CYOODA
CYBER SECURITY SIMPLIFIED

Data Security & Privacy **Solutions** Guide

Summary

Protect your data and control your data so that you can reduce the risk within your business more effectively.

> Not a day goes by without hearing about yet another data breach and the millions of people affected. That's why data security and privacy have never been as important as they are today. For all businesses the changes to the Australian data privacy laws should be a wake up call. The clock is ticking, and the reforms will be here soon. You need to act now!

John Reeman

Cyooda Security - CEO & Founder

Content

Data Privacy and Security Solution Guide

Overview

This guide has been developed to help commercial organisations and government agencies to understand the Australian data privacy laws and assist them in providing a core set of foundational security controls to protect their data and reduce risk more effectively.

In this guide you will find a summary of the main points of the Privacy Act, what you need to do to prepare, and practical approaches to applying the principles of the act. There is also a summary matrix of services and solutions provided by Cyooda Security that map to the 13 Australian Privacy Principles.

Both the published standards and technological services offerings from our portfolio are subject to change. As such this guide can only be a snapshot of the situation at the time of going to press, May 2024.

About

Cyooda Security

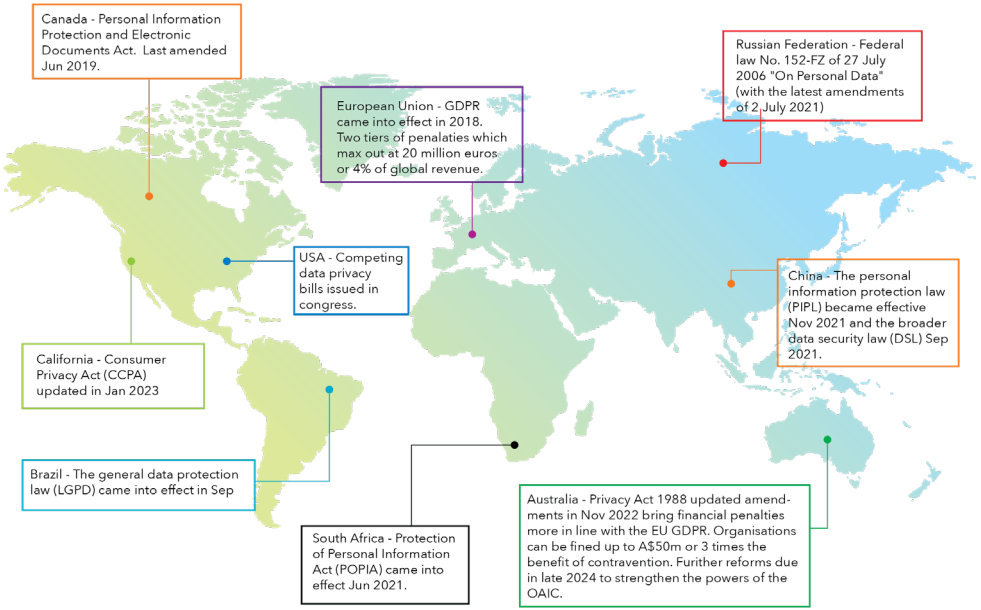
Cyooda was founded by John Reeman, a former CISO and cybersecurity advisor with over 30 years of extensive business experience gained by working with some of the largest global organisations.

We share our knowledge of running security operations, compliance, risk management, responding to incidents, and building a culture of security awareness so that you can learn what works and doesn't.

Together we help you build your high-performing cybersecurity program and reduce your risks.

This personal approach is what makes Cyooda different from the crowd.

Data Privacy | A Global Issue



71%
Countries with data privacy legislation

9%
Countries with draft data privacy legislation

15%
Countries with no data privacy legislation

Australia

What is the Data Privacy Act?

Overview

The Privacy Act 1988 was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations, with an annual turnover of more than $3 million, handle personal information.

The Privacy Act includes 13 Australian Privacy Principles (APPs) that apply to some private sector organisations and most Australian Government agencies. These organisations and agencies are collectively known as 'APP entities.' The Privacy Act also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.

The Australian Privacy Principles are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers.

Penalties for non-compliance

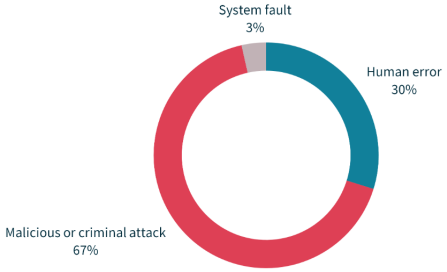
In response to the high profile data breaches that significantly affected a large number of Australian citizens in 2022 (Optus, Medibank and others), the Australian Parliament has passed key privacy reforms under the Privacy Legislation Amendment Bill 2022. Financial penalties for repeat or serious offenders is now the greater of A$ 50 million, three times the benefit of a contravention, or (where the benefit cannot be determined) 30% of domestic turnover.

Australia cybercrime by the numbers

Why it matters

One cybercime is reported every 6 minutes in Australia

Sources of data breaches



JAN - MAR 2024

1.8Million

Australian User Accounts Compromised

Top causes of human error breaches

- PI sent to wrong recipient (email) 33%
- Unauthorised disclosure (unintended release or publication) 20%
- PI sent to wrong recipient (mail) 10%

At a glance

Australian Privacy Principles

Principle	Description
Consideration of personal information privacy	**APP1** and **APP2** require organisations to consider the privacy of personal information, and ensure that they manage personal information in an open and transparent way.
Collection of personal information	**APP3**, **APP4** and **APP5** address the collection of personal information, including unsolicited personal information.
Dealing with personal information	**APP6**, **APP7**, **APP8** and **APP9** deal with personal information and government related identifiers, including principles about the use and disclosure (including cross-border disclosure) of personal information and identifiers.
Integrity of personal information	**APP10** and **APP11** are concerned with the integrity, quality and security of personal information.
Access to and correction of personal information	**APP12** and **APP13** deal with requests for access to, and correction of, personal information.

What it means to you

Latest reform changes

Overview

The financial penalty updates from the November 2022 review are now in force but reform changes are still under review and will likely come into force later in 2024. This means that every organisation will need to review its existing privacy policy, collection notices and privacy consents.

Small Businesses and exemptions

In late November 2023 the government agreed in principle to remove the small business exemption and it is expected that this will take a phased approach until removed entirely. The employee records exemption will be narrowed, with an increased obligation on employers to notify staff and the OAIC of data breaches affecting employee personal information.

Broader definition of personal information

The definition of personal information is under review and likely to be expanded to include information that "relates" to individuals, such as IP addresses, location data, and more. Also under review is any inferred or generated information deemed to have been 'collected' within the meaning of the act. When this comes into effect, organisations will need to assess this usage and determine how best to manage compliance in the context of this expanded definition.

Enhanced powers

What you need to do

Enhanced Powers

Following the last 18 months of high profile data breaches, last year the Australian Government appoint ed a dedicated privacy commissioner. This will bolster the OAIC structure to its original form of 3 commissioners, including one for freedom of information.

It is also likely that the OAIC will obtain further powers so that together with the Federal court, Federal Circuit and Family Court of Australia civil penalties can be delivered with impact to those that contravene the act. The threshold for a "serious" privacy breach is also lowered and it will no longer be required that a breach be a "repeated" interference.

What you need to do

Start getting your house in order now! Even if you have started to identify your sensitive data or think you have, this is a continuous process. Data is dynamic and everywhere. Automation is key here for efficiencies and to remove any errors caused by the human element.

The OAIC has published some useful guidance which you can find on their website.

Further information about how Cyooda Security can assist you is summarised in this guide. More detailed information can be found on our website.

Power Up Your Privacy

OAIC Guidance

TRANSPARENCY

- Do the house keeping
- Seek informed consent
- Apply privacy by design

ACCOUNTABILITY

- Apply high standards
- Act fast - don't delay
- Embed a strong privacy culture

SECURITY

- Guard against impersonation
- Use the right tools
- Lock the doors

Data Security & Privacy

Services & Solutions

"Our services enable you to gain visibility and take back control of your data."

Cyooda Security - Risk Assessment

Data Security & Privacy

Our Data Security Risk Assessment (DSRA) aims to help you start on your journey to continuous data security improvement. We use a holistic approach that encompasses data security as a whole and not just through a “privacy lens” in isolation. This ensures you are looking at the full lifecycle of your data, correlating and reducing risk, as well as meeting compliance obligations with the Privacy Act and other regulations.

The Five Core Areas:

- Policies and Procedures
- Data Security Life Cycle Management
- Data discovery, mapping and monitoring
- Network and systems security
- Security awareness

Looking at:

- People
- Process
- Technology

“Providing an actionable prioritised roadmap for continuous improvement to future proof your data privacy and security risks”

Data Management - Six Step Process

Data Security Life Cycle

6. MONITOR

Continually monitoring your data is key to protecting it and you need to do this at scale wherever your data resides.

1. DISCOVER & AUTOMATE

Automate the discovery of your most sensitive data wherever it resides, so you know who has access, when and how.

5. SECURITY CULTURE

Your employees need to understand how important data is as well as having the right skills to protect your organisation from attacks. Training is essential.

2. REDUCE DATA FOOTPRINT

Take a hard look at the data you are collecting and if you don't need it then delete it. Repeatable processes and automation are necessary to get this right.

4. SECURITY FOUNDATIONS

Building solid security foundations is key to having a successful cyber security program and protecting your sensitive data.

3. POLICIES & PROCESS

- Privacy Policies
- Data Classification
- Notifications
- Consents

Cyooda Security Services and Solutions

Data Security & Privacy Guide

Cyooda Security Data Security, Privacy and GRC Solutions Guide								
	Services		Solution Categories					
	DPRA	Security Advisory	Data Security Management	Data Privacy Management	Data Loss Prevention	GRC	Monitoring & Alerting	Security Awareness
APP 1	●	●	●	●	●	●	●	●
APP 2	●	●	●	●	●	●	●	
APP 3	●	●				●		
APP 4	●	●				●		
APP 5	●	●	●	●		●		●
APP 6	●	●				●		
APP 7	●	●				●		

Cyooda Security Services and Solutions

Data Security & Privacy Guide

Cyooda Security Data Security, Privacy and GRC Solutions Guide								
	Services		Solution Categories					
	DPRA	Security Advisory	Data Security Management	Data Privacy Management	Data Loss Prevention	GRC	Monitoring & Alerting	Security Awareness
APP 8	●	●	●	●	●	●	●	●
APP 9	●	●				●		
APP 10	●	●				●	●	
APP 11	●	●	●	●	●	●	●	●
APP 12	●	●				●		
APP 13	●	●				●		

Think about how you...

Correlate your risks

Sensitivity Risk

What data do I have?

Different data represents different levels of risk to your organisation.

Duplication Risk

Data redundancy

Unnecessary copies of data increase cost and expand attack surface.

Third Party Risk

External data sharing?

Detect and report on external sharing of data.

Access Risk

Who has access to data

Who can access, and who should have access to your sensitive data.

Residency Risk

Is data crossing borders?

Can you flag data that is leaving countries.

Regulatory Risk

Comply with regulations

Businesses need to find simple ways to manage and comply with regulations.

Encryption Risk

Ensure data satisfies policy

Is data hashed, encrypted, and masked appropriately.

Configuration Risk

How do you detect insecure configs

How do you support a holistic view across data storage and usage natively and via partnerships.

Anomaly Risk

How to detect unusual activity?

How do you leverage systems to detect data risk changes.

Further Information...

References

Office of the Australian Information Commissioner (OAIC) - www.oaic.gov.au/

Privacy Legislation Amendment (Enforcement and other measures) Bill 2022 (Bills Digest No. 30, 2022–23) - Privacy Amendment Legislation

Australian Research Data Commons - ardc.edu.au/

European Union Data Privacy Legislation - GDPR

2022 - 2023 Cyber Threat Trends - Cyber.gov.au

Contact Us

If you would like further information on how Cyooda Security can help you transform your data security and prepare for and comply with the Privacy Act, please get in touch.

Get In Touch

02 7230 1350

hello@cyooda.com

www.cyooda.com

Lvl 17, Angel Place, 123 Pitt Street,

Sydney NSW 2000