

# AML/KYC Policy

## 1. Introduction

The Anti-Money Laundering and Know Your Customer Policy (the “**AML/KYC Policy**”) of **CRXT Limited**, company number **11689557**, registered 4 Claridge Court, Lower Kings Road, Berkhamsted, Hertfordshire, England, HP4 2AF (“**we**”, “**our**”, “**us**” or “**Company**”) is established to prevent and mitigate possible risks of Company being involved in illegal or illicit activities and to enable Company to meet its legal and regulatory obligations in this area (if any, where applicable). This AML/KYC Policy is subject to changes and updates by Company from time to time to ensure compliance with any applicable legislation and global AML/KYC practices.

## 2. Subject matter

CRXT AML & KYC Policy covers the following areas:

- KYC/AML identification procedures
- Ongoing monitoring of Users
- Sanctioned and Prohibited Jurisdictions
- Record-keeping
- Money Laundering Reporting Officer
- Training

## 3. KYC/AML identification procedures

Prior to enabling or entering into a transaction with or for or on behalf of a User or providing any Service to a User, Company will:

- a) identify the User and verify the User’s identity on the basis of documents, data or other information based on a reliable and independent source;
- b) if there is a Beneficial Owner in relation to the User, identify the beneficial owner and take reasonable measures to verify the beneficial owner’s identity;

To identify a User who is an individual, Company will collect information from the User, including but not limited to, his full name, date of birth, citizenship, place of residence, email address, and the identity document type. Company will verify the identity of the User with documents such as his national ID, passport and/or driver’s license and utility bill.

To identify a User who is a legal entity, Company will collect information from the User, including but not limited to, its full legal name, registration number, date of incorporation / registration, country of incorporation / registration and lists of directors (as applicable to the entity). Company will verify the User with documents such as Memorandum and Articles of Association (or equivalent), additional beneficial ownership information and documents, and a detailed corporate chart (as applicable to the entity).

#### **4. Ongoing monitoring of Users**

Company reserves the right to continuously monitor, on a risk sensitive basis, the business relationship with a User (as applicable) by:

- a) reviewing from time to time documents, data and information that have been obtained by Company to ensure that such documents, data and information are up to date;
- b) conducting appropriate scrutiny of Transactions and activities carried out by Users to ensure that they are consistent with Company's knowledge of the User's business and risk profile, and to ensure that such Transactions and activities are in line with Company's knowledge of the User's or User's source of funds and source of wealth; and
- c) identifying transactions that are unusually large in amount or of an unusual pattern and have no apparent economic or lawful purpose.

For the avoidance of doubt, Company may undertake ongoing monitoring on Users in order to ensure that any Transactions equal to or in excess of € 10 000 (or its equivalent in any other currency) shall be subject to Enhanced Customer Due Diligence in relation to the source of funds and source of wealth of the User.

To continuously monitor the business relationship with a User (as applicable), Company may carry out a file review to ensure that information held about the User is up-to-date and that identification documents held are still valid. In addition, on a more frequent basis, Company may also monitor transactional activity to identify any red-flags or 'out of the norm' activity.

As part of the second line of defense, the MLRO will carry out checks to ensure that regular and effective on-going monitoring is being effected and ensure that irregular or suspicious activities are effectively escalated.

#### **5. Sanctioned and Prohibited Jurisdictions**

Company have integrated with a leading electronic data provider to fulfil the regulatory obligations in line with the UK's financial sanctions regime. Company will (with assistance of advisors and service providers, when necessary) establish and maintain the following lists of jurisdictions (i) Sanctioned Jurisdictions (any country or territory to the extent that such country or territory is the subject of any sanction issued by the United Nations, United States and/or the European Union) (ii) Prohibited Jurisdictions. In determining the list of Sanctioned Jurisdictions, Prohibited Jurisdictions, Company shall take into account the lists issued by the Financial Action Task Force and by other organizations issuing guidelines and lists relating to the adequacy of legislative measures adopted by jurisdictions in relation to money laundering, funding of terrorism and transparency.

Users which are (i) resident or domiciled in, or (ii) have their source of wealth or source of funds linked to a Sanctioned Jurisdiction and/or a Prohibited Jurisdiction shall not be accepted as clients of Company.

Company will (and will always reserve a right to) screen a User on an ongoing basis, to ensure that such User is not a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction.

In carrying out this screening Company shall ensure to adopt software to enable comprehensive screening to be carried out and which captures all sanctions that Company is bound to follow.

In addition to the aforementioned measures, we are integrated with the largest database of Politically Exposed Persons (PEPs), as well as those of their family members. Whenever a client has been identified as a PEP, enhanced due diligence measures are applied, senior management approval is necessary for establishing or continuing, a business relationship with such a customer.

## **6. Record-keeping**

Company will keep (a) transaction records including but not limited to the nature of the transaction, the amount of the transaction and the currency thereof, the date on which the transaction was conducted, the parties to the transaction, for a period of ten (10) years beginning on the date on which a transaction is completed, or for such other minimal period as may be required by applicable law; and (b) other information collected by Company for AML/KYC purposes, throughout the continuance of the business relationship with the User and for a period of ten (10) years beginning on the date on which the business relationship with the User ends, or for such other minimal period as may be required by applicable law.

The Company may be required to cooperate the government authorities within the territory of United Kingdom of Great Britain and Northern Ireland or from outside the said territory therefore the Company may be obliged to disclose any information about the User to the said authorities, in particular, to the OPBAS.

## **7. Money Laundering Reporting Officer**

The Money Laundering Reporting Officer (“MLRO”) shall be the person, duly authorized by Company, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Money Laundering Reporting Officer’s responsibility to supervise all aspects of Company’s anti-money laundering and counter-terrorist financing. Once such officer is appointed, all our employees will report any suspicious behavior or activities to the MLRO.

MLRO shall have the following duties:

- Receiving reports of any suspicious behavior or activities from our employees;

- Submitting Suspicious Transaction Reports to the authorities;
- Improving, updating and maintaining AML policies and procedures, incorporating new or changed regulations in the different markets;
- Monitoring, identifying and investigating suspicious activities whilst promptly implementing the right processes to mitigate such incidences;
- Maintaining and improving tools that inspect, analyze and report suspicious AML and fraud activity;
- Acting as the main point of contact for the local regulator;
- Ensuring that the Company complies with all applicable requirements;
- Establishing and maintaining effective systems and controls for compliance with applicable requirements and standards under the regulatory system;
- Providing advice to management of the Company on all applicable laws, regulations, rules & standards;

## **8. Training**

The Company maintains an ongoing employee training program so that the staff is adequately trained in AML/KYC procedures. Staff compliance with this policy will be monitored on a regular basis to ensure that Company remains compliant with UK AML law and regulation.

Last updated on March 26, 2019