INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT

Definitions

- Section 26ZE defines harm to 'include' the three elements under that section. The Explanatory Memorandum (p.57) indicates this section is included to provide clarity, that the list is 'non-exhaustive' and is in addition to the ordinary meaning of the word 'harm'.

  It is considered however that this only serves to increase uncertainty as it potentially means a range of matters not specified in the Bill could also be considered 'harm'.

  There is also no explanation under s26ZE as to what 'economic harm' and 'financial harm' means and it is unclear how these two are to be differentiated.

  Further uncertainty exists as the Explanatory Memorandum (p. 42) notes that the ability to make regulations to specify particular situations that may also be serious data breaches is intended to provided flexibility to deal with data breaches that may not reach the threshold of a real risk of serious harm but should nonetheless be subject to notification.

- There is concern around what 'serious' in the Bill means. In the definition of a 'serious data breach' the Bill refers to 'a real risk of serious harm to any of the individuals to whom the personal information relates' 'Real risk of serious harm', an essential element of a serious data breach, is left undefined. Uncertainty as to how 'serious' is to be determined creates the possibility of it being interpreted at a very low benchmark when linked to an individual.

  Insurance Council members have raised concerns that the proposed response (publication) could be disproportionate to the nature of the breach involved particularly taking into account the number of transactions that a large insurance company processes on a regular basis.

- As noted above, OAIC is expected to provide guidance on the concept of 'real risk of serious harm'. To ensure a balanced view, it has been suggested that the 'serious data breach' definition should take into account factors such as those outlined in section 912D(b) of the Corporations Act.

  These factors, which are considered when determining whether a breach is significant and whether there is a requirement to notify ASIC include: the number or 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. Another factor which may also be relevant in determining whether a breach is serious relates to the type of information which has been accessed or disclosed and whether it is classified as sensitive information.

  The Insurance Council submits it makes sense to harmonise the approach in reporting breaches to ASIC and the OAIC. ASIC's principle-based breach reporting process is set out in Regulatory Guide 78 and enables each entity to take into account the nature, scale and complexity of their business when determining significance.

Publication

- As explained above, it is difficult in the absence of draft regulations to comment definitively on how the proposed publication sanction would impact general insurers. For example, the Explanatory Memorandum (p.56) states the regulations will deal with situations where it is impossible for the entity to contact each affected individual or where an attempt to contact each individual would be ineffective.

  The Insurance Council has previously submitted to the OAIC that the existing arrangements and voluntary guidance are sufficient and appropriately flexible to take into account the individual circumstances of a breach. The current voluntary guidance notes that notification may not be appropriate in all cases.

  While section 26ZB(5) in the Bill provides that the Commissioner may issue an exemption notice from publication where there is 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. The public interest test should apply prior to requiring disclosure so that publication were only required where it was in the public interest.

  It is also unclear how the publication conditions are likely to assist an aggrieved consumer and broader community. The requirement to publish, for instance in the case of one breach for one consumer, may be excessive and have little public interest value. Furthermore, there may be legitimate family law and potential criminal issues which need to be considered. If publication is required, only relevant information should published.

  It is acknowledged that for privacy breaches involving bank accounts or websites that are password protected, consumers should be advised of breaches as soon as possible to allow them to take steps to change passwords and protect their information. It is unlikely this situation would arise in the day to day business of general insurance and the prescriptive approach may be excessive for all possible types of potential privacy breaches. In any event, a serious data breach may not affect all customers and it is unclear what benefit would be achieved in causing unnecessary alarm and angst to customers who are not impacted by the breach.

- The legislation should also be written in a technology neutral language so that it does not become outdated and does not exclude other methods of effective publication.

Overseas recipient

- Section 26X(3) appears to make the local entity responsible for notifying a serious data breach of personal information held by the overseas recipient, but it is not clear that this is the intended effect. Following on from that, s26X(3)(b) makes the application of APP8.1 a prerequisite to s26X(3)(d). It is not sufficiently clear whether, in circumstances where an entity successfully invokes one of the defences in APP8.2, a serious data breach of personal information held by an overseas recipient is not required to be reported. This should be clarified.

Interference with the privacy of an individual

- Schedule 1, Clause 3 inserts s13(4A) which makes a failure to notify or failure to comply with a direction to notify an 'interference with the privacy of an individual'. The Insurance

Council considers the wording is ambiguous. It should be clarified whether the intention is to tie this back to the civil penalty provision so as to allow a fine to be imposed for serious and repeated interference with the privacy of an individual (i.e. for repeated and serious failure to notify).

Resourcing of OAIC

- 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.