Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Naomi Burley Managing Director GRC Institute
Contact details *(one or all of the following: postal address, email address or phone number)*	[contact details redacted]

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

The GRC Institute would like to thank the Attorney-General's Department for providing an opportunity for us to comment upon the proposed Privacy Amendment Bill.

The GRC Institute is the peak industry body for the practice of compliance, risk and governance in the Asia Pacific region. Our members are compliance, risk and governance professionals who are actively engaged in the private, professional services and Government sectors.

GRCI conducts a monthly discussion group for members on both the topic of Privacy and Regulatory Engagement and there has been much interest in the proposed changes required for mandatory breach reporting. Whilst our members are currently working to best practice in regard to their privacy requirements, their experience with the existing voluntary reporting mechanisms and guidance has prompted them to provide the following feedback and queries in regard to the proposed changes.

Transition period:

In regard to the date it takes effect, the Attorney-General would be strongly encouraged to ensure that the transition period is a minimum of 12 months. Although many organisations may already have voluntary reporting mechanisms in place, given the size of APP entities, this would be a reasonable period for the updating of policies, procedures and training for staff as well as ensuring clear communication throughout the relevant sections of the business in regard to the change to mandatory reporting and how that will be dealt with within their organisation. Any shorter period and there may not be enough time to embed the changes needed.

Interpretation – "real risk of serious harm":

The key issues for most members centre about the possibly subjective interpretations of definitions, such as "real risk of serious harm". We appreciate that the proposed amendments provide some suggested parameters and that the OAIC will potentially update the guidance it currently provides for voluntary reporting to support the mandatory reporting requirements. However there are a number of areas of concern that should preferably be clarified within the legislation:

1. As guidance cannot be relied upon by our members with any certainty and their responsibility to their boards includes an expectation that they are preparing their compliance programs against a known quantity. Boards and GRC Professionals need to be able to establish controls, programs and training that provide clear guidance for expected behaviours from staff. Guidance, provided by the regulator can be a useful tool but can be amended at any time without notice and gives no assurance to entities that the measures are established firmly. GRC professionals also frequently experience push back on resourcing and change unless there is definitive legislative imperative and we would encourage the Attorney-General's Department to include it within the legislation rather than any non compulsory guidelines.
2. For GRC Professionals to gain traction for their programs within their organisations they need clear legislative instruction.

3. Has the Attorney-General's Department given consideration to giving latitude to organisations for reasonably general assumptions about the circumstances of the individuals affected by the breach and/or the circumstances of the breach (whether by unauthorised access or loss) by the entity, unless there are other variables "known" by the entity.

An entity cannot possibly anticipate every eventuality or circumstance that may pose a real risk and clarity around this ideally would be provided in the wording of the legislation. For instance, an individual may be involved in an issue where their personal safety is at greater risk than usual (for example if they have taken out an AVO against a former partner, as an example.) If an organisation is not in possession of this knowledge it could be reasonable for them *not* to give this kind of situation consideration. In this scenario, if the privacy breach resulted in the information becoming available to the ex-partner, there is obviously a real risk of serious harm issue. However, if the entity reasonably would not have known any of these factors, is the expectation that the entity should assume the extreme scenario – in which case every breach would need to be reported and we will experience low value and time consuming over reporting – or can the APP entities rely on some allowance for reasonableness?

Should an issue arise, as per the example above, hindsight may prompt the regulator to take a different view and we wish to ensure that entities can rely on a retained a level of reasonable expectation both in the assessment process by an entity and by the regulator or an individual who may complain at a later date.

Similarly, there are many quickly emerging new trends and risks that may affect privacy security that it may be difficult for entities to anticipate with the rate of change taking place currently, especially in the cyber risk and AML space for instance, which may also affect the likelihood of a breach and/or the likelihood of serious harm, although it may not be directly related to the individuals whose data has been compromised. Will the regulator and/or the Attorney-General be able to give assurances that they would be able to give latitude to entities in light of the rapidity of this change and emerging, unanticipated risks?

Overseas recipients:

Whilst GRCI members would undertake as much due diligence as possible when storing data with overseas recipients, as well as establish compliance controls and scheduled reviews and audits, they would seek either inclusion of allowance for:

1. The additional time it might take to discover or be informed of a breach from a third party. The interpretation we have made of the current draft is that the time allowed for notification might be considered to commence from the time the third party becomes aware of it 'as if' they were the APP entity themselves. There may be instances of reasonable delay in notification to the APP entity from their third party recipient and we feel there should be allowances made for this overtly as in practice the reality is that it would not be instantaneous.

2. Allowance for the APP entity if they make discovery of a breach when conducting a scheduled review of the compliance structures of the third party supplier in cases where they were not informed at the time of the breach. As outlined above, it is suggested that the legislation include an allowance that the time for notification should begin from the time the APP is informed and/or first becomes aware of the breach.

3. Similar to both points 1 and 2 above, if the APP entity is deceived as to the level of compliance (or non-compliance) by the third party recipient, despite the APP entity's best efforts and discover the non-compliance and/or breach, that the time for notification be considered to commence from the time the APP Entity has become aware of the issue.

4. That the earlier points apply where an APP entity is part of a business structure where the overseas recipient of the data may be a parent company. The Australian entity within the business may undertake reasonable steps to establish compliance but may also be reliant on being informed by the overseas section of the business, when a breach has occurred and may need allowances for this delay as well.

Notification:

GRCI members also seek further clarification around the notification period maximum and whether it is correct to interpret the amendment 26WC (2) to read that the entity has up to a maximum of 30 days from the time of becoming aware of the breach to investigate, assess whether a "serious breach" has occurred and thereafter notify those affected, should the investigation confirm this is the case.

Organisations may find it more useful to have parameters established for the investigation and notification separately. Depending on the complexity of the breach and the level of comfort required to be assured of how the breach occurred and what may have then happened to the data it may take a significant portion of the 30 day allowance. It might be more reasonable to

give a 21-30 day allowance for the assessment and a 14 day allowance for notification for instance.

Similarly, the amendment is currently lacking guidance about the expectation for notification after the Commissioner has made a decision in response to an application for exemption. Will the Commissioner make these expectations known at the time of advising of their decision? Or will the 30 day period commence from receipt of the notification of the decision? Clarity around such issues do empower GRC Professionals to construct compliance programs with appropriate training, policies and controls to ensure the entity is compliant. Where there are no parameters established in advance, there can be resulting weaknesses and a reliance on manual intervention and human interpretation.

General – 26WE Entity:

Some clarification is sought with this amendment as currently written "For the purposes of this Part, **entity** includes a person who is a tax file number recipient" is it the intention of the Attorney-General's Department to capture this range, which could include sole traders, small businesses, small not for profit organisations and the like, rather than APP entities, as the interpretation could be made that it is anyone employing another individual and by necessity needing to obtain their tax file number.

Guidance from OAIC:

GRCI Members would like to invite the OAIC to engage in stakeholder consultation when reviewing the guidance document, should they be updating this guidance in light of changes from voluntary to mandatory reporting. Their practical input could be very valuable to this process and would assist GRCI Members from all industry sectors to better understand, implement and comply with the new requirements.