INSURANCE COUNCIL OF AUSTRALIA

Commercial and Administrative Law Branch
Attorney-General's Department
3 - 5 National Circuit
BARTON ACT 2600

Email: privacy.consultation@ag.gov.au

3 March 2016

Dear Sir/Madam

Privacy Mandatory Breach Notification

The Insurance Council of Australia (the Insurance Council) welcomes the opportunity to comment on the mandatory data breach notification discussion paper (the Discussion Paper); the Privacy Amendment (Notification of Serious Data Breaches) Exposure Draft Bill 2015 (the draft Bill); the consultation draft Explanatory Memorandum (draft EM); and the consultation draft Regulation Impact Statement.

The Insurance Council is supportive of a mandatory breach notification regime for serious data breaches. The Insurance Council's members collect, use and disclose a significant amount of personal and sensitive information in the course of providing insurance quotes, issuing policies and paying insurance claims. Our members take their privacy obligations seriously and are cognisant of the increasing risks posed by data security.

While we are supportive of a mandatory breach notification regime as proposed, it is important that this regime is pragmatic and minimises the regulatory burden on entities subject to the Australian Privacy Principles (APPs). In this regard, our submission raises a number of issues that require further consideration or clarification.

Scope of notification regime

Definition of "harm" and "risk"

Division 2 of the draft Bill limits the scope of the data notification regime to serious data breaches. A serious data breach occurs if:

a) there is unauthorised access to, disclosure of or loss of personal information held by an entity; and
b) as a result, there is a real risk of serious harm to any of the individuals to whom the information relates.

Section 26WF further defines "harm" to include:

a) physical harm;
b) psychological harm;
c) emotional harm;
d) harm to reputation;

e) economic harm; and
f) financial harm.

The draft EM indicates that this list is non-exhaustive, is in addition to the ordinary meaning of the word "harm" and intended to provide clarity[1]. However, this creates substantial uncertainty as a range of matters not specified in the legislation could also be relevant.

In determining whether a breach has caused a real risk of harm to an individual, it would be preferable to establish an objective standard of assessment. However, the addition of subjective elements to the definition of harm, including psychological and emotional harm, is problematic. It is particularly difficult to make an assessment on these subjective elements where more than one individual has been involved in a data breach.

For example, "emotional harm" is a very broad and fluid concept. It could be any emotion which an APP entity may not be able to anticipate in relation to an individual. For example, it would be reasonable to assume that sending an insurance policy schedule to the wrong address would not cause emotional harm; however, individuals that are particularly sensitive could become distressed. The draft EM recognises that where information about multiple individuals is compromised but only some of these individuals are at real risk of serious harm, it would be more pragmatic for the entity to notify the entire population of individuals affected[2]. The triggering of notification to a large group because there may be risk of emotional harm to a few individuals would be contrary to the objective of the legislation to set a high notification threshold to avoid 'notification fatigue'.

In addition, none of the elements of harm referenced in the draft Bill are defined, and APP entities will require further clarity. For example, it is unclear how economic harm differs from financial harm. As well, section 26WG defines "real risk" to mean a risk that is not a remote risk. However, "remote" is not defined and it is not clear from whose perspective (the APP entity or the individual) this should be considered. These issues should be clarified through guidance by the Office of the Australian Information Commissioner (OAIC).

The Insurance Council submits that, to provide certainty to APP entities, the draft Bill should be amended so that an exhaustive list detailing the elements of harm is provided. While our members believe the emotional and psychological wellbeing of individuals is important and relevant in considering any risk of harm caused, their inclusion is unworkable for APP entities in practice. As such, we also submit that this exhaustive list should remove subjective elements of harm, including psychological and emotional harm.

Health and medical information

Section 26WB(2)(a)(ii) provides that unauthorised access to or unauthorised disclosure of information specified in the regulations is taken to be a serious data breach. The draft EM notes that a data breach of such information, regardless of the risk of harm to individuals, will be taken to be a serious breach[3]. The draft EM suggests that such information could include health records, which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection.

[1] Draft EM, paragraph 127.
[2] Draft EM, paragraph 78.
[3] Draft EM, paragraph 28.

While our members value the importance of protecting medical and health information, given the amount of data collected by our members, we would be concerned about any requirement to report all breaches regardless of whether there is a real risk of serious harm. Like other information, where a data breach occurs, APP entities should be able to make a full assessment of whether there is a real risk of serious harm.

Encrypted information

The draft Bill also suggests that in determining whether there is a real risk of serious harm to an individual, an APP entity should have regard to:

- whether the information is in a form that is intelligible to an ordinary person (section 26WB(3)(c)); and
- if the information is not in a form that is intelligible to an ordinary person, the likelihood that the information could be converted to such a form (section 26WB(3)(d)).

The draft EM further elaborates that section 26WB(3)(d) is not intended to preclude consideration of a person with knowledge or capabilities exceeding those of an ordinary person[4]. For example, encrypted information may not be intelligible to an ordinary person, but encrypted information that could be broken by a sophisticated attacker creates the risk of a serious data breach.

However, given this description, in practice this would significantly limit the ability of an APP entity to rely on encryption as a risk mitigating factor and avoid triggering the notification obligations. From our perspective, the draft EM sets a higher standard than sections 26WB(3)(c) and (d) in the draft Bill, and is likely to cause confusion for APP entities. From a policy perspective, encryption should be encouraged as an important security safeguard in protecting information when lost or compromised.

As encryption methods and standards are constantly evolving, it would be helpful for the OAIC to continue to publish and revise the de-identification guidelines as a standard that our members can adopt. This will ensure that if there is a de-identified data breach, an APP entity can be satisfied that the level of encryption/de-identification is of a sufficient standard.

Overseas recipients

Section 26WB(5) establishes circumstances under which an APP entity will retain accountability for a serious data breach for information that has been disclosed to an overseas recipient. It is not clear whether, in circumstances where an entity successfully invokes one of the defences in APP 8.2, a serious data breach of personal information held by an overseas recipient is not required to be reported.

OAIC guidance

Due to the broad and diverse range of situations which the breach notification regime is intended to address, it will be necessary for the legislation to be supplemented by guidance by the Office of the Australian Information Commissioner (OAIC). As this guidance is expected to define, to a large extent, whether a breach is subject to the breach notification regime, it should be subject to public consultation as soon as possible, and before the legislation is finalised.

---

[4] Draft EM, paragraphs 44 and 46.

In determining the content of this guidance, it may be appropriate to consider existing breach reporting regimes, such as the rules governing breach reporting to the Australian Securities and Investments Commission (ASIC). In particular, the guidance may draw on factors outlined in section 912D(b) of the Corporations Act 2001 in determining whether a breach is significant, including:

- the number and frequency of similar previous breaches;
- the extent to which the breach indicates that the entity's arrangements to ensure compliance with the obligations are inadequate; and
- the actual or financial loss to the individuals affected.

ASIC provides further principles-based guidance on its breach reporting process in Regulatory Guide 78, and enables each entity to take into account the nature, scale and complexity of their business when determining significance. The Insurance Council submits that, to the greatest extent possible, the breach reporting regimes for ASIC and OAIC should be consistent. This would facilitate ease of compliance for APP entities.

Threshold for notification

Section 26WC triggers notification when an entity is aware or "ought reasonably be aware" that there are reasonable grounds to believe there has been a serious data breach. In effect, the 30 day period in which to notify affected individuals will commence the earlier of the date the entity actually became aware of the breach and the date on which the entity ought reasonably be aware.

The draft EM explains that the inclusion of the "ought reasonably be aware" requirement is intended to address circumstances where an entity fails to consider evidence suggesting a serious data breach has occurred. While the inclusion of this requirement adds additional complexity by inserting another test in determining when the 30 day period commences, it is in our view unnecessary as the poor conduct being addressed is already protected in the APPs (such as APP 11). In addition, section 26WB enables the Commissioner to direct an entity that has failed to notify a serious data breach to do so. We note that the breach reporting requirements contained within the *Corporations Act 2001* only require actions to commence when an entity is aware of a breach, and implementing a new supplementary test is inconsistent with existing breach reporting requirements.

It is also unclear how sections 26WB(1) and 26WC are intended to interact. Section 26WB(1) states that for an APP entity that holds personal information and is required to comply with the APPs, the 'serious data breach' definition applies. Section 26WC then provides 'if an entity is aware' (of a serious data breach) then it must notify by following the procedural requirements in section 26WC. This suggests that all entities, whether or not they are an entity that falls under section 26WB(1), need to notify. It can also be read that if the serious data breach definition does not apply, section 26WC is not triggered (therefore there is no need to notify); that is, section 26WB must be satisfied before section 26WC is triggered. Clarity should be provided in the EM on how these sections are intended to interact.

Content of notification

Section 26WC(3)(d) requires an entity to set out recommendations about the steps that individuals should take in response to a serious data breach. It is unclear what is expected of APP entities, and this is a requirement that the OAIC should provide further guidance on.

Actions that individuals can take may be clear-cut for some breaches; for example in relation to credit card information, individuals could monitor unusual transactions or cancel their credit cards. In other instances, the individual is unlikely to be able to take any meaningful action in response to the data breach; for example, where an insurance policy document is sent to the wrong recipient. We note that entities would be hesitant to provide recommendations on issues that are particularly sensitive. The OAIC should issue guidance on what entities can recommend to individuals in different situations.

The Insurance Council submits that it would be helpful for the OAIC to make available an online factsheet or provide guidance on a standard form FAQ that would provide impacted individuals with consistent guidance. Without a common source of information, it is inevitable that notifying APP entities will differ in the content and quality of information given.

Section 26WD(2)(b) enables the Commissioner to require publication of a description of the serious data breach that the Commissioner ***believes*** has happened. The Insurance Council submits that this requirement should be limited to factual descriptions, rather than simply what the Commissioner "believes" has happened. At a minimum, section 26WD(2)(b) should be modified so that the Commissioner can require publication of a description of the breach that the "…Commissioner believes has happened ***on reasonable grounds***" or the "…Commissioner believes has happened ***having made reasonable efforts to verify facts with the APP entity***" (amendments in bold and italicised).

State government contracts

Currently, any use/disclosure of information by an insurer for the purpose of administering a workers compensation scheme under a state contract falls outside of the *Privacy Act 1988*. Section 7B(5) of the Privacy Act states that:

> *An act done, or practice engaged in, by an organisation is exempt for the purposes of paragraph 7(1)(ee) if:*
>
> a) *the organisation is a contracted service provider for a State contract (whether or not the organisation is a party to the contract); and*
> b) *the act is done, or the practice is engaged in for the purposes of meeting (directly or indirectly) an obligation under the contract.'*

It is unclear whether APP entities are required to notify serious breaches in relation to information that falls under the section 7B(5) exemption. The wording of section 26WC ('an entity' needs to report a serious data breach) could be read to mean that all entities are within scope of the breach notification regime regardless of any exemption for an act or practice that applies under the Privacy Act. Alternatively, the new sections 26WB and 26WB, along with existing section 7B(5), could be read to suggest that any breach arising from acts or practices which are carried out to fulfil a state contract are exempt from the Privacy Act altogether (including the breach notification requirements).

An additional complication is that state contracts often opt the insurer (who administers the scheme) into complying with the Commonwealth Privacy Act. It is unclear whether this contractual obligation would in effect require the insurer to comply with the breach notification regime regardless of the application of the section 7B(5) exemption.

INSURANCE COUNCIL OF AUSTRALIA

Similarly, acts and practices regarding employee records are exempt under section 7B(3). As with state contracts, there should be clarity on whether employee records are within scope of the breach notification regime.

The OAIC should also clarify whether it expects entities to notify serious data breaches when there is no statutory trigger (due to an exemption) but a private contract requires a party to comply with the Commonwealth Privacy Act. From our perspective, the OAIC should not be adjudicating on these breaches because there are matters within the purview of the state privacy regulators.

OAIC reporting processes, governance and resourcing

The implementation of a mandatory breach notification regime requires the establishment of clear processes and governance arrangements around notifications that are submitted to the OAIC. Entities should have a clear understanding about the uses to which notification data will be put to.

Section 26WC(6) enables the Commissioner to exempt an entity from the requirement to provide a notification where there is a public interest not to notify. How this exemption is to work needs to be clarified. For example, there is no explanation as to when the proposed exemption would be given along a data breach timeline.

Adequacy of the resourcing of the OAIC is another significant consideration having regard to the expansion of the functions and powers of the Commissioner proposed under a mandatory data breach regime. The OAIC would need to be resourced to prevent, for example, limitations in its governance and consideration of applications for exemptions. If too great a burden is placed on the OAIC, it may be unable to effectively perform the functions conferred upon it by the privacy reforms.

If you have any questions or comments in relation to our submission, please contact John Anning, the Insurance Council's General Manager Policy, Regulation Directorate, on [redacted] or [redacted]

Yours sincerely

[redacted]

Robert Whelan
Executive Director and CEO