gemalto
security to be free

EBOOK

The Australian Privacy Amendment (Notifiable Data Breaches) Act 2017

What is it?

Why was it created?

How can organisations prepare for it?

How did the Privacy Amendment Act evolve and what does it mean for businesses?[1]

How/why

The *Australian Privacy Amendment (Notifiable Data Breaches) Act 2017* (Act) is the latest amendment to the *Privacy Act 1988*. .The Australian Law Reform Commission first reviewed data breach in 2008[2].

After lengthy delays and a 4-year passage through Parliament that started in 2013, the Act brings Australia in line with other countries in the world that have long had mandatory data breach laws. Some countries, like California, began enforcing the world's first data breach law in 2003. Nearly all US states have breach notification laws of varying strength. The EU General Data Protection Regulation, which comes into effect in May 2018, includes mandatory breach notifications. The APAC Region, which previously preferred the free flow of information for trade over security and privacy is seeing more breach notification laws introduced (China[3], India[4] Indonesia[5]).

What does the amendment mean?

On 19 October 2016, the Privacy Amendment (Notifiable Data Breaches) Bill 2016 was An eligible data breach means that there is unauthorised access to, unauthorised disclosure of, or loss of personal information held by an accountable organisation; and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates. An organisation must give notification if it has reasonable grounds to believe that an eligible data breach has happened; or if it is directed by the Privacy Commissioner to do so.

Because privacy cannot exist without security, the requirement to notify breach arises from a failure in security.

"This amendment will require government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in serious harm. The new scheme will strengthen the protections afforded to everyone's personal information, and will improve transparency in the way that the public and private sectors respond to serious data breaches. It will also give individuals the opportunity to take steps to minimise the damage that can result from unauthorised use of their personal information."[7]

- Timothy Pilgrim PSM

Australian Privacy and Information Commissioner

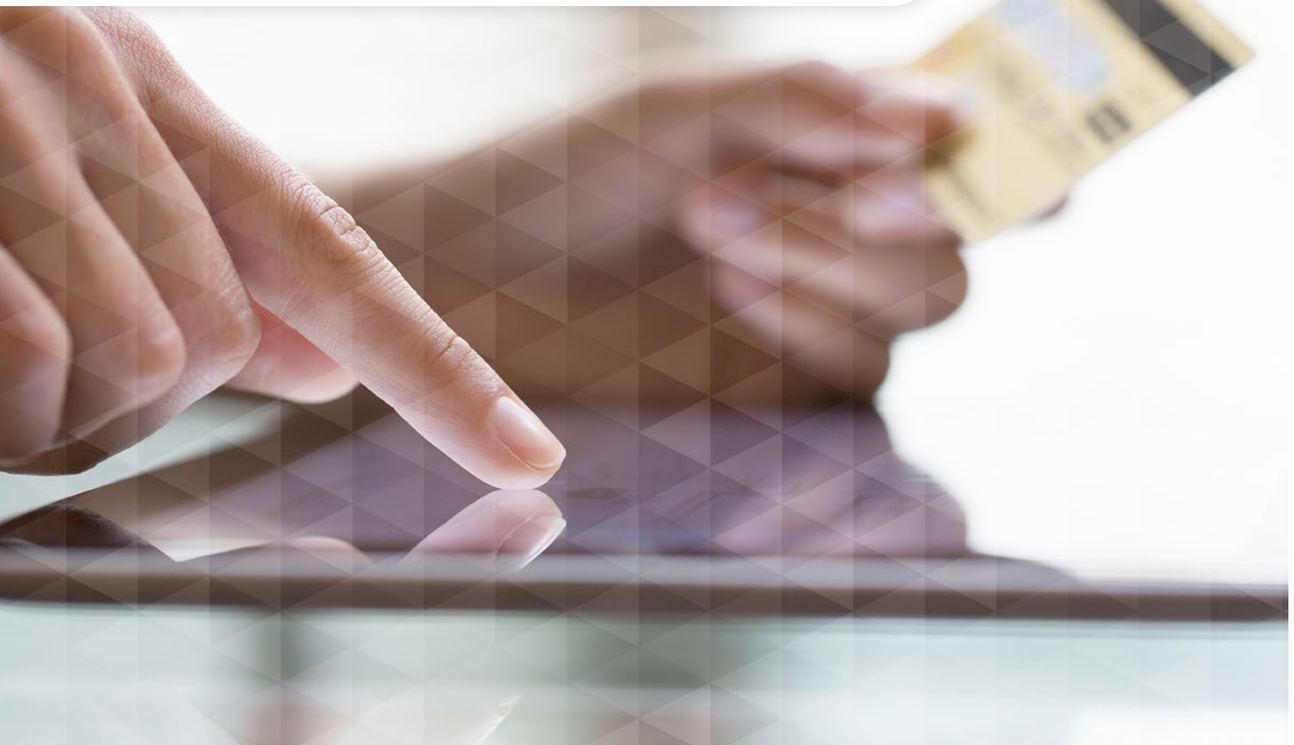
The origin of Australia's Privacy Regulations – How did we get here?[6]

The *Privacy Act 1988* (Privacy Act) was passed by the Australian Parliament at the end of 1988 and commenced in 1989. Initially the Privacy Act had two objectives; to protect personal information in the possession of Australian Government agencies, and to implement safeguards for the collection and use of tax file numbers. Through the years, the Privacy Act evolved to include credit reporting, establishment of the Office of the Australian Information Commissioner (OAIC), inclusion of the private sector and various reforms including the establishment of the Australian Privacy Principles, to regulate the handling of personal information by Australian Government agencies and private sector organisations.

This latest Amendment introduces a mandatory "eligible data breach" notification scheme for entities regulated by the Privacy Act.

- **End 1988 to 2013**
  The Australian Privacy Act passed & commenced in 1989 and amended numerous times
- **June 2013**
  Privacy Amendment (Privacy Alerts) Bill 2013 (2013 Bill) which introduced the concept of "serious data breach" was introduced to the Senate.
- **March 2014**
  Major privacy reform with the introduction of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and Australian Privacy Principles (APPs)
- **December 2015**
  The Australian Government released draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (2015 Bill) for public submission. This Bill was replaced by the Privacy Amendment (Notifiable Data Breaches) Bill 2016.
- **October 2016**
  The Privacy Amendment (Notifiable Data Breaches) Bill 2016 (2016 Bill) was introduced into the Australian Parliament.
- **February 2017**
  The 2016 Bill was passed on 13 February 2017 and became the Privacy Amendment (Notifiable Data Breaches) Act 2017.
- **22 February 2018**
  The Privacy Amendment (Notifiable Data Breaches) Act 2017 commences.

Key aspects of the Privacy Amendment (Notifiable Data Breaches) Act 2017[8]



When does it come into effect?

22 February 2018.

Who must comply?[9]

The Notifiable Data Breach (NDB) Scheme applies to applicable entities under the Privacy Act:

- Australian, ACT and Norfolk Island public sector agencies;
- Private sector organisations with an annual turnover over $3 million;
- Health service providers; and
- Some small businesses and non-government organisations.

"Eligible data breach"[10]

The NDB scheme only requires organisations to notify when there is a data breach (eg unauthorised access, unauthorised disclosure) that is likely to result in serious harm to any individual to whom the information relates. Exceptions to the NDB scheme will apply for some data breaches, meaning that notification to individuals or to the Commissioner may not be required.

"Serious harm"[11] and "Reasonableness"

Under the NDB Scheme, serious harm will be assessed as having regard to the kinds of information involved, its sensitivity, whether it was protected (including by encryption and access controls), and the kinds of persons who have obtained the information. The objective test will apply to assess reasonableness, meaning that what is reasonable is a question of fact in each individual case.

Examples of harm to individuals include:

- identity theft
- financial loss
- threat to physical safety
- threat to emotional wellbeing
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships, or
- workplace or social bullying or marginalisation

Suspected Eligible Data Breaches

If an entity is aware that there are reasonable grounds to suspect an eligible data breach, but not aware that there are grounds to believe it, the entity must carry out a reasonable and expeditious assessment, and complete this assessment in 30 days.

General Notification

When an entity is aware that there are grounds to believe that there has been an eligible data breach, it must, as soon as practically possible:

- Prepare a statement; and
- Give a copy to the Commissioner.

Statement

The statement must set out:

- The identity and contact details of the entity;
- A description of the eligible data breach that the entity has reasonable grounds to believe has happened;
- The kind or kinds of information concerned; and
- Recommendations about the steps that individuals should take in response.

Notification

As soon as practical after the statement is prepared, using the usual means of communicating with individuals, the entity must notify:

- Each of the individuals to whom the information relates, or
- Each of the individuals who are at risk

Or, if this is not possible:

- Publish a copy of the statement on the website; and
- Take reasonable steps to publicise the contents of the statement.

Exceptions

Not all data breaches are notifiable. If remedial action is taken before unauthorised access, disclosure or loss result in harm, the obligation to notify the Commissioner or affected individuals is avoided.

Other exceptions to notify breaches include where the applicable entity is required to notify under the My Health Records Act 2012, and for reasons involving notifiable data breaches of other entities, law enforcement, secrecy, and where the Commissioner makes a declaration not to notify.

Commissioner Direction

The Commissioner himself may direct an entity to notify eligible data breach if the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity, and may, by written notice direct the entity to:

- Prepare a statement; and
- Give a copy of the statement to the Commissioner.

The direction might also require the entity to:

- Notify contents to individuals;
- Notify contents to individuals at risk; and
- Publish on entity's website and elsewhere.

Commissioner Powers and Sanctions

The sanctions for non-compliance with the NDB scheme are the same sanctions as those that apply under the Privacy Act. The Commissioner has powers to investigate, make determinations and provide remedies. Sanctions include civil penalties for serious or repeated interferences with privacy, and penalties up to $360,000 for individuals and $1.8M for organisations.

Key Steps for Addressing Privacy Amendment (Notifiable Data Breaches) Act 2017

1. Identify Where Sensitive Data Resides

A critical first step will be establishing a complete, accurate picture of where sensitive personal data resides.

- For each system or service, who has access to data? How will access and other activities be tracked and assigned to specific individuals?

- How many different locations and environments does the data reside in? This includes detailing geographic locations as well as locations within a data center or extended data center (including virtual and cloud environments), and whether data resides on servers (whether file servers, databases, or virtual machines), storage volumes or shares, or disk drives, tapes, or other media.

- How many different data types need to be secured? Are sensitive data elements solely housed in structured data formats, for example as fields in a database, or are they housed in unstructured files like PDFs, images, or word processing documents?

- Where does data get transmitted? This can include data traversing networks between data centers, whether in point-to-point or multi-point environments.

2. Minimise the Number of Data Repositories Where Possible

Once data locations are identified and understood, it's important to take steps to minimise the number of locations housing sensitive data wherever possible. Particularly with respect to Privacy Amendment (Notifiable Data Breaches) Act 2017, if a business could reduce the number of environments or systems that contain personal data, they could potentially significantly streamline their compliance efforts.

3. Safeguard Data Leveraging Encryption and Key Management

Encryption represents an essential way to establish data confidentiality and integrity. In fact, the Privacy Amendment (Notifiable Data Breaches) Act 2017 will only intensify the demand for encryption.

> Encryption offers the possibility of obviating the need for breach notification, as required by the Privacy Amendment (Notifiable Data Breaches) Act 2017 unless proper technological protection measures are implemented. If a breach occurs but data was encrypted and keys were protected, a cyber attacker would be unable to decrypt the data and access the actual information.

> Organisations can ensure that, even if another government issues a subpoena or is secretly accessing a private repository, an organisation can retain control over who can ultimately decrypt the data.

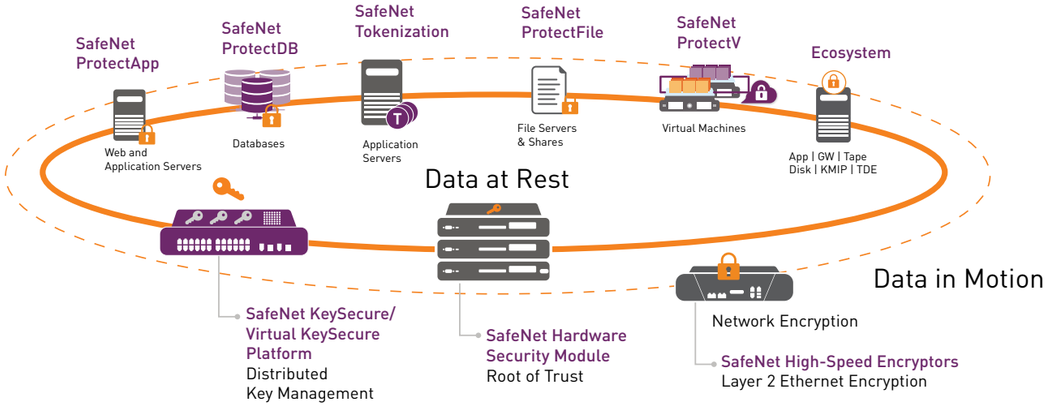
> By deleting a key associated with a consumer's encrypted records, a business could ensure that data will never be accessed in the clear.

4. Control Access

Repeatedly, it is weak, static credentials that are exploited to gain unauthorised access to sensitive resources or perpetuate a full-blown data breach. It is therefore essential for organisations to eliminate this vulnerability by establishing strong, multi-factor authentication to any resource that holds value, be it a network, portal, or application.

Look for an experienced vendor who can offer you a complete solution.

Gemalto delivers the breadth of solutions that enable global enterprises to effectively address their evolving business, security, and privacy objectives. With Gemalto solutions, security teams can centrally employ defence-in-depth strategies that deliver holistic, persistent security.



Gemalto offers solutions that address Privacy Amendment (Notifiable Data Breaches) Act 2017 requirements

> **Encryption.** Gemalto data-at-rest encryption solutions deliver transparent, efficient data protection at all levels of the enterprise data stack, including the application, database (column or file), file system, full disk (virtual machine), and network-attached storage levels. In addition, SafeNet High Speed Encryptors deliver proven and certified Layer 2 encryption capabilities that secure data in transit, while addressing business requirements for real-time response and high throughput.

> **Key management.**With Gemalto solutions, organisations can centrally, efficiently, and securely manage and store cryptographic keys and policies—across the key management lifecycle. These solutions can manage keys across heterogeneous encryption platforms, offering support for the KMIP standard as well as proprietary interfaces. Gemalto offers enterprise key management solutions as well as a range of hardware security modules (HSMs).

> **Identity and access management (IAM).** Gemalto's portfolio of IAM solutions feature market-leading strong authentication and digital signing products. These offerings enable organisations to secure access to online resources and protect the digital interactions of employees, partners, and customers.

For more information on complying with the Privacy Amendment (Notifiable Data Breaches) Act 2017, please contact our Security Consultants at InfoAPAC@gemalto.com

1 https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act

2 http://www.alrc.gov.au/sites/default/files/pdfs/108_vol1.pdf. ALRC Report 108 (tabled August 2008) represents the culmination of a 28-month inquiry into the extent to which the Privacy Act 1988 (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia.

3 China Cybersecurity Law, network operators must promptly inform data subjects if their personal information is disclosed, tampered with or destroyed, and notification must also be made promptly to the relevant authorities

4 The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain 'cyber security incidents'

5 Article 15 (2) of Reg. 82 provides that the provider of an Electronic System must provide written notification to the owner of personal data, upon its failure to protect the personal data.

6 https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act

7 https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification

8 Privacy Amendment (Notifiable Data Breaches) Act 2017, No. 12, 2017, Schedule 1 - Amendments

9 https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

10 Privacy Amendment (Notifiable Data Breaches) Act 2017, No. 12, 2017, Schedule 1 – Amendments, 26WE Eligible data breach

11 Data breach notification guide: A guide to handling personal information security breaches, August 2014, STEP 2: (d), (e), Evaluate the risks associated with the breach

ABOUT GEMALTO'S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilising innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organisations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

GEMALTO.COM