Bird & Bird

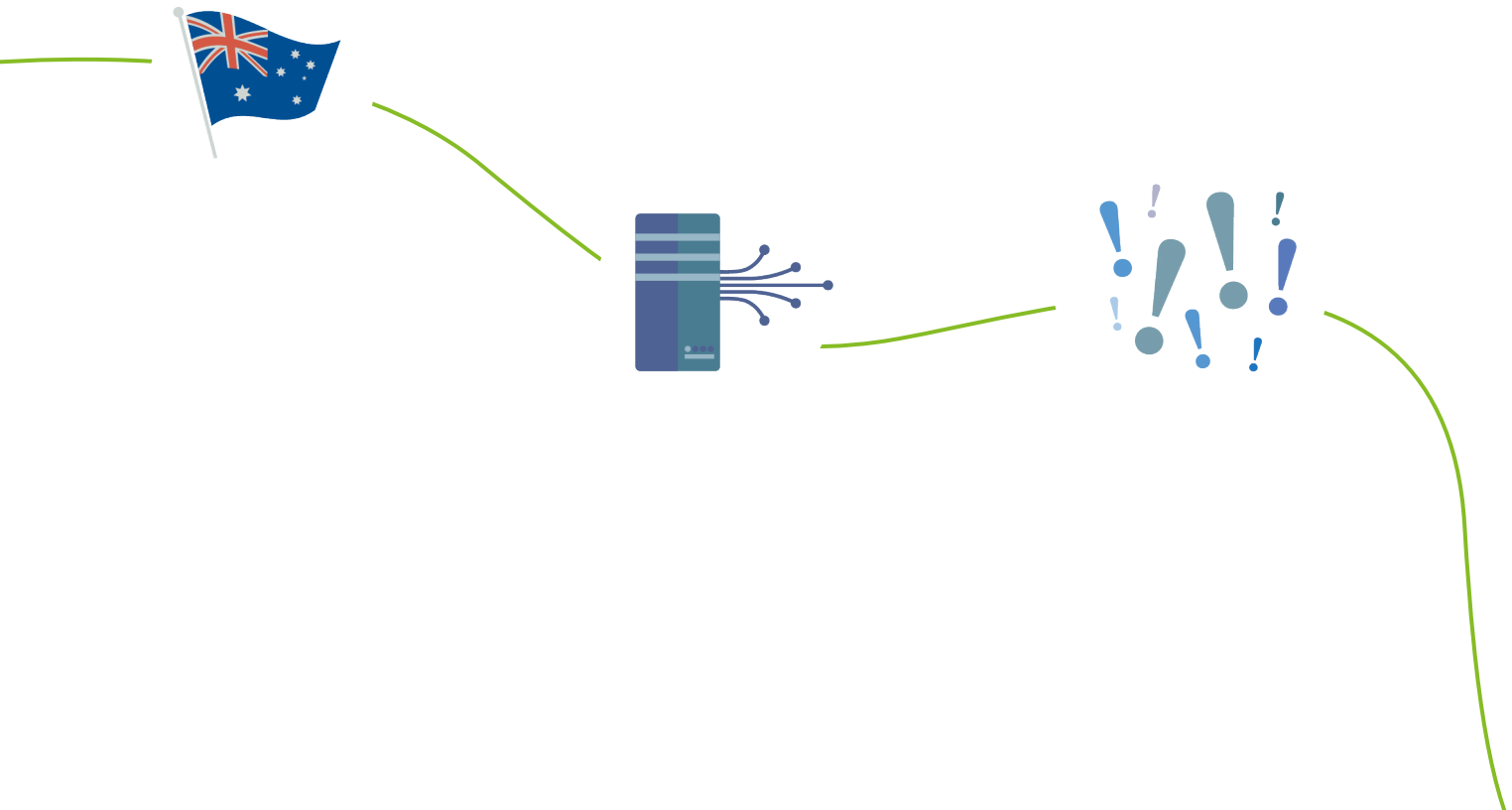
Australian Mandatory Data Breach Notification Guide

Protecting information in an Australian context

2018

twobirds.com

Contents



< Back to contents

Outline

This guide has been compiled to assist organisations to understand the new mandatory data breach reporting obligations.

What does the law cover?

It requires any organisation which is bound by the Privacy Act 1988 to notify the OAIC and affected individuals if it suffers an eligible data breach.

An eligible data breach, also known as a notifiable data breach, is a data breach that a reasonable person would believe is likely to result in serious harm to an individual.

When does it apply?

From 22 February 2018

Who does it apply to?

Any organisation that is established, or does business, in Australia with an annual turnover over $3 million, and certain organisations with a turnover of less than $3 million.

What are the penalties for non-compliance?

- Determinations
- Enforceable undertakings
- Penalties of up to $420,000 for individuals, and $2.1 million for corporations

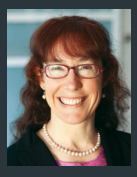
What does this guide cover?

The purpose of this guide is to assist organisations that are established, or conduct business, in Australia to understand and comply with their data breach notification obligations.

It is not intended to address obligations specific to Commonwealth government agencies.

Who can help me?

Our data protection team can help you understand the specific obligations that apply to your organisation, provide guidance in the event of a data breach, and help you prepare a data breach response plan.



Lisa Vanderwal
Special Counsel
lisa.vanderwal@twobirds.com
Tel: +61 2 9226 9832

Hamish Fraser
Partner
hamish.fraser@twobirds.com
Tel: +61 2 9226 9815

Sophie Dawson
Partner
sophie.dawson@twobirds.com
Tel: +61 2 9226 9887

Who has to comply?

Annual turnover > $3 million

Any organisation that has an annual turnover over $3 million has to comply with the data breach notification regime.

Small business operator

Most organisations with an annual turnover of less than $3 million do not have to comply with the data breach legislation, other than those set out below.

Exceptions

Small businesses have to comply with the data breach notification regime regardless of their annual turnover if they:

- provide a health service and hold health information:
- deal in personal information:
- are a contracted service provider for a Commonwealth contract;
- are a credit reporting body or a credit provider;
- are part of a larger corporate group:
- operate a residential tenancy data base;
- are required to comply with anti-money laundering obligations;
- conduct a protected action ballot; or
- are subject to the telecommunications mandatory data retention scheme.

Note: This doesn't apply to employee records

This can apply to child care centres and aged care facilities;

In particular, disclose personal information for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information. Examples: selling or swapping marketing lists

Where one or more members of the corporate group have an annual turnover of more than $3 million

Reporting under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

Applies in relation to industrial action

Telecommunications (Interception and Access) Act 1979

Scope of application

The Privacy Act applies to acts and practices in Australia. Organisations need to comply if they:

- are established in Australia; or
- carry on business within Australia; and
- collect personal information from an individual in Australia.

What is carrying on business in Australia?

Just having a website that is accessible from Australia does not necessarily mean an organisation is conducting business in Australia.

Indicators that an organisation may be carrying on business in Australia include having:

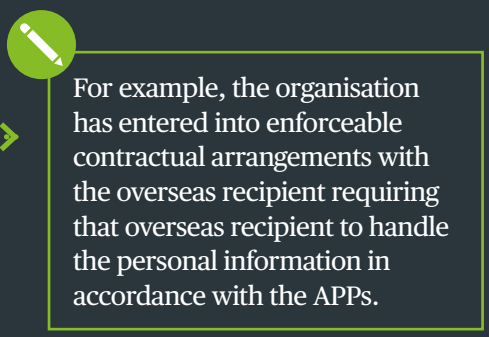
- a place of business in Australia;
- agents or others located in Australia who conduct business on its behalf;
- a website that specifically offers goods or services in Australia;
- a registered trademark in Australia.

This is not an exhaustive list, and whether or not an organisation is actually carrying on business in Australia will depend on the circumstances.

Overseas recipients

If an organisation has disclosed personal information to an overseas recipient, and that overseas recipient suffers a data breach, then the organisation will need to treat the overseas recipient's data breach as if it were its own.

However this only applies where the organisation disclosed the personal information to the overseas recipient pursuant to APP 8.1.



What is an eligible data breach?

Not all data breaches have to be reported. Only those that are eligible data breaches have to be reported.

An eligible data breach occurs where the following elements are present, and no successful remedial steps (see page 7) have been taken.

There is either	
a. any loss of personal information; or	This can include losing your device (phone, tablet, laptop), leaving a USB, device or papers on the plane/in the taxi/in clothes sent to the dry-cleaner.
b. any unauthorised access to or disclosure of personal information; and	This can include malware, ransomware, innocent or malicious employee action, sending emails to the wrong person, hacking or other unauthorised systems' access, or a contractor's innocent or malicious action.
a reasonable person	The OAIC has indicated that a reasonable person is a person in the organisation's position who is properly informed - that is, they have made reasonable enquiries and an assessment of the data breach based on the information which is available at the time. The OAIC has stated that a reasonable person is not the individual whose personal information was part of the data breach.
would believe that the loss or unauthorised access or disclosure is likely to cause	Likely means more than just a possibility. However, it also means less than certain or highly probable. Any data breach that is certain to, or there is a high probability that it will, cause serious harm is an eligible data breach. The general rule is that if it is more probable than not that the data breach will cause serious harm to an individual, it will be an eligible data breach.
serious harm	See page 5 for what constitutes serious harm.
to the individual to whom that personal information relates	An individual is defined in the Privacy Act as a natural person - so not a company. But it could be a director of a company, or sole trader.

What is serious harm?

What will be serious harm will depend on the circumstances of each data breach. Here are some of the things that organisations need to consider.

The kind of information

Some types of information are more likely in and of themselves to result in serious harm:

- credit information;
- health information; or
- identity information (passport, drivers' licence, Medicare card).

Large scale breaches may be more likely to cause serious harm.

The sensitivity of the information

Some information is likely to be more sensitive than others:

- criminal history;
- health information; or
- information about vulnerable individuals (children, the elderly, those with disabilities).

Protected by security measures

Information which is encrypted or password protected is less likely to cause serious harm.

However, if it's possible that those security measures could be overcome, serious harm is more likely, particularly if there's malicious intent.

Organisations should assume that any theft, hacking, ransomware, malware or phishing attacks are malicious.

Who has the information?

Was there malicious intent in accessing the information? If so, the risk of serious harm is higher.

If the access to the information is accidental, the risk of serious harm may be lower - for example leaving an electronic device in an uber.

The nature of the harm

There are a number of different types of serious harm that can be caused by a data breach:

- damage to personal or business relationships;
- bullying or marginalisation;
- identity theft;
- emotional (such as humiliation, embarrassment);
- economic (loss of business or other opportunities);
- reputational damage;
- physical (such as physical safety);
- psychological; or
- financial.

Remember that there could be other types of harm. Don't limit the assessment of whether serious harm could result from the data breach just to those listed above.

Other relevant matters

How long has the information been accessible? The longer the period of access, the more likely serious harm could result.

Is there anything specific to the organisation, or the individual involved?

Keep in mind that organisations won't generally be required to make external enquiries about the circumstances of each individual whose information is involved in the breach.

What are the timeframes?

Do organisations have to assess every data breach?

No.

If an organisation is confident that no serious harm will be caused by the data breach, then it does not have to assess it, as it will not be an eligible data breach.

But if an organisation is:

- unsure whether or not a person could suffer serious harm; or
- suspects that a person could suffer serious harm

as a result of the data breach, the organisation must assess it.

How long can an organisation take to assess a data breach?

Organisations should complete their assessment within 30 days of discovering the breach.

In some circumstances this may not be practical, and in that case organisations need to be able to justify to the OAIC why they couldn't complete the assessment within this time period. This could include where there is a significant amount of information involved, or a number of organisations have suffered the same data breach - see page 8 for more information.

If an organisation takes remedial steps during this investigation period to ensure that it is unlikely that any individuals will suffer any significant harm, then it will not have to notify the OAIC and individuals - see page 7 for more information.

When does an organisation have to notify the OAIC?

Organisations have to notify the OAIC as soon as practicable after becoming aware that there has been an eligible data breach.

See page 9 for information that needs to be included in the notice to the OAIC.

Do organisations need to notify individuals at the same time?

Yes.

Unlike the GDPR, if an organisation is required to notify the OAIC of an eligible data breach, it automatically has to notify the relevant individuals.

See page 9 for more information on what has to be included in the notice to individuals, and the different ways that organisations can notify individuals of the data breach.

Rectification: How to take remedial steps

What can organisations do if there is a data breach?

Organisations can take steps so it is unlikely that there will be any serious harm to any of those individuals whose personal information was the subject of the breach.

What those steps are will depend on the circumstances. Here are a few examples.

- If an email containing personal information was sent to the wrong person, contact that person to make sure they will destroy the email without reading or acting on it. Organisations will need to consider whether that person will do what has been requested - for example, there is an existing business relationship with, or otherwise sufficient confidence in, the other person.
- If a phone has been lost or stolen, wipe it remotely.
- If a storage device (such as a USB) has been left in an uber/ taxi/airplane, get it back promptly and be confident that no-one has accessed it.
- If a current employee has accessed personal information without authorisation, speak to the employee and be satisfied that the access was accidental with no malicious intent.

Beware of malware and ransomware

It is unlikely that remedial action will be fully effective where malware is involved, or where there has been hacking or a phishing or other type of cyber-attack.

In the case of ransomware, can you trust that the person holding the material to ransom won't keep a copy after the ransom has been paid?

Should organisations report data breaches if they aren't eligible data breaches?

Some organisations may choose to report data breaches, even if they aren't eligible data breaches, for a number of reasons, such as:

- corporate values;
- commercial considerations;
- additional legal obligations;
- circumstances specific to the data breach;
- customer relationships; or
- reputational issues.

Keep in mind that over-reporting of privacy breaches can result in notification fatigue.

< Back to contents

What if more than one organisation suffers the same data breach?

When could this occur?

It is possible for more than one organisation to suffer the same data breach. This could occur where the organisation that collected the information discloses it to a service provider, and the service provider suffers the data breach.

In that case, provided one of the organisations investigates the data breach to decide whether or not it is an eligible data breach, then the other organisation doesn't have to.

Similarly, if one organisation notifies the OAIC and relevant individuals of the eligible data breach, the other organisation doesn't have to.

Examples include cloud service providers, document storage providers, car and other dealerships, joint ventures, delivery providers, market research providers, and health service providers.

Which organisation?

The legislation is silent on this. This means that each organisation will have to consider this on a case by case basis. However, usually the organisation that has the closest relationship with the individual should investigate the data breach, and notify the OAIC and relevant individuals.

It is recommended that organisations agree clear procedures on:

- who will lead a data breach investigation;
- what cooperation is required between them;
- how to agree on what remedial action will be taken and who will take it;
- who will prepare the notice to the OAIC and relevant individuals;
- what consultation and approval mechanisms should be put in place (as the organisation who drafts the notification can include the names of any other entities involved in the data breach those other entities may wish to be consulted about the content of the notice); and
- who will pay for the investigation and notification costs - see page 16 for insurance considerations.

What if none of the organisations investigate and report?

In that case, all affected organisations are likely to be in breach of their obligations under the Privacy Act, and penalties may apply - see page 12 for more information about penalties.

Data breach notification statement

What has to be included?

The data breach notification statement to the OAIC and to the affected individuals must include the following information:

- the organisation's identity and contact details;
- a description of the data breach (how did it happen, and when?);
- the kind or kinds of information concerned (name, credit card details, drivers licence); and
- recommendations about the steps that individuals should take in response to the data breach (such as cancelling credit cards, changing passwords).

If another entity suffered the same data breach (see page 8) then organisations can also include the name and contact details of those other entities.

Who has to receive the data breach notification statement?

The data breach notification statement must be given to the OAIC.

The OAIC has an interactive statement available on-line at www.oaic.gov.au, or organisations can create their own statement, provided it includes the required information.

Organisations will also need to give a copy of the statement to individuals who were affected by the breach. This needs to done either at the same time, or as soon as practicable after, the data breach notification statement is given to the OAIC.

Levels of notification to individuals

There are three different levels of notification to individuals, and organisations should choose the one that best suits their circumstances.

Generic

To all individuals who may have been affected by the data breach, regardless of whether they may have suffered serious harm. While this will ensure that organisations comply with their notification obligations to individuals, it may not suit every data breach.

Targeted

Only to those individuals who may be at risk of suffering serious harm because of the data breach. There are a number of considerations to take into account (cost and timing, for example), so whether or not this is the best option will depend on the circumstances of the data breach.

Public

If neither of the first two types of notification apply (for example the organisation can't contact all individuals who may have been affected because their contact details haven't been kept up to date). This includes publishing a copy of the statement on the organisation's website and taking other reasonable steps to publicise the statement. Such other steps could include a social media campaign, or publication of the notice in industry journals or major newspapers.

How to respond to a data breach

Have a data breach plan and follow it!

It is best practice to consider in advance what needs to be done in the event of a data breach. The data breach plan should help organisations respond quickly and effectively to a data breach, and should include a degree of flexibility to consider the circumstances that are specific to each data breach.

The following are some examples of issues that will need to be considered.

☑ When was the data breach discovered?	This will dictate when the 30 day period starts.
☑ How was the data breach discovered?	Was it an employee? A customer? As a result of an audit or other process?
☑ What steps have been taken to stop the data breach?	Timely steps could reduce the seriousness of the damage.
☑ Who needs to be involved in the data breach investigation in the organisation?	The Board, legal, marketing, IT, customer support?
☑ Are any service providers or suppliers involved or affected?	Only one organisation needs to notify the OAIC of an eligible data breach - see page 8 for more information.
☑ What type of a data breach was it?	Employee error, malware, hacking, fraudulent emails or websites, ransomware, third party service providers, accidental loss or disclosure, malicious access by disgrunted employees.
☑ Was the breach intentional or accidental?	This will influence whether or not individuals are likely to suffer serious harm.
☑ What steps have been taken to recover the information?	Taking remedial action could mean that the data breach won't be an eligible data breach - see page 7.
☑ Who has the information now?	If you know, can you get it back or stop it being used or disclosed? This could mean that the data breach won't be notifiable - see page 7.
☑ Was the information protected in any way?	Password, encryption, locked briefcase?
☑ What kind of information is involved?	For example, is it sensitive information, health information, credit information, or employee information? See glossary on page 17 for more information.
☑ How many individuals may have been affected?	Can they be identified?
☑ What kind of damage could the individuals suffer as a result of the breach?	Examples could include physical, mental, emotional, reputational, financial or psychological - see page 5 for more information.
☑ What external parties should be involved?	Some examples are external lawyers, insurers, public relations, IT forensics teams, and call centres.

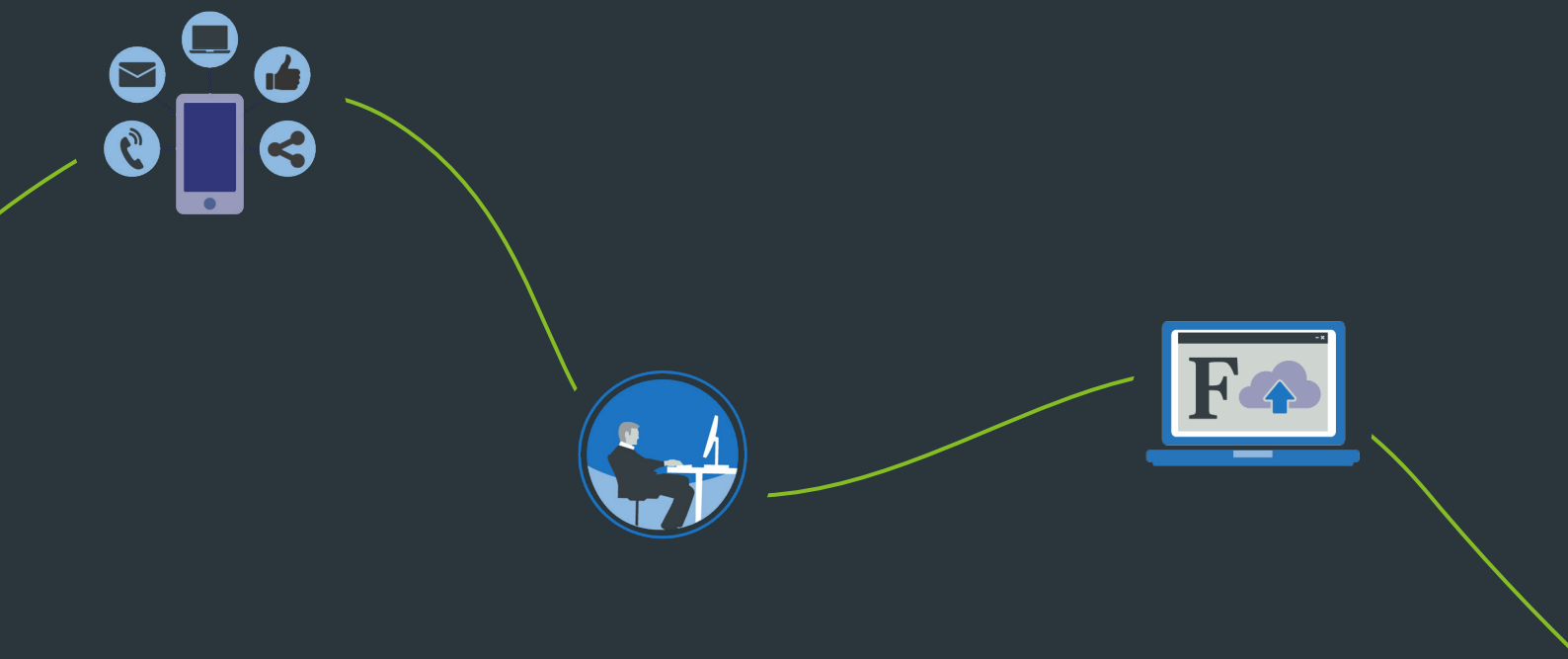
< Back to contents

After the breach

Don't leave what has been learnt as a result of the data breach for too long. It will be easier to get changes made if the data breach remains at front of mind.

Here are some questions to guide future action.

- ☑ What caused the data breach in the first place?
- ☑ Can whatever caused the data breach be prevented in future?
- ☑ Is additional training required?
- ☑ Do policies, practices and/or procedures need to be updated?
- ☑ Does the data breach response plan need to be revised? What worked? What didn't work?
- ☑ If your organisation didn't have a data breach response plan, make sure that it has one going forward.
- ☑ Make sure the organisation fully complies with any findings and recommendations of the OAIC.



What are the penalties?

Interference with the privacy of an individual

Failure to comply with the data breach obligations is an interference with the privacy of an individual, and a breach of the Privacy Act.

Other consequences

Depending on the circumstances, the organisation may be at risk of additional liability on other grounds. For example, the data breach may also be a breach of APP 11.1, a breach of confidentiality, negligence, or involve some of the other issues identified on pages 13 and 14.

Organisations must take must take such steps as are reasonable in the circumstances to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

What are the penalties?

The OAIC has the power to investigate any eligible data breach and can take the following action.

Determinations	The OAIC can issue determinations which can require an organisation to provide an apology, or pay damages, to affected individuals, pay the individual's costs, undertake specific training, or take other specified action. This is the most common outcome of an investigation.
Enforceable undertakings	The OAIC has issued a number of enforceable undertakings to date. Enforceable undertakings can be enforced by court order, and the OAIC has done so in the past.
Civil penalty order of up to $420,000	If an organisation has engaged in a serious or repeated interference with an individual's privacy, the OAIC can seek a civil penalty order.
Pecuniary penalty order of up to $2.1 million	The OAIC can apply to the Federal Court to seek a pecuniary penalty order where the organisation has engaged in a serious or repeated interference with privacy. Fines of up to $2.1 million can apply.

Approach of the OAIC

The OAIC has indicated that during 2018 it will take a compliance approach to data breaches, rather than an enforcement approach.

The OAIC is nonetheless likely to take action in the event of a flagrant data breach, or where an organisation responds to individuals or the OAIC in a manner that indicates it doesn't value the importance of data protection.

Does the organisation have other obligations? (part 1)

Organisations should take into account other legal issues and obligations when planning for and managing data breaches. Here are some examples of additional issues to consider.

Criminal offence

- Some computer and other crimes can be punishable by imprisonment for more than 5 years, which means they are an indictable offence.
- A failure to report such crimes to the police can itself be a criminal offence.
- Does the data breach warrant using the specialist cybercrime reporting facilities at acorn.gov.au?

Insurance

- If your organisation has cyber insurance, when does the insurer need to be notified?
- What information will be required?
- Does the insurer require use of professional firms (such as lawyers or forensics) nominated by the insurer, or can the organisation use its own?

Old Conviction Information

- Part VII *Crimes Act 1914*

Enforceable Privacy Codes

- Check whether there are any enforceable privacy codes approved and registered by the OAIC under Part IIIB of the Privacy Act at https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/

Health Records

- *My Health Records Act 2012*
- *Healthcare Identifiers Act 2010*
- Privacy Guidelines for Medicare benefits and Pharmaceutical Benefits Program issued under *National Health Act 1953*
- *Health Records and Information Privacy Act 2002* (NSW)
- *Health Records (Privacy and Access) Act 1997* (ACT)
- *Health Records Act 2001* (Vic)
- *Health Care Act 2008* (SA) (handling of personal information by public sector employees)

Tax File Numbers

If the breach involved tax file numbers, consider the following:

- *Taxation Administration Act 1953*
- *Income Tax Assessment Act 1936*
- *Data-matching (Assistance and Tax) Act 1990*
- Tax File Number Guidelines issued under the Privacy Act

Official Secrets

- *Crimes Act 1914*

< Back to contents

Does the organisation have other obligations? (cont)

Australian Prudential Regulatory Authority

- CPS 220 Risk Management
- CPS 231 Outsourcing
- CPS 232 Business Continuity Management

Telecommunications

- *Telecommunications Act 1997 (Cth)* (including keeping records of disclosures under sections 301 and 306A);
- *Telecommunications (Interception and Access) Act 1979* (Cth)

Anti-Money Laundering

- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- Money Laundering and Counter-Terrorism Financing Rules

State Privacy Laws

- *Information Privacy Act 2014 (ACT)*
- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *Information Act 2002 (NT)*
- *Information Privacy Act 2009 (Qld)*
- *Personal Information and Protection Act 2004 (Tas)*
- *Privacy and Data Protection Act 2014 (Vic)*

Common law and equity

- Negligence or breach of confidentiality

Contractual

- Contractual provisions may require notification of data breaches. This may also apply to breaches that would not otherwise be notifiable under the Privacy Act.

Surveillance and Workplace Surveillance Legislation

- *Surveillance Devices Act 2007 (NSW)*
- *Surveillance Devices Act 1999 (Vic)*
- *Listening and Surveillance Devices Act 1972 (SA)*
- *Surveillance Devices Act 1998 (WA)*
- *Surveillance Devices Act 2007 (NT)*
- *Invasion of Privacy Act 1971 (Qld)*
- *Listening Devices Act 1991 (Tas)*
- *Listening Devices Act 1992 (ACT) and s61B Crimes Act 1900 (ACT)*
- *Workplace Surveillance Act 2005 (NSW)*
- *Workplace Privacy Act 2011 (ACT)*

Managing risks

There are a number of physical and technological mechanisms that can be put in place to help protect and secure information from loss and unauthorised access and disclosure. Here is a list of some risks that organisations may wish to consider.

Restrict access to information

This can help comply with an organisation's obligations under the Australian Privacy Princples, as well as reduce the possibility of internal data breaches.

Electronic - passwords, biometric access, restrictions on installation of software, copy and print restrictions. Consider encrypting data at rest as well as data in transit.

Physical - pass cards, storage of physical files, providing secure disposal methods (and making sure employees use them).

Access rights (physical and electronic) should be regularly reviewed, particularly where there has been a restructure, change in office-holder, or employee termination.

Regular back-ups of data

Regular data back-ups reduce risk, and the isolation of data helps protect from on-site attacks. Organisations should regularly check that the backups are occurring successfully, as data may need to be restored from a back up in the event of a data breach.

Security testing, monitoring, and audits

Testing and audits of security systems can expose weaknesses or flaws, and determine whether they are functioning and resilient.

This can be undertaken internally, or by specialist firms. Specialist firms can also offer systems monitoring to reduce risks.

Internal risk management

Governance - a culture of security and privacy awareness starting at the board or senior manager level. This may include the appointment of a privacy officer (required for Australian government agencies from July 2018).

Employment contracts - ensuring contracts contain clear confidentiality obligations and transition-out provisions.

Policies - clear policies, regularly provided to staff, on security and safety such as the use of personal devices or BYOD, regular changes to passwords, employee surveillance, working out of the office.

Effective training - new staff and transient/temporary staff training before commencing duties, and on-going regular training for permanent staff.

Tests of data breach response plans

The more often the data breach response plan is tested and refined, the more effectively the data breach team will swing into action when an organisation actually suffers a data breach. These can be run internally, or there are a number of external organisations that will run scenarios.

Managing risks (cont)

Insurance

Organisations need to consider whether their insurance policies cover the risks that are relevant to them.

Organisations may wish to consider whether their insurance policies do, or need to, cover:

- ☑ hacking;
- ☑ third party actions (such as publication of personal information);
- ☑ breaches of law;
- ☑ loss of or damage to electronic data;
- ☑ ransomware;
- ☑ systems under a third party's control (such as a cloud provider);
- ☑ costs where notification to the OAIC and individuals is not mandatory (notification is undertaken from a public relations perspective or for other reasons such as those outlined on page 7);
- ☑ breaches that occurred before the cover but were not discovered until after the policy was effective (some cyber-attacks can take months to be discovered);
- ☑ phishing and other social engineering scams (where employees may have inadvertently disclosed personal information); and
- ☑ other costs associated with a data breach (assessments, preparation of notices, provision of credit to customers, third party costs).

Consider Your Contractual Obligations

- ☑ Do your contracts with third party suppliers (such as cloud providers or customer relationship management operators) detail disclosure and notification obligations where a data breach occurs, and dictate which party is obliged to notify OAIC and affected individuals?
- ☑ Do third parties have adequate policies and mechanisms in place for disaster recovery and business continuity?
- ☑ Do your contracts with third parties require them to abide by laws or policies which may not otherwise apply (for example Commonwealth or other security policies)?
- ☑ Do your contracts deal with the overseas disclosure of information?
- ☑ Do your contracts adequately allocate risk and liability for data breaches, including reimbursement relating to assessments of, and notifications relating to, data breaches?
- ☑ Could an incident affect physical security for individuals for whom the organisation is responsible?

Glossary of terms

Australian Privacy Principles (or APPs)

The 13 principles set out in Schedule 1 to the Privacy Act which impose obligations on how organisations must handle, use and manage personal information.

Credit information

Personal information (other than sensitive information) about an individual that is identification information, consumer credit liability information, repayment history or information made by a credit provider, or mortgage insurer or trade insurer. It can also include information about the types of consumer or commercial credit sought by an individual, default or payment information, court proceedings information and personal insolvency information.

Employee information

Personal information which directly relates to an individual's current or previous employment. Employee information is not covered by the Privacy Act, but information about prospective employees collected during the application process does fall with the Privacy Act.

GDPR

The General Data Protection Regulation, which comes into effect in the European Union on 25 May 2018.

Health information

Information or an opinion about the health or disability of an individual, the individual's wishes about future health services, or the actual or anticipated provision of health services. Personal information (such as name and address) collected in association with such information becomes health information.

Notifiable Data Breach

An alternative way to refer to an eligible data breach.

OAIC

Office of the Australian Information Commissioner, www.oaic.gov.au.

Personal information

Information or an opinion about an individual whose identity is apparent, or can be reasonably discovered, from that information. Information may be personal information even if it is untrue, or communicated verbally.

Privacy Act

Commonwealth *Privacy Act 1988*

Sensitive information

Information or an opinion about an individual's:

- racial or ethnic origin (the languages a person speaks, citizenship, birthplace, attire or photographs which indicate racial or ethnic origin);
- philosophical beliefs (examples include pacifism or veganism, which could originate from a person's dietary requirements, uniform requirements (non-leather shoes), or participation in volunteer activities);
- criminal record (background check, working with children check, or information about convictions requested during a job application process);
- health information (including genetic information, biometric templates, or biometric information used for verification or identification purposes);
- political opinions or membership (membership of political societies, major political parties or activist groups such as GetUp).
- membership of a professional association, or a trade union or association (but not where it is part of an employee record);
- sexual preferences or practices (could be collected through requests for details of spouses/partners); and
- religious beliefs (information collected about a person's diet such as kosher or halal foods may indicate religious beliefs, as may photos of a person in religious attire).

Contacts

Lisa Vanderwal

Special Counsel

lisa.vanderwal@twobirds.com
Tel: +61 2 9226 9832

Hamish Fraser

Partner

hamish.fraser@twobirds.com
Tel: +61 2 9226 9815

Sophie Dawson

Partner

sophie.dawson@twobirds.com
Tel: +61 2 9226 9887

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Sydney & Warsaw