

GENERAL DATA PROTECTION REGULATIONS (GDPR) DATA PRIVACY & ANTI MONEY LAUNDERING POLICY (“GDPR-AML”)

1. This document summarises the GDPR/ AML policy of **Alexander Byrne Sidhu & Partners SA (“ABS&P”)**.

This policy declares that during its business operations, ABS&P shall endeavour to protect the data privacy of its customers and others they interact with in accordance with law and to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with as far as possible with all applicable requirements in the relevant jurisdictions for themselves and its Associates.

These GDPR-AML policies, procedures and internal controls are designed to ensure compliance with all relevant and applicable compliance regulations concerning money laundering and other criminal activities and data privacy and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for changes in the applicable regulations.

2. GDPR-AML Compliance Officers Designation and Duties

ABS&P has designated its Managing Partner and Senior Partner as its Data Privacy & Anti-Money Laundering Policy Compliance Officers (GDPR-AML Compliance Officers), with full responsibility to act in its individual, or joint capacities in respect to this GDPR-AML policy.

ABS&P’s GDPR-AML Compliance Officers will be qualified to undertake their duties by virtue of professional training in GDPR-AML procedures and/ or will have been qualified by experience, knowledge. The duties of the GDPR-AML Compliance Officers will include monitoring ABS&P’s compliance with GDPR-AML obligations as well as overseeing communication and training for its employed and business partners (where appropriate).

GDPR-AML Compliance Officers shall also ensure that ABS&P keeps and maintains all of the required GDPR-AML records and will ensure that Suspicious Activity Reports (SAF’s) are filed with all relevant Financial Crimes Enforcement Networks (FinCEN) when appropriate. The GDPR-AML Compliance Officers are vested with full responsibility and authority to enforce this GDPR-AML policy. ABS&P will provide its bank and all/ any relevant associated institutional financier/s with contact information for its GDPR-AML Compliance Officers, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number upon its request.

ABS&P will promptly notify its bank and relevant associated institutional financiers with any change in this information and will review, and if necessary update, this information within 17 business days after the end of each calendar year.

The annual review of this GDPR-AML Program will be conducted by the Managing Partner of ABS&P with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, they will update the information promptly, but in any event not later than 30 days following the change.

3. Giving GDPR-AML Information to Relevant Law Enforcement Agencies and Other Financial Institutions

ABS&P shall co-operate with and respond to all requests from GDPR-AML Regulated Firms, relevant Law Enforcement Agencies and Authorised Individuals concerning data privacy and engagements with its customers and relevant transactions where this is supported by evidence that GDPR-AML laws and regulations in any jurisdiction may have been breached. This co-operation shall include providing the information required in the time limit specified by the requester.

4. Voluntary Information Sharing With Other Financial Institutions

ABS&P will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that its suspects may involve possible terrorist activity or money laundering and/ or breaches of any relevant data privacy laws. ABS&P shall employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating them from its other books and records. ABS&P shall also employ procedures to ensure that any information received from another financial institution will not be used for any purpose other than:

- satisfying in full its data privacy obligations to data privacy subjects
- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

5. KYC/ KYB - Required Customer Information

Prior to delivering the services requested of them ABS&P shall collect the following information in respect to any person, entity or organization whose name is on the application document to ABS&P:-

- (1) the full name of all individuals concerned with the application and its date of birth (for individuals);
- (2) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and an identification document number (eg., passport)
- (3) where the applicant is an legal entity, ABS&P will procure information from its agents that identifies its owners/ directors and the firm in a public registry.

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, ABS&P will not engage with them and if this occurs after engagement, after considering the risks involved, shall terminate the existing engagement agreement. In either case, its GDPR-AML Compliance Officers will be notified so that ABS&P can determine whether they should report the situation to relevant institutions. All relevant ABS&P companies shall use its best endeavours to collect and deal with the data in full compliance with GDPR and/or other relevant data privacy regulations.

6. Verifying Information

Based on the risk, and to the extent reasonable and practicable, ABS&P will ensure that it has reasonable belief that it knows the true identity of its customers by using risk-based procedures to verify and document the accuracy of the information they get about its customers. Its GDPR-AML Compliance Officers will analyze the information obtained to determine whether the information is sufficient to form a reasonable belief that ABS&P knows the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

ABS&P shall verify its customers' identities through documentary means, non-documentary means or both. ABS&P will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud. It will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. Non-documentary means may also be used if it is still uncertain about whether it knows the true identity of the customer. In verifying the information, ABS&P will consider whether the identifying information that is received, such as the customer's name, street address, post/ zip code, telephone number (if provided), date of birth and Social Security number, allows it to determine that it has reasonable belief that it knows the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

7. Appropriate documents for verifying the identity of customers include the following:

For an individual: an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
For a person other than an individual: documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

ABS&P appreciates that it is not required to take steps to determine whether the document that the customer has provided to them for identity verification has been validly issued and that it may rely on a government-issued identification as verification of a customer's identity. If, however, if ABS&P finds that the document shows some obvious form of fraud, it must consider that factor in determining whether it can form a reasonable belief that it knows the customer's true identity.

ABS&P will use the following non-documentary methods of verifying identity:

1. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other such sites.
2. Checking references with other financial institutions; or
3. Obtaining a financial statement.

ABS&P will use non-documentary methods of verification when:

1. The customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
2. Where ABS&P is unfamiliar with the documents the customer presents for identification verification;

3. The customer and ABS&P do not have face-to-face contact; and
4. There are other circumstances that increase the risk that AB&SP will be unable to verify the true identity of the customer through documentary means.

ABS&P shall verify the information within a reasonable time before or after they engage with the customer. Depending on the nature of the engagement and facilities/services requested, it may refuse to deliver a facility/ service before it has verified the information, or in some instances when more time is needed, it may, pending verification, restrict the types of facilities/ services requested. If it finds suspicious information that indicates possible money laundering, terrorist investment activity, or other suspicious activity, ABS&P will, after internal consultation with its relevant GDPR-AML Compliance Officers, file a report in accordance with applicable laws and regulations.

ABS&P recognises that the risk that it may not know the customer's true identity may be heightened for certain types of customer engagement such as applications for facilities/ services in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by relevant international regulatory agencies (eg., IMF) as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. ABS&P shall identify customers that pose a heightened risk of not being properly identified. It will also take such additional measures that it may deem necessary to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient.

8. Records Keeping

Without prejudice to other privacy regulations as well as AML rules and regulations that may apply, the general policy of ABS&P is never to retain any personal records of those it has any kind of interaction with unless there is a strict legal obligation upon it to do so.

9. Notice to Customers

AB&SP will provide notice to customers when they are requesting information from it for its GDPR-AML compliance obligations and that the information collected will be processed in accordance with such compliance obligations.

10. General Customer Due Diligence

It is important for GDPR-AML reporting that ABS&P has sufficient information about each customer to allow it to evaluate the risk presented by that customer and to detect and report suspicious activity. When ABS&P engages with a customer, the due diligence that it performs may be in addition to customer information obtained for purposes of its providing facilities/ services for the customer.

11. GDPR-AML Record-keeping

The relevant ABS&P GDPR-AML Compliance Officers will be responsible for ensuring that GDPR-AML records are maintained properly and all relevant reports, disclosures and adjustments to them are filed as required in compliance with all relevant legal obligations upon them. The overall policy though of Vantage10 is endeavour not to retain its customers' data unless this is required by law.

12. Training Programs

ABS&P will develop ongoing employee/ solutions partners training under the leadership of its GDPR-AML Compliance Officers. The training will occur on at least an annual basis and will be regularly updated to reflect any new developments in the law concerning GDPR-AML. Their training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of its employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of suspicious activity reports, etc.); (3) what employees'/ business partners roles are in ABS&P's compliance efforts and how to perform them; (4) data privacy and records retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with any relevant data privacy regulations.

ABS&P will develop its own GDPR-AML training program, or contract for its delivery. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. ABS&P will maintain records to show the persons trained, the dates of training and the subject matter of its training.

13. Confidential Reporting of GDPR-AML Non-Compliance

Employees/ directors/ solutions partners at ABS&P will promptly report any potential violations of this GDPR-AML compliance program to the relevant GDPR-AML Compliance Officers, unless the violations implicate the GDPR-AML Compliance Officers, in which case the employee shall report the matter to the CEO of ABS&P. Such reports shall be confidential, and the employee/ director/ business partner will suffer no retaliation for making them.

14. Board Approval

ABS&P's Board has approved this GDPR-AML compliance program as reasonably designed to achieve and monitor its respective ongoing compliance with the requirements of all legal obligations upon it and its Associates in relation to their applicable GDPR-AML obligations.

09.05.2022