



Privacy change is coming

**Why you should be preparing
now for changes that are
coming in 2018.**

May 2017

KPMG.com.au

Notifiable Data Breaches Scheme

Data breach notification will become mandatory for all entities required to comply with the Australian Privacy Act 1988 in February next year. Then in May, the European Union's General Data Protection Regulation (GDPR) also comes into force. Together, these new requirements require fundamental changes to how Australian organisations handle personal information, and set the stage for some of the largest changes to privacy regulation in the last decade.

On 13 Feb 2017, both Houses of the Australian Parliament passed the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NDB scheme). In many cases, these amendments make notification of eligible data breaches mandatory beginning 22 February 2018.

This is the first time in Australia that all entities who are covered by the Australian Privacy Principles (APPs) have clear obligations to report eligible data breaches. Breaches are to be notified to the Office of the Australian Information Commissioner (OAIC) and any potentially affected individuals.

What is a data breach?

A data breach is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity. This breach may be in relation to one record or many records, and may be electronic records or a physical document.

What is an eligible data breach?

An eligible data breach occurs where:

- A reasonable person would conclude that the unauthorised access to or disclosure of the personal information would be likely to result in serious harm to any of the individuals to whom the information relates; or

- Information is lost (such as leaving a laptop or documents in a taxi), unauthorised access to or disclosure of the personal information is likely to occur, and a reasonable person would conclude that this would be likely to result in serious harm to any of the individuals to whom the information relates.

How soon is notification required?

When an organisation suspects that there may have been an eligible data breach, but aren't yet sure, then all reasonable steps are required to be taken to ensure an assessment is completed within 30 days. If all reasonable steps are taken but due to the complexity of the investigation it takes longer than 30 days, then this is allowable.

When an entity becomes aware that there has been an eligible data breach, they must, as soon as practicable:

- prepare a statement that includes details of the breach and recommendations of the steps individuals should take; and
- give a copy of the statement to the OAIC.

If the OAIC has reasonable grounds to believe that there has been an eligible data breach, they can also direct the entity to provide notice of the breach.



The NDB scheme requires that an entity's assessment of whether serious harm is likely to occur as a result of a data breach takes into account a number of factors, including whether the information is protected by one or more security measures, and the likelihood that any of those security measures could be overcome by the persons or kinds of persons who have obtained or could obtain the information.



To avoid a data breach becoming a notifiable data breach you must be actively monitoring data breach and data loss events, and have in place a process to assess and take action to respond to those events. Then, if a reasonable person would conclude that the data breach would not likely result in serious harm to those individuals, a data breach can avoid becoming an eligible data breach.

Who must be notified of an eligible data breach?

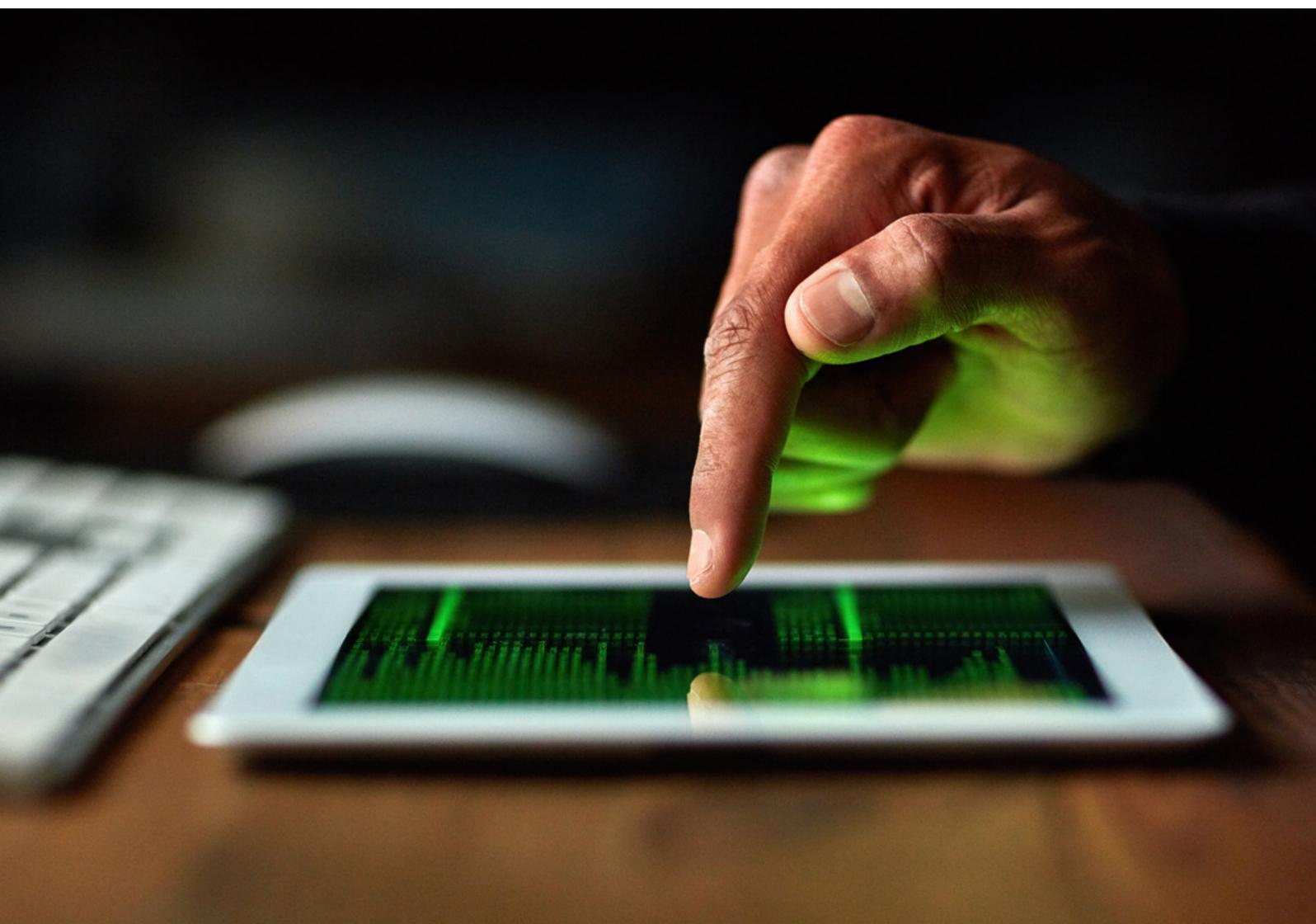
The contents of the statement that is given to the OAIC must also be provided to each of the individuals whose data was breached or who are at risk (again, as soon as practicable). Where the time, effort or cost of individual notifications would render such notification impracticable, then the statement may be published on the entity's website and reasonable steps must be taken to publicise the contents of the statement.

Are any APP entities exempt from the NDB scheme?

For enforcement bodies (such as police forces, the Immigration Department, and certain regulatory bodies), if the notification to individuals of the breach would be likely to prejudice enforcement activities, then the OAIC must still be notified, but individuals whose data was breached do not need to be notified.

Also, where secrecy provisions prohibit the use or disclosure of information to the OAIC or the individuals, then the NDB scheme does not apply.

Finally, the NDB scheme does not apply if the data that is the subject of the breach requires notification under the *My Health Records Act 2012*.



General Data Protection Regulation

While the NDB scheme implements changes to an existing law, the GDPR introduces a whole new regulation with global implications.

When the GDPR comes into force on 25 May 2018, it will replace the existing EU Data Protection Directive (Directive), which has been in place since 1995. Unlike the Directive, the GDPR does not need to be enacted into local law by the EU member states, so for the first time there will be one uniform data protection law in place across the EU.

How does this affect Australian organisations?

The GDPR not only applies to the processors of personal data and the controllers of the processing of personal data (the outsourcing party in an outsourced relationship, for example), that are established inside the EU – whether or not that processing actually occurs within the EU, but also to the processors and controllers outside the EU where an organisation:

- offers goods or services to individuals inside the EU, even if no payment is required; or
- monitors the behaviour of individuals within the EU – especially if you perform analysis or profiling of that activity for predictive purposes.

Whilst it may seem clear that by having a website that allows people in the EU to use your products or services you are captured by the requirements of the GDPR, it isn't quite that simple. Other factors such as whether you accept payment in Euros, or offer a native-language version of your site are important considerations when determining whether the GDPR applies to you.

If they are covered by the GDPR, organisations will also need to appoint a representative within the EU to be the point of contact for supervisory authorities and data subjects on all issues related to processing of personal data.

Key differences to the Privacy Act 1988

While there are many commonalities between the GDPR and the Australian law – they share the goal of privacy by design and transparency, for example, there are some key differences to take note of. Where the Australian law takes a largely principles-based approach supplemented by recommendations, the GDPR is far more prescriptive in defining specific obligations, so requires close attention.

Key examples are:

1 Data Protection Officers

Where the processing of personal data is more than occasional, data controllers and processors must appoint a data protection officer. The data protection officer must report directly to the highest management level of the organisation, have expert knowledge of data protection law, be involved in all issues which relate to the protection of personal data, and be provided with the resources necessary to carry out their tasks freely and independently.

2 The right to erasure

Also known as the right to be forgotten, this requires organisations to delete all data held about an individual upon request by that individual under certain conditions. There is no equivalent under the Australian Privacy Act 1988 – APP 11.2 is similar in that it requires an APP entity to take reasonable steps to destroy information or to ensure it is de-identified if the information is no longer needed, but an individual cannot request this.

3 The right to data portability

Data portability gives individuals the right to request and receive all personal data provided by them to a data controller or processor in a structured, commonly used and machine-readable format that can be provided to another data controller or processor.

Transfer of data outside the EU

The GDPR allows the transfer of personal data outside the EU to countries that provide an adequate level of data protection, with adequacy determined by the EU Commission's Data Protection Board. However, Australia has not yet been determined to have an adequate level of data protection with only 12 months left until compliance with the GDPR is required.

Without this determination, overseas transfers can only occur if the controller or processor have provided appropriate safeguards, and if enforceable data subject rights and effective legal remedies are available to the data subjects.

Key requirements of the GDPR

	Fines	A tiered fine structure depending on infringement. Level 1 is 2% of global turnover or €10m (whichever is higher). Level 2 is 4% of global turnover or €20m (whichever is higher).
	Data Protection Officer (DPO)	DPO required for 'government bodies' and organisations conducting mass surveillance or mass processing of Special Categories of data.
	Supervisory Authorities (SA) enforcement powers	SAs' will be given wide-ranging powers.
	Inventory	Generally organisations will need a personal information inventory.
	Breach notification	Requirement to report privacy breaches to regulator within 72 hours and potentially to the Data Subject.
	Security	Explicit requirements around monitoring, encrypting and anonymisation.
	Privacy Impact Assessments (PIAs)	Companies should perform PIAs if activity is considered 'high risk'.
	Data Subject's rights	Rights extended to include Data Portability and the Right to Erasure.
	Sensitive Personal Data	Similar but extended to include biometric and genetic data.
	Consent	Requirement to gain unambiguous consent (i.e. explicit).
	Data Processors (DP)	Processors are also covered. Controllers must conduct due diligence into processors' suitability.

KPMG Privacy Management Framework

KPMG’s Global Privacy Management Framework is a formalised modular framework, composed of the Generally Accepted Privacy Principles (GAPP) and other elements and sub-components, which together define the foundation for Privacy Risk Management across an organisation. The Framework ensures a shared understanding of Privacy through a clear and consistent language.

Our team of over 200 privacy professionals from around the world use this framework every day to help our clients to assess, design, implement and monitor their privacy programs, controls and risks.



Privacy Principles

Privacy components are viewed against the internationally-recognised ‘Generally Accepted Privacy Principles’, which provide the foundation for our Privacy Management Framework.



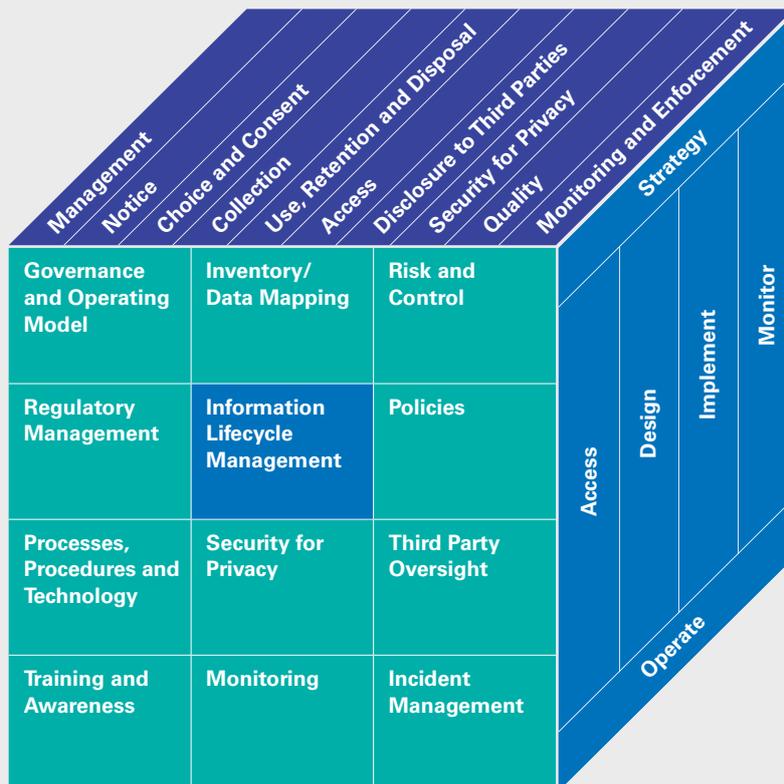
KPMG Support

Our Privacy Service has been designed on the basis that organisations need tailored risk-based solutions to address their individual privacy needs, risk appetite and future business strategy. Its modular and layered structure enables targeted and tailored solutions to be designed, developed, implemented and monitored consistently, cutting through the complexity of privacy and complex global organisations.



Privacy Management Framework

Our framework elements are the distinct components that organisations employ to help ensure compliance with applicable privacy laws and regulations. They provide a practical and pragmatic structure for organising the day-to-day management and oversight required to mitigate privacy risk exposures.



How can KPMG help?

With so much change coming in 2018, now is the time for all organisations to take stock of their current privacy programs and data breach processes to ensure that they are setup to meet these new requirements.

Regulatory Management

Identifying and assessing both current and future privacy requirements to enable the organisation to adopt appropriate processes and controls to monitor regulatory relationships, acknowledge and respond to a privacy regulator, determine the impact of regulatory change and identify action plans to adopt changes.

Ongoing Operations

Supporting the ongoing management of the creation, update, and retirement of policies (including drafting privacy policies and collection statements), procedures and controls around privacy. Monitoring the ongoing processes by which the organisation assesses the design and operational effectiveness of the embedded privacy controls. This can incorporate dashboard reporting, management self-testing and internal audit reviews.

Third Party Assessments

Assesses how suppliers and other third parties manage the privacy risks for personal data they hold or manage. This can be a simple risk assessment (drafting, negotiating and advising on privacy issues in contracts), or a detailed audit of controls with an associated attestation report.

Sensitive Data Finder Services

KPMG's Sensitive Data Finder service uses specifically designed software to identify sensitive data held by organisations, enhance privacy compliance and minimise risk by assisting with classification and remediation activities. It is a powerful data discovery tool providing a leading edge capability to examine unstructured data in many different file types.

Incident Management

The organisation's procedure for identifying, assessing and responding to incidents involving personal information. This includes mechanisms for performing root cause analysis, undertaking corrective actions and testing current incident procedures through mock-incident workshops aligned to privacy requirements.

Data Breach Response Services

KPMG offers a rapid 24/7 response to data breaches. Through deep dive forensic analysis we identify attack sources and problem areas across an organisation's infrastructure. We assist with defining and implementing a recovery strategy in collaboration with local IT. After the data breach is contained and additional fall-out dealt with, we can assist in implementing stronger controls in the medium-to-longer term. Examples are on-going attack detection, improvement of monitoring capabilities and the use of KPMG monitoring services to detect more specialised breaches.

Data Breach Investigation Services

Using our Global Investigations Methodology, KPMG investigates the root cause of data breaches or any other specific question that exists around the occurrence of a data breach, and puts you in an informed position in order to make important decisions.

Contact us



Jacinta Munro
Partner, Privacy
T: +61 3 9288 5877
E: jacintamunro@kpmg.com.au



Stan Gallo
Partner, Forensic
T: +61 7 3233 3209
E: sgallo@kpmg.com.au



Gordon Archibald
Partner, Cyber
T: +61 2 9346 5530
E: garchibald@kpmg.com.au



Kate Marshall
Partner, Legal
T: +61 3 9288 5767
E: katemarshall@kpmg.com.au

[KPMG.com.au](https://www.kpmg.com.au)

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

© 2017 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Liability limited by a scheme approved under Professional Standards Legislation.

May 2017.VIC N15481ADV