Australian Government
Office of the Australian Information Commissioner

Privacy Agency Resource 2

May 2013

Privacy Act reforms—Checklist for APP entities (agencies)

The reforms to the *Privacy Act 1988* introduce the concept of an 'APP entity'. An APP entity can be an agency or an organisation. If your agency is an APP entity you will need to understand the impacts of the reforms before they commence in March 2014.

Use the checklist below to help understand the main changes you may need to make. The checklist is not intended to be a comprehensive list of an APP entity's obligations under the Privacy Act and is not a substitute for an APP entity determining its full obligations under the Privacy Act.

Most of the requirements set out below are outlined in the Australian Privacy Principles (APPs) in the Privacy Act. The APPs are reproduced in *Fact Sheet 17 — Australian Privacy Principles* available on the OAIC website (www.oaic.gov.au). A summary of the APPs is also available on the OAIC website.

There may be other changes you should be aware of depending on your circumstances, eg in the area of credit reporting. More information is available on our website.

The change	Relevant part of the Privacy Act	Consider	Action	Complete?
There are some changes to what constitutes 'personal information' and 'sensitive information' under the Privacy Act.	Section 6 of the Privacy Act	Do we handle 'personal information' or 'sensitive information'?	Review information holdings to determine whether 'personal information' or 'sensitive information' is handled. If 'yes', ensure that APPs are complied with.	
APP entities must take reasonable steps to implement new practices, procedures and systems that will ensure compliance with the new APPs and any registered APP Codes. This may include training staff or establishing procedures to identify and manage privacy risks.	APP 1—Open and transparent management of personal information	What reasonable steps do we need to take to implement new practices, procedures and systems that will ensure compliance with the new APPs and any registered APP Codes?	Review practices, procedures and systems to ensure compliance with the new APPs and any registered APP Codes. Working through the actions in the rest of this checklist will assist APP entities to meet their obligations under this APP.	
APP entities should have an up to date APP privacy policy that is reviewed regularly. The new laws set out some requirements for privacy policies, including requirements for content and availability.	APP 1—Open and transparent management of personal information	Do we have a privacy policy? If so, is it up to date? Does it cover the matters listed in APP 1.4? Is it freely available?	Review or draft APP privacy policy. Make APP privacy policy available in an appropriate form and for free.	

The change	Relevant part of the Privacy Act	Consider	Action	Complete?
APP entities must take reasonable steps to implement new practices, procedures and systems that will ensure the APP entity can handle privacy inquiries and complaints from individuals.	APP 1—Open and transparent management of personal information	What reasonable steps do we need to take to ensure we have practices, procedures and systems in place for handling privacy inquiries and complaints?	Review practices, procedures and systems for handling privacy inquiries and complaints.	
APP entities must give individuals the option to interact with their APP entity anonymously or by using a pseudonym. You may not have to do this if an exception applies in relation to a particular matter.	APP 2—Anonymity and pseudonymity	How can we ensure that individuals can interact with our APP entity anonymously or by using a pseudonym? Is it impracticable to allow this for particular transactions? Are we required or authorised by or under an Australian law or an order of a court/tribunal to deal with individuals who have identified themselves for particular transactions?	Implement practices, procedures and systems to enable your APP entity to allow individuals to interact with you anonymously or by using a pseudonym, unless an exception applies in relation to a particular matter.	
There are new rules that apply to collection practices and notices when collecting personal information and/or sensitive information (such as health information). These rules include proscriptive requirements about the content of notices.	APP 3—Collection of personal and sensitive information APP 5—Notification of collection	Do we collect personal and/or sensitive information? Do we ensure that sensitive information is collected in accordance with the higher protections in APP 3.3? How and what matters do we notify individuals about when collecting their personal or sensitive information?	Review collection practices, procedures and systems, including collection notices.	
There are new rules on how to deal with unsolicited personal information, including when this information must be destroyed or de-identified.	APP 4—Dealing with unsolicited personal information	Do we receive unsolicited personal information? What are our practices, procedures and systems for dealing with unsolicited information?	Review practices, procedures and systems for dealing with unsolicited information.	
There are new rules on when personal information and sensitive information can be used or disclosed.	APP 6—Use or disclosure	For what purposes do we use and disclose personal information and sensitive information?	Review practices, procedures and systems for the use and disclosure of personal information and sensitive information.	

The change	Relevant part of the Privacy Act	Consider	Action	Complete?
There are new rules on when personal information can be used or disclosed for the purpose of direct marketing. These rules primarily apply to organisations, but could apply to agencies in some circumstances.	APP 7—Direct marketing	Does APP 7 apply to us? If so, do we, or do we want to, use or disclose personal information for the purpose of direct marketing? Do we meet any of the exceptions in APP 7 that permit us to do so?	Review direct marketing practices, procedures and systems (including whether individuals are provided with an easy way to opt out of receiving direct marketing).	
There are new rules about an APP entity's accountability for personal information that it has disclosed to overseas recipients.	APP 8—Cross border disclosure	Do we send personal information overseas? Do we have appropriate arrangements with overseas recipients to ensure that personal information that is disclosed overseas is handled in accordance with the APPs?	Review practices, procedures and systems for sending personal information overseas (this may include reviewing outsourcing agreements).	
There are new exceptions to the general prohibition against the adoption, use or disclosure of government related identifiers by organisations. In some circumstances, APP 9 will apply to agencies.	APP 9—Adoption, use or disclosure of government related identifiers	Does APP 9 apply to us? If so, do we collect government related identifiers? Are we permitted to adopt, use or disclose government related identifiers under the new exceptions?	Review practices, procedures and systems for the adoption, use or disclosure of government related identifiers.	
APP entities must take reasonable steps to ensure that the personal information that they collect, use or disclose is up to date, complete and accurate (personal information used or disclosed must also be relevant, having regard to the purpose of the use or disclosure).	APP 10—Quality	What reasonable steps do we need to take to ensure that the personal information we collect, use or disclose is up to date, complete and accurate and relevant for the purpose of the use or disclosure?	Review practices, procedures and systems for ensuring personal information collected, used or disclosed is up to date, complete and accurate and relevant for the purpose of the use or disclosure.	
APP entities must take reasonable steps to protect the personal information they hold from misuse, interference (this may include introducing measures to protect against computer attacks), loss and from unauthorised access, modification or disclosure	APP 11—Security	What reasonable steps do we need to take to ensure that the personal information we collect is protected from misuse, interference, loss and from unauthorised access, modification or disclosure?	Review practices, procedures and systems for ensuring personal information is protected from misuse, interference, loss and from unauthorised access, modification or disclosure (refer to the OAIC's *Guide to information security*).	

The change	Relevant part of the Privacy Act	Consider	Action	Complete?
APP entities are required to take reasonable steps to destroy or de-identify personal information if it is no longer needed for any authorised purpose, subject to some exceptions	APP 11—Security	What reasonable steps do we need to take to ensure personal information is destroyed or de-identified when it is no longer needed for any authorised purpose? Do any exceptions apply to the information we hold?	Review practices, procedures and systems for ensuring personal information is destroyed or de-identified when it is no longer needed.	
There are new rules on how APP entities are to respond to requests for access to and correction of personal information (including timeframes, the manner in which access is to be given, when written reasons are required and charging). There is also a new rule about when an APP entity should correct personal information, even if it has not received a request from an individual.	APP 12—Access APP 13—Correction	What are our processes for responding to requests from individuals for request for access to and correction of personal information? What are our processes for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?	Review practices, procedures and systems for correcting personal information and/or responding to requests from individuals for access to and correction of personal information (including timeframes for responding, the manner in which access is given, the provision of written reasons and charges for access and correction).	

For further information
telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
or visit our website at www.oaic.gov.au