COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

14 July 2017

Mr Timothy Pilgrim PSM
Australian Information Commissioner and Australian Privacy Commissioner
Office of the Australian Information Commissioner
175 Pitt Street
SYDNEY NSW 2000

RE: Draft OAIC resources for the Notifiable Data Breaches NDB Scheme

Dear Timothy,

Thank you for giving us the opportunity to provide feedback on the four Draft Resources (Draft Resource(s)/Guidance Document(s) for the Notifiable Data Breaches (NDB) Scheme:

1. *Entities covered by the NDB scheme*
2. *Notifying individuals about an eligible data breach*
3. *Identifying eligible data breaches*
4. *Australian Information Commissioner's role in the NDB scheme*

Our feedback can be summarised as follows:

Structure: Generally, the Guidance Documents are well structured, well written and comprehensive. The layered approach (with the *Key Points* overview followed by more detailed areas of guidance) works well and appears to be a particularly accessible format for online consumption.

Timing: We note that the OAIC is proposing to publish Guidance Documents iteratively with the intention to finalise all Guidance Documents by November 2017. We appreciate the early release of the bulk of the Guidance Documents as it assists Industry with the timely update and alignment of existing processes and procedures.

Industry is keen to understand the design of the proposed online form[1] to be used for lodgement of notification statements and any supporting information as those resources will need to be incorporated into complex business/corporate processes. We encourage a timely release of the online form and supporting information.

Flow chart: The topic may be overwhelmingly comprehensive for many entities not already familiar with the OAIC's existing guidance in this area (*Data breach notification: A guide to handling personal information security breaches*). To assist in ensuring it meets the stated aims of being clear, relevant and practical, we suggest the OAIC looks to publish a one-page flowchart showing the key decision points, similar to the diagram that currently appears on page 41 of the guidance *Data breach notification: A guide to handling personal information security breaches*.

[1] Draft Resource *Australian Information Commissioner's role in the NDB scheme*, section *How the Commissioner will receive notification*.

Future of existing guidance: The OAIC's website[2] notes that the existing guidance *Data breach notification: A guide to handling personal information security breaches* will be updated in consultation with stakeholders ahead of commencement of the Scheme. It is not quite clear to us whether that document will continue to exist in some form or be replaced by the Guidance Documents. The coexistence of two separate but similar pieces of guidance post commencement of the Scheme in February 2018 might be confusing.

Review: The OAIC appears to acknowledge that entities bound by the Scheme may be challenged with the correct understanding and implementation of the Scheme.[3] Consequently, Industry recommends that the OAIC commit to a review of the Guidance Documents within 12 months after the commencement of the Scheme, i.e. around February 2019, to allow stakeholders to feed-back experiences gained from the practical operation of the Scheme and the Guidance Documents.

Meaning of 'holding of information': A key concept in the Scheme is that it applies in relation to personal information 'held' by an entity.[4] The question of who holds information can be complex. Consider, for example, that is possible for the customer of a cloud service provider to maintain complete control of personal information stored in a cloud system such that the information is not disclosed to the cloud service provider (also refer to para. 8.14 of the OAIC APP Guidelines). The Guidance Documents should include a discussion of what it means to hold information in the NDB Scheme. Items for discussion ought to include: Is the information held by a party that controls access or is the information held by the party that has ownership or control of the systems where the information is physically or virtually present? Is the party that collected the information from the public holding the information even though the actual location of the information is on a third-party system? Are all such parties deemed holding the information? The Guidance Documents might make reference to para. B.79 to B.82 of the OAIC APP Guidelines and give examples of the operation of the Scheme in practice. A key issue in applying the 'possession or control' test for 'holding of information' is whether a breach by the party who stores the information should be regarded as a breach by every party with potential access to and/or control of the information. Some examples of the meaning of 'holding of information' and the relationship between disclosure, use and holding should be included in the Draft Resources.

APP entities vs entities: The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Act) as well as the Guidance Documents differentiate between APP entities (i.e. Part IIIC Division 1 and 2 of the Act carefully distinguish APP entities and credit providers etc.) and entities more generally (Part IIIC Division 3 of the Act only uses the term entity). The Act also states that the definition of entity for the entire Part IIIC of the Act includes a person who is a file number recipient, thereby widening the definition beyond the scope of an APP entity. This leads to confusion at least or, even worse, to a scenario where Division 1 and 2 of the Act only apply to APP entities (and credit providers etc.) while the requirement for notification (Division 3 of the Act) applies to a wider set of entities, even beyond credit providers etc.

If this differentiation in the legislation is the result of inaccurate drafting, then the Guidance Documents ought to attempt to rectify this inaccuracy and provide clarity. If the Parliamentary drafters purposefully made this distinction, then the Guidance Documents ought to clearly highlight the diverging requirements and explain their background.

Notification example: The OAIC's website[5] also indicates that the OAIC will provide further information about what information to include in a notification statement. Although the legislation

---

[2] Section *Resources to prepare for the NDB scheme* at https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/.
[3] Draft Resource *Australian Information Commissioner's role in the NDB scheme,* section *Enforcing compliance with the scheme*.
[4] Privacy Amendment (Notifiable Data Breaches) Act 2017, Part IIIC, Division 1, Section 26WA
[5] Section *How to Notify* at https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/.

does not prescribe a form, it would be helpful if the OAIC created an example of a notification to the Commissioner. This would be particularly useful for smaller entities.

Confidentiality of notification statement: The Guidance Documents[6] indicate that entities can request supporting information be treated as confidential. Can we conclude that the notification statement itself would not be subject to the same confidentiality arrangements? If so, it is likely that entities will keep the statement itself rather brief in order to avoid the risk of exposing vulnerabilities to fraudsters and placing themselves at risk of becoming a target for future attacks or put additional individuals at serious risk as a result of the notification. This in turn means that the provision of supporting information becomes virtually compulsory.

Multiple notifications/diverging assessments: Data breaches in the value chain (across multiple organisations) require a coordinated response. We foresee issues that arise when there are divergent assessments of the risk of serious harm and where notification and control of the breach may sit separately from the organisation with the closest or only relationship with the end-user. In our industry, the obvious example is in the wholesale market where the wholesaler has no or hardly any information about the end-user. Even if the wholesaler was to believe that an eligible breach may have occurred (and the reseller may not share that opinion), the ability to investigate whether a breach is actually an eligible breach and the decision of notification would ultimately rest with the reseller as the entity which has the most direct relationship with the affected individual and which is the only entity that has access to the affected individual(s).

Remedial action and containment: By definition, the Draft Resource *Notifying individuals about an eligible data breach* focuses on the notification aspects of eligible breaches. Where entities have not read the accompanying Draft Resource *Identifying eligible data breaches*, entities may skew their assessment process in favour of notification to the OAIC over the interests of affected individuals. Any entity's primary focus ought to rest on protecting individuals and, therefore, the containment and remediation elements of any data breach are crucial. Efforts should be directed first and foremost to identifying and containing a data breach and, contemporaneously, initiating remediation activities so that the risk of serious harm is minimised, rather than being distracted by notifications. Given the importance of containment and remediation, we suggest including information that a data breach is not eligible or notifiable if an entity acts promptly to remediate and, as a result of this action, the data breach is not likely to result in serious harm. At a minimum, the *Key Points* to the Draft Resource *Notifying individuals about an eligible data breach* ought to cross-reference the relevant section of the Draft Resource *Identifying eligible data breaches*

We also note that the Guidance Documents state that "Once an entity has reasonable grounds to believe there has been an eligible data breach and is not exempted from notifying, it is required to provide notification to the Commissioner and, usually, individuals at risk of serious harm." [emphasis added].[7] Once a breach has been identified as eligible (and no exemptions apply), what would be the circumstances that require notification to the OAIC but not the affected individual(s)?

Conversely, note that in *Example 2 – notification following unintentional publication of sensitive data* of the Draft Resource *Identifying eligible data breaches* the entity under consideration concludes that an eligible data breach has occurred and, consequently, notifies the respective customers through various means. However, the example does not indicate that the entity also notifies the OAIC. Is this a unique example where the entity is not required to notify the OAIC or is this an unintentional omission in the Draft Resource? If it was the former, it would be helpful if the OAIC clarified the different circumstances when notification to the OAIC is required and when it is not.

---

[6] Draft Resource *Australian Information Commissioner's role in the NDB scheme,* section *Confidentiality of information provided in notifications.*
[7] Draft Resource *Australian Information Commissioner's role in the NDB scheme,* section *How the Commissioner will receive notification*.

Overseas disclosure: We suggest including a summary of the section *Information disclosed overseas* contained in the Draft Resource *Entities covered by the NDB Scheme* in the *Key Points* of this Draft Resource as some entities might specifically search for this piece of information and otherwise miss it.

Serious harm: The risk of serious harm is to be assessed holistically and its assessment includes a very broad range of factors for consideration by the entity. While the detailed examination of the key considerations and given examples are helpful, we note that our members do not necessarily agree with some of the decisions in the examples which serves to highlight the differing views that a reasonable person might take. In practice, many entities may choose to notify affected individuals to ensure an open and transparent conversation with their customers even though, on strict assessment, there may be no legal compulsion to do so. Consequently, the OAIC is also more likely to be notified in circumstances not requiring it as entities strive to use the OAIC to assist them with the fielding of customer queries or general customer awareness.

Reasonable person: We welcome the clarification that the objective test in assessing whether a breach is likely to result in serious harm is to come from the perspective of the entity, i.e. "a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach)".[8]

Number of individuals involved: Throughout the Guidance Documents, in particular in the Draft Resource *Identifying eligible data breaches*, it appears that the number of potentially affected individuals receives a disproportionate weight in the assessment of a data breach. It would be beneficial to convey that other factors, such as the type of information involved, its protection through encryption or other means and potential remedial action, play an equally or even more important role in the assessment. We are conscious that the Draft Resources could bias entities to notify breaches simply on the basis of the number of individuals involved.

Declaration of no notification: We note the guidance about the circumstances where the Commissioner might decide that a notification need not be made.[9] It would assist Industry if the Draft Resource included some examples illustrating cases where the Commissioner might decide that notification need not be made and cases where the Commissioner would decline to make such a decision.

We look forward to further engaging with your Office on the NDB Scheme. Please contact Christiane Gillespie-Jones (c.gillespiejones@commsalliance.com.au) or myself (stanton@commsalliance.com.au) if you have further questions or would like to discuss.

Yours sincerely,

John Stanton
Chief Executive Officer
Communications Alliance

[8] Draft Resource *Identifying eligible data breaches* , section *Is serious harm likely?*
[9] Draft Resource *Australian Information Commissioner's role in the NDB scheme,* section *Declaration that notification need not be made, or that notification be delayed (s 26WQ).*