

Australia now has mandatory data breach notification legislation - blueAPACHE

Canonical: <https://www.blueapache.com/blog/australia-now-has-mandatory-data-breach-notification-legislation>

Details:

In this 2017 update, we explain the data breach notification legislation introduced at the time.

2017

The recent passing of mandatory data breach notification laws through the senate imposes on organisations a need for increased transparency and accountability. Australian government agencies, businesses and not-for-profit organisations with an annual turnover of more than \$3 million will soon be legally obliged to disclose eligible data breaches. The Privacy Amendment (Notifiable Data Breaches) Bill 2016 has been passed by both houses of parliament and will come into effect within the next 12 months. Unlike many other countries, Australia does not currently have a mandatory data breach notification law. Organisations could voluntarily undertake notification of data breaches, however, there has been no express requirement under the Privacy Act for them to do so. The new bill makes it a legal requirement for organisations subject to the Privacy Act to make notification of data breaches as soon as they are aware of it. This includes organisations with an annual turnover of more than \$3 million, smaller organisations in the health and education sectors covered under the Privacy Act and individuals who handle personal information for a living, including those who handle credit reporting information, tax file numbers and health records.

Eligible data breaches

Once the law is passed, if organisations have reasonable grounds to suspect that there may have been an eligible data breach, they must carry out, and complete, an assessment within 30 days. Notification of such breaches must be made to the Australian Information Commissioner and affected individuals. An eligible data breach is one where there has been unauthorised access to, or disclosure of, personal information and there is a likely risk of serious harm to any of the affected individuals, or where personal information is lost in circumstances that are likely to give rise to unauthorised access to or disclosure. Whether an individual was at risk of “serious harm” would depend on a number of factors, such as whether the information is encrypted (and how hard that encryption would be to break) and the sensitivity of the information. The notification to the Australian Privacy and Information Commissioner and affected individuals should contain a description of the data breach, the kind of information involved, and steps that individuals can take to respond to the security incident.

Non-compliance

Disclosure in a timely manner can be a daunting task for many Australian businesses that are ill-equipped to detect a breach, often not finding out until months later. On average, breaches remain unnoticed for 229 days. Even then, while the company may know an intruder has accessed its systems, it might not be able to determine what, if anything, was stolen. The need to make a potentially damaging declaration in the event of a breach is now an incentive for organisations to review their information handling processes and ensure security systems are as tight as possible. Failure to comply with the notification scheme will be deemed an interference with the privacy of an individual and

penalties include fines of \$360,000 for individuals and \$1.8 million for organisations. To assess if your customer data has been adequately secured and to equip your organisation with a response plan in the event of a data breach, contact the our team .

What is the name of the legislation discussed in this blueAPACHE article?

We discuss the Privacy Amendment (Notifiable Data Breaches) Bill 2016, which was passed by both houses of the Australian parliament and was set to come into effect within 12 months of the article's publication (dated April 6, 2017).

Which organisations are required to comply with the mandatory data breach notification law?

the law applies to Australian government agencies, businesses and not-for-profit organisations with an annual turnover of more than \$3 million, smaller organisations in the health and education sectors covered under the Privacy Act, and individuals who handle personal information for a living, including those who handle credit reporting information, tax file numbers and health records.

What is an 'eligible data breach' under this legislation?

An eligible data breach is one where there has been unauthorised access to, or disclosure of, personal information and there is a likely risk of serious harm to any of the affected individuals, or where personal information is lost in circumstances likely to give rise to unauthorised access to or disclosure. Whether an individual is at risk of 'serious harm' depends on factors such as whether the information is encrypted (and how hard that encryption would be to break) and the sensitivity of the information.

How much time do organisations have to assess a suspected data breach?

Once the law is passed, if organisations have reasonable grounds to suspect an eligible data breach, they must carry out and complete an assessment within 30 days.

Who must be notified of an eligible data breach, and what must the notification contain?

Notification of an eligible data breach must be made to the Australian Information Commissioner and affected individuals. The notification should contain a description of the data breach, the kind of information involved, and steps that individuals can take to respond to the security incident.

What penalties apply for failing to comply with the data breach notification scheme?

Failure to comply with the notification scheme is deemed an interference with the privacy of an individual, and penalties include fines of \$360,000 for individuals and \$1.8 million for organisations.

Did Australia have mandatory data breach notification requirements before this bill?

No. , unlike many other countries, Australia did not currently have a mandatory data breach notification law at that time. Organisations could voluntarily undertake notification of data breaches, but there was no express requirement under the Privacy Act for them to do so.

How long do breaches typically go unnoticed, ?

on average, breaches remain unnoticed for 229 days, and even after a company knows an intruder has accessed its systems, it might not be able to determine what, if anything, was stolen.

What can organisations do to prepare for this data breach notification requirement, according to you?

We advise that the need to make a potentially damaging declaration in the event of a breach is an incentive for organisations to review their information handling processes and ensure security systems are as tight as possible. It suggests contacting our team to assess whether customer data has been adequately secured and to equip the organisation with a response plan in the event of a data breach.