

Proposed legislation means data breaches must be reported - blueAPACHE

Canonical: <https://www.blueapache.com/blog/proposed-legislation-means-data-breaches-must-be-reported>

Details:

2016

We examine the proposed data breach reporting requirements discussed at the time of this update.

Australian businesses turning over more than \$3 million a year will be forced to notify customers of serious data breaches if the federal government successfully passes its proposed data breach legislation. The draft Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, introduced at the end of last year by the Attorney-General's Department, requires any company or government agency subject to the Privacy Act 1998 to make the notifications within 30 days. If passed, the bill will require companies to disclose a breach within 30 days if it concerns personal information and "there is a real risk of serious harm to any of the individuals" to whom the information relates. Smaller organisations may also be subject to the scheme (health service providers, for example, and businesses that trade in personal information, employee associations, and credit reporting bodies). Breach notifications are important because they give individuals a chance to change their passwords, cancel their credit cards or take other preventative action before the attackers can use any stolen data against them. For a company however, acknowledging the breach can mean substantial damage to reputation and business. Many businesses are ill-equipped to detect a breach, often not finding out until months later. Satya Nadella, the CEO of Microsoft, recently stated that breaches remain unnoticed for 229 days on average. 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 result of a breach would act as an incentive to make sure security systems are as tight as possible. As it currently stands, Australian businesses do not have to notify customers or the privacy watchdog of data breaches, however, they may do so voluntarily. During the 2014-15 financial year, the Office of the Australian Information Commissioner received 110 voluntary data breach notifications from government organisations and the private sector, up from 67 notifications the previous year. Under the government's proposed legislation, businesses will be forced to notify the Australian Information Commissioner and affected individuals if there is a "serious data breach". The draft legislation defines a serious data breach as one that involves personal information, credit reporting information, or tax file information being subject to unauthorised access or disclosure and putting those individuals affected at "real risk of serious harm". 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 government has indicated it wants to streamline the mandatory reporting process for businesses as much as possible to reduce the impact of additional regulatory burdens.

"The government intends to consult extensively with industry and other stakeholders on the proposed scheme, in particular with a view to minimising costs and regulatory impact," a statement issued by Attorney-General George Brandis said.

Not complying with the law would be subject to the range existing penalties under the Privacy Act. The government is seeking feedback on the proposed data breach legislation, with the deadline for submissions being March 4, 2016. To better understand your requirements, contact the blueAPACHE Consulting Team.

What proposed legislation is discussed in this blueAPACHE article?

We discuss the draft Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, introduced at the end of 2015 by the Attorney-General's Department.

Which Australian businesses would be forced to notify customers of serious data breaches under the proposed bill?

Australian businesses turning over more than \$3 million a year would be forced to notify customers of serious data breaches if the federal government's proposed data breach legislation passes.

Within how many days would companies need to disclose a data breach under the proposed bill?

If passed, the bill would require companies to disclose a breach within 30 days if it concerns personal information and there is a real risk of serious harm to the individuals to whom the information relates.

How does the draft legislation define a 'serious data breach'?

The draft legislation defines a serious data breach as one that involves personal information, credit reporting information, or tax file information being subject to unauthorised access or disclosure and putting affected individuals at 'real risk of serious harm.'

What factors determine whether an individual is at 'real risk of serious harm' from a data breach?

Whether an individual was at risk of 'serious harm' would depend on factors such as whether the information is encrypted (and how hard that encryption would be to break) and the sensitivity of the information.

Can smaller Australian organisations be subject to the proposed data breach notification scheme?

Yes, smaller organisations may also be subject to the scheme, including health service providers, businesses that trade in personal information, employee associations, and credit reporting bodies.

What is the current requirement for Australian businesses regarding data breach notification, ?

As it currently stands (at the time of the article), Australian businesses do not have to notify customers or the privacy watchdog of data breaches, but they may do so voluntarily.

How many voluntary data breach notifications did the Office of the Australian Information Commissioner receive in the 2014-15 financial year?

The Office of the Australian Information Commissioner received 110 voluntary data breach notifications from government organisations and the private sector during the 2014-15 financial year, up from 67 notifications the previous year.

According to Satya Nadella, how long do breaches typically remain unnoticed on average?

Satya Nadella, the CEO of Microsoft, stated that breaches remain unnoticed for 229 days on average.

What would happen to businesses that fail to comply with the proposed data breach notification law?

Not complying with the law would subject businesses to the range of existing penalties under the Privacy Act.

What did Attorney-General George Brandis say about the government's approach to the proposed scheme?

Attorney-General George Brandis stated, 'The government intends to consult extensively with industry and other stakeholders on the proposed scheme, in particular with a view to minimising costs and regulatory impact.'

When was the deadline for submissions on the proposed data breach legislation?

The deadline for submissions on the proposed data breach legislation was March 4, 2016.

Who should businesses contact for help understanding data breach legislation requirements, ?

We advise contacting our Consulting Team to better understand data breach legislation requirements.