 869

Key Compliance trends and predictions for 2025

The changes introduce significant penalties and providers will have until 28 November 2025 to ensure they have developed and implemented suitable systems.

7. AI—Data Integrity and Regulatory Challenges

Artificial Intelligence (AI) technologies are expected to continue to emerge in 2025 and with them come regulatory challenges for both legislators and organisations using such technologies. Data integrity, and ensuring that data is accurate, reliable and ethical, is critical.

In September 2024 the Commonwealth Department of Industry, Science and Resources published a 'Voluntary AI Safety Standard' to guide safe and responsible use of AI in Australia. It includes 10 voluntary "guardrails" that are aimed at establishing consistent practices for organisations, and which align with proposed mandatory "guardrails" for AI in high-risk settings.

With rapid evolution of AI, businesses will need manage regulatory compliance as it also evolves.



8. Governance and directors' duties

In late 2024, the Australian Securities and Investments Commission (**ASIC**) took enforcement action in a number of high-profile proceedings against companies and directors and has indicated it will continue to pursue its enforcement priorities throughout 2025.

In one recent case which serves as an indication of ASIC's approach to serious governance failings, in December 2024 ASIC sought leave to issue proceedings against Regional Express Holdings Limited (administrators appointed) (**Rex**) and its directors, alleging that Rex had engaged in misleading and deceptive conduct and had contravened its continuous disclosure obligations. Leave was required as Rex was in administration and while ASIC indicated it will not seek pecuniary penalties against the company, it would be seeking declarations, pecuniary penalties and disqualification orders against the directors of Rex. Leave was granted and the matter will proceed before the NSW Supreme Court in April 2025.





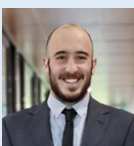









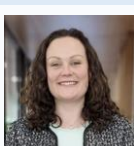


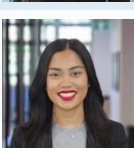
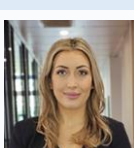
ASIC alleges REX published an ASX announcement in 2023 predicting positive operating profits without a reasonable basis for the claim. It is alleged that Rex also failed to disclose material downgrade despite knowing that it was unlikely to achieve an operating profit. Further, ASIC alleges that the directors contravened the *Corporations Act 2001* (Cth) by failing to take steps to correct the announcement.



Key Compliance trends and predictions for 2025

Contact us

For further information please contact:

<p>Natalie Franks CEO and Legal Counsel Direct: 03 9865 1324 Email: natalie.franks@lawcompliance.com.au</p>		<p>Karen Cusack Senior Consultant Direct: 03 9865 1349 Email: karen.cusack@lawcompliance.com.au</p>	
<p>Chris Martin Director – Client Success Direct: 03 9865 1341 Email: chris.martin@lawcompliance.com.au</p>		<p>Teresa Racovalis General Manager – Client Success Direct: 03 9865 1340 Email: teresa.racovalis@lawcompliance.com.au</p>	
<p>Adriano Stenta Compliance Solicitor Direct: 1300 862 667 Email: adriano.stenta@lawcompliance.com.au</p>		<p>Amanda Roberts Compliance Solicitor Direct: 1300 862 667 Email: amanda.roberts@lawcompliance.com.au</p>	
<p>Anna Pantazis Law Clerk Direct: 1300 862 667 Email: anna.pantazis@lawcompliance.com.au</p>		<p>Andrew Gill Legal Consultant Direct: 03 9865 1322 Email: andrew.gill@lawcompliance.com.au</p>	
<p>Astrid Keir-Stanley Chief Legislative Advisor Direct: 1300 862 667 Email: astrid.keir-stanley@lawcompliance.com.au</p>		<p>Caitlin Nixon Compliance Associate Direct: 1300 862 667 Email: caitlin.nixon@lawcompliance.com.au</p>	
<p>Dana Popovic Compliance Solicitor Direct: 1300 862 667 Email: dana.popovic@lawcompliance.com.au</p>		<p>David McKessy Compliance Solicitor Direct: 1300 862 667 Email: david.mckessy@lawcompliance.com.au</p>	
<p>Fatuma Jacob Compliance Solicitor Direct: 1300 862 667 Email: fatuma.jacob@lawcompliance.com.au</p>		<p>Filomena Rosella Specialist Compliance Solicitor Direct: 1300 862 667 Email: filomena.rosella@lawcompliance.com.au</p>	
<p>James Low Compliance Solicitor Direct: 1300 862 667 Email: james.low@lawcompliance.com.au</p>		<p>Jillian Britton Senior Compliance Solicitor Direct: 1300 862 667 Email: jillian.britton@lawcompliance.com.au</p>	
<p>Ksandra Palinic Head of Client Services Direct: 03 9865 1340 Email: ksandra.palinic@lawcompliance.com.au</p>		<p>Lauren Heyward Senior Compliance Solicitor Direct: 1300 862 667 Email: lauren.heyward@lawcompliance.com.au</p>	
<p>Margarette Natividad Compliance Solicitor Direct: 1300 862 667 Email: margarette.natividad@lawcompliance.com.au</p>		<p>Maria Toma Compliance Solicitor Direct: 1300 862 667 Email: maria.toma@lawcompliance.com.au</p>	

Key Compliance trends and predictions for 2025

Melissa Knoll
Compliance Associate

Direct: 1300 862 667
Email: melissa.knoll@lawcompliance.com.au



Serena Waterworth
Compliance Solicitor

Direct: 1300 862 667
Email: serena.waterworth@lawcompliance.com.au



Sue Allen
Senior Consultant

Direct: 03 9865 1334
Email: sue.allen@lawcompliance.com.au



William Snowdon
Law Clerk

Direct: 1300 862 667
Email: william.snowdon@lawcompliance.com.au



Law Compliance

Law Compliance provides compliance services to hundreds of organisations (and thousands of users) across Australia and this number grows each month. Our aim is to make compliance easy.

Our clients range from small rural organisations to government related entities to some of Australia's largest organisations, retailers, schools, health care providers, local councils, universities, charities, community service organisations and aged care providers.

Our services are cost effective and easy to use.

Our clients can receive our content and updates via their GRC provider or via our online platform, **Comply Online**®.



For more information about Law Compliance and to arrange a free demonstration, please go to: <https://lawcompliance.com.au> or contact **Chris Martin** on **(03) 9865 1341** or chris.martin@lawcompliance.com.au.



SCAN HERE

Copyright and disclaimer

If you would like to reproduce any part of this Report please contact Law Compliance.

This Report has been prepared by Law Compliance. Professional advice should be sought before applying this information to particular circumstances. No liability will be accepted for any losses incurred by those relying solely on this publication.