galexia

– AUSTRAC –

Enhanced Customer Due Diligence (CDD) Requirements – Privacy Impact Assessment (PIA)

FINAL (v16 31 January 2014)

(GC427)

Contact: Galexia
Level 18, 323 Castlereagh St, Sydney NSW 2000
ACN:097 993 498
Ph: +61 2 9660 1111
www.galexia.com
Email: manage@galexia.com

Document Control

Client

This document has been written for AUSTRAC.

Document Purpose

Galexia is conducting a Privacy Impact Assessment (PIA) for proposed changes to the Customer Due Diligence (CDD) requirements of Australia's Anti-Money Laundering and Counter-Terrorism Financing Framework (the CDD project).

Document Identification

Document title:	Galexia PIA - AUSTRAC CDD PIA (Final)
Document filename:	gc427_austrac_cdd_pia_v17_20140425_FINAL_TO_CLIENT.docx
Document date:	31/01/2014 11:05 AM

Document Production

Client Contacts:	**AUSTRAC** Level 7, Tower A, Zenith Centre 821 Pacific Highway Chatswood NSW 2067 www.austrac.gov.au
Consultant Contact:	**Peter van Dijk** (Managing Director) Galexia – www.galexia.com Level 18, 323 Castlereagh St, Sydney 2000 Phone: +612 9660 1111 Project Email: austrac@galexia.com
Document Authors:	Galexia
Galexia Reference:	GC427

DOCUMENT STATUS

CLIENT-FINAL

COMMERCIAL-IN-CONFIDENCE

Copyright

Contents

1. Executive Summary

Galexia has conducted a Privacy Impact Assessment (PIA) for proposed changes to the customer due diligence requirements of Australia's Anti-Money Laundering and Counter-Terrorism Financing Framework (the CDD project).

This PIA is being conducted in accordance with *PIA Guidelines* issued by the Office of the Australian Information Commissioner. Those Guidelines have not been updated to incorporate the new Australian Privacy Principles (APPs) that apply from March 2014, but Galexia has incorporated the APP requirements into the structure of this PIA.

The broad purpose of this PIA is to assess the impact of the specific reforms being proposed in the CDD project – it is not a general assessment of all privacy aspects of AUSTRAC's work.

Information contained in this PIA is based on:

- Meetings with AUSTRAC;
- A meeting with a representative of the Office of the Australian Information Commissioner (OAIC);
- Documentation related to the proposed CDD reforms, including the FAT-F recommendations and the AUSTRAC/AGD consultation paper;
- Submissions from key stakeholders regarding the proposed CDD reforms;
- AUSTRAC privacy compliance and governance documentation, including privacy policies and relevant record keeping policies;
- Selected samples of the privacy policies and relevant forms used by Reporting Entities;
- Data provided by AUSTRAC on the number and scale of data subjects and information flows that will be affected by the proposed reforms;
- General research and literature review on privacy and identity verification issues;
- Review of relevant privacy legislation; and
- Review of relevant Anti-Money Laundering and Counter-Terrorism Financing legislation.

Our advice in this PIA concentrates on the following areas:

- **Privacy Act compliance**
  This PIA has briefly assessed the CDD reforms against each of the Australian Privacy Principles. Compliance with the APPs will generally be an issue for Reporting Entities, although in some sections we recommend that AUSTRAC considers steps to help ensure Reporting Entities meet their Privacy Act obligations in a consistent manner. The PIA includes some key recommendations relating to APP 1 (Openness and transparency); APP 5 (Notification) and APP 8 (Cross border transfers). The CDD reforms do not have a significant impact on many areas of Privacy Act compliance as the reforms only introduce some new categories of data, rather than completely new processes.
- **Public perceptions**
  This PIA has also identified some public perception issues that are likely to arise in relation to the CDD reforms, and includes some recommendations on education, awareness raising and governance issues.

Our overall conclusion, based on Galexia's understanding of the current CDD project, is that the reforms can proceed without having a significant or negative impact on privacy. The PIA includes a small number of recommendations to help AUSTRAC and Reporting Entities ensure compliance with the APPs, manage public perception and improve public awareness of the reforms, and monitor some key future developments.

Additionally, the PIA has identified that the proposed CDD reforms may have a number of privacy positive aspects as they include measures to deter and prevent identity fraud, and focus on identifying the relevant individuals in complex business structures rather than just the nominated representatives.

2. Privacy Compliance and Perception Summary Table

A number of individual privacy compliance steps have been identified in this assessment and are summarised in the table below.

2.1. Australian Privacy Principle (APP) Compliance Summary

Australian Privacy Principle (APP)	Recommended Privacy Compliance Action	Notes	Recommendation
APP 1 – Openness and Transparency (Refer to *Section 5* at page 17).	**Further action by AUSTRAC recommended.** Public awareness of AUSTRAC / Reporting Entity collection practices	One area where the targets of AUSTRAC collection practices may be unaware of the full extent of collection and use of their information is in relation to Politically Exposed Persons (PEPs). This group may not be aware of the enhanced monitoring by Reporting Entities that occurs, especially where they are a relative or associate of a PEP.	**R1.** This is an area where AUSTRAC could conduct more awareness raising activities and provide clear information on its website and in its publications. However, it is unnecessary to include this information in every public privacy policy, as it is targeted at a very small group.
APP 2 – Anonymity and Pseudonymity	**None**	–	–
APP 3 – Collection of solicited personal information	**None**	–	–
APP 4 – Dealing with unsolicited personal information	**None**	–	–

Australian Privacy Principle (APP)	Recommended Privacy Compliance Action	Notes	Recommendation
APP 5 – Notification (Refer to *Section 9* at page 25).	**Further action by AUSTRAC recommended.** Notice of third party collection	The CDD reforms may lead to a moderate increase in the reliance on third party collection, particularly in relation to PEPs and verification of documents.	**R2.** Reporting Entities may need guidance from AUSTRAC about domestic PEPs and how third party collection should be disclosed in notices. It is clear that a form of notice must be provided, and there do not appear to be any relevant exceptions. This third party collection should be overt, not covert. For third party verification services, Reporting Entities will need to include a short statement notifying customers that any information and documents they provide may be verified by third parties, and this may involve the collection of some personal information from those third parties. Again, this is a clear requirement and no relevant exceptions appear to apply. AUSTRAC should remind Reporting Entities of their need to comply with APP 5.2 (b) when using third party providers. An additional step for AUSTRAC could be to monitor the provision of this information over the first twelve months of implementation of the reforms. AUSTRAC would then be in a position to assess whether it should provide some basic advice or guidance to Reporting Entities on the information that should be included in notices.

Australian Privacy Principle (APP)	Recommended Privacy Compliance Action	Notes	Recommendation
APP 5 – Notification (Refer to *Section 9* at page 25).	**Further action by AUSTRAC recommended.** Notice of consequences for failing to provide information	The CDD reforms include extension of the requirement to collect information on source of funds and source of wealth. This type of inquiry may not be welcomed by all consumers. Under the Privacy Act, if there are any consequences for consumers not providing this information, then these consequences must be disclosed to consumers. For Reporting Entities, this may be one of the greatest challenges under the CDD reforms. If a customer refuses to provide the information, will they be refused service? Will they be reported to AUSTRAC in a suspicious matter report? There are no relevant exceptions to this requirement in the Privacy Act. In practice the exact consequences for not providing this information are difficult to anticipate in advance. There are no proscribed consequences for the refusal to provide specific information. Rather, the whole context of the relationship and transactions will be relevant. Ultimately, the Reporting Entity is required to 'know their customer' and assess the risks given the information that they have on the customer, the type of product or service, the delivery method (i.e. – in person, or online), and other factors.	**R3.** AUSTRAC's role in resolving this issue may be to clarify the exact consequences where individuals refuse to answer questions about source of funds and source of wealth. If there are no specific consequences the issue will not arise. If there are specific consequences then AUSTRAC may need to provide guidance to Reporting Entities on how to comply with APP 5.2 (e). An additional step for AUSTRAC may be to monitor the provision of this information and consumer responses (e.g. inquiries and complaints) over the first twelve months of implementation of the reforms. AUSTRAC would then be in a position to assess whether it should provide some basic advice or guidance to Reporting Entities on the interaction between the AML / CTF requirements on source of funds, and the requirements in APP 5.2 (e).
APP 6 – Use or Disclosure	**None**	–	–
APP 7 – Direct Marketing	**None**	–	–
APP 8 – Cross Border Disclosure (Refer to *Section 12* at page 33).	**Further action by Reporting Entities recommended.** Ensuring compliance with the new APP 8	The CDD reforms may result in Reporting Entities increasing their reliance on information exchanges with third party providers in relation to the identification of PEPs and the verification of information and documents. Some of these organisations are global organisations and personal information may be transferred outside Australia during these information exchanges. This is a trend that was already occurring, prior to the CDD reforms.	**R4.** APP 8 represents a significant change from previous requirements relating to cross border disclosures. At this early stage, Reporting Entities may not have identified all cross border disclosures or how they will ensure compliance with the new rules under APP 8. This will initially be an issue for Reporting Entities, not for AUSTRAC.

Australian Privacy Principle (APP)	Recommended Privacy Compliance Action	Notes	Recommendation
APP 8 – Cross Border Disclosure (Refer to *Section 12* at page 33).	**Further action by AUSTRAC recommended.** Ensuring standards are maintained in cross border transfers	At this early stage it is unclear what steps Reporting Entities are taking to ensure compliance with APP 8.	**R5.** This issue may need to be the subject of a future review by AUSTRAC if the use of global third party verification providers becomes widespread.
APP 9 – Government Related Identifiers	**None**	–	–
APP 10 – Quality of Personal Information	**None**	–	–
APP 11 – Security	**None**	–	–
APP 12 – Access	**None**		–
APP 13 – Correction	**None**		

2.2. Perception Risks

Australian Privacy Principle (APP)	Perception Risk	Notes	Recommendation
APP 5 – Notification (Refer to *Section 9* at page 25).	Potential perception that the Government is collecting a database on source of funds and source of wealth. (This is a 'worst case' scenario of potential perceptions and could be prevented by careful management).	The reality is that Reporting Entities are collecting enough information on source of funds and source of wealth to meet the KYC requirements – no information on these topics is provided to AUSTRAC unless a report is submitted. The risk of the perception of Government intrusion may be increased by Reporting Entities stating that they have to collect this information to meet government requirements, and it may be practically difficult to prevent all Reporting Entities making such statements. It may also be difficult to manage this issue if some Reporting Entities are over eager in questioning clients about source of funds / source of wealth.	**R6.** Firstly, it may be possible to limit the requirement to collect information on source of funds and source of wealth. This could include restricting it to certain types of Reporting Entities or to certain types of transactions. Secondly, AUSTRAC should consider developing some guidance on how the information is collected. For example, if AUSTRAC is satisfied for information to be categorised in very broad categories (e.g. occupation types, investment types) then this may allay consumer fears. Thirdly, in line with other recommendations regarding perceptions and awareness, it may be beneficial to raise public awareness about the use of this information. Although this information may be collected by Reporting Entities as a matter of course, individual's may not understand that only a small fraction of that data is passed on to AUSTRAC or other agencies.

Australian Privacy Principle (APP)	Perception Risk	Notes	Recommendation
APP 5 – Notification (Refer to *Section 9* at page 25).	Potential perception that irrelevant information is being collected (e.g. source of funds and source of wealth for a non-credit product)	The information may not be relevant to the financial product, but it is relevant to the KYC requirements.	**R7.** It may be necessary for AUSTRAC to raise public awareness about the role and relevance of this information.
APP 1 – Openness and Transparency (Refer to *Section 5* at page 17). **APP 5 – Notification** (Refer to *Section 9* at page 25).	Potential surprise that a person is on a list as a PEP or is subject to enhanced monitoring as a PEP.	The concept of Politically Exposed Persons (PEPs), the existence of a list of PEPs, the inclusion of family and associates, and the enhanced monitoring of the accounts of PEPs is not well known by the Australian public. Organisations and individuals that are involved with AML / CTF regulation may be aware of PEPs, but this is a very small group. The broader public, including those people within the definition of PEPs, may not be aware of the concept of PEPs, let alone the details.	**R8.** AUSTRAC may need to consider options for a public awareness campaign, or targeted activities.
Function creep (Refer to *Section18* at page *43*).	Potential expansion of the role of third party service providers	Third party service providers may become an integral part of the AML / CTF system. It is too early, at this stage, to anticipate what services these third parties might provide, how they will obtain and structure their information, and how they will comply with Privacy Act requirements.	**R9.** The development of third party services should be monitored closely. AUSTRAC may need to play a role in ensuring that the sector complies with appropriate standards, and that consumers do not lose their existing access, correction and complaint rights when their personal information is being handled by third parties. If these third parties are based overseas, then there will be an additional need to ensure that standards are not lowered, as APP 8 only provides a very minimal level of protection for information that is transferred offshore.

3. Scope and Methodology

Galexia is conducting a Privacy Impact Assessment (PIA) for the CDD Project.

3.1. Scope

The scope of this PIA is limited to the following items:

In Scope	Out of Scope
• Compliance with the general Australian privacy legal framework	• Compliance with specific sectoral legislation (e.g. banking or gambling related laws)
• Review of key public documents and submissions related to the CDD proposals	• Review of detailed draft legislation or draft legal agreements
• Limited stakeholder consultation	• Extensive stakeholder consultation, or assessment of public attitudes etc.
• Assessment of the *broad* proposals to amend CDD	• Assessment of any *specific technical* proposals to implement the CDD reforms, for example: i. Establishment of national registers to assist Reporting Entities determine beneficial owners; or ii. Establishment of specific information sharing protocols between Reporting Entities.

3.2. PIA Guidelines

This PIA is being conducted in accordance the PIA Guidelines issued by the Office of the Information Commissioner.[1] Those Guidelines have not been updated to incorporate the new Australian Privacy Principles (APPs) that apply from March 2014, but Galexia has incorporated the APP requirements into the structure of this PIA.

3.3. Privacy legislation

This PIA has been written in the light of current Commonwealth privacy legislation – the *Privacy Act 1988*. The Act sets out the Australian Privacy Principles (APPs), which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations. The Act also includes a complaints, audit and enforcement regime.

[The 13 APPs are in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*. They come into force on 12 March 2014.]

[1] http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide

3.4. Specific Anti-Money Laundering and Counter-Terrorism Financing Legislation

AUSTRAC is Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulator. In this role, AUSTRAC educates, monitors and works with regulated entities to improve their compliance with obligations under the:

- *Financial Transaction Reports Act 1988* (FTR Act);
- *Financial Transaction Reports Regulations 1990*;
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act);
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*;
- *Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006*;
- *AML/CTF Rules* (The Rules are a legally binding instrument. The AUSTRAC CEO makes the Rules, but they must be tabled in Parliament, and can be disallowed by Parliament).

In this role AUSTRAC oversees the compliance of Australian businesses (defined as Reporting Entities), including: implementing programs for identifying and monitoring customers and for managing the risks of money laundering and terrorism financing; reporting suspicious matters, threshold transactions and international funds transfer instructions; and submitting an annual compliance report.

3.5. Acronyms in this report

Abbreviation	Expansion
AGD	Attorney-General's Department
AML/CTF	Anti-Money Laundering / Counter Terrorism Funding
APP	Australian Privacy Principle
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDD	Customer Due Diligence
FATF	Financial Action Task-Force
KYC	Know Your Customer
MoU	Memorandum of Understanding
OAIC	Office of the Australian Information Commissioner
PEP	Politically Exposed Person
PIA	Privacy Impact Assessment

4. Customer Due Diligence (CDD) Project Overview

This Privacy Impact Assessment (PIA) covers the proposed changes to the customer due diligence requirements of Australia's Anti-Money Laundering and Counter-Terrorism Financing Framework (the CDD project).

The AML/CTF regime is set out in the AML/CTF Act and the AML/CTF Rules. The Rules provide the detail to the obligations set out in the Act. The most significant amendments concerning the proposed changes to the customer due diligence requirements are contained proposed amendments to the AML/CTF Rules – in Chapters 1 (definitions), 4 (customer identification), and 15 (relating to ongoing customer due diligence). Other changes are also contained in Chapters 5, 8 and 9 (relating to AML/CTF programs), and Chapter 30 (relating to disclosure certificates).

The proposed changes are designed to ensure Australian law is consistent with the Financial Action Task Force (FATF) recommendations, which are recognised as the global standard. Global consistency is considered to be particularly important, as money laundering, terrorism financing and financing of proliferation of weapons of mass destruction are trans-national problems which requires a coordinated approach to combat. Australia is a founding member of FATF. Australia currently holds the position of Vice President and will assume the Presidency in 2014.

One of the core recommendations concerning the proposed changes relates to the identification of customers, and this is an area where Australia's regime has been subject to international criticism. It is considered that there is too much discretion afforded to Reporting Entities in Australia, and that this is now out of step with equivalent jurisdictions around the world, including the United Kingdom, the United States, Canada and New Zealand.

The Australian AML/CTF regime requires that Reporting Entities 'know their customer' and assess the risks of doing business with that customer. The AML/CTF Rules set out safe harbour 'minimum' requirements in relation to identification of customers. However, each Reporting Entity would need to develop their processes, systems and controls, taking into account the risks associated with their products, delivery channels and geographical risk factors, and collect as much information as necessary in the circumstances. As noted above, this has been criticised by FATF, noting that the FATF standards require prescription of certain aspects of identification, and that these must be required by law. These reforms bring Australia's regime into line with the FATF standards in relation to customer due diligence. While there will be greater prescription regarding the collection of identification information, in many cases it is understood that this will reflect and codify existing practices of Reporting Entities. It will clarify expectations for both businesses and individuals, and it will create more consistency.

In general terms, the proposed reforms extend the requirements in relation to beneficial ownership of a customer; introduces the explicit requirement to identify the settlor of a trust; amends the requirements in relation to Politically Exposed Persons (PEPs); and introduces a clear requirement to keep customer information up to date. Additionally, a Reporting Entity will be required to understand the control structure of a customer, and will need to understand the customer's business or occupation and the source of funds. Some of the proposed changes are of a minor technical nature. However, some of the proposed changes involve an increase in the amount and type of information being collected by Reporting Entities (and potentially shared with AUSTRAC and other agencies).

The proposed reforms are intended to equip Reporting Entities with the information they need to manage their risks, and facilitate information flows to law enforcement to combat organised crime, tax evasion, money laundering and the financing of terrorism. The reforms are aimed at reducing the ability for a person to hide behind the corporate veil to conduct these illegal activities. The reforms will also help to protect Australia's economic interests as it is important to ensure Australia's financial system is hostile to money laundering and terrorism financing.

Under the proposed reforms, AUSTRAC's role and processes are not changing. However, new requirements are being introduced for Reporting Entities, including requirements relating to the collection of information.

4.1. Beneficial owners

The proposed reforms extend the requirements to identify and verify the beneficial owner of a customer, which currently apply to a customer that is a company, to other types of legal persons or legal arrangements (such as a trust, partnership or association). As Australia does not have open registers for many types of business structure (e.g. trusts), it is likely that these requirements will be met by requesting clients for additional information and documentation.

For some complex business structures a type of 'self-certification' disclosure certificate can be used, but for most structures original documents will need to be provided. Reporting Entities are required to verify this information, and it is likely that verification services will be provided by third parties.

Reporting Entities are also required to take steps to make sure that documents are not stolen or forgeries. Again, this task may rely on verification services provided by third parties.

4.2. Source of funds

The proposed reforms require Reporting Entities to make reasonable inquiries regarding the source of funds and source of wealth of their customers, and to use this information on a risk basis to identify suspicious activity.

This requirement must now be included in the Reporting Entity's risk based AML/CTF procedures. For many organisations this information will already be captured and verified (for example, the occupation of clients and the type of business will be known to most financial institutions, or public and listed companies on the ASX).

The obligation on the Reporting Entity is for them to have a reasonable understanding of who their customer is and who controls the account, which is informed by asking the customer for information directly and monitoring the activity on the account. The source of a customer's funds, and whether this matches with the Reporting Entity's understanding of the customer, will inform the Reporting Entity's risk assessment.

4.3. Politically Exposed Persons (PEPs)

The proposed reforms also expand and clarify existing requirements for conducting enhanced monitoring on Politically Exposed Persons (PEPs), including a new emphasis on enhanced monitoring of domestic PEPs. The reforms introduce a definition of PEPs, consistent with the FATF requirements, which includes politicians, senior officials, the senior management of government owned agencies etc. It also includes their immediate families and close associates.

The majority of Reporting Entities already have systems in place to help them identify foreign PEPs. This is usually a twofold approach: Firstly, a PEP may be identified or self-identified through a question on account opening; and secondly the names of clients may be 'washed' against a list of PEPs provided by a third party (such as WorldCheck).

Even after these two steps, a Reporting Entity may still be unaware that they have a customer that is a PEP. This is generally acceptable as long as they have reasonable processes in place.

At this stage there is no list of domestic (Australian) PEPs available, but many domestic PEPs will already be included in the global lists (e.g. WorldCheck) as these will be foreign PEPs for Reporting Entities based in other countries.

4.4. Use and disclosure of information by AUSTRAC

Reporting Entities provide routine information to AUSTRAC on cash transactions above a certain value (currently AUD 10,000) and on international funds transfers of any amount. This information must be reported to AUSTRAC.

Reporting Entities are also required to make a suspicious matter report where they believe that it is appropriate. AUSTRAC publishes extensive guidance on when an organisation should submit a suspicious matter report.

It is unlikely that the additional information collected under the CDD reforms will be included in any routine reports to AUSTRAC. However, there will be many instances where the new information collected under the reforms will just remain with the Reporting Entity.

Overall AUSTRAC receives over 80 million reports per year, and most data is retained for 8 years. Only a small fraction of this data will include new information resulting from the CDD reforms – the bulk of this collection is not affected by the reforms.

In 2013-13 AUSTRAC received 45,000 suspicious matter reports. Some suspicious matter reports are held for longer periods.

AUSTRAC analyses all of this data and develops intelligence assessments. These assessments can then be shared with designated State and Commonwealth agencies. In some circumstances the intelligence assessments can be shared with international agencies, subject to a Memorandum of Understanding (MoU) with the recipient country. Once again, this sharing of information is not significantly affected by the CDD reforms.

5. APP 1. Open and transparent management of personal information

5.1. The Law

Australian Privacy Principle 1 — Open and transparent management of personal information

[Relevant Extract:]

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

5.2. CDD Reform Compliance Assessment with APP 1.

Openness and transparency (APP 1)	Compliant	Relevant Exception	Notes
A. Does AUSTRAC provide a public privacy policy?	Yes	–	The AUSTRAC privacy policy is not as important in the CDD context as the Reporting Entity privacy policy. The rest of this table concentrates on Reporting Entities.
B. Do Reporting Entities provide a public privacy policy?	Yes		No significant change from existing requirements.
C. Does the Policy include the kinds of personal information that the entity collects and holds;	Yes	–	No significant change from existing requirements.

Openness and transparency (APP 1)	Compliant	Relevant Exception	Notes
D. Does the Policy include how the entity collects and holds personal information;	Yes	–	No significant change from existing requirements.
E. Does the Policy include the purposes for which the entity collects, holds, uses and discloses personal information;	Yes	–	No significant change from existing requirements.
F. Does the Policy include how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;	Yes	–	No significant change from existing requirements. (Note: The AUSTRAC privacy policy is also relevant for access rights).
G. Does the Policy include how an individual may complain about a breach of the APPs / registered code, and how the entity will deal with such a complaint;	Yes	–	No significant change from existing requirements. (Note: The AUSTRAC privacy policy is also relevant for complaints).
H. Does the Policy include whether the entity is likely to disclose personal information to overseas recipients;	Yes	–	No significant change from existing requirements.
I. Does the Policy include if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.	Yes	–	No significant change from existing requirements.
J. Overall, will existing Reporting Entity privacy policies contain sufficient information to cover the CDD reforms?	Yes	–	Overall there are no significant changes in the CDD reforms that would require an update to public privacy policies.
K. Overall, will the existing AUSTRAC privacy policy contain sufficient information to cover the CDD reforms?	Yes	–	The existing AUSTRAC privacy policy is a very brief document that provides key contacts and information on access and complaints. It has sufficient information to cover the CDD reforms.
L. Has AUSTRAC taken appropriate additional steps to ensure that the public is generally aware of its collection practices?	Further action by AUSTRAC required.	–	There is one area where the targets of AUSTRAC collection practices may be unaware of the full extent of collection and use of their information – Politically Exposed Persons (PEPs). This group may not be aware of the enhanced monitoring by Reporting Entities that occurs, especially where they are a relative or associate of a PEP. This is an area where AUSTRAC could conduct more awareness raising activities and provide clear information on its website and in its publications. However, it is unnecessary to include this information in every public privacy policy (of AUSTRAC and Reporting Entities), as it is targeted at a very small group.

5.3. APP 1. Finding

The Privacy Commissioner has always advised agencies and organisations to have a 'no surprises' approach to the collection of personal information. This can usually be addressed by including clear statements in a public privacy policy, but in some circumstances additional steps may be required.

Overall, the CDD reforms do not have a significant impact on APP 1 (Open and transparent management of personal information). The privacy policies available from AUSTRAC and Reporting Entities already summarise the main types of information collected.

However, the requirement to undertake enhanced monitoring of Politically Exposed Persons (PEPs) in Australia is generally not included in these statements, and it is unlikely that most PEPs are aware of this activity. The definition of PEPs is very broad, and includes family members and associates of PEPs.

Some additional effort will be required to ensure that the enhanced monitoring of PEPs is also done in an open and transparent manner.

An amendment to the public privacy polices of either AUSTRAC or the Reporting Entities may not be an appropriate response, as the target group is very small and niche. Instead, this issue may require a targeted awareness raising campaign.

6. APP 2. Anonymity and Pseudonymity

6.1. The Law

Australian Privacy Principle 2 — Anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

6.2. CDD Reform Compliance Assessment with APP 2.

Anonymity and Pseudonymity (APP 2)	Compliant	Relevant Exception	Notes
A. Where lawful and practicable, are individuals given the option of: not identifying themselves OR identifying themselves with a pseudonym?	Yes (a relevant exception applies)	Identification is required by the AML / CTF legal framework in all cases.	This issue is easily addressed by the exception.

6.3. APP 2. Finding

APP 2 is not applicable as the CDD project relies entirely on identity and identity verification, and the collection of information in relation to the true identity of the customer is a legal requirement under the AML / CTF legal framework.

7. APP 3. Collection of solicited personal information

7.1. The Law

Australian Privacy Principle 3 — Collection of solicited personal information

[Relevant Extract:]

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

….

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

7.2. OAIC Guidelines

The *PIA Guidelines* issued by the OAIC contain a set of hints and risks under the category of personal information to be collected.

The Privacy Risks they have identified include:

- Collecting unnecessary or irrelevant personal information, or intrusive collection;
- Bulk collection of personal information, some of which is unnecessary or irrelevant;
- Individuals unaware of the collection or its purpose; and
- Covert collection is generally highly privacy invasive, and should only occur under prescribed circumstances.

In addition to these risks, the collection of personal information should generally be kept to a minimum and personal information should normally be collected from the data subject.

7.3. CDD Reform Compliance Assessment with APP 3.

Collection of solicited information (APP 3)	Compliant	Relevant Exception	Notes
AGENCIES (AUSTRAC) **A.** Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	Yes	–	AUSTRAC has shown that the additional information being collected in the CDD reforms is necessary for its detection and analysis of AML / CTF related crime, especially where the perpetrators are using complex corporate structures to hide their true identity, ownership and control.
ORGANISATIONS (Reporting Entities) **B.** Is collected information reasonably necessary for one or more of the entity's functions or activities?	Yes	–	Reporting Entities are required by law to meet the KYC requirements – the CDD reforms are part of this requirement.
C. Is NO sensitive information about an individual collected (unless a relevant exception applies)?	Yes	Although some sensitive information is collected in relation to PEPs, the exception in APP 3.4 (A) applies, as the collection is specifically required by the AML / CTF legal framework.	Generally, no sensitive information is collected. In the rare circumstances where it is collected (in relation to PEPs), it is covered by a relevant exception.
D. Is personal information collected only by lawful and fair means?	Yes	–	No significant change from existing requirements.
E. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	Yes	Although some information is collected from third parties, the exceptions in APP 3.6 apply, as the collection from third parties (e.g. for identifying PEPs or for document verification purposes) is specifically required by the AML / CTF legal framework, and it would be unreasonable or impracticable to rely only on information provided by the client.	Generally, most information is collected directly from the individual. However, some information is collected from third parties in order to identify PEPs and to verify documents that are presented by clients. These circumstances are covered by the exceptions in the Act.

7.4. APP 3. Finding

Both AUSTRAC and Reporting Entities are collecting information that is required by the AML / CTF legal framework.

Generally, the information is not sensitive information. In the rare circumstances where it is sensitive information (for example in relation to the identification of PEPs), this is a specific requirement of the AML / CTF legal framework, and is therefore covered by relevant exceptions in the Privacy Act.

The majority of personal information is being collected directly from the individual concerned. However, the CDD reforms also require Reporting Entities to identify PEPs, and while this generally involves collecting the information directly from the individual who is a PEP, this may sometimes involve the confirmation or verification of this information by reference to lists provided by third parties. In some cases, such as where the individual customer becomes a PEP after becoming a customer (and as such could not have provided the information at the time of the commencement of the business relationship) the individual's status as a PEP will be collected directly from the third party service provider. This activity is covered by an exception in the Privacy Act that allows organisations to collect information from third parties where it would be unreasonable or impracticable to collect the information from the individual.

The CDD reforms also require Reporting Entities to verify some of the information that they collect from individuals, and to take steps to ensure that documents are not stolen or forged. Again, this would be impossible to achieve without collecting some further information from third parties. This activity is covered by an exception in the Privacy Act that allows organisations to collect information from third parties where it would be unreasonable or impracticable to collect the information from the individual. The activity may also be covered by the exception in the Act for *consent*, but relying on consent may introduce additional compliance burdens, and the earlier exception is sufficient.

8. APP 4. Dealing with unsolicited personal information

8.1. The Law

Australian Privacy Principle 4 — Dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

8.2. CDD Reform Compliance Assessment with APP 4.

Dealing with unsolicited information (APP 4)	Compliant	Relevant Exception	Notes
A. Are there circumstances in which either AUSTRAC may receive unsolicited personal information?	Yes	–	AUSTRAC has advised that it does receive unsolicited 'tip offs' from the public regarding suspected AML / CTF activity.
B. Does AUSTRAC have a policy in place for managing unsolicited personal information in accordance with the Privacy Act?	Yes	–	APP 4 is a new requirement, and AUSTRAC has advised that it has a policy and standard operating procedure in place for staff to deal with the receipt of unsolicited information, and the appropriate considerations as to whether the information can be retained and used. It is considered that this meets the requirements of APP 4.

8.3. APP 4. Finding

APP 4 is not particularly relevant to the CDD reforms. However, as this is a new requirement, it may be useful to review AUSTRAC policy and procedure on 'tip-offs' to ensure compliance with APP 4.

Reporting Entities may also receive unsolicited personal information, but that issue is beyond the scope of this PIA.

9. APP 5. Notification of the collection of personal information

9.1. The Law

Australian Privacy Principle 5 — Notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

9.2. CDD Reform Compliance Assessment with APP 5.

Notification (APP 5)	Compliant	Relevant Exception	Notes
A. Does the entity provide notice of its identity and contact details?	Yes	–	No significant change from existing requirements.
B. Does the entity provide notice of third party collection? (if relevant)	Further action by Reporting Entities recommended	–	The CDD reforms may lead to a moderate increase in the reliance on third party collection, particularly in relation to PEPs and verification of documents. For domestic PEPs, Reporting Entities may need some guidance from AUSTRAC about how this collection should be disclosed in notices. It is clear that some form of notice must be provided, and there do not appear to be any relevant exceptions. This third party collection should be overt, not covert. For third party verification services, Reporting Entities will need to include a short statement notifying customers that any information and documents they provide may be verified by third parties, and this may involve the collection of some personal information from those third parties. Again, this is a clear requirement and no relevant exceptions appear to apply. AUSTRAC's minimum role may be to remind Reporting Entities of their need to comply with APP 5.2 (b) when using third party providers. An additional step for AUSTRAC may be to monitor the provision of this information over the first twelve months of implementation of the reforms. AUSTRAC would then be in a position to assess whether it should provide some basic advice or guidance to Reporting Entities on the information that should be included in notices.
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	Yes	–	No significant change from existing requirements.
D. Does the entity provide notice of the purpose of collection?	Yes	–	Currently, Reporting Entities include sufficient notice of the purpose of collection under the existing KYC rules. However, the CDD reforms place a new emphasis on verifying the source of funds and source of wealth. This may lead to a moderate increase in the amount of personal information collected regarding the financial affairs of individuals. It is unclear, at this early stage, whether Reporting Entities will notify customers that these new questions are for the purpose of complying with the AML / CTF legal framework – this seems a likely outcome. This issue is closely related to the next requirement.

Notification (APP 5)	Compliant	Relevant Exception	Notes
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	Further action by both AUSTRAC and Reporting Entities recommended	–	The CDD reforms include expansion of the requirement to collect information on source of funds and source of wealth. This type of inquiry may not be welcomed by all consumers. Under the Privacy Act, if there are any consequences for consumers not providing this information, they must be disclosed to consumers. For Reporting Entities, this may be one of the greatest challenges under the CDD reforms. If a customer refuses to provide the information, will they be refused service? Will they be reported to AUSTRAC in a suspicious matter report? There are no relevant exceptions to this requirement in the Privacy Act. In practice the exact consequences for not providing this information are difficult to anticipate in advance. There are no proscribed consequences for the refusal to provide specific information. Rather, the whole context of the relationship and transactions will be relevant. Ultimately, the Reporting Entity is required to 'know their customer' and assess the risks, given the information that they have about the customer, the type of product or service, the delivery method (i.e. – in person, or online), and other factors. AUSTRAC's role here may be to clarify the exact consequences where individuals refuse to answer questions about source of funds and source of wealth. If there are no specific consequences the issue will not arise. If there are specific consequences then AUSTRAC may need to provide guidance to Reporting Entities on how to comply with APP 5.2 (e). An additional step for AUSTRAC may be to monitor the provision of this information and consumer responses (e.g. inquiries and complaints) over the first twelve months of implementation of the reforms. AUSTRAC would then be in a position to assess whether it should provide some basic advice or guidance to Reporting Entities on the interaction between the AML / CTF requirements on source of funds, and the requirements in APP 5.2 (e).
F. Does the entity provide notice of any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected?	Yes	–	No significant change from existing requirements.
G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	Yes	–	No significant change from existing requirements.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	Yes	–	No significant change from existing requirements.

Notification (APP 5)	Compliant	Relevant Exception	Notes
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	Yes	–	No significant change from existing requirements.

9.3. APP 5. Finding

APP 5 presents some challenges for the implementation of the CDD reforms.

Firstly, AUSTRAC recognises that the CDD reforms are likely to result in an increased reliance on the collection and verification of information from third party service providers. The identification of PEPs and the verification of business structure information and documentation will be very difficult without the assistance of third party sources.

Although it is theoretically possible to have data 'washed' and 'verified' by third parties without actually collecting any new personal information, such processes are slow and cumbersome, and they may 'leak' personal information unintentionally. It is more realistic to assume that the third parties will indeed be providing some personal information.

APP 5 requires Reporting Entities to inform their customers about any third party collection. There are no relevant exceptions to this requirement. Compliance with APP 5 may be difficult for Reporting Entities, and they are unlikely to implement the requirements consistently (or at all). There may be a role for AUSTRAC to ensure that Reporting Entities are reminded of the need to comply with APP 5.2 (b) when using third party providers.

Also, APP 5 requires Reporting Entities to inform their customers of any consequences if some information is not provided. This is potentially a significant issue. The CDD reforms require Reporting Entities to collect (amongst other things) information on source of funds and source of wealth. The proposed CDD reforms (including the Issues Paper and the proposed revisions to the Rules) have drawn attention to this requirement, and many of the submissions in response to the Issues Paper raised concerns about the requirement to make inquiries about source of funds and source of wealth.

This type of collection may reasonably lead to queries, or possibly confusion, and may even result in complaints attributed to perceived unwarranted intrusion. Importantly, if there are any consequences for consumers not providing this information, they must be disclosed to consumers.

At this stage it is unclear whether there *are* any consequences. Will customers be refused service? Will customers be reported to AUSTRAC in a suspicious matter report? In practice the exact consequences for not providing this information are difficult to anticipate in advance. There are no proscribed consequences for the refusal to provide specific information. Rather, the whole context of the relationship and transactions will be relevant. Ultimately, the Reporting Entity is required to know their customer and assess the risks given the information that they have on the customer, the type of product or service, the delivery method (i.e. – in person, or online), and other factors.

As there are no relevant exceptions to this requirement in the Privacy Act, the notices may have to incorporate a short statement on the consequences for not providing information on source of funds or source of wealth.

It is recommended that AUSTRAC provide some advice or guidance to Reporting Entities on the information that should be included in notices, and given the context, this may appropriately take the form of advice to customers on the potential collection of information from third party sources, and potential consequences for failure to provide adequate CDD information overall.

It is also important to note that if there *are* serious consequences for not providing this information, such as refusal of service, then this may have broader ramifications. Any serious consequences may have an impact on the public perception of the overall package of AML / CTF laws. The requirement may also drive some consumers to change their behaviour or use alternative services. It may be difficult to anticipate the exact consequences of this reform.

AUSTRAC may need to investigate additional steps to manage this issue.

Firstly, it may be possible to limit the requirement to collect information on source of funds and source of wealth. This could include restricting it to certain types of Reporting Entities or to certain types of transactions.

Secondly, AUSTRAC should consider developing some guidance on how the information is collected. For example, if AUSTRAC is satisfied for information to be categorised in very broad categories (e.g. occupation types, investment types) then this may allay consumer fears.

Thirdly, in line with other recommendations regarding perceptions and awareness, it may be beneficial to raise public awareness about the use of this information. Although this information may be collected by Reporting Entities as a matter of course, individual's may not understand that only a small fraction of that data is passed on to AUSTRAC or other agencies. (This perception will only be exacerbated where Reporting Entities advise clients that they are collecting this information to meet Government requirements).

Some further work may be required to manage the interaction between APP 5 and the AML / CTF requirements to collect personal information, in particular in relation to source of funds and source of wealth.

10. APP 6. Use or disclosure of personal information

10.1. The Law

Australian Privacy Principle 6 — Use or disclosure of personal information

[Relevant Extract:]

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

10.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of purpose, use and disclosure.

The Privacy hints they have identified include:

— No surprises! Use personal information in ways that are expected by the individual

— No surprises! Tell the individual about disclosures

The Privacy Risks they have identified include:

— Using personal information for unexpected secondary purposes

— Unnecessary or unexpected data linkage

— Unexpected disclosures can lead to privacy complaints

10.3. CDD Reform Compliance Assessment with APP 6.

Use or Disclosure (APP 6)	Compliant	Relevant Exception	Notes
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	Yes	–	No significant change from existing requirements.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)?	Yes	The exception in APP 6.2 (b) will apply in all relevant circumstances.	For the CDD reforms, some of the new categories of information will be disclosed to AUSTRAC. This will be in accordance with the AML / CTF legal framework, and will be clearly covered by the exceptions in the Privacy Act.
C. Is any biometric information only disclosed in accordance with Clause 6.3 and the relevant OAIC Guidelines?	–	–	Not relevant.
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	Yes	–	No significant change from existing requirements.

10.4. APP 6. Finding

The CDD reforms do not have a significant impact on APP 6. There are no new 'purposes' under the reforms, just new categories of data.

Reporting Entities will be using and disclosing the new data under the relevant exception in the Privacy Act (required or authorised by or under an Australian law).

11. APP 7. Direct marketing

Australian Privacy Principle 7 — Direct marketing is not relevant to the CDD reform project.

12. APP 8. Cross-border disclosure of personal information

12.1. The Law

Australian Privacy Principle 8 — Cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For ***permitted general situation***, see section 16A.

12.2. CDD Reform Compliance Assessment with APP 8.

Cross-border Disclosure (APP 8)	Compliant	Relevant Exception	Notes
A. Has the entity identified all relevant cross border disclosure of personal information?	Further action by Reporting Entities recommended	–	The CDD reforms may result in Reporting Entities increasing their reliance on information exchanges with third party providers in relation to the identification of PEPs and the verification of information and documents. Some of these organisations are global organisations and personal information may be transferred outside Australia during these information exchanges. This is a trend that was already occurring prior to the CDD reforms. APP 8 represents a significant change from previous requirements relating to cross border disclosures. At this early stage, Reporting Entities have not identified all cross border disclosures or how they will ensure compliance with the new rules under APP 8. This will initially be an issue for Reporting Entities, not for AUSTRAC.
B. Has the entity taken such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs? (unless a relevant exception applies)	Further action by Reporting Entities recommended	–	At this early stage it is unclear what steps Reporting Entities are taking to ensure compliance with APP 8. This issue may need to be the subject of a future review by AUSTRAC if the use of global third party providers becomes widespread.

12.3. APP 8. Finding

AUSTRAC engages in some limited international exchanges of information with other relevant AML / CTF agencies (about 200 per year). These are all subject to formal MoUs with the counterpart agency, and the exchanges are clearly covered by several exceptions in APP 8 that may be relevant.

Reporting Entities are also likely to engage in some cross border transfer of information. The CDD reforms may prompt inquiries about PEPs, foreign trusts, etc. Some of this data will have to be verified by third party providers, which are often global organisations. This is a small part of an ongoing trend towards the globalisation of inquiries and verification services for personal information.

APP 8 requires reporting entities to take reasonable steps to ensure the protection of personal information when it is overseas, or to rely on a relevant exception. Although APP 8 introduces new requirements, it still sets a fairly low bar for overall compliance, so most Reporting Entities should be able to comply with the requirements with ease.

At this early stage, it is difficult to anticipate the extent of reliance on cross border transfers following the CDD reforms, and the management of these transfers under the new requirements in APP 8. This issue may need to be reviewed at a future date to ensure that privacy standards are not lowered by the extensive use of offshore providers. APP 8 may not be the best benchmark to use to assess this issue – if extensive amounts of personal financial information are being transferred offshore as a result of the CDD reforms and other developments in the AML / CTF sector, AUSTRAC may have concerns that go beyond simple compliance with APP 8.

13. APP 9. Adoption, use or disclosure of government related identifiers

Australian Privacy Principle 9 — Adoption, use or disclosure of government related identifiers is not relevant to the CDD reforms.

14. APP 10. Quality of personal information

14.1. The Law

Australian Privacy Principle 10 — Quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

14.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of data quality.

The Privacy Risks they have identified include:

— Retaining personal information unnecessarily

— Making decisions based on poor quality data

14.3. CDD Reform Compliance Assessment with APP 10.

Data Quality (APP 10)	Compliant	Relevant Exception	Notes
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **collected** is accurate, up-to-date and complete?	Yes	–	The CDD reforms include requirements for Reporting Entities to review and update the information that they hold on clients. These requirements are likely to strengthen and improve the quality assurance process that Reporting Entities have in place.
B. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **that the entity uses or discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant?	Yes	–	The CDD reforms include requirements for Reporting Entities to review and update the information that they hold on clients. These requirements are likely to strengthen and improve the quality assurance process that Reporting Entities have in place.

14.4. APP 10. Finding

The CDD reforms are likely to have a positive impact on the quality of data that is collected, used and disclosed by Reporting Entities. For example, the CDD reforms include requirements for Reporting Entities to review and update the information that they hold on clients, rather than relying only on the information originally submitted (e.g. during account opening).

The CDD reforms also require Reporting Entities to verify documents, to check for forgeries and stolen documents, and to search 'behind the corporate veil' for the real owners and controllers of businesses. These reforms mean that the quality of data disclosed to AUSTRAC and other agencies should also improve – it is more likely to target the real perpetrators rather than identifying the 'nominal' parties who may appear on corporate documents.

Improvements in the quality of data are a privacy positive aspect of the reforms.

15. APP 11. Security of personal information

15.1. The Law

Australian Privacy Principle 11 — Security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

15.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of security.

The Privacy Risks they have identified include:

— Unauthorised internal and external access and use.

15.3. CDD Reform Compliance Assessment with APP 11.

Security (APP 11)	Compliant	Relevant Exception	Notes
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss?	Yes	–	No significant change from existing requirements.
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	Yes	–	No significant change from existing requirements.
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	Yes	–	No significant change from existing requirements.
D. Will detailed access trails be retained and scrutinised for security breaches?	Yes	–	No significant change from existing requirements.
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	Yes	The AML / CTF legal framework requires some key data to be kept for long periods.	No significant change from existing requirements.

Security (APP 11)	Compliant	Relevant Exception	Notes
F. Is personal information de-identified as soon as possible?	Yes	The AML / CTF legal framework requires some key data to be kept for long periods.	No significant change from existing requirements.

15.4. APP 11. Finding

The CDD reforms have no significant impact on security requirements.

16. APP 12. Access to personal information

16.1. The Law

Australian Privacy Principle 12—access to personal information

[Relevant extract]

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

….

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

16.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of personal information to be collected.

The Privacy hints they have identified include:

— Getting access to personal information should be clear and straightforward.

The Privacy Risks they have identified include:

— Inaccurate information can cause problems for agencies and individuals

16.3. CDD Reform Compliance Assessment with APP 12.

Access (APP 12)	Compliant	Relevant Exception	Notes
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	Yes	–	No significant change from existing requirements.
AGENCIES **B.** If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply in FOI legislation)	Yes	–	No significant change from existing requirements.

Access (APP 12)	Compliant	Relevant Exception	Notes
ORGANISATIONS **C.** If an organisation holds personal information about an individual, does the organisation, on request by the individual, give the individual access to the information? (unless relevant exceptions in the Privacy Act apply)	Unclear	The general Privacy Act exception for publicly available information may be relevant for PEP lists.	Reporting Entities have appropriate access provisions in place. However, there may be a question about the lists of PEPs that have been developed by third party providers. Do individuals have access rights to these lists? (This issue is outside the scope of the current PIA).
AGENCIES **D.** Will information be provided within 30 days?	Yes	–	No significant change from existing requirements.
ORGANISATIONS **E.** Will information be provided within a reasonable period?	Yes	–	No significant change from existing requirements.
AGENCIES **F.** Will accessing personal information be provided at no cost?	Yes	–	No significant change from existing requirements.
ORGANISATIONS **G.** Will the costs incurred in accessing personal information be reasonable?	Yes	–	No significant change from existing requirements.

16.4. APP 12. Finding

The CDD reforms are not particularly relevant to access rights, as the reforms make no changes in this area. However, the increased use of PEP lists may raise an issue about whether an individual can access the PEP list if they believe they are on it. (This issue is outside the scope of this PIA).

17. APP 13. Correction of personal information

17.1. The Law

Australian Privacy Principle 13 — Correction of personal information

[Relevant extract]:

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

17.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of personal information to be collected.

The Privacy hints they have identified include:

— Getting access to personal information should be clear and straightforward.

The Privacy Risks they have identified include:

— Inaccurate information can cause problems for everyone!

17.3. CDD Reform Compliance Assessment with APP 13.

Correction (APP 13)	Compliant	Relevant Exception	Notes
UPON REQUEST **A.** Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	Yes	The general Privacy Act exception for publicly available information may be relevant for PEP lists.	Reporting Entities have appropriate correction provisions in place. However, there may be a question about the lists of PEPs that have been developed by third party providers. Do individuals have access and correction rights to these lists? (This issue is outside the scope of this PIA)
UPON LEARNING OF INACCURACIES **B.** Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	Yes	–	No significant change from existing requirements.
UPON REQUEST ONLY **C.** Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	Yes	–	No significant change from existing requirements.
UPON REQUEST ONLY **D.** Will the entity take such steps as are reasonable in the circumstances to associate a statement by the data subject that the accuracy of the information is challenged in such a way that will make the statement apparent to users of the information?	Yes	–	No significant change from existing requirements.
AGENCIES **E.** Will requests for corrections be addressed within 30 days?	Yes	–	No significant change from existing requirements.
ORGANISATIONS **F.** Will requests for corrections be addressed within a reasonable period?	Yes	–	No significant change from existing requirements.

17.4. APP13. Finding

The CDD reforms are not particularly relevant to correction rights, as the reforms make no changes in this area. However, the increased use of PEP lists may raise an issue about whether an individual can access and correct the PEP list if they believe they are on it. (This issue is outside the scope of this PIA).

18. Function creep

The Privacy Commissioner has defined function creep as:

> Function creep is a progressive accumulation of uses for an application or identifier. An example of function creep relates to the TFN which initially was to be used only for taxation purposes but which additionally came to be used for other purposes including the administration of the welfare system.

Function creep is considered a significant privacy risk in Australia. However, the management of function creep is difficult, and there are no 'magic bullets' available to help avoid function creep.

The core mechanisms for avoiding function creep at the time of a new technology implementation are:

- Having a clearly defined primary purpose;
- Prohibitions on use for other purposes (e.g. use in another sector);
- Limiting 'discretionary' secondary use and disclosure;
- Monitoring complaints; and
- Reviewing purpose and use (e.g. every three years);

18.1. CDD Reform and Function Creep

Overall, this PIA has not identified a significant risk of function creep. The CDD reforms introduce some new categories of data that are very closely related to the existing information that is collected in the AML / CTF Framework.

The one area where a small risk of function creep may emerge is the increased use of third party service providers. They are likely to play a key role in the identification of domestic PEPs (they already play this role for foreign PEPs), and the verification of information and documents relating to business structures.

18.2. Finding

It is too early at this stage to anticipate what services these third parties might provide, how they will obtain and structure their information, and how they will comply with Privacy Act requirements. They may become an integral part of the AML / CTF system, or they may not be needed at all (for example, if better public registers are developed for trusts etc.)

However, it is clear that the development of third party services should be monitored closely. AUSTRAC may need to play a role in ensuring that the sector complies with appropriate standards, and that consumers do not lose their existing access, correction and complaint rights when their personal information is being handled by third parties. If these third parties are based overseas, then there will be an additional need to ensure that standards are not lowered, as APP 8 only provides a minimal level of protection for information that is transferred offshore.

19. Privacy Positive Aspects

It is important in a PIA process to consider the privacy positive aspects of the application. This helps in the overall assessment of whether privacy risks are balanced by the benefits of the project.

19.1. Privacy Positive Aspects of the CDD Reforms

Improvements in identity verification lie at the heart of the proposed CDD reforms. Current requirements focus on identifying the customer, which may be an individual or another entity type (e.g. company, trust, partnership, association) that is seeking to obtain a designated service from the Reporting Entity. The proposed reforms to the CDD requirements will oblige the reporting entity to identify the owners or controllers of the customer. It will, for the business, mean that there should not be any surprises about with whom they are doing business. It will also mean that any attention from law enforcement, should it be required, is addressed to the appropriate people, rather than any nominal 'front person'.

From a privacy perspective, identity fraud, identity mistakes and even deliberate identity misdirection can all cause serious problems for individual victims. Recovering an identity or correcting the trail of misinformation left by identity fraud can be very difficult and time consuming. Adverse impacts can include a negative credit record, unwarranted attention from police and legal authorities and even trust issues with employers, friends and family. It is therefore important to focus on deterring and preventing identity fraud.

The proposed CDD reforms should therefore have a positive privacy impact, as they should deter and prevent identity fraud and the use of 'nominal' individuals to represent business structures.

In addition to this privacy benefit, the CDD process delivers two *structural* privacy protections that may be as important as some of the legal and policy privacy requirements:

— **Data collected by Reporting Entities is generally retained by the Reporting Entities.**
The bulk of the CDD data is distributed across thousands of organisations and is not collected in a central location. This avoids a range of privacy and security issues that arise where data is collected and stored in a single database.

— **Key CDD activities, such as reporting transactions to AUSTRAC, or engaging in enhanced surveillance of accounts, is only conducted on a risk basis, in accordance with guidance issued by AUSTRAC.**
This includes transactions above the $AUD 10,000 threshold, international transfers, and suspicious matter reports. There is no automated surveillance of *all* financial activity. These three tests provide an important layer of privacy protection, ensuring that collection and use of data can be justified by reference to the known risks in the AML / CTF context.

Finally, the CDD reforms are also likely to have a positive impact on the quality of data that is collected, used and disclosed by Reporting Entities. For example, the CDD reforms include requirements for Reporting Entities to review and update the information that they hold on clients, rather than relying only on the information originally submitted (e.g. during account opening). The CDD reforms also require Reporting Entities to verify documents and to check for forgeries and stolen documents. These improvements in the quality of data are a privacy positive aspect of the reforms.

19.2. Finding

The proposed CDD reforms should deliver a clear privacy benefit as they include measures to deter and prevent identity fraud. They also focus on identifying the relevant individuals in complex business structures rather than just the nominated representatives.

Existing AUSTRAC processes in relation to CDD also deliver some *structural* privacy protection. Firstly, the bulk of the CDD data is distributed across thousands of organisations, rather than being stored in a central location. Secondly, use and disclosure of the information is not automated – it is always subject to a 'risk' test.

Additionally, the finding for APP 10 indicated improvement of data quality is a privacy positive aspect of the CDD reform (refer to Section 14.4 at page 36).