Australian Government

AUSTRAC

Privacy implications of collecting know your customer (KYC) information from sources other than from the customer

Reporting entities need to comply with privacy requirements in relation to AML/CTF–related activities

1. Carrying out an applicable customer identification procedure (ACIP) for AML/CTF purposes involves the collection of some form of 'personal information' about an individual. Common examples of 'personal information' are an individual's name, signature, address, telephone number and date of birth.

2. Reporting entities are required to comply with the *Privacy Act 1988* (Privacy Act) in relation to all AML/CTF Act related activities, even if they would otherwise be exempt from the Privacy Act (subsection 6E(1A) of the Privacy Act). This also includes complying with the Australian Privacy Principles (APPs). It should be noted that the APPs place more stringent obligations in relation to the handling of 'sensitive information' (for example, health, genetic or medical information, information about racial or ethnic origin or political opinions), although the collection of such information is not mandatory for AML/CTF purposes.

3. The Australian Information Commissioner has issued APP guidelines which outline the mandatory requirements of the APPs and how the Office of the Australian Information Commissioner (OAIC) will interpret the APPs.

4. The privacy legislation refers to 'APP entities' – a phrase which includes Australian and Norfolk Island Government agencies as well as various other private sector and not-for profit organisations (referred to here as 'non-agency entities').

Optional change to how reporting entities can identify their customers

5. As a result of the amendments in *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2016 (No. 1)*, from 16 September 2016 reporting entities now have the option to collect KYC information from sources other than the customer in relation to:

    - individual customers;
    - beneficial owners of non-individual customer entities and politically-exposed persons (PEPs); and
    - individuals who are not customers of reporting entities, but are associated with a customer a reporting entity (for example, directors of companies in the identification of companies).

6. Prior to 16 September 2016, Chapter 4 of the AML/CTF Rules required reporting entities to collect KYC information directly from their customers for the purposes of carrying out the ACIP.

7. Carrying out an ACIP involves the collection of personal information about an individual, such as the name, signature, address, telephone number and date of birth.

8. Normally, where personal information is collected directly from an individual, the individual has greater control over what, and how much, personal information is shared or revealed to a reporting entity. However, where personal information about an individual is collected by

reporting entities from sources other than from the individual, there are privacy implications as the individual no longer has control over the quality of, or what, information a reporting entity may collect or which third party source the reporting entity will use.

9. The new optional requirements will have privacy impacts on the following:

    - individual customers of reporting entities from whom personal information has historically been collected, but which now may be collected from other sources;
    - individuals who are not customers of reporting entities, but are associated with a customer and who need to be identified and verified as part of the ACIP (for example, PEPs). It should be noted that prior to these amendments, information about beneficial owners was required to be provided by the customer.

10. AUSTRAC undertook a Privacy Impact Assessment on the amendments which is published on the AUSTRAC website: *Privacy Impact Assessment – Amendments to Chapter 4 of the AML/CTF Rules*.

Collecting personal information which is 'reasonably necessary'

11. Although reporting entities need to adhere to all Australian Privacy Principles (APPs), APP 3 (Collection of solicited personal information) is particularly relevant to reporting entities.

12. In relation to non-agency APP entities (generally an entity which is not a government agency), APP 3 provides that personal information about an individual:

    - must only be collected by lawful and fair means;
    - must only be collected from the individual concerned unless it is unreasonable or impracticable to do so (or one of the other exceptions applies); and
    - may only be collected where it is reasonably necessary for the organisation's functions or activities (and not for a secondary purpose, unless consent is obtained).

13. Paragraph 3.65 of the APP guidelines lists various matters which may be considered to determine whether it is 'unreasonable or impracticable to collect directly from the individual' for the purposes of APP 3. While the 'time and cost involved in collecting directly from the individual' is one factor to be considered, the APP Guidelines make it clear that it is only where something is excessively inconvenient, time-consuming or costly that an APP entity will be excused from collecting the information directly from an individual. Reporting entities should still consider the other factors in paragraph 3.65 to assess whether it is reasonable and practicable to collect information about individuals from other sources.

Relevance of 'consent' when collecting KYC information from other sources

14. Although APP 3.6 includes an exception that allows a customer to consent to the collection of personal information from a source other than themselves, the 'consent exception' only applies to government agencies, not reporting entities. For reporting entities 'consent' can, however, be relevant to determining whether the collection of personal information directly from an individual is unreasonable or impracticable, and whether or not the individual 'reasonably expects' their information to be collected from another source.

15. If an individual has been informed by a reporting entity that their information will, in certain circumstances, be collected from other sources, and has consented to that collection, this factor will help assess whether the unreasonable or impracticable exception applies.

16. Nevertheless, consent does not necessarily need to be obtained from every individual about whom a reporting entity needs to collect information for ACIP purposes provided the APP requirements are adhered to and the factors in paragraph 3.65 of the APP guidelines are

considered and apply. For example, if there is publicly-available information already in existence about the individual.

17. 'Consent', for the purposes of assessing whether the 'unreasonable or impracticable exception' in APP 3.6(b), means 'express consent or implied consent'.

18. Only adequately informed, voluntary and current and specific consent by a person with capacity is acceptable for assessing the applicability of the 'unreasonable or impracticable exception' in APP 3.6(b).

19. However, even where an individual has consented to indirect collection, reporting entities should assess the situation as a whole when considering whether the exception in APP 3.6(b) applies (including the factors listed in paragraph 3.65 of the APP guidelines). Examples of other factors which may be relevant to consider include:

    - how long ago consent was given;
    - whether consent was given specifically for indirect collection (or bundled together with other matters); and
    - whether indirect collection is a practice accepted by both industry and customers.

20. Reporting entities should also be mindful about 'bundled consents' where one consent is given to a wide range of collections, uses and disclosures of personal information, and 'opt-out mechanisms'. Reporting entities need to obtain informed and specific consent or refusal from individuals about whom personal information is collected from other sources. This is in relation to each of the proposed collections, uses and/or disclosures that the reporting entity proposes to undertake (including any proposed overseas disclosures of personal information).

Sourcing publicly-available KYC information for ACIP purposes

21. The Office of the Australian Information Commissioner considers that where information, including personal information, is contained in a public register (such as an ASIC registry), generally individuals would reasonably expect their information to be collected from such third parties and accordingly, the exception in APP 3.6(b) would likely apply (provided the collection otherwise complies with APP 3).

Use of KYC information collected from other sources for direct marketing

22. APP 7 (Direct marketing) generally prohibits reporting entities from using personal information for direct marketing. Additional restrictions apply if the personal information was collected from a third party. Consent is required from the relevant individual prior to using or disclosing such personal information for direct marketing, unless it is impracticable to obtain that consent. In addition, individuals need to be informed of 'opt-out mechanisms' whereby they may request not to receive direct marketing communications or request the disclosure of the reporting entity's source of their personal information.

23. A reporting entity should also assess whether the other factors listed in paragraph 3.65 of the APP guidelines are relevant in order to determine whether the 'unreasonable and impracticable' exception applies.

24. These include whether the individual would reasonably expect personal information about them to be collected directly from them or another source, the sensitivity of the information being collected, whether direct collection would jeopardise the purpose of collection, any privacy risk if it is collected from another source and the time and cost of collecting directly from the individual.

Practical implications for reporting entities

25. A reporting entity which decides to collect personal information from sources other than from the customer will need to consider the following to ensure that its identification procedures comply with Privacy Act requirements:

- Implementing revised practices, procedures and systems in relation to the collection, use, security, storage and disclosure of personal information about individuals, especially for information collected from other sources and about individuals who may not be customers of the reporting entity (for example, beneficial owners and in some circumstances, PEPs). This may include having a revised privacy policy;
- Ensuring that only personal information which is 'reasonably necessary' for one or more of the reporting entity's functions or activities is collected from third party sources about an individual;
- Ensuring that personal information is collected from third parties only when it is unreasonable or impracticable to collect it directly from an individual;
- Checking whether there have been appropriate and timely notifications to, and consents from, affected individuals in relation to the collection of personal information from third party sources;
- Re-evaluating whether, and how, a reporting entity 'bundles' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, especially in relation to obtaining information from third party sources. This is also relevant where a reporting entity uses personal information collected about non-customers for direct marketing;
- Ensuring compliance with all other APPs in relation to personal information collected from other sources, particularly for personal information relating to non-customers of a reporting entity.

Further information

The OAIC has published information on privacy obligations when undertaking AML/CTF–related activities: *'Does my business have privacy obligations in relation to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006?"*