SQUIRE PATTON BOGGS

Australia Gets Serious on Data Breaches

Increased Penalties and Changes Proposed to Australia's Notifiable Data Breach (NDB) Scheme

Australia – October 2022

In the wake of Australia's most public and impactful data breach, the Australian federal government has signalled harsher penalties for repeated and serious data breaches under Australia's NDB scheme.

Optus, one of Australia's largest telecommunications providers, was subject to a cyberattack in September 2022 that resulted in the loss of personal information of approximately 10 million Australians. With more than one third of Australia's population affected by this breach, public outrage has been high.

In the weeks since the breach, there have been reports of blackmail and scam activities taken against affected individuals whose critical personal information, including names, phone numbers, passport numbers, driver's licence numbers and Medicare details were leaked by cyberattackers online.

While Optus complied with its obligations under Australia's NDB scheme, notifying current and past customers of the breach, the impact has still been substantial. Both in direct response to leaked information and as a precaution, millions of Optus customers have had to obtain newly issued identification documents and generally respond to identity theft risks. At least 90 individuals have been the subject of ransom demands, with Australia's federal police concerned that further identity theft or blackmail incidents will occur.

The seriousness of this data breach has driven Australia to update its existing data breach framework. On Friday 22 October 2022, Australia's attorney-general, the Hon. Mark Dreyfus, flagged that the Albanese government would introduce legislation in the coming weeks to significantly increase penalties for repeated or serious data privacy breaches. In the announcement, the attorney-general stated that "when Australians are asked to hand over their personal data, they have a right to expect it will be protected" and flagged that the Optus data breach indicated that Australia's current data breach regime was "inadequate".

Under the proposed changes, Australia's Privacy Act 1988 (Cth) would be updated to increase the maximum penalties for serious or repeated data breaches. Notably, this includes a twenty-fivefold increase in the maximum cash penalty from AU$2.1 million to the greater of:

- AU$50 million
- Three times the value of any benefit obtained through the misuse of information
- 30% of the concerned company's adjusted turnover during the relevant period

The changes will not be limited merely to increased penalties, with Australia proposing to implement further powers for the Office of the Australian Information Commissioner to resolve privacy breaches and to allow greater information sharing powers to combat data breach harm.

Final details of the proposed changes, including when increased penalties will apply from, will not be known until the Albanese government introduces legislation in the coming weeks.

If your business is subject to Australia's Privacy Act, we recommend revisiting your company's existing data security framework to reduce the risk of a serious data breach impacting your customers. You may also already be required to maintain a data breach response plan under existing legislation. If you do not have a data breach response plan currently in place, or if you are concerned your plan may not adequately respond in the event of a serious data breach, we are available to assist in the preparation of best practice and bespoke data breach response frameworks to mitigate your company's risk.

Contacts

Connor McClymont
Associate, Perth
T +61 8 9429 7534
E connor.mcclymont@squirepb.com

Chris Rosario
Partner, Perth
T +61 8 9429 7553
E chris.rosario@squirepb.com