Australian Government

Office of the Australian Information Commissioner

Privacy Essentials Checklist for AML/CTF reporting entities

This checklist is intended to help 'reporting entities' under the AML/CTF Act and authorised agents of reporting entities prepare for key privacy obligations. Changes to AML/CTF obligations for current reporting entities come into effect on **31 March 2026**. AML/CTF obligations commence for tranche 2 entities on **1 July 2026.** The checklist does not cover the entirety of privacy obligations and should be read in conjunction with the OAIC's Privacy guidance for reporting entities under the AML/CTF Act, as well as the Privacy Act, the Australian Privacy Principles guidelines (APP guidelines) and other OAIC resources referred to in this checklist.

☐	**Does your organisation have someone responsible for overall privacy management?**	
	• Guidance	• Resources
	An appropriately resourced role or team should be given accountability for privacy matters in the business.	Chapter 1: APP 1 Open and transparent management of personal information
☐	**Does your organisation have a privacy policy?**	
	• Guidance	• Resources
	Have a privacy policy that describes in plain English what personal information you collect, how you collect that information, and how and why you use that information. See Section A. Implementing good governance to ensure APP compliance and having a privacy policy (APP 1) for more information.	Chapter 1: APP 1 Open and transparent management of personal information. Guide to developing an APP privacy policy What is personal information?
☐	**Does your organisation have a process for recording and considering privacy risks and issues?**	
	• Guidance	• Resources

	Have an established process for reporting privacy risks to the person or team responsible for privacy management. For example, establish a privacy risk register where management is responsible for signing off on privacy risks, include privacy issues as a standing agenda item in team meetings, and undertake a privacy impact assessment of business systems and processes relating to AML/CTF obligations.	Guide to undertaking privacy impact assessments
☐	**Does your organisation have a process for assessing a third party for privacy risk when procuring their solution or service?**	
	• Guidance	• Resources
	Before entering into a contract with a third party, review the terms of the agreement to understand how personal information is collected, handled and stored, and make sure you are satisfied the third party has appropriate processes in place to protect personal information and comply with any obligations it has under the Privacy Act. See Section N. Considerations when engaging a third party provider for more information.	Guide to securing personal information
☐	**Does your organisation take reasonable steps to notify your customers why their personal information is being collected and how it will be used?**	
	• Guidance	• Resources
	Make sure individuals are clearly informed of why their personal information is being collected and how it will be used. However, you should not notify the individual if it would be inconsistent with your AML/CTF tipping off obligations. See Section E. What should customers be notified about? (APP 5) for more information.	Chapter 5: APP 5 Notification of the collection of personal information. Tipping off | AUSTRAC [Template OAIC CDD APP 5 collection notice coming soon]

☐	**Does your organisation only collect the minimum amount of personal information you need to carry out your AML/CTF obligations or your other functions and activities?**	
	• Guidance	• Resources
	You must limit your collection to what is 'reasonably necessary' (under APP 3.2). See Section B. Collecting personal information for AML/CTF Act purposes (APP 3) for more information.	Chapter 3: APP 3 Collection of solicited personal information
☐	**Does your organisation only use and disclose personal information for the purpose you collected it, or where an exception applies?**	
	• Guidance	• Resources
	Generally, under APP 6, you should only use or disclose personal information for the purpose you collected it (the primary purpose). You can't use or disclose personal information for another reason (a secondary purpose) unless an exception applies or you obtain consent. If you are required or authorised to use or disclose the personal information under the AML/CTF Act or AML/CTF Rules, you are permitted to use and disclose it (including without consent). See Section F. Using and disclosing personal information collected for AML/CTF Act purposes (APP 6) for more information.	Chapter 6: APP 6 Use or disclosure of personal information | OAIC
☐	**Does your organisation have an inventory of your personal information holdings?**	
	• Guidance	• Resources
	Have a personal information inventory if it helps you to understand and manage your privacy risks, including keeping track of personal information with multiple purposes.	What is personal information? Rights and responsibilities

	Having an inventory of personal information holdings is best practice under the Privacy Act.	
☐	**Does your organisation have cyber security processes and controls in place to secure personal information you hold for AML/CTF purposes?**	
	• Guidance	• Resources
	You must take reasonable steps to protect personal information you hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This includes technical and organisational measures. Implement cyber security controls on systems that store personal information. Controls could include role-based access controls and multi-factor authentication. See Section I. Securing personal information you hold for AML/CTF purposes (APP 11) for more information.	Chapter 11: APP 11 Security of personal information Small business cyber security guide | Cyber.gov.au
☐	**Does your organisation have a process to identify and manage a data breach?**	
	• Guidance	• Resources
	Assign roles and responsibilities to legal advisers/leadership in responding to a data breach. Include staff, like IT, whose support is necessary not only to prevent a breach, but to identify affected individuals. Document the process. Organisations are responsible for the actions of third party providers when outsourcing their personal information handling. Organisations that implement strong supplier risk management frameworks, together with more robust security measures, can substantially minimise the impact of a data breach in the supply chain.	Data breach preparation and response guide

	See Section K. Have a data breach response plan for more information.	
☐	**Does your organisation have processes in place to ensure that personal information is de-identified or destroyed once it is no longer needed, including for any AML/CTF purposes?**	
	• Guidance	• Resources
	Give a role or team responsibility for regularly destroying personal information your business no longer needs. Instate a register or schedule which tracks when to destroy or de-identify personal information. Enforce data destruction periods. Ensure staff are adequately trained and aware of the need for de-identification or destruction. Audit de-identified data to ensure it remains de-identified. See Section J. Retaining and deleting personal information (APP 11) for more information.	Chapter 11: APP 11 Security of personal information Guide to securing personal information
☐	**Does your organisation have processes for receiving and responding to privacy enquiries, complaints or requests from an individual that relates to their personal information? This should also include access and correction requests.**	
	• Guidance	• Resources
	Organisations should have one or more staff responsible for managing privacy, including a key privacy officer. These staff should be responsible for handling internal and external privacy enquiries, complaints, and access and correction requests in a timely manner. Small-sized service providers may have one person occupying this role at the same time as other operational roles.	Chapter 10: APP 10 Quality of personal information Chapter 12: APP 12 Access to personal information. Chapter 13: APP 13 – Correction of Personal Information

	For more information see: Section H. Ensuring the quality of personal information collected for AML/CTF Act purposes (APP 10) Section L. Providing access to personal information (APP 12) Section M. Correcting clients' Know Your Customer information (APP 13).	Dealing with requests for access to personal information Dealing with requests for correction of personal information Handling privacy complaints
☐	**Does your organisation monitor and address new security risks and threats that may be relevant to the personal information you hold in relation to your AML/CTF obligations?**	
	• Guidance	• Resources
	Stay informed of issues and developments in privacy law and changing legal obligations by subscribing to the OAIC's newsletter for updates. Organisations should monitor and address new security risks and threats. Sign up for alerts from ASD's ACSC and follow the steps it suggests for ensuring online security, including implementing software updates and patches.	Information Matters newsletter Alerts and advisories | Cyber.gov.au
☐	**Does your organisation provide privacy training to your staff on how to appropriately handle and protect personal information in relation to or in connection with their AML/CTF Act obligations?**	
	• Guidance	• Resources
	Staff need to understand the business' privacy obligations and their role in handling personal information in relation to or in connection with their AML/CTF Act obligations correctly. Train staff on privacy and cybersecurity fundamentals. Monitor and enforce training completion.	Research and training resources