

# HOW TO COMPLY WITH DATA REGULATIONS

As the world becomes more connected, the mountain of sensitive data given and recorded online only gets bigger. From credit card details to email addresses, identifiable information needs robust governance. That's why all businesses need to ensure they comply with the latest privacy and data regulations. Here's what you need to know.



## WHY DO I NEED TO BE COMPLIANT?

Any company covered under the Australian Privacy Principles (APPs) and therefore The Privacy Act that collects data about its customers must meet certain obligations to ensure that data's security. Any [eligible data breaches](#) must be reported, and significant fines and penalties can apply when a business is found to have failed to do this. If your business is collecting customer information, you owe it to your them to protect that information.



## WHAT DO I NEED TO ALIGN WITH?

### You must make sure you:

- ✓ take particular care when collecting health information; a security breach involving this information is deemed more serious than other types of personal info.
- ✓ say what personal info you will collect, and how complaints about any breaches of the APP can be made.
- ✓ say whether any personal info will be disclosed overseas.
- ✓ give people the option to remain anonymous when they deal with your business, if possible.
- ✓ say what info will be used for direct marketing purposes (if exceptions apply).
- ✓ respond to access requests within a reasonable amount of time.
- ✓ keep any personal info you hold up to date and accurate.

### What happens if I don't comply?

Your business could risk being fined up to AU\$2,100,000 - [potentially even more](#) in the future.



## WHAT DO I NEED TO DO ABOUT DATA BREACHES?

### You must:

- ✓ notify anyone who could be affected by an eligible data breach at your business.
- ✓ thoroughly investigate any breach to understand whether it is an 'eligible data breach' – this must be done within 30 days of discovering the breach.
- ✓ try to take steps to prevent a data breach becoming an eligible data breach before any serious loss of data happens.

## DO I NEED TO TAKE ACCOUNT OF GDPR?

GDPR, or General Data Protection Regulation, has changed the way personal data is managed in the European Union (EU). If you have customers there, you must make sure you are compliant with GDPR. Interestingly, the Australian Consumer and Competition Commission (ACCC) has drawn up a series of [data recommendations](#) that takes GDPR into account.



Contact our experts at [Australian Business Lawyers & Advisors](#) to learn more about business compliance.