Your Beautiful Guide To Australian

Privacy Law & Data Security

The Australian Privacy Act | Notifiable Data Breaches Scheme | Australian GDPR

Three Key Parts

What Australian businesses need to know:

PART 1

The Australian Privacy Act

How to handle personal information in Australia.

Current Law

PART 2

Notifiable Data Breaches Scheme

New legislation dealing with data breaches.

New Law

PART 3

GDPR For Australians

How GDPR is affecting Australian organisations.

From 25th May 2018

We take no responsibility for the completeness or accuracy of this information.
Please do your own research, or seek consultation around your own specific obligations.

Good Software Is Key

Comply with all current and future laws more easily with the right software.
Here's a checklist of the essential features you will need:

Auto-Filing & Archiving

Organise your data, store it easily & accurately in a compliant manner.

Manage Internal Processes

Workflows + tasks to streamline & document your business processes.

Centralise Your Data

Copy all data from network, local, USB, paper & Outlook to 1 place.

Right To Be Forgotten

Find all of a customer's records if you need to delete them.

Secure Customer Portal

Secure all external correspondence. Plus retract messages + more.

Audit Trails

Easily carry out reviews & report on data breaches within 72 hours.

Security & Encryption

2-step verification, end-to-end encryption & access permissions.

Document Retention

Set an expiry date on documents after which they are auto-deleted.

Principle Of Least Privilege

Minimise personally identifiable data managed by your teams.

Need To Know

Grant access on specific role or involvement, not hierarchy.

Privacy By Design

Software that lets privacy become a default part of your operation.

Staff Training

The tools & processes your staff need for ongoing compliance.

Tip: Virtual Cabinet's software does all of the above and more. Visit VirtualCabinet.com to book a Demo.

Quick Practical Example Of The Legislation

It's worth highlighting one of the many hundreds of practical implications of the legislation, to highlight the importance of getting this right:

Email Insecurity Consequences:

1

E.g. Sending Secure Information To The Wrong Person

Simply sending a tax return to the wrong person will expose you to **fines** from governing bodies, and **lawsuits** from your client. The predictive nature of Outlook when typing an email means this is unfortunately a common issue.

2

E.g Email Interception

If your outbound communication is not secured / encrypted you are an easy target for hackers. If someone gains access to any unsecured sensitive information you may have sent - again you are liable for the beach and exposed to **fines** and **lawsuits**.

Solution

The most popular method of secure document transmission is a 'Client Portal'.
A software system like **VirtualCabinet.com** has a Portal, encryption and live document retraction features.

Before We Dive Into It

We know understanding your legal requirements can be difficult, proposed solutions often don't meet your intended needs, and every effort incurs significant time and disruption costs - **so please don't suffer it alone!**

Virtual Cabinet's software and specialists have helped 1,000's of businesses of every size become compliant with the law. Plus while you're at it, you'll get an instant return on your investment with better security, team workflows, collaboration, client communication, faster turnaround times, automated administration and more.

Become compliant **and** get a more efficient business - in less time, and with fewer headaches. Win-win. Why not talk to one of our specialists today by clicking the link below:

Talk To A Specialist

Or visit VirtualCabinet.com

Tom
Available

Murray
Available

Lee
Available

Australia Direct Contact
+ 61 2 8319 9494
anz.hello@virtualcabinet.com

PART 1

The Australian Privacy Act

How to handle personal information in Australia.

Australian Privacy Law

At the federal level, the Privacy Act 1988 governs the handling of personal data. Entities should also comply with state and territory legislation.

Personal data is also dealt with by:

- Health Records Legislation (Victoria, NSW & ACT)
- State & Federal Surveillance Legislation deals with video surveillance, geographical tracking, data/computer surveillance and listening devices.
- Federal legislation deals with email marketing and telemarketing, such as the Spam Act 2003 and Do Not Call Register Act 2006.

Privacy Act Principles

The rights every Australian is entitled to:

Disclosure

Know why information is being collected, how it will be used and who it will be disclosed to.

Anonymity

Australians can choose not identify themselves.

Access

Australians can access all their personal information.

Security

All data must be kept safe and secure.

Collection

How to collect both solicited and unsolicited information.

Complaint

How Australians can make a complaint about an entity.

Accuracy

Data relating to Australians must be up to date and accurate.

Usage

How information can be used and disclosed.

Tip: software can help you become compliant with the least effort.

VirtualCabinet.com does a good job of this. Visit their site to book a demo and see if they can help.

Sensitive Information

More stringent obligations are placed on entities when they handle the following types of information:

Health

Race

Political

Religion

Beliefs

Sexual

Memberships

Criminal

Biometric

Who Needs To Comply?

The Privacy Act imposes obligations on 'APP entities', defined as:

Australian Government agencies

Businesses And Not-For-Profit Organisations

With an annual turnover of $3m or more.

Some Small Business Operators:

- A health service provider.
- Trading in personal information (e.g. buying or selling a mailing list).
- Related to a larger business.
- A contractor that provides services under a Commonwealth contract.
- A reporting entity for the purpose of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
- An operator of a residential tenancy database.

The 13 Privacy Principles

A meaty breakdown of what each practically means for you:

1 Transparent Information Management

Entities must manage information in an open and transparent way.

Privacy Policy

You must have a clear policy detailing:

- The kinds of data you hold.
- How data is collected and held.
- Purpose of collection.
- How data can be accessed and corrected.
- How an individual can complain.
- If data is disclosed overseas.

Availability

The Privacy Policy must be free to view, and in an appropriate form.

Complaints

You must be able to deal with inquiries or complaints from individuals.

2 Anonymity

Individuals right to anonymity.

Rights

Individuals must have the option of:

- Not identifying themselves.
- Using a pseudonym.

3 Solicited Information

Information Collection

An entity must only collect information if:

- 'Reasonably necessary' for a function or action.
- Consent is given, and is lawful and fair.

The 13 Privacy Principles

A meaty breakdown of what each practically means for you:

4 Unsolicited Information

How to collect unsolicited information.

Assess

If an entity receives unsolicited information:

- Within a reasonable period of time it must decide if it could have collected it under Principle 3 ('Solicited' above).

Action

If an entity determined they could not have collected the information it must be destroyed (if lawful) as soon as practicable.

5 Notification Of Collection

Notification Principles:

- The individual must be aware of collection.
- The purposes of collection must be clear.
- Their rights must be understood as detailed in your Privacy Policy.

6 Use Or Disclosure

Purpose Of Information

You must not use information collected for a different purpose unless consent is given.

The 13 Privacy Principles

A meaty breakdown of what each practically means for you:

7 Direct Marketing

How you can market to an individual.

Direct Marketing Is Allowed If:

The individual:

- Allowed the entity to collect the information.
- Would reasonably expect to be marketed to.
- Can easily request not to receive marketing, & this is highlighted in every communication.

Other Legislation

This principle does not apply to the extent that any of the following apply:

- The 'Do Not Call Register Act 2006'
- The 'Spam Act 2003'
- Any other Act

8 Cross-Border Disclosure

Requirements before an entity sends data overseas.

Only Send Data Overseas If:

- It is, in effect, protected in a similar way to these Australian Privacy Principles.
- The individual can take actions to enforce.
- If the individual consents after being informed they will not be protected.

The 13 Privacy Principles

A meaty breakdown of what each practically means to you:

9 Government Related Identifiers

Usage:

A government identifier must not be used or disclosed unless:

- Reasonably necessary to verify an identity for the purpose of an activity or function.
- Authorised by law, enforcement body, or court / tribunal.

10 Quality

Entities Must Ensure Their Data Is:

- Accurate
- Up-to-date
- Complete

11 Security

You must protect user data, and destroy it if no longer needed.

Security Obligations:

An entity must take steps to protect data from:

- Misuse, interference and loss; and
- Unauthorised access, modification or disclosure.

Data Destruction:

The entity must destroy the data, or make sure it is de-identified if:

- If no longer needed for the purpose it was collected for.
- It is not contained in the Commonwealth record.

The 13 Privacy Principles

A meaty breakdown of what each practically means to you:

12 Access And Correction Of Information

If the individual requests their information, they must be given access.

Exceptions To Access

- Would pose health or security risk
- Would impact privacy of others.
- Is frivolous or vexatious.
- Relates to legal proceedings, and would not be accessible in those proceedings.
- Would reveal negotiation intentions.
- Access would be unlawful.
- Would reveal a commercially sensitive decision making process.

Timeliness

The information must be given in a manner requested by the individual, if reasonable and practicable, within:

- 30 days, and for free, for agencies.
- Within a reasonable period for organisations. If there is a charge it must not be excessive and not apply to the making of the request.

Refusal

If access is refused the entity must give written notice to the individual stating the reasons for the refusal, and the way to lodge a complaint.

The 13 Privacy Principles

A meaty breakdown of what each practically means to you:

13 Correction Of Information

If the individual requests their information they must be given access.

Correction Of Information

The entity must correct inaccurate, out of date, incomplete, irrelevant or misleading information if they are aware of this.

Third Parties

If an individual request an entity correct information it has disclosed to a third party, the entity must take reasonable steps to give that notification.

Timeliness

There must be no charge for a correction. And requests must be completed within:

- 30 days for agencies.
- Within a reasonable period for organisations.

Refusal

If a correction is refused the entity must give written notice to the individual stating the reasons for the refusal, and the way to lodge a complaint.

The Information Life-cycle

A useful guide to an entity's obligations when collecting personal information.

FIRST

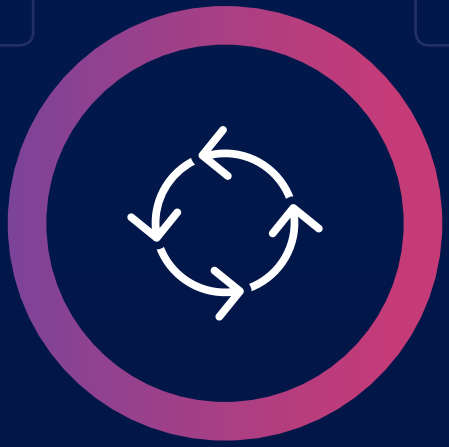
Is it necessary to collect & hold the information to carry out your activity?

SECOND

Embed privacy protections into the design of the info handling process.

THIRD

Constantly assess the risks associated with the collection of personal info.



FORTH

Put strategies in place to protect the personal information you hold.

FIFTH

Destroy or de-identify the information when it is no longer needed.

SIXTH

Repeat all steps!

Final Note On The Australian Privacy Act

The European Union's upcoming 'GDPR' data protection legislation has many common requirements with the Australian Privacy Act.

If you're an Australian business storing any EU data you must also comply with GDPR, so it is worth considering them together. We cover GDPR in Part 3 of this guide:

PART 3

GDPR For Australians

How GDPR is affecting Australian organisations.

From 25th May 2018

PART 2

Notifiable Data Breaches Scheme

New mandatory requirements

for Australian businesses.

Prevent breaches by encrypting all your communication, setting clear permissions on documents, audit trails and more with Virtual Cabinet.

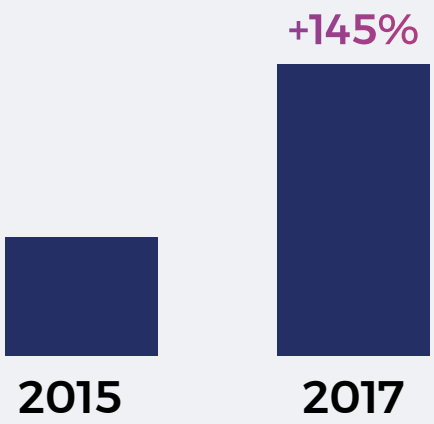
Book Demo At VirtualCabinet.com

"If an organisation does not demonstrate a commitment to privacy, people will look for alternative suppliers, products, and services."

Timothy Pilgrim PSM
Australian Information And Privacy Commissioner

Community Expectations

The greater community is expecting organisations to show ever greater transparency and accountability when handling their personal data.



Organisations in Australia that have detected a business interrupting security breach on at least a monthly basis.

94%

Of people stated they should be told if a business loses their personal information.

95%

Of people stated they should be told if a government agency loses their personal information.

Sources: ACAPS Report 2017, Telstra Cyber Security Report 2017

Australian Government 2017 Survey

Australian Community Attitudes To Privacy

Most trustworthy

- **79%** Hospitals / Health
- **59%** Banking / Finance
- **58%** Government
- **40%** Insurance

69% of us are **more concerned** about online privacy than we were **five years ago**

Security concerns mean

93% don't want their data to be sent overseas

79% don't want their data shared with other organisations

58% decided not to deal with some businesses

44% avoid downloading smartphone apps

We could take more responsibility

61% **check website security** before giving personal information...

but we **don't** usually

- Read privacy policies **65%**
- Ask organisations why? **54%**
- Clear browsing history **50%**
- Shred documents **50%**
- Adjust privacy settings **43%**

HANDLE WITH CARE **VISIT WWW.PRIVACY.GOV.AU**

Australian Government
Office of the Australian Information Commissioner

What Is An 'Eligible' Data Breach?

An Eligible data breach occurs when three criteria are met:

CRITERIA 1

The Breach

There is unauthorised access, disclosure or loss of personal information that an entity holds.

CRITERIA 2

Harm

It is likely to cause **'serious harm'**. This be psychological, emotional, physical, reputational, or other. It requires an evaluation of the context of the data breach.

CRITERIA 3

Remedial Action

Remedial action taken has not prevented the risk of serious harm.

EXAMPLES:

1. Customer's personal information is stolen, lost or hacked.
2. Personal information is sent to the wrong person.

YOUR OBLIGATION

If an Eligible data breach occurs, you must promptly notify affected individuals and the Commissioner about the breach.

“When a data breach occurs, a quick and effective response can have a positive impact on people’s perceptions of an organisation’s trustworthiness.”

Timothy Pilgrim PSM
Australian Information And Privacy Commissioner

Who Needs To Comply?

Australian Government agencies

Businesses And Not-For-Profit Organisations

With an annual turnover of $3m or more.

Some Small Business Operators:

- All private sector health service providers.
- Those that trade in personal information.
- TFN recipients (if annual turnover is below $3 million, the NDB scheme will apply only in relation to TFN information).
- Those that hold personal information in relation to certain activities, for example, providing services to the Commonwealth under a contract.

The Fines Are Severe

Avoid high fines, and brand damage, by preparing now

Individual Fines

Up to $420,000

Company Fines

Up to $2,100,000

3 Steps To Compliance

1

Review

Reviewing existing policies and practices for data collection.

2

Secure

Strengthen online security strategies.

3

Education

Educate staff on emergency response, mitigation and notification procedures.

Conducting An Assessment

If you **suspect** a data breach which may 'likely to result in serious harm', you must conduct a 'reasonable' and 'expeditious' assessment.

Initiate

Decide whether an assessment is necessary and who is responsible for undertaking it.

Investigate

Gather information, including what information is affected, who may have had access, and likely impact.

Evaluate

Make a decision whether the identified break is an **Eligible data breach.**

Timing

You have 30 days from when you become aware of a potential breach to conduct an assessment.

Communication

Create a data breach response framework to ensure relevant personnel are made aware of a breach as soon as practicable.

Action

Once you believe an Eligible data breach has occurred you must notify appropriate individuals immediately, not wait 30 days.

"It reinforces organisations' accountability for personal information protection and encourages a higher standard of personal information security across the public and private sectors."

Timothy Pilgrim PSM
Australian Information And Privacy Commissioner

Your Breach Action Plan

Maintain Security

Take reasonable steps to protect personal information.

→

Possible Breach

A possible data breach occurs.

→

Contain

Your first priority is to take immediate steps to contain the breach.

↓

Assess

Will it result in serious harm for individuals?
If you have reasonable grounds to **believe** it is an eligible breach, you must notify. If you only **suspect** it might be, you must conduct a reasonable and expeditious assessment within 30 days.

Take Remedial Action

Where possible take steps to reduce likelihood of harm.
E.g. recover the info, or provide assistance to those affected.
If remedial action is able to make **serious harm** not likely, then notification is **not** required. Go directly to 'Review'.

↓

Notify

When **serious harm** is likely you must notify those individuals & Commissioner with, at a minimum, your contact details, description of the breach, the information concerned, and recommended steps for the individuals.

If possible notify directly, otherwise publish a statement on your website, and take steps to draw it to attention.

→

Review

Consider how the breach occurred & whether to enhance your personal information security measures.

PART 3

GDPR

How the EU's new law will impact Australian businesses.

Who Does GDPR Apply To?

From the 25th of May 2018 Australian and New Zealand businesses who have EU operations, offer goods and services, or monitor the behaviour of individuals in the EU need to comply.

pwc

GDPR will apply to every entity that holds or uses European personal data both inside and outside of Europe.

"Three quarters of us don't trust businesses to do the right thing with our emails, phone numbers, preferences and bank details. I find that shocking."

Elizabeth Denham
UK Information Commissioner

Myths & Facts Leading To Complacency

GDPR applies to Australian businesses if they store any EU data.
You should start getting prepared now for May 2018.

48% of UK citizens are planning on using their new GDPR rights on companies worldwide. Get ready!

Doesn't Apply

It applies to all sizes, anywhere in the world.

Serious Offenses

Up to €20m or 4% of turnover.

Lesser Offenses

Up to €10m or 2% of turnover.

Current Data

It's not only future data, it's your current data too.

Have Time

There isn't much time left to become compliant.

Only Security

Having good data security is not enough.

Opportunities & Consequences

The focus is usually on the negatives of non-compliance,
but there are a lot of positives businesses should take advantage of.

Non-Compliance

Fines Up To **4% Of Revenue**

Fines Up To **€20 million**

Class Action Lawsuits

Disruption To Business

Brand Damage

No Case Law

Compliance

Efficient Data Management

Streamlined Processes

Transparency

Security

Data Encryption

Better Internal Controls

Risk Reduction

Data Encryption

Less long-term cost

Updated Technology

What Data Is Affected?

Any information relating to an identified natural person.
This could include a broad range of data including:

Name

Number

Location

Online ID

Physical

Physiological

Genetic

Mental

Economic

Cultural

Social

ACTION

Understand Your Data

What personal data do you hold? Where did it come from? Who is it shared with? Where do you keep it?

Consider an information audit to fully document & appreciate your data.

ACTION

Special Categories

Certain categories of data require particular care:

Race, Ethnic Origin, Politics, Religion, Trade Union Membership, Genetics, Biometrics, Health, Sex Life, Sexual Orientation.

GDPR ‘Rights’ Overview

EU citizens are being given powerful new ‘super-powers’ over their Personal Data

Right To be Informed

Individuals need to be informed when you collect or process their data.

Right Of Access

Individuals can now ask for access to their data, and why you are processing it.

Right To Rectification

Data that is inaccurate or incomplete must be corrected on request.

Right To Be Forgotten

Individuals can ask to have all their data deleted from your records.

Right To Restrict Processing

Individuals can ‘block’ any further processing of their data.

Right To Data Portability

Individuals can obtain and reuse their data on different services if they choose.

Right To Object

Individuals can object to data being processed in marketing, research etc.

Automation & Profiling Rights

Safeguards to protect individuals against automated decisions & profiling.

Tip: software can help you become GDPR compliant with the least effort.

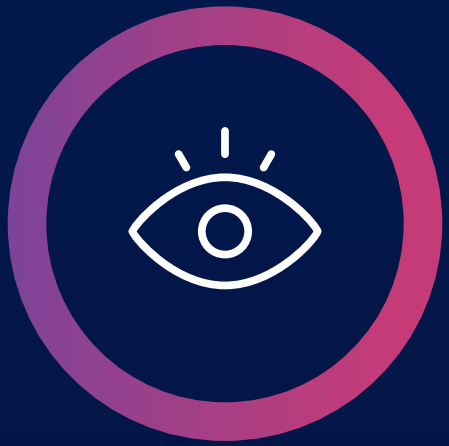
VirtualCabinet.com does a good job of this. Visit their site to book a demo and see if they can help.

Privacy By Design

GDPR wants you to think about privacy and data protection from the beginning, not as a bolted-on after-thought. This is 'Privacy By Design':

Limit Data
Only collect what is necessary.

Limit Processing
Only process data for the purpose that it was collected for.



Impact Assessment
Conduct assessments for personal data that is high risk to individuals.

Limit Access
Only authorised individuals should be able to access data.

Keep Reviewing
Keep checking the confidentiality, availability & resilience of your systems.

Record Keeping
Note processing, data categories, erasure time & storage locations.

Top Questions To Ask Your Departments

Legal

What's your plan for personal data requests? Is your process documented? Can it be automated? Can it scale? Response timescale? Published data retention policies?

Finance

Have you reviewed your processes to make sure they are managed securely? Potential penalties? Have you done risk planning?

IT

Which systems hold Personal Data? Could you find all data relating to an individual and delete it? Is it stored securely (office + cloud)? Any potential security breaches? Process for breach notification within 72 hours?

Marketing

When you capture consent for the use of Personal Data, do you explain why you need to have it and how it will be processed? Consent needs to be explicit. Individuals giving consent need to be fully informed.

HR

What personal data do you collect? Have you documented why it is captured? Do you obtain consent & explain how it will be processed? Have policies, forms & training been updated with new Personal Data categories?

Procurement

If a sub-contractor processes data on your behalf are their sufficient guarantees (especially expert knowledge, reliability & resources) to meet GDPR requirements?

Source: gdprcoalition.ie

7-Step Checklist To GDPR Compliance

STEP 1 Raise Awareness

- [ ] Make sure key decision makers know what is happening with GDPR (share this guide with them!)
- [ ] Staff training: most breaches occur through staff ignorance.
- [ ] Get strong commitment from the board & C Level Officers to build compliance culture.

STEP 2 Form A Team

- [ ] Form a cross functional data team including the IT team & business leadership.
- [ ] Appoint a Data Protection Officer (DPO) if needed.
- [ ] Team should be responsible for GDPR.
- [ ] Team should own the documentation process.
- [ ] Team should regularly review policies, processes and technology.

STEP 3 Do An Audit

- [ ] Start with an information audit & risk assessment of your data.
- [ ] Audit risk of servers, storage, end-point devices & cloud locations.
- [ ] Ensure you have a legal basis for carrying out data processing.
- [ ] Make sure you have consent for all your Personal Data.
- [ ] Review existing policies.
- [ ] Conduct a data-flow analysis to see how data moves & is stored.

7-Step Checklist To Compliance

STEP 4 Create A Plan

- [ ] Be proactive, don't think GDPR won't affect you – it will.
- [ ] Create a list of recommendations.
- [ ] Prioritise recommendations and assign resources and budget.
- [ ] Put together a roadmap to achieve compliance.
- [ ] Review your plan regularly.

STEP 5 Technology

- [ ] Move towards a single platform to organise all of your data.
- [ ] Get a single source of truth to better respond to data access, portability, erasure requests, data breaches, etc.
- [ ] Use technology from best vendor to stay ahead of the technology curve
- [ ] Try VirtualCabinet.com as a good software and systems solution.

STEP 6 Communication

- [ ] Put together an incident response process.
- [ ] Ensure you have a strong governance process.
- [ ] Plan how you will handling data requests within 30 days at no cost to individuals.

STEP 7 Individuals rights

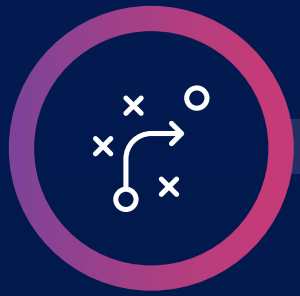
- [ ] Be aware of the new Rights given to individuals under GDPR, as detailed in Part 1 of this guide.

If you want more GDPR info:

For an even more detailed overview of GDPR (that you'll actually enjoy reading!) we recommend downloading our free ebook: **GDPR In A Nutshell**

Click To Download

Or visit VirtualCabinet.com



Where Do I Start?

The easiest way to become GDPR compliant is with the right software.

No matter your company size, book in a demo with a leading GDPR software provider like Virtual Cabinet to see if they can make your life easier.

Click To Book Demo

or visit VirtualCabinet.com

Still Confused?

We know understanding your legal requirements can be difficult, proposed solutions often don't meet your intended needs, and every effort incurs significant time and disruption costs - **so please don't suffer it alone!**

Virtual Cabinet's software and specialists have helped 1,000's of businesses of every size become compliant with the law. Plus while you're at it, you'll get an instant return on your investment with better security, team workflows, collaboration, client communication, faster turnaround times, automated administration and more.

So become compliant **and** get a more efficient business - in less time, and with fewer headaches. Win-win. Why not talk to one of our specialists today by clicking the link below:

Talk To A Specialist

Or visit VirtualCabinet.com

Tom
Available

Murray
Available

Lee
Available

Australia Direct Contact
+ 61 2 8319 9494
anz.hello@virtualcabinet.com