



# Dun & Bradstreet (Australia) Pty. Ltd

**Independent review of compliance with Part IIIA of the  
Privacy Act 1988, the Privacy Regulations 2013 and the  
Privacy (Credit Reporting) Code 2014**

External Report

## ***Inherent Limitations***

As set out in our Engagement Letter dated 29 May 2017 ("Engagement Letter"), KPMG has undertaken an independent review of compliance with Part IIIA of the Privacy Act 1988, the Privacy Regulations 2013 and the Privacy (Credit Reporting) Code 2014 (collectively "the Privacy Requirements"), for Dun and Bradstreet (Australia) Pty. Ltd (D&B), as required in accordance with paragraph 24.2 of the Privacy (Credit Reporting) Code 2014, ("the Engagement").

The services provided in connection with the Engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions intended to convey such assurance have been expressed.

As part of the Engagement we have delivered an "External Report" to D&B, providing a summary of the findings set out in our Internal Report dated 30 June 2017. This document is the External Report ("this Report") and contains our key findings. Our detailed findings for management purposes are contained in our Internal Report dated 30 June 2017.

No warranty of completeness accuracy or liability is given in relation to the statements and representations made by, and the information and documentation provided by D&B or D&B management and personnel consulted as part of the process.

The information and conclusions set out in this Report have been extracted from our Internal Report dated 30 June 2017. KPMG has not, and is not obliged, to undertake any procedures in relation to, or update this Report for events occurring subsequent to 30 June 2017 that may be relevant to this Report.

Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected. Further, the internal control structure, within which the control procedures that have been subject to the procedures we have performed, has not been reviewed in its entirety, and therefore, no opinion or view is expressed as to the effectiveness of the greater internal control structure.

The procedures performed were not designed to detect all weaknesses in control procedures as they were not performed continuously throughout the period and the tests performed on the control procedures were performed on a sample basis. Any projection of the evaluation of control procedures to future periods are subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

The observations contained within this Report have been formed on the above basis.

## ***Third Party Reliance***

This Report has been prepared solely for the purpose set out in Section 2 and for D&B's information, and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent. This Report has been prepared at the request of D&B in accordance with the terms of KPMG's Engagement Letter dated 29 May 2017. Other than our responsibility to D&B, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this Report. Any reliance placed is that party's sole responsibility. In that regard, we consent to this Report being released to the OAIC on the basis set out in our Engagement Letter.

We disclaim any assumption of responsibility by KPMG to any person other than D&B, or for any use of this Report for any purpose other than that for which it was prepared.

The definitive version of this Report is the one bearing our original signature and D&B management is responsible for any errors or in accuracies appearing in any reproduction in any form or medium.

# Contents

1. Introduction	1
2. Background	1
3. Scope and Approach	1
4. Overall Conclusion	2



# 1. Introduction

As set out in our Engagement Letter dated 29 May 2017 (“Engagement Letter”), KPMG has undertaken an independent review of compliance with Part IIIA of the Privacy Act 1988, the Privacy Regulations 2013 and the Privacy (Credit Reporting) Code 2014 (collectively “the Privacy Requirements”), for Dun and Bradstreet (Australia) Pty. Ltd (D&B), as required in accordance with paragraph 24.2 of the Privacy (Credit Reporting) Code 2014, (“the Engagement”).

As part of the Engagement we have delivered an “External Report” to D&B, providing a summary of the findings set out in our Internal Report dated 30 June 2017. This document is the External Report (“this Report”) and contains our key findings. Our detailed findings for management purposes are contained in our Internal Report dated 30 June 2017.

# 2. Background

In accordance with paragraph 24.2 of the Privacy (Credit Reporting) Code 2014 (Version 1.2) (“CR Code”), every 3 years (or more frequently, if the Commissioner requests) a Credit Reporting Body (“CRB”) must commission an independent review of its operations and processes to assess compliance by the CRB with its obligations with the Privacy Requirements. In addition, the CRB must consult with the Commissioner as to the choice of reviewer and scope of the review. This Report and the CRB’s response to this Report must be provided to the Commissioner and made publicly available.

D&B engaged KPMG to undertake the independent review of the design and operating effectiveness of its Privacy Framework for compliance with the Privacy Requirements. This review is necessarily a point in time review focusing on the Privacy Framework of the D&B credit reporting business entity. This Report, for completeness, recognises through management comments and our observations, the ongoing changes and improvements the business is making in order to ensure ongoing compliance with their obligations.

# 3. Scope and Approach

The scope of the Engagement is agreed as follows:

- Perform a Governance, Policy and Process assessment to gain an understanding of the Privacy Framework implemented by D&B to comply with the Privacy Requirements.
- Review and testing of process controls against the Privacy Framework.
- Prepare a final report to present findings and observations in accordance with the obligations under the Privacy Requirements (collectively, Scope).



In light of the Scope, a summary of the approach is as follows:

- We reviewed copies of documents provided by D&B and made further enquiries of D&B management and personnel as required.
- We conducted interviews with members of D&B management and personnel in order to understand the level of awareness and how D&B's Privacy Framework is applied in practice.
- We undertook on-site walk throughs of key processes and controls and areas identified by management for continuous improvement and action.

Our observations set out in this Report should be considered in this context.

## 4. Overall Conclusion

We acknowledge the cooperation that has been provided by D&B in our preparation for this report and throughout the course of our review.

Based on the work performed during the Engagement, we make the following observations:

- We consider that the relevant D&B management and personnel have a strong understanding of D&B's Privacy activities, designed to manage D&B's compliance with the Privacy Requirements.
- There is a strong appetite within D&B management to be compliant with the obligations of CRBs, with the Privacy Requirements and a recognition of the importance of individual responsibilities in applying D&B's Privacy Framework as designed.
- We have evidenced a strong "tone from the top" regarding the importance of applying D&B's Privacy Framework effectively and managing D&B's ongoing Privacy compliance obligations.
- We recognise that D&B has been proactive in engaging in initiatives to strengthen their Privacy Framework.
- We consider that appropriately qualified and experienced people have been appointed into the key roles within D&B's Privacy Framework. These individuals have displayed the right mindset, level of influence and desire to apply D&B's Privacy Framework. Whilst we observed there is a key person risk associated with several key roles in D&B's Privacy Framework, we note management's awareness of this risk and the appropriate focus on the documentation of policies and procedures in this regard.
- We observed that certain processes and controls supporting D&B's monitoring of Privacy compliance activities are impacted by their manual nature.
- We observed that the limited operationalisation of certain reporting and storage (outside D&B's primary consumer credit bureau database) procedures impacts D&B's ability to identify, assess and manage Privacy obligations.



We raised a number of findings during the course of the Engagement and provided associated recommendations in our Internal Report. Whilst we acknowledge D&B's ongoing journey to strengthen their Privacy Framework, we consider that by implementing these recommendations, D&B will further enhance their ability to comply with obligations under the Privacy Requirements.

Given the reliance on third parties to originate credit reporting information, particularly as it relates to Privacy obligations, it is expected that CRBs may be prone to instances of non-compliance. An effectively governed CRB is therefore not expected to be a business that always avoids compliance issues, but rather a business that supports and actively promotes compliant outcomes and behaviours and responds to breaches or other compliance issues promptly and appropriately, including relevant remediation activity as required.



|

[kpmg.com.au](http://kpmg.com.au)



[kpmg.com.au/app](http://kpmg.com.au/app)

