

Australian Data Compliance



Privacy Amendment (Notifiable Data Breaches) Act 2017

.....

Commencement date: 22nd February, 2018

.....

Eligible Data Breaches

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

After reporting to the OAI, all affected individuals must be directly notified of eligible data breaches

.....

Entities Subject to Mandatory Reporting

- Most Australian Government Agencies
- All private sector and not-for-profit with an annual turnover of more than \$3 million
- All private health service providers; and
- some small businesses
- certain credit providers, reporting bodies, and holders of tax file number information

Exceptions and consequences do apply; find out more about the new Australian Privacy Principles
probax.io/data-breach-compliance



Does your DR plan comply?

Understand your obligations and optimise

sales@probax.io

1300 885 117

Notifiable Data Breaches Act and Malware

Is a Malware infection a Notifiable Data Breach?

Can Malware cause "serious harm"?

Yes. Malicious software or 'Malware', is specifically designed to disrupt, damage or gain access to a computer system. Variants of malware differ in how they infect and spread, including:

- Ransomware
- Bots
- Adware
- Bugs
- Rootkit
- Spyware
- Trojan Horse
- Virus
- Worms

It is generally possible for unauthorised access, disclosure, or loss of personal information to occur regardless of the means or technology involved in the data breach.

If the unauthorised access to, disclosure or loss of information from malware could result in serious harm to the individual the information pertains to, notification is required

Reporting requirements and Penalties

- If an entity determines that the data breach is an eligible data breach, it will be required to notify affected individuals and the Information Commissioner (OAIC).
- The NDB scheme does not prescribe that the OAIC is notified before individuals and is flexible in this regard, provided notification requirements are met.
- Penalties for non-compliance have a minimum penalty of \$2,000 for individuals; \$350,000 up to \$2 million for corporations



Is your DR setup secure?

sales@probax.io

1300 885 117