Australian Government
Office of the Australian Information Commissioner

November 2017

Privacy agency resource 7

The Australian Government Agencies Privacy Code Checklist

Introduction

The Office of the Australian Information Commissioner (OAIC) has developed this checklist to assist agencies meet their obligations under the Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Code).[1]

The checklist sets out the Code's key requirements, and will help your agency identify the steps it needs to take to meet its obligations under the Code and improve its existing privacy practices.

Agencies will still need to take other steps under Australian Privacy Principle (APP) 1.2 to ensure compliance with all the APPs, such as ensuring that they have implemented practices, procedures and systems to enable the agency to deal with privacy inquiries and complaints.

How do I use the checklist?

When completing this checklist, we would also encourage agencies to review the OAIC's other relevant resources and the text of the Code. This will help ensure that agencies understand the context of the Code requirements and that all requirements are meaningfully met. In particular, reviewing and using the OAIC's Privacy Self-Assessment Tool will help give you a more in-depth understanding of your agency's privacy maturity levels.

- This checklist can be used by the Privacy Champion, Privacy Officer or a person in the agency who has the relevant internal privacy governance expertise and authority.
- Each question in the checklist prompts a 'yes' or 'no' answer.
- Alongside most questions, there are links to relevant OAIC resources that provide guidance and will assist you in meeting specific obligations. There are also examples of answers that highlight the types of responses agencies might include in the checklist. Where your agency has answered 'yes' to a question, you should generally be able to point to a policy, procedural document or system from your agency that supports your response. For example, if you answer that your agency has a privacy management plan, you should be able to link to the relevant documentation.

[1] The Code commences on 1 July 2018.

- If you are unable to identify a document or system that supports your response, you will need to consider creating one for your agency, or updating existing documentation to ensure that your agency's governance arrangements are up to date and comply with the Code requirements.

Question	Y/N	Agency Details/documentation	OAIC Resources
1 – Privacy management plan (section 9 of Code)			
Does your agency have a privacy management plan?		*E.g. We have created a privacy management plan, available at [link].*	The OAIC has developed a Privacy Management Plan template and a Privacy Self-Assessment Tool, to assist agencies assess their current privacy practices and set privacy goals and targets to maintain or improve these practices.
Does your privacy management plan identify specific, measurable privacy goals and targets and set out how your agency will meet its compliance obligations under APP 1.2?		*E.g. We have used the OAIC's Privacy Self-Assessment Tool to identify our privacy goals and targets for the coming financial year. This has been incorporated into our privacy management plan.*	
2 – Privacy Officer (section 10 of Code)			
Does your agency have a Privacy Officer?		*E.g. The Privacy Officer in the Corporate Services Branch is our designated Privacy Officer.* *The Privacy Officer's duties and functions are outlined in a position description for the role, available at [link].*	The OAIC has developed a Privacy Officer Toolkit to assist Privacy Officers to understand and perform their responsibilities.
Has your agency advised the OAIC of your Privacy Officer and their contact details?		*E.g. On 6 December 2017, we advised the OAIC of the name and contact details of our Privacy Officer via email.*	
3 – Privacy Officer functions (section 10 of Code) The below functions are usually performed by the Privacy Officer, but may also be performed by another person or team in your agency, in accordance with your agency's structure and processes.			
Does your agency have a process in place to ensure the proper handling of internal and external privacy enquiries, privacy complaints, and requests for access to and correction of personal		*E.g. The Privacy Officer has developed an internal framework on handling privacy enquiries, complaints and requests for access to and correction of personal information. This framework is used by our service officers that handle enquiries on a day-to-*	The OAIC's Privacy Officer Toolkit will assist agencies to understand and perform their responsibilities, and ensure their Privacy Officer functions are performed as required by section 10(5) of the Code.

Question	Y/N	Agency Details/documentation	OAIC Resources
information made under the Privacy Act?		*day basis and guides their approach to dealing with any privacy issues raised by customers. The framework is available at [link].*	The OAIC's Privacy Officer Toolkit also includes guidance on maintaining a centralised record of personal information.
Does your agency have a process in place to ensure that it maintains a centralised record of the personal information that it holds?		*E.g. We have documented our personal information holdings in an excel spreadsheet, available at [link].* *Ownership and accountability for specific IT systems and databases that hold personal information are clear and documented.*	
Does your agency ensure that the Privacy Officer, or other relevant staff member, assists with the preparation of PIAs, where appropriate?		*E.g. Generally, each separate business area is responsible for preparing PIAs for their specific projects. The Privacy Officer is available to provide guidance on conducting PIAs and to review PIAs when requested by the business area. In the last year, the Privacy Officer has provided guidance on and reviewed 5 PIAs from various project teams.*	
Does your agency ensure that a register of PIAs is maintained?		*E.g. The Privacy Officer works with our records management staff to ensure the register of PIAs is up-to-date.*	
Does your agency have processes in place to ensure that its performance against its privacy management plan is measured and documented?		*E.g. The Privacy Officer is responsible for measuring and documenting our performance by 30 June each year.*	

Question	Y/N	Agency Details/documentation	OAIC Resources
4 – Privacy Champion (section 11 of Code) Please note, an agency's designated Privacy Officer may also be its designated Privacy Champion.			
Has your agency appointed a senior official as the agency's Privacy Champion?		*E.g. The Chief Information Officer is our designated Privacy Champion.*	
5 – Privacy Champion functions (section 11 of Code) The below functions are usually performed by the Privacy Champion, but may also be performed by another person or team in your agency, in accordance with your agency's structure and processes.			
Does your agency promote a culture of privacy within the agency that values and protects personal information?		*E.g. The Privacy Champion harnesses available and relevant opportunities to promote a culture that values and protects privacy. For example, each year during Privacy Awareness Week, the Privacy Champion organises guest speakers involved in the field of privacy to discuss emerging trends and issues.*	
Does your agency ensure the Privacy Champion provides leadership within the agency on broader strategic privacy issues?		*E.g. the Privacy Champion includes privacy issues as a standing agenda item at senior executive meetings. The Privacy Champion is accountable for privacy issues, and, for example, reviews and signs-off on, the agency's data breach response plan.*	
Does your agency ensure the Privacy Champion reviews and/or approves the privacy management plan?		*E.g. the Privacy Champion reviews and approves the privacy management plan, which is drafted by the Privacy Officer. The brief, available at [link], describes the process for review, approval and clearance of the privacy management plan through our senior executive.*	

Question	Y/N	Agency Details/documentation	OAIC Resources
Does your agency have processes in place so that regular reports are provided to the agency's executive on privacy issues arising from the agency's handling of personal information?		*E.g. The Privacy Champion provides bi-annual reports to executive committees on privacy matters.*	
6 – Privacy Impact Assessments (PIAs) (sections 12 and 15)			
Does your agency have a process in place to ensure that PIAs are conducted for all high privacy risk projects?		*E.g. We have developed a clear PIA process for staff to follow, which is integrated into our risk assessment and change-management processes and documented at [link]. PIAs are completed by the relevant project manager in collaboration with the Privacy Officer, where appropriate.*	The OAIC has general guidance on conducting PIAs, such as the *Guide to undertaking privacy impact assessments* and our *Privacy Impact Assessment eLearning program*. The OAIC is developing guidance on the PIA requirements in the Code, including how to assess whether a project is a 'high privacy risk'. The OAIC Privacy Officer Toolkit includes guidance on maintaining and publishing PIA registers.
Does your agency keep a register of all PIAs conducted?		*E.g. We have published an internal PIA register, available on our intranet. The Privacy Officer will co-ordinate updates to the PIA registers as soon as practical after the PIA has been completed, but at the latest, twice a year by 30 June and 31 December.*	
Does your agency publish this register, or a version of the register, on its website?		*E.g. We have published an external PIA register, available at [link].*	
7 – Privacy training and education (section 16)			
Does your agency include appropriate privacy education or training in its staff induction programs?		*E.g. All new staff members are required to complete a privacy module in our induction program, which includes the OAIC's eLearning course on the privacy framework.*	The OAIC is currently developing an eLearning program that will provide an overview of the privacy legislative framework.

Question	Y/N	Agency Details/documentation	OAIC Resources
Does your agency provide appropriate annual privacy education or training to staff members who have access to personal information in the course of performing their duties?		*E.g. Each year, staff who have access to personal information must undertake privacy education, which is run internally by the Privacy Officer.* *Privacy resources are also published on the intranet for staff to access. Contact details of the Privacy Officer are published and promoted to ensure staff know who to contact for any privacy-related questions.*	The OAIC has a number of education and training resources on its website, including: • PIA eLearning program • Privacy in the Australian Public Service • Privacy for Policy Developers and Project Managers. These can be incorporated in to your agency's privacy induction processes, as appropriate.
8 – Proactive reviews of privacy practices (section 17)			
Does your agency proactively review and update its privacy practices (including its privacy policies and privacy notices)?		*E.g. Internal privacy policies and procedures are proactively reviewed on a bi-annual basis by the Privacy Officer to ensure:* • *they take into account feedback, complaints and enquiries we receive from the public* • *compliance with current law* • *they meet community expectations* • *remain relevant to current agency practices, and* • *are responsive to new privacy risks and opportunities.*	
Does your agency monitor compliance with its privacy practices, procedures and systems regularly?		*E.g. This year we engaged external auditors to assess our agency's compliance with our privacy practices, procedures and systems. The auditor's final report – including recommendations – is available at [link].*	

For further information

GPO Box 5218 Sydney NSW 2001 | **P** 1300 363 992 | **E** enquiries@oaic.gov.au

Or visit our website www.oaic.gov.au