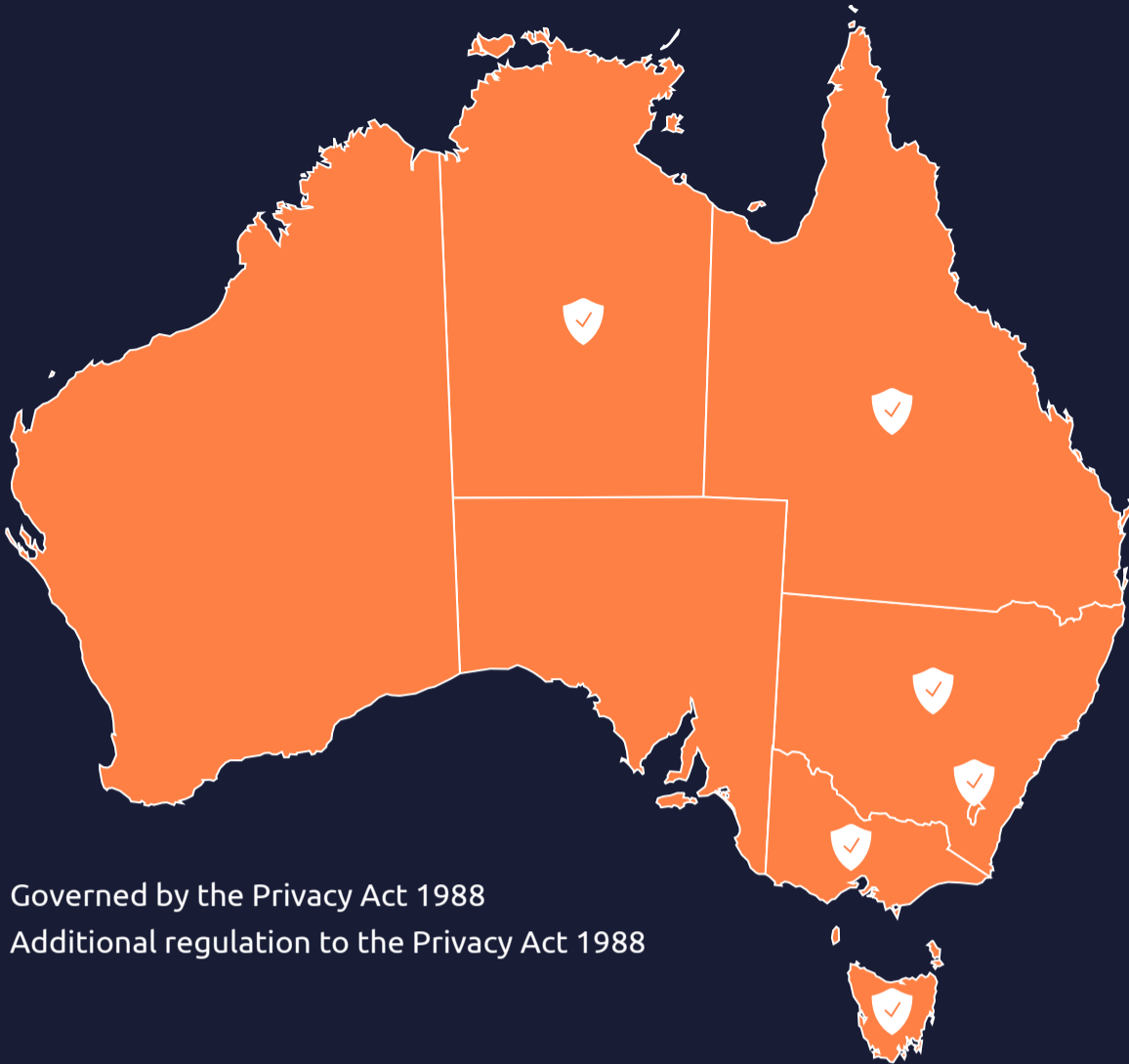




DATA PRIVACY IN AUSTRALIA

THE STATE OF LEGISLATION BY STATE/TERRITORY IN 2022



-  Governed by the Privacy Act 1988
-  Additional regulation to the Privacy Act 1988

About the Privacy Act 1988

The [Privacy Act 1988](#) (Privacy Act) is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector. Other statutory provisions also affect privacy and separate privacy regimes apply to state and territory public sectors. This department assists the Attorney-General to administer the Privacy Act. The Privacy Act was significantly amended in 2014 and 2017 to enhance the protection of privacy in Australia.

Additional Regulations

The following states/territories have additional policies and regulations in place to support the Privacy Act:

- [Australian Capital Territory](#)
- [New South Wales \(2\)](#)
- [Northern Territory](#)
- [Queensland](#)
- [Tasmania](#)
- [Victoria \(2\)](#)

PCI DSS 4.0



[PCI DSS v4.0](#) was officially released at the end of March 2022. As a result, organisations managing environments within its scope must prepare for significant changes to the PCI Data Security Standard (DSS) over the next 18 months.

PROMOTE SECURITY AS A CONTINUOUS PROCESS

Security testing has to be a continuous process, rather than a snapshot of an organisation's PCI DSS compliance taken once a year during the annual audit. Documentation tells assessors (QSAs) that they must select samples over a period of time to prove compliance.

ENHANCE VALIDATION METHODS & PROCEDURES

V4.0 contains revisions to the authentication requirements to reflect the latest industry best practices for password and multi-factor authentication (MFA). Passwords must be longer and consist of at least 12 characters containing a mixture of numbers and letters. Multi-factor authentication will become mandatory for all accounts that provide access to the card data environment.

ADD FLEXIBILITY TO ACHIEVE MORE STRINGENT SECURITY

V4.0 allows organisations to design their own controls and implement them based on the intent of the requirements in lieu of compensating controls. V4.0 supports the use of technologies, such as cloud-based hosting services, by introducing more flexible wording around requirements and adding intent statements to address the evolving threats to the payment ecosystem.



THE SOLUTION

As data privacy standards are continuously evolving, regulators encourage organisations to descope their contact centres and ensure they are free from sensitive data passing through. PCI Pal's suite of cloud-based solutions can provide this descope process across a list of channels. Learn more [here](#).



*Last updated May 2022, data is subject to change/evolve.
Sources: Various