The following table outlines some of the key factors to be considered as RTOs plan for their implementation of systems in line with the APPs. The information 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.

Relevant APP	Key Questions to Consider	Key Actions to Consider
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? Do we have a privacy policy? If so, is it up to date? Does it cover the matters listed in the APPs? Is it freely available? 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 to ensure compliance with the new APPs. Implement an APP privacy policy. Make APP privacy policy available in an appropriate form and for free. Review practices, procedures and systems for handling privacy inquiries and complaints.
APP 2 – Anonymity and pseudonymity APP 3 – Collection of personal and sensitive information APP 5 – Notification of collection	Do we ensure that sensitive and personal information RTOs are required to collect is collected in accordance with the higher protections in the APPs? 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.
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.
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.
APP 7 – Direct marketing	Does APP 7 apply to our RTO? If so do we want to use or disclose personal information for the purpose of direct marketing?	Review direct marketing practices, procedures and systems (including whether individuals are provided with an easy way to opt out of receiving direct marketing).
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).
APP 9 – Adoption, use or disclosure of government related identifiers	Does our RTO collect government related identifiers currently? How will we manage the new USI when it is implemented?	Review practices, procedures and systems for the adoption, use or disclosure of government related identifiers.
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.

Relevant APP	Key Questions to Consider	Key Actions to Consider
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? 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?	Review practices, procedures and systems for ensuring personal information is protected from misuse, interference, loss and from unauthorised access, modification or disclosure. Review practices, procedures and systems for ensuring personal information is destroyed or de-identified when it is no longer needed.
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).