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)*	The Department of Employment (the Department) and the following agencies in the Employment portfolio (portfolio agencies): • Asbestos Safety and Eradication Agency • Comcare • Fair Work Building and Construction • Fair Work Commission • Fair Work Ombudsman • Safe Work Australia • Workplace Gender Equality Agency
Contact details *(one or all of the following: postal address, email address or phone number)*	Shari Beaumont, Principal Government Lawyer Information Law, Practice Management and Corporate Advising Branch, Department of Employment [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The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.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? YES / **NO**

Your submission

Insert your text here and send the completed submission to the Attorney-General's Department, preferably via privacy.consultation@ag.gov.au

Thank you for inviting us to provide comments on the draft *Privacy Amendments (Notification of Serious Data Breaches) Bill 2015* (Cth) (the Draft Bill).

The Department and portfolio agencies support the proposed scheme to notify individuals and the national privacy regulator of serious data breaches, noting that there will be appropriate exceptions to this requirement, including for enforcement related activities or where notification would not be in the public interest. In our view, the proposed scheme is unlikely to have a significant administrative or ongoing compliance burden for the Department and portfolio agencies, noting it is in line with our current practices in the event of a data breach and the "*Data breach notification – A guide to handling personal information security breaches"* issued by the Office of the Australian Information Commissioner (OAIC).

In relation to the specific questions outlined in the draft Regulation Impact Statement, we provide the following comments:

1. *What are likely to be the administrative costs and ongoing compliance burden of these requirements?*
   In our view, there will be little additional administrative and ongoing compliance costs for the Department and portfolio agencies in relation to implementing the proposed notification scheme, as it aligns with current best practices in the event of a serious data breach. We anticipate there would be some initial administrative costs for most entities, particularly in creating or updating appropriate data breach policies and procedures, and briefing staff and third party providers. The compliance burden of the notification requirements will depend on the particular circumstances of the breach, but would generally be manageable with existing resources. Overall, we consider that both the administrative and the ongoing

compliance burdens will be minimal, but note that they are likely to be most burdensome on small agencies.

2. *What form of communications do we foresee utilising to notify affected individuals of a serious data breach?*
   The Draft Bill provides that where entities normally communicate with an individual using a particular method, notifications may be provided using that method. We support this flexible approach and believe it will help ensure that individuals receive notifications through communication channels that they expect us to use and do not erroneously consider notifications to be spam or a scam. The Department and portfolio agencies currently communicate with individuals through a broad variety of mediums, including email, formal letter, telephone, text message, in person, notifications in official mobile device applications, messaging through official Departmental or government sites (e.g. jobsearch or myGov) and through an authorised representative. Generally, the most common notification methods are likely to be email, telephone or formal letter.

3. *How can a mandatory data breach notification scheme be implemented in a cost effective manner?*
   As stated above, the proposed scheme is unlikely to impose a significant burden on the Department and portfolio agencies. However, we have identified the following strategies that could assist in implementing the scheme in the most cost-effective way:

   - the development of a standard communication model or template notification statement;
   - the development of robust guidance material, particularly in relation to requirements of the notification statement and assessing whether a breach poses a reasonable risk of serious harm; and
   - the availability of an 'online portal' or web form for the online lodgement of notification statements.

We have also considered the Draft Bill more generally and have the following comments:

- The Draft Bill currently provides that a serious data breach occurs in circumstances of "unauthorised access to, unauthorised disclosure of, or loss of,

personal information". We note it may be appropriate to consider whether the language could be made more consistent with that used in Schedule 1 of the *Privacy Act 1988* (Cth) (Privacy Act). For example, Australian Privacy Principle (APP) 11 refers to protecting information from misuse, interference, loss, unauthorised access, modification or disclosure. This would provide further clarity for entities and align the Draft Bill with existing obligations to protect information.

- The practical implication of section 26WC(2) of the Draft Bill is that entities will have 30 days to carry out an assessment as to whether there are reasonable grounds to believe that the relevant circumstances amount to a data breach. We consider this would generally be adequate time to conduct such an assessment, but note that for small agencies or particularly complex matters (e.g. where data is handled overseas) it is foreseeable that entities may require additional time to perform an adequate assessment. Accordingly, we would support a provision that would allow entities to apply for an extension of this timeframe.
- Section 26WC(3)(d) of the Draft Bill requires entities to include in the notification statement "recommendations about the steps that an individual should take to in response to the serious data breach". In some circumstances, it will be straight forward to identify and recommend steps, such as the example in the explanatory memorandum of "recommending that individuals request a copy of their credit report". However, we note that APP entities may not always be best placed to advise on such steps. It may be helpful to consider whether this step would be more appropriately discussed as best practice in guideline material rather than being a legislative requirement.
- We would support the development of guidelines from the national privacy regulator to assist in interpreting notification requirements, particularly in relation to the creation of data breach policies. It would also be helpful for the national privacy regulator to provide guidance as to which entity is responsible for notification requirements where multiple entities handle information that is subject to a breach. For example, some databases contain information that is collected and used by multiple Government agencies and, if that database was subject to a breach, it is unclear if one or all of the agencies would be required to notify the affected individuals.
- The Department notes the Productivity Commission will be undertaking a review of data availability and use as part of its response to the Financial System Inquiry in October 2015. Given this review will consider current legislative frameworks, we recommend that the timing of the Draft Bill is reconsidered so as to reflect the review's findings.

Thank you again for providing the opportunity for us to comment on the Draft Bill. The Department and portfolio agencies are committed to our privacy obligations under the Privacy Act and strive to manage personal information with the utmost care and protection. In our view, the proposed formal notification scheme will complement these existing obligations and, in the unlikely event of a serious data breach, allow individuals whose personal information has been compromised to take appropriate measures to avoid adverse consequences.