Law Council
OF AUSTRALIA

Office of the President

15 August 2017

Mr Timothy Pilgrim PSM
Australian Information Commissioner and Privacy Commissioner
Level 3, 175 Pitt Street
SYDNEY NSW 2000

By email: consultation@oaic.gov.au

Dear Commissioner

Privacy (Australian Public Service – Governance) APP Code

1. Thank you for the opportunity to provide comment on the proposed *Privacy (Australian Public Service – Governance) APP Code* (**the Code**).

2. The Law Council acknowledges the assistance of its Privacy Law Committee of the Business Law Section in the preparation of this submission.

3. The Law Council supports the efforts being taken by the Office of the Australian Information Commissioner (**OAIC**) to support a culture of transparency and privacy compliance within the public sector.

4. The Law Council has confined our review and comments to some key substantive and procedural legal issues. The Law Council considers that the Code as currently drafted can be improved by addressing the issues as set out below.

Highly prescriptive nature of the Code

5. The key substantive issue is the highly prescriptive nature of the Code. This puts it at odds with the principles and outcomes driven nature of the *Privacy Act 1988* (Cth) or its counterpart data protection and privacy related legislation in other countries. Considering that the Code is intended to apply to a wide range of entities that carry out vastly different social and public functions, this move to prescription may be counterproductive. This can be addressed by redrafting the Code to focus on privacy enhancing outcomes and making it clear that the required steps (if any) must be 'reasonable in the circumstances'. The Law Council, primarily through its Privacy Law Committee of the Business Law Section, would be pleased to work with the OAIC and other stakeholders as relevant to assist with appropriate redrafting.

Other comments

6. In addition, the Law Council provides the following comments.

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Clause	Issue	Recomendation
Personal liability of the Privacy Officer (Clause 10 (4))	The Code contemplates that the Privacy Officer will have 'responsibility for ensuring' certain matters. This is at odds with the *Privacy Act 1988* which imposes obligations on the 'agency' as defined. The standard of compliance required under the Act is to 'take steps as are reasonable in the circumstances...'. It is not appropriate to impose personal liability on the Officer in question. Nor is it appropriate to hold an Officer to a higher standard of compliance than the standard applicable to the agency. A requirement to carry out the duties in an independent manner is sufficient.	Remove all references to personal responsibility of the Privacy Officer and replace with a description of the role and that the Privacy Officer may play recognising that compliance is the responsibility of the agency. Article 29 Working Party *Guidelines on Data Protection Officers* provides a useful point of reference. Note that it provides that a DPO is **not** personally responsible for ensuring compliance.
Role of Privacy Champion (Clause 11)	This is potentially at odds with the role of the Privacy Officer.	Remove the reference and replace with a description of the role and qualifications that the Privacy Officer may play as noted above.
Privacy Impact Assessments (Part 3)	PIAs are an effective risk management tool. However, the requirement to publish (clause 13) is at odds with the fact that often an assessment of any detail will contain confidential legal advice or deal with very sensitive commercial or security related matters. This difficulty is magnified by the broad definition of 'projects'. This seems excessive and disproportionate. Clause 15 (2) provides that an agency **may** produce a PIA to the OAIC on	Refine the definition of 'project' by limiting it to reflect the nature of the risks posed. The Law Council recommends that these references are removed or (as a minimum) expressly limited to particular outcomes. *Guidelines on Data Protection Impact Assessment and determining whether* *processing is "likely to result in a high risk" for the*

	request. It will be important that this is not a mandatory obligation. If it were mandatory there would need to be the ability to withhold production on (at least) the same grounds as those in clause 13(1).	*purposes of Regulation 2016/679* issued by the Article 29 Working Party, adopted on 4 April 2017, provides a useful reference  . It notes that, while publishing a PIA may be good practice, it is not a legal requirement under the EU *General Data Protection Regulation.*
Reference to 'Australian Public Service' in the name of the Code	The reference to 'Australian Public Service' in the name of the Code may have the potential to mislead staff of agencies who are not employed under the *Public Service Act 1999* and who do not consider the definition of 'agency' in the *Privacy Act 1988* (Act).	Refer to Agencies in the title of the Code.

7. In the first instance, please contact Olga Ganopolsky, Chair of the Privacy Law Committee of the Business Law Section of Law Council, on 02 8237 9194 or olga.ganopolsky@macquarie.com; or, Dr Natasha Molt, Senior Legal Adviser, at natasha.molt@lawcouncil.asn.au or (02) 6246 3754 if you would like any further information or clarification.

8. Thank you for the opportunity to provide these observations.

Yours sincerely

Fiona McLeod SC
President