ADMA Association for data-driven marketing & advertising

Privacy Amendment Notifiable Data Breaches Bill 2016 Q&A

1. What is the history behind the Privacy Amendment Notifiable Data Breaches Bill 2016?

The Privacy Amendment Notifiable Data Breaches Bill 2017 has had a long history. The Australian Law Reform Commission published its four-year information report on the privacy landscape in Australia in 2008. As part of that Australian Law Reform Commission Report, they recommended that a mandatory data breach notification law should be introduced.

Under the last Labour Government, a Bill was proposed, heard and passed by the House of Representatives. It was ready to go through second reading in the format, and would have been passed, had Kevin Rudd not called an election early – and so the Bill lapsed.

A later attempt by Senator Lisa Singh for Tasmania to resurrect it under the Private Members Bill failed.

At the start of 2015 the current Government wanted to introduce the mandatory data retention rules in the telecommunications industry. The Government agreed that it would introduce a mandatory data breach notification law to apply to all businesses in Australia, not just the

telecommunications industry.

Despite a commitment to get it into law, it didn't happen until now, in 2017.
Back to top

2. What is the Privacy Amendment Notifiable Data Breaches Bill 2016 about?

The amendment to the existing Privacy Act is to introduce a new mandatory data notification scheme.

This means that when organisations have reasonable grounds to believe that they suffered an eligible data breach they must notify a number of different organisations and people.

Firstly, the Office of the Australian Information Commissioner, the OAIC.

Secondly, affected individuals.

And thirdly, individuals at risk of certain particular matters.

Most importantly, it's the OAIC and individuals who have been impacted by the data breach that need to be contacted. Broadly, this means that you don't have to notify your entire customer base, only affected individuals.

Back to top

3. When will the Privacy Amendment Notifiable Data Breaches Bill become law?

The Bill received Royal assent on 22 February, which means that it will become law on the date 12 months after assent (unless the Minister decides to proclaim it coming into force before then, but that's unlikely).

It should take effect on 22 February 2018.

Back to top

4. What impact will the Privacy Amendment Notifiable Data Breaches Bill have on business?

Australian business has a year to prepare itself for the Bill.

Should a breach occur, businesses will need to be able to identify an eligible data breach and that it needs to be reported, as well as know how and who to report it to.

Processes and procedures will need to be in place so that the Privacy Commission and the affected individuals are notified, and the business is able to deal with the impact the breach.

As data breach notification is not new, many businesses already have relevant processes in place.

Organisations that don't have these procedures in place need to review what framework they need to be operating under, what policies and procedures do they need to put in place, so that they can comply with the law in 2018.

The new law doesn't impose any new requirements in relation to security measures or technical protections that you would put in place in relation to personal information that's governed by the Act. That position is still governed by Australian Policy Principle 11 (APP 11), and will continue to be the case.

That said, the expectation is that for some organisations, bringing into force this Act or this amendment will trigger a renewed focus on what technical measures, security measures that they have in place given the obligations that would flow if they suffer a breach.

Please refer to the Privacy Commission's *Data breach notification guide* for some great direction on how to prepare for it.

Back to top

5. How is the new law different from the existing one?

There is currently no obligation in law to notify either the OAIC or individuals, if you suffer a security breach or a cyber-attack that impacts on personal information of individuals.

The Privacy Commissioner has previously imposed a pseudo obligation via the Australian Policy Principle 11 (APP 11), the security measures principle, whereby the Commissioner would consider the possibility of an organisation being in breach of APP 11 if it had not taken steps after a security breach to allow individuals to secure their own data and prevent further harm from occurring.

The idea of having a mandatory of breach obligations is new and there are some subtle differences between the Privacy Commission's *Data breach notification guide* and the new Act in the wording, none of which are substantive. For instance, it used to refer to the concept of there being a 'real risk of serious harm' and now the assessment needs to be made as to whether there is a 'likelihood of an event resulting in serious harm'.

Back to top

6. Is every breach reportable?

Not every breach is automatically reportable.

Breaches are only reportable where there are reasonable grounds to believe that there has been what is called an eligible data breach.

The existing OAIC series guide is a really good place to start for guidance on making that decision.

Back to top

7. What are the criteria for a reportable data breach?

The criteria don't exist at the moment.

There are two tests that need to be applied to confirm that a breach is notifiable. First, what is the likelihood that a breach has occurred? Second, is it likely to result in serious harm?

Both of these are grey concepts at the moment and Data Governance Australia (DGA) and the Association for Data-Driven Marketing (ADMA) are working towards compiling a joint guideline to assist with assessing these.

Back to top

8. What are some examples of notifiable data breaches?

The definition of an eligible data breach is:

"It's an unauthorised access to or unauthorised disclosure of information which a reasonable person would conclude will be likely to result in serious harm to any of the affected individuals. A loss of information in circumstances which are likely to result in unauthorised access to or unauthorised disclosure of the information and if that disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm."

Some practical examples of this are below.

Say you hold a database of medical records of individuals and that database is hacked in some shape or form and you know someone has been able to extract the medical records on an identified basis about individuals. Clearly, in this instance, the risk of harm arising from that for individuals is significant.

Similarly, with financial information, the risk of harm is serious and so it would need to be reported and the OAIC and individuals would need to be notified.

Attacks that result in less obviously impact for information being extracted or taken are tricky, for example email addresses or home addresses. Businesses will have to make a judgment call on whether those things are likely to result in serious harm given the circumstances of the situation.

It's important to keep in mind that something that may look like it doesn't have a real risk of harm, actually could do, if it's matched up with other data. Considering how the data could be used and what it could be put together with is imperative to assess the risk of serious

harm.

Email addresses could potentially be harmless, but they have a currency and largely used for phishing attacks. The potential for phishing attacks is considered to be a risk of harm. And in some cases, if you know that it has been taken by hackers, who could then use them to get to individuals, it would end up a notifiable breach.

Back to top

9. **Is there a template that organisations can use to ensure notifications are compliant in the event of a reportable breach?**

Not yet.

In the event of a breach, an internal compliance team and a marketing / customer experience team can work together to come up with a communication that goes out to the consumer that isn't fearmongering, but provides information about what has happened in a consumer friendly way, providing guidance on the steps that an individual can take to protect their data.

This can be a good opportunity for a company to prove that they take protecting their customers seriously.

Be prepared to present a notification that customers can understand, that is not fear mongering and delivers back to helping the consumer to take the next steps.

Back to top

10. **What is the timeframe for reporting data breaches?**

Companies have 30 days to determine whether there has been an eligible breach.

If you have a suspicion of breach (which might actually occur much later than the actual breach date), you are under obligation to conduct investigations to establish whether it is an eligible breach i.e. one that will cause serious harm – this triggers the 30-day window.

Once you have determined that there is an eligible breach, then you must notify individuals promptly.

However, if you have reached the determination that there has been an eligible breach you will have to act straight away.

Back to top

11. **Does hacked data that is encrypted need to be reported?**

If you believe that encryption is going to protect the data and that there is no risk of serious harm because it is encrypted, then as a business, you could make the determination that it doesn't need to be reported.

The test will need to be applied still to determine whether a risk of serious harm exists. Encryption technology change, so just because data is encrypted, it doesn't mean that it is entirely fool-proof.

The particular circumstances need to be assessed: what sort of encryption has been used, is it still strong in market and could the encryption be hacked.

Back to top

12. What penalties apply for not reporting an eligible data breach?

The fines are quite substantial.
For companies, fines can reach up to $1.8 million per infringement.
For individuals, fines go up to a maximum of $360,000 per infringement.

Back to top

13. What is the 'threshold test'?

The threshold test determines if there are reasonable grounds to believe that an eligible data breach has occurred.

Back to top

14. Are the any exemptions to the Bill?

There are to exemptions to the Bill.

One is small business.

Small business is defined as "businesses with an annual turnover of less than $3 million".

However, handling personal information comes with the potential of major reputational damage.

Small business will need to make an assessment as to whether to report breaches to individuals and/or the Commissioner. Failing to do so may result in significant reputation damage.

The other exemption is companies or individuals who have identified a breach and rectified it, eliminating serious harm.

For example, if a file containing personal information is sent to the wrong recipient, the recipient is notified immediately, the file was deleted from the system on a permanent basis and it has been confirmed that it has not been passed onto anyone else and will not be accessed by anyone else.

Another example may be where you identify that there is a security flaw in the system but you close it and you are able to prove that there is no extraction of data or access to data during the period that it was thought existed.

Back to top

15. **If a third party service provider becomes aware of an eligible breach who then is responsible for notifying the OAIC and the impacted individuals? Who wears the penalty in the event that failing to report the breach?**

Responsibility for investigating and reporting breaches depends on who holds and controls the information.

Depending on how a third party service arrangement is set up, the third party service provider may either hold the information or it may not.

For example, if you use a cloud service provider, let's say you use AWS or Microsoft Azure or something like that, then it's generally to be the position that the AWS and Azure don't have control over the personal information of companies who have stored their information in the cloud. They don't have access to that information and often it's encrypted, and so AWS or Azure in those sorts of cases would not be responsible for a breach of the personal information. And because in most cases they would never know what the data was at all.

But if you use an external service provider, for example, to be running a payroll or something along those lines where they're actually handling personal information and they're doing other things with the personal information, then it's likely that that third party service provider would be planned to have control over the information and would be using that information and holding it and therefore the regime would apply to that third party.

The responsibility in this case maybe with both you and external service provider.

Where a third party service provider does hold the information for the purposes of the Privacy Act, they would have to make a notification. You need to make sure that your contract with the third party service provider is clear on how to deal with this if it happens.

However, in the case of contacting individuals, it should be you who notifies them of the breach, as they are your clients and you need to control the flow of information.

Responsibility is part contractual, part on the analysis of the nature of the holding and use of the personal information.

If you use an overseas third party provider, and a breach occurs offshore, responsibility will lie with you.

Make sure to revisit your service provider contracts, which address arrangements for the handling and transfer of personal information. Also ensure that you have indemnities and protections in place.

Back to top

16. **What if the data breach has occurred in a company that generates less than $3 million revenue per annum that is a subsidiary of a larger organisation? Is it then reportable by the smaller company?**

    Yes. The small business exception does not allow large companies to set up subsidiaries that hold all the personal information of their customers in a database and then say that it has very little turnover and therefore there's no need to notify.

Back to top

17. **What is this going to cost my business in terms of compliance? Won't this just be a burden on the business?**

    There is a compliance cost, but this is an issue that business should be looking at anyway.

    As consumer trust becomes incredibly important moving into the future, it is something business should be investing in.

Back to top

18. **How do you report to the Privacy Commission?**

    Currently you simply email the Privacy Commission.

    It is expected that in advance of this new regime coming into force in 2018 there may be updates to the method of notification.

Back to top