FORTRA

FACT SHEET (Boldon James)

Ensuring Compliance with the Australian Privacy Act

Protect personal data and avoid financial penalties and reputational damage in the face of constantly evolving privacy legislation.

Privacy laws are front and centre for most countries in 2022, and Australia is no exception. The Australian Privacy Act addresses the management and handling of personal data. It applies to any organisation that holds data on Australian citizens, irrespective of where it is located. The penalty for non-compliance with this regulation is severe, with fines of up to $1.8million. That's to say nothing of the long-term damage to reputation. How can organisations ensure they are compliant?

It's a significant challenge, because the Australian Privacy Act is constantly evolving. Following a major round of amendments in 2014, the Privacy Amendment (Notifiable Data Breaches) Bill 2017 meant that all entities covered by the Australian Privacy Principles (APPs) now have clear obligations to report eligible data breaches.

Furthermore, in late 2021 a consultation took place around the Online Privacy Bill. This sought to introduce a binding online privacy code for social media and other online platforms and increase penalties and enforcement measures. In early 2022, another consultation concluded. The Privacy Act Review seeks to build on the Online Privacy Bill to ensure that Australia's privacy law framework fully protects consumers' data and better serves the Australian economy.

Key Current Requirements

- Failure to report a breach can result in fines of up to $1.8million for organisations with an annual turnover of more than $3 million or $360,000 for individuals.
- Organisations must ensure that any citizens affected, as well as the information commissioner, are informed within 30 days of a data breach occurring.
- The act is not just applicable to organisations based in Australia, but to any organisation globally that holds data on Australian citizens.

Organisations must be aware of any changes that may occur due to these consultations. For now, though, the focus is to notify users when their data has been compromised in a data breach. Organisations will need to inform those affected and the information commissioner within 30 days of a data breach occurring.

The first step should always be to understand what private personal data needs to be protected before putting the right resources and policies in place. This should involve data classification, which enables a data-centric approach to protecting personal information.

Understanding Your Data

The first step in using a data classification approach to achieving compliance, is to understand all the personal or sensitive data you hold and the potential risks to its security.

You will need to ask the following:

- What data do you hold on Australian citizens?
- What data is being collected, and from where?
- Where is that data being stored and processed?
- Why do you have it?
- How sensitive is it?
- How is it accessed, used, or shared?

The data must then be classified or tagged according to its sensitivity. Once you have singled out the most confidential information, you can determine what higher-grade controls need to be applied to ensure it is adequately protected.

Don't Delay Your Preparations

The sheer volume of unstructured data in modern business and the ever-increasing technical abilities of hackers to breach perimeters make it impossible to rely on people and processes alone to ensure that sensitive personal data is handled appropriately. The right technology platform is also essential.

Data classification embeds a culture of compliance by involving users in identifying, managing and controlling regulated data, while automating parts of the protection process to enforce rules and policies consistently.

As you meet current Australian Privacy Act requirements and prepare for any future amendments, classifying data as a first step enables the protection strategy and solutions you implement to be built around the types of data you have and the levels of security they require.

How Can Boldon James Help?

Market-leading data classification from Boldon James supports compliance with regulations by:

- Ensuring appropriate control of confidential or sensitive information
- Classifying or labelling data with visual (and metadata) labels to highlight any special handling requirements
- Alerting users when personal data leaves the organisation to warn or prevent them from sending messages that contain sensitive information
- Educating users about the sensitivity of data whilst ensuring adherence to corporate policy
- Providing critical audit information on classification events to enable remediation activity and demonstrate compliance position to regulatory authorities
- Enabling rapid search and data retrieval based on classification labels to support subject access requests
- Utilising metadata labels to drive additional security controls and solutions, such as DLP, encryption, and rights management
- Orchestrating data management solutions, such as data retention and archiving, to ensure adherence to data storage requirements

The Australian Privacy Act is constantly evolving to reflect changing uses of technology and their impact on data privacy. It can be challenging to keep up with these changes, but data classification should always be your first step if you want to avoid the financial penalties of non-compliance.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.