Privacy Statement as to the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the "AML/CFT Act")

[1] Introduction

Customer Due Diligence ("CDD") is required to be completed by:
G M Bilkey t/a Graham & Co
("we") under the AML/CFT Act.[1] CDD requires that we collect documents such as; Identification, proof of address, Information relating to the nature and purpose of a proposed business relationship or transaction, information required to assess if Enhanced Customer Due Diligence should be applied; and Enhanced Customer Due Diligence documentation where applicable.[2] CDD requires that we verify the identification documents obtained under the relevant sections of the AML/CFT Act.[3]

[2] Collection, storage, use, and destruction of personal information

We are subject to the Privacy Act 2020 ("Privacy Act") and we are committed to ensuring that your privacy is protected. The information which is collected in accordance with part 1 above is managed and collected in accordance with the privacy act but governed by our obligations under the AML/CFT Act.

We will collect information directly from the person[4] concerned. In addition:

i. We will retain such information for a period of 5 years after the business relationship has ended.[5] Once 5 years have passed, we will arrange for the safe destruction of any electronic and paper-based records.
ii. We will store such information through the Realyou Limited (RealAML) dashboard.
iii. We provide access to such personal information collected from you and provide an allowance for the correction of any information held which is factually incorrect. We will not provide access to information that may prejudice obligations under the AML/CFT Act; and
iv. We will disclose personal information which may be required to uphold, or enforce the law or otherwise in accordance with the AML/CFT Act or Privacy Act.

We will use the information pursuant to our obligations under the AML/CFT Act. We will also, in relation to identification information and documentation obtained in accordance with the AML/CFT Act:

v. Electronically verify any identity (and address) information provided, by a third-party biometric identification platform, RealAML.
vi. RealAML securely stores personally identifiable information (PII) data encrypted on Amazon Web Services (AWS) in Sydney, Australia.
vii. We will use personal information such as names, dates of birth, nationalities, and sex to determine if there are any matches on global sanctions registers, or connections to being a politically exposed person.

How to use this Privacy Policy

[1] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 11.
[2] In accordance with s 22 – 30 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
[3] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 16, 20, 24, and 28.
[4] Person means any natural person or legal personality including a Company, Trust, Partnership, or other legal arrangement.
[5] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, subpart 3.

P: +6448894788 | E: jordan@realaml.com | W: www.realaml.com

This Privacy policy is prepared specifically for the collection and management of AML/CFT documentation, as well as its use when using the services of Realyou.

The Privacy Act [2020] places obligations on businesses, and individuals to collect, handle, store and destroy personal information in accordance with the Privacy Principles. Any claims for breaches of the Privacy Act when handling personal information related to AML documentation can have severe reputational, and monetary consequences.

Most likely, you will have your own methods of onboarding your clients and customers. This policy is designed to fit into an existing method of onboarding, and I have laid out some suggestions below on how to do this.

a) **Letters of engagement:** If your business uses a letter of engagement, you can simply annex the policy into the section where you discuss the AML/CFT requirements. Depending on whether you have an existing policy, you may simply modify your own to match our suggested template.
b) **RFI (Request for Information):** Some businesses simply send a document to their client, which their client then fills out. You can include this as an additional attachment to either method.
c) **Include it as an attachment if requesting via email only:** When communicating and doing the request by email, in your initial request to your client you can include this as an attachment.
d) **Passport Verification (DIA) Application:** To be granted access to verify New Zealand passports you will need to provide a copy of your privacy policy (this policy).

Modifications

This policy may require modification specific to your business. I recommend adding a small section about the security of the client's information – for example, where you store results of screening tests using your business's Microsoft OneDrive, or by using other local/cloud-based storage solutions.

Jordan McCown
Chief Executive Officer

P: +6448894788 | E: jordan@realaml.com | W: www.realaml.com