Draft data breach notification Bill released

Dated: 10 December 2015
Published by IDM

Australia's Federal Government has released a Discussion Paper as well as its Exposure Draft of Legislation to make it mandatory for certain organizations to report data breaches. If passed, the bill would require large private sector organisations and Federal government agencies to notify the Federal Privacy Commissioner and affected individuals of serious data breaches.

The Draft Bill would apply to entities that are currently bound to the Privacy Act including most government agencies and businesses with over $A3 million annual turnover.

Writing on the law firm's web site, Philip Catania and Tim Lee of Corrs Chambers Westgarth, observe that "One key area of improvement under the new bill is the greater emphasis placed on establishing "reasonable grounds" for determining that a "serious data breach" has occurred before deciding to notify. This is an issue of critical importance, as it marks the line between notifiable and non-notifiable breaches.

"Accurate information can be difficult to come by in the immediate aftermath of a data breach incident, and assessments of the scale and severity of a data breach incident often evolve rapidly as new information becomes available.

"There are significant potential pitfalls for entities in choosing to notify individuals or publicising information before the entity has the full picture. In light of this, the introduction of an "assessment period" of 30 days to allow the entity to more fully investigate the breach seems sensible.

"It's interesting to note that, under the current drafting, the Commissioner needs to be satisfied that "reasonable grounds" exist before he can assert that the notification obligation applies. It's not yet entirely clear how the Commissioner will apply this requirement when reviewing an entity's handling of a data breach incident, given that risk assessments are often conducted under time pressure and with limited information."

Patrick Gunning and Michael Swinson at King & Wood Mallesons note there are some important differences between the 2015 draft Bill and the 2013 Bill which lapsed when the then Labor Government entered into the caretaker period prior to the September 2013 election.

"The obligation under the 2013 Bill required entities that suffered a serious data breach to notify individuals that were "significantly affected" by the data breach. The concept of "significantly affected" has been removed from the 2015 Bill – the obligation is now to notify any individual to whom the relevant information relates, which may include individuals whose particular information has not been lost or subject to unauthorised access.

"Even if this may mean that more individuals are notified than would have been the case under the 2013 Bill, it has the advantage of practical simplicity – affected entities are not obliged to make an assessment of how significantly each individual would have been affected by a data breach, a very difficult task."

The exposure draft and accompanying discussion paper can be found here. Submissions are due by 4 March 2016. https://idm.net.au/article/0010840-draft-data-breach-notification-bill-released

Submitted by Alan Kong - PROV