

**TSIRADU
SOLUTIONS
Sp. z.o.o.**
(Reg.Nr. 0000968707)

**KYC/Onboarding
Policy and Procedure**

INTRODUCTION.....	3
1. OVERALL ONBOARDING PROCESS.....	4
2. APPLICATION FORM.....	8
3. AML RISK ASSESSMENT	9
3.1. AML Risk Score Matrix	9
4. CUSTOMER DUE DILIGENCE.....	19
4.1. Know Your Business (KYB).....	19
4.1.1. Corporate Documents	19
4.1.2. Identification of Directors.....	20
4.1.3. KYC for Ultimate Beneficial Owners (UBO's).....	21
4.2. Know Your Client (KYC).....	24
5. ENHANCED DUE DILIGENCE	25
5. SIMPLIFIED DUE DILIGENCE	26
6. PEP/SANCTION SCREENING.....	26
6.1. PEP's	27
6.2. Sanction Screening	28
7. RECORD KEEPING.....	30
8. STAFF TRAINING.....	32
APPENDIX 1 – ACCEPTED/PROHIBITED INDUSTRIES.....	33
APPENDIX 2 – PROHIBITED LIST OF COUNTRIES.....	40

INTRODUCTION

A sound customer due diligence (CDD) program is one of the best ways to prevent money laundering and other financial crime. Knowledge is what the entire AML/CFT compliance program is built upon. The more our company knows about its customers, the greater chance of preventing money laundering abuses.

In order to fulfil its responsibilities to prevent money laundering and terrorist financing, it is TSIRADU SOLUTIONS Sp. z.o.o. (hereinafter “The Company”) policy to assess the money laundering (ML) and the terrorist financing (FT) risk presented by each applicant for business and/or each existing client taking into account the services the Company will be providing to such corporate customers (hereinafter “Customers”), so that the Company can appropriately mitigate that risk by applying an appropriate level of client due diligence.

The ML & FT risk represented by each Customer will be assessed:

- As part of the customers onboarding process;
- Whenever the Company’s ongoing monitoring processes indicate that a change in the business or operating environment of the Customer represents a change in the money laundering risk presented by it.

The assessment will be carried out by the responsible AML Officer through the AML Scorecard Matrix for Customers, which will aid the AML Officer to assess the AML Risk Category of the customer and the level of due diligence that the customer will be subject to. The AML Scorecard is derived by taking into account the risks defined in Companies Risk Assessment, as updated from time to time.

This policy lays down the due diligence checks that will be conducted at onboarding stage by applying a risk-based approach and taking into consideration the specific AML risk profile of each customer. Any waivers to this policy are to be signed off by the Head of Compliance, whose approval must be documented in the Merchant File. Any escalations of onboarding rejections which are AML related; and ultimate decisions which affect Company’s AML regulatory obligations, must include the involvement of the MLRO, where appropriate. Any update to this policy should be proposed by the Head of Compliance, reviewed by the MLRO, and approved by the Board of Directors.

1. OVERALL ONBOARDING PROCESS

The AML Officer is required to run checks on the Corporate customers manually. These checks will give the AML Officer a preliminary impression of the Corporate customers.

a) Business Model

The business model of a Customer is reviewed to understand the type of product/service offered by the customer, and the resulting ML/FT. Refer to this policies Appendix 1 – Accepted/Prohibited Industries to understand the Companies risk appetite for various industries and any additional document that requires for each industry. This check is performed by both Customer Support Agent during legal document preliminary revision and by AML Officer during onboarding process. Refer to this policy further section for full KYC requirements for Corporate customers.

b) Screening

The AML Officer must run checks sanction screening system on all involved entities (including all entities involved in the shareholding structure of the Customer), any natural persons (Directors, UBOs and Authorized Signatories). Screening provides information on whether an entity or natural person qualifies as a PEP¹, is subject to any local or international sanctions or other economic measures, and other intelligence obtained from the public domain (Such as any negative news, regulatory issues, court orders, litigations etc. in which the entity or person was involved).

c) Other Searches

The AML Officer must also run additional searches on the corporate customer, such as adverse media searches in search engines (google, yahoo etc.), to mitigate the risk that the customer may be involved in ML/FT by understanding the types of goods/services the customer offers and confirming the legitimacy of the customer's business operations.

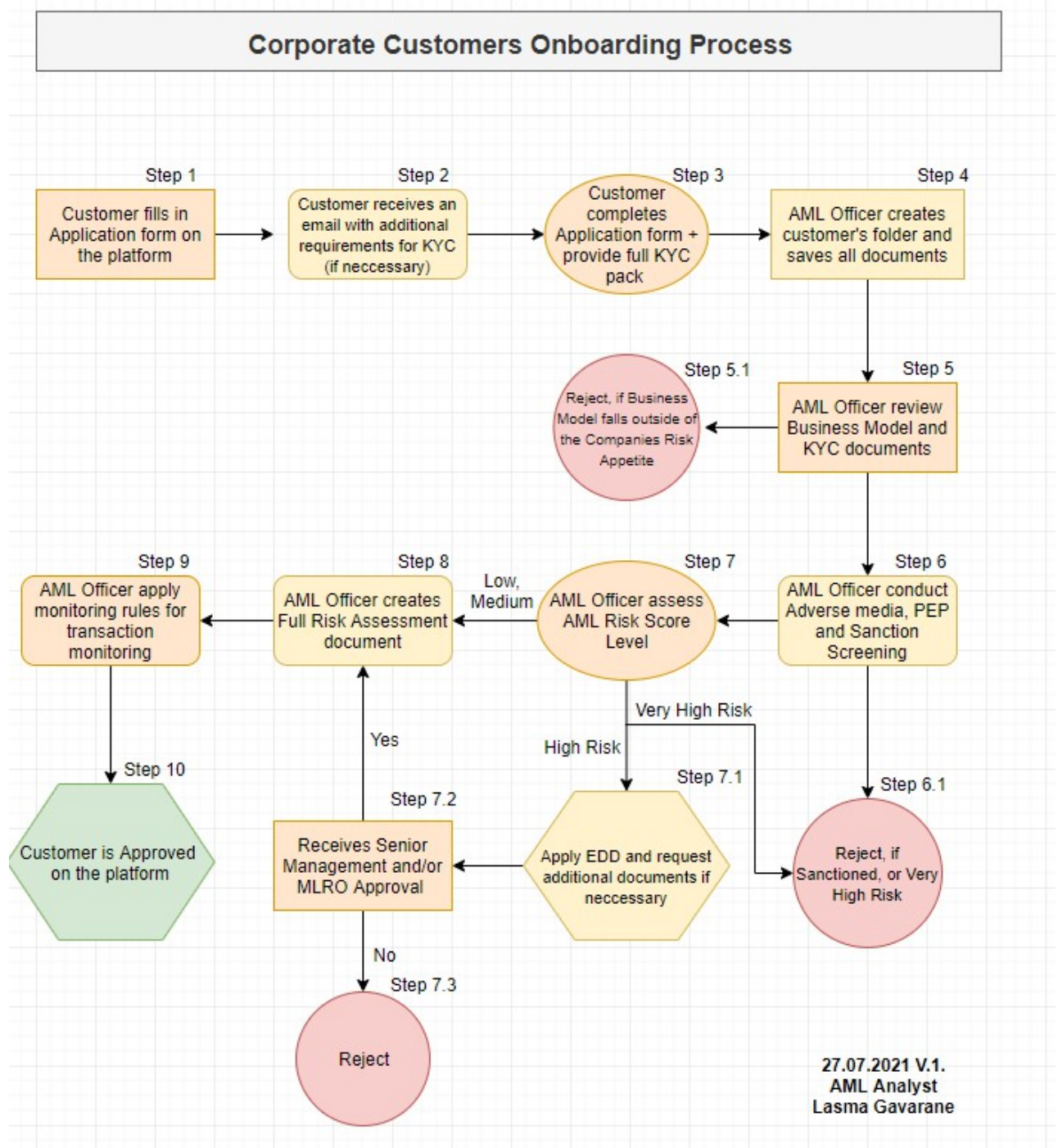
d) Findings (PEP/Sanctions/Adverse Media)

Any PEP findings on Jumio (Comply Advantage) must be approved by the Head of Compliance, as described in further detail below. Any Sanction hits must be treated with high priority. All PEP's has to be reviewed by Head of Compliance and decision is taken by Head of Compliance. Adverse Media findings which are older than 5 years and those, which are not

¹ Comply Advantage follows FATF recommendation on PEP classifications. Thus, their research analysts gather information on around 240 countries and territories from different sources such as:

- International Organizations
- Local Governments
- National Governments
- Non-Governmental
- Regional Organizations
- State-Owned Entities
- Sub-National Governments

connected with ML/TF issues, may be disregarded, unless the content of the findings is of such a concerning nature that in the opinion of the AML Officer, they should be taken into account, despite the lapse of time. In case of doubt, the AML Officer may refer the matter to Head of Compliance for further guidance.



Step 1

Customer create application form within TSIRADU SOLUTIONS Sp. z.o.o. platform <https://cryptozilla.io/Account/Register>

Step 2

Customer receives an email with the list of documents that has to be provided during onboarding, if additional documents is necessary. Standard KYC pack together with Application form is required to be provided to TSIRADU SOLUTIONS Sp. z.o.o. All documents and communication with costumers are conducted via email: support@cryptozilla.io by Customer Support Agent (hereinafter - CSA).

Step 3

Once documents have been provided, CSA reviews initially provided documents and potential customer's business model and, if any documents are missing, CSA requests to provided additional points. CSA must refer to this KYC/Onboarding policy and procedure. Once in CSA opinion all documents are provided together with filled Application form, CSA forwards all documents to Compliance team for further review.

Step 4

AML Officer must create folder with corporate customer name, for example, "TSIRADU SOLUTIONS Sp. z.o.o." and saves all provided documents in the folders.

Step 5

AML Officer must review customer business model, application form and provided documents. Business model AML Officer can check as per *Appendix 1-Approved/Prohibited Industries* and refer to guidelines there. Some business models may require additional documents to be provided. If additional documents must be provided AML Officer sends request first to CSA, and CSA sends request further to the customers.

Step 5.1

If AML Officer noticed that Business Model falls outside of the Companies Risk Appetite, customer must be declined, and information also must be sent first to CSA and CSA replies back to the customer.

Step 6

AML Officer manually conducts Adverse Media checks in search engines (google, yahoo, Bing etc.), conducts PEP/Sanction screening on all directors, involved entities, authorised signatories, UBO's via Comply Advantage screening system or other screening system used by TSIRADU SOLUTIONS Sp. z.o.o. Results of all screenings must be saved in the customers folder and are also available in the back office platform system.

Step 7

Once all necessary documents received and screening is conducted, AML Officer must fill in AML Risk Score Matrix in excel file. AML Risk Score Matrix will outline AML Risk Score Level and necessity to apply additional Due Diligence measures. Please refer to section 2.1. for AML Risk Score Matrix guideline and section 4 for Due Diligence guide.

Step 7.1.

If Corporate customer AML Risk Score Level resulted as High Risk, Enhanced Due Diligence measures must be applied as per this KYC/Onboarding policy and procedure section 4.1. and additional documents need to be requested. Request must be sent to CSA and CSA further sends request email to the customer.

Step 8

AML Officer creates Corporate Customers Risk Assessment in the Word document. The Risk Assessment must include all information with regards to the customer in question, description of customer's business, ownership structure, due diligence measures taken during onboarding process and a final decision made. Risk Assessment word document can be initiated once all documents are received and updated during onboarding process until the final decision is made and customer is Approved.

Step 9

Initial and standard transaction monitoring rules will be applied to all Corporate customers. Depending on customer's risk level, business industry and other factors, customers might require to be applied with additional transaction monitoring rules. AML Officer before accepts Corporate Customer on the platform, must either check if existing rules are sufficient to this customer and/or apply new monitoring rules (alerts) for specific customers.

Step 10

AML Officer manually accepts customer on the platform. Only AML Officer can accept Corporate customer manually on the platform. CSA is not allowed to change status in the platform to "Approved".

2. APPLICATION FORM

The Company receives the Customer Application Form (CAF) as part of the documents submitted during the Customers onboarding process. The duly completed CAF will give the AML Officer insight about the customers business and the type and volume of transactions proposed to be processed by the Customer. The AML Officer will then be required to verify this information through the checks conducted as part of the onboarding process. If the CAF is signed by any individual other than a company director, the AML Officer must ensure that a document providing the signatory with power of attorney or a Board Resolution duly authorising the signatory, is submitted with the application. In addition, the authorised signatory must be subject to individual KYC as described in further detail below.

It is important to note that the Company does not under any circumstance permit the onboarding of Customers accounts which are anonymous, or which hold fictitious names. The AML Officer must ensure that the corporate is incorporated and/or residing in one of the countries that are accepted by the Company and are not incorporated and/or residing in the country that are included in the Company's Internal Blacklist.

3. AML RISK ASSESSMENT

The AML Officer should conduct an AML Risk Assessment by using the AML Risk Score Matrix to assess the money laundering risk represented by the customer, so an appropriate level of client due diligence may be applied.

The AML Risk Score Matrix classifies customers into four risk categories depending on the risk profile score allocated to them:

- **Green** – Low Risk
- **Yellow** – Medium Risk
- **Red** – High Risk
- **Black** – Very High Risk

With respect to customers that present Low to Medium Risk, the AML Officer should apply initial CDD as described below. With respect to customers that present High Risk, the AML Officer should onboard by applying additional Enhanced Due Diligence on such customers. The additional due diligence applied must be recorded. In addition, High Risk Customers should be escalated and approved by the MLRO and/or Senior Management.

Customers who are classified as presenting Very High Risk should be declined on the basis that the client falls outside of the Company's risk appetite. This rejection may only be superseded with the approval of the MLRO and Members of the Board.

It should be noted that the AML risk factor allocated does not necessarily give grounds to suspect money laundering, and on the other hand, a low AML risk score does not necessarily preclude the possibility of ML/FT. The AML Officer should raise an STR with the MLRO in all cases where there is reason to suspect ML/FT, in accordance with the AML Policy.

The AML Risk Matrix should be reconducted on an ad hoc basis depending on a change of circumstances warranting a re-review of the client, such as following any one of the events listed below

- Change in the corporate structure
- Change in business model
- Any related individual (director and/or shareholder) has become a PEP
- Adverse media found about customer or its beneficiary, shareholder or representative.

3.1. AML Risk Score Matrix

The AML Officer should conduct manually AML Risk Score Matrix for Corporate customers before business relationships has been established and before any transaction has been made.

Sample of AML Risk Score Matrix for Corporate customers can be found in the Compliance-General folder -> 02 Internal Procedures and Policies -> 5. AML Risk Score Matrix.

AML Risk Score Matrix is implemented in excel and should be conducted in excel format and saved in Customers folder "AML Risk Score Matrix".

A	B	C	D	E	F
	1. Customer Risk				AML Officers
	High Risk [Specific: Forex, EMI, Gambling, Virtual Service Providers (VSP), MSBs etc.]	9			Lasma Gavarane
Industry Risk	Tangible Goods	1			
	Intangible Goods	5			
	Services	5			
	Other Restricted Industry	4			
	BLANK	3			
License	Yes, licensed	3			
	Does not hold any license	5			
	License not required for this business field	1			
	BLANK	3			
Corporate Structure	UBO cannot be independently verified (UBO Declaration required)	10			
	Non-complex corporate Structure	2			
	Complex corporate structure and/or trusts, foundations, other legal vehicles or nominee shareholders	5			
	Entities listed on a regulated market (NASDAQ) subject to transparency requirements	1			
	Licensed financial business (Hold License)	2			
	Bearer shares or undisclosed nominee shareholders	20			
	Public administration or public enterprise	1			
	Other structures	3			
	BLANK	3			
Adverse media	No relevant adverse media	1			
	Subject to criminal proceedings and/or asset freeze	20			
	Supervisory sanctions	7			
	Allegations of ML/FT/financial crime	10			
	Other Adverse media (not older than 5 years)	5			
	BLANK	3			
Age of client's business	5+ years	1			
	2-5 years	2			
	1-2 years	3			
	6 months - 1 year	4			
	less than 6 months	5			
	BLANK	3			
Turnover	Less than Euro 10,000 per month	1			
	Between 10,000 and Euro 50,000 per month	2			
	Between 50,000 and Euro100,000k per month	3			
	Between 100k and Euro 1M	4			
	Over Euro 1M per month	5			
	BLANK	3			
Duration of Business Relationship	Applicant for Business	5			
	Less than 1 Year	4			
	More than 1 Year	1			
	More than 5 years				
	BLANK	3			
Is there PEP involvement?	YES	5			
	NO	1			
	BLANK	3			
Source of Wealth/Source of Funds known ?	Known (Supported with documents)	1			
	Known (From Application form)	3			
	Unknown	5			
	BLANK	3			
Delivery channel	Face-to-face	1			
	Non-face-to-face	5			
	BLANK	3			
	2. Interface Risk				
Interface with Cidrus Ltd.	IBAN service	3			
	Other	2			
	BLANK	3			
Cidrus Ltd. Interface with Customer	Direct (Customer reached out Cidrus Ltd.)	5			
	Direct (Cidrus Ltd. Sales Agent reached out Customer)	4			
	Referral (Referrer, Intermediary)	3			
	Referral (Reputable, Trustable Referrer or Intermediary)	2			
	BLANK	3			
	3. Geographical Risk				
The main market where merchant operating	EU and EEA countries	1			
	Non-EU countries (CIS countries)	3			
	Other (US, Latin America, Africa, Asia, Arabic)	5			
	BLANK	3			
	Reason for risk classification				
	Scorecard (default)				
	PEP				
	Request for information (Law Enforcements, Regulators etc.)				
	MLRO or Senior Management Request				
	Other				

Customer Risk:

1.1. What is the Industry Risk?

AML Officer should identify customer in which industry customer is operating. This information can be obtained from Customers Application Form or from the customers website.

Possible Answers:

- *High Risk [Specific: Forex, EMI, Gambling, Virtual Asset Service Providers (VASP), MSBs etc.]* – type of the business model that is considered High Risk and therefore is subject to heightened AML/CFT scrutiny;
- *Tangible Goods* – type of goods that has physical nature, for example, gadgets, electronics, furniture etc.;
- *Intangible Goods* – type of goods that does not have a physical nature, for example, music, e-books, virtual courses;
- *Services* - describes work that supports a business but does not produce a tangible commodity, for example – consulting, vendor services etc.;
- *Other Restricted Industry* – other industries that are not described above, however, is restricted/prohibited or High Risk.

1.2. Does Customer hold License?

There are multiple industries that must be licensed in order to operate in the industry, for example, all High-Risk industries. AML Officer must verify license in the regulated authority's public register.

Possible Answers:

- *Yes, licensed.*
- *Does not hold any license* – if customer is operating in High Risk industry, where license is required and cannot provide such, it is prohibited to establish business relationships with such customer, there can be some exceptions, cases when such customer has been approved by Senior Management.
- *License not required for this business field* – customers that operate in industries that does not requires license to operate.

1.3. What is Corporate Structure?

Different corporate structures provide different AML/CFT risk level. More complex corporate structure has higher risk to be involved in suspicious activities.

Possible Answers:

- *UBO cannot be independently verified (UBO Declaration required)* – refers to cases where UBO cannot be verified via State Business Registers, Provided Documents and Organogram.
- *Non-complex corporate Structure* – refers to cases where corporate structure is very simple, for example, company itself and straight after one UBO, or 2 level company structure and at the end UBO.
- *Complex corporate structure and/or trusts, foundations, other legal vehicles or nominee shareholders* – refers to cases where nominee shareholder, trusts, foundations is involved and multiple level structure created, therefore is difficult to identify UBO. Multiple companies involved that makes hard to identify UBO.
- *Entities listed on a regulated market (NASDAQ) subject to transparency requirements* – customers that are publicly listed are considered as lower risk customers given they went through heightened scrutiny to become publicly listed. For publicly listed companies UBO cannot be identified, UBO's can change any minute and can be more than 100 of them.
- *Licensed financial business (Hold License)* – are considered lower risk as they are regulated by financial supervisor authority, for example, Electronic Money Institution, Payment Institution, Banks that holds financial license.
- *Bearer shares or undisclosed nominee shareholders* – Bearer shares are unregistered equity securities owned by the possessor of the physical share documents. If the customers holds bearer shares or undisclosed nominee shareholders it is prohibited to establish business relationship with such customer.
- *Public a TSIRADU SOLUTIONS Sp. z.o.o. administration or public enterprise* – Public enterprise, a business organization wholly or partly owned by the state and controlled through a public authority.
- *Other structures* – other structures not described above.

1.4. Are there any relevant Adverse Media on client?

This question assesses Adverse Media risks, including also Sanction risks. TSIRADU SOLUTIONS Sp. z.o.o. will not establish business relationships with sanctioned entities.

Possible Answers:

- *No relevant adverse media*
- *Subject to criminal proceedings and/or asset freeze* – refers to cases when customer is listed in the international/national sanctions list. If this section is chosen AML Risk Score Matrix should result as Very High Risk, meaning that it is prohibited to establish business relationships with this customer.
- *Supervisory sanctions* – refers to cases when customer is licensed and regulator has imposed warnings/fines to the customer, however customer license is still valid meaning that regulator does not revoke license.

- *Allegations of ML/FT/financial crime* – refers to cases where Adverse Media have results with allegation of ML/FT/financial crime. Article should be listed in reputable, trustable, and reliable source.
- *Other Adverse media (not older than 5 years)* – other relevant Adverse Media that are not older than 5 years and article is listed in the reputable, trustable, and reliable source.

1.5. What is the age of client's business?

Newly established business has higher risk of being involved in suspicious activities than entities that operates in the industry for many years, therefore it is important to consider age of client's business.

Possible Answers:

- *5+ years*
- *2-5 years*
- *1-2 years* – High Risk entities that are established less than 2 years should provide Business plan.
- *6 months - 1 year*
- *less than 6 months*

1.6. What is Monthly Turnover?

Turnover that is not significant is considered less risky than customers whose turnover is significant, therefore it is necessary to take into consideration customers expected monthly turnover via TSIRADU SOLUTIONS Sp. z.o.o.

Possible Answers:

- *Less than Euro 10,000 per month*
- *Between 10,000 and Euro 50,000 per month*
- *Between 50,000 and Euro 100,000k per month*
- *Between 100k and Euro 1M*
- *Over Euro 1M per month*

1.7. Duration of business relationships with TSIRADU SOLUTIONS Sp. z.o.o.

Customer who are Applicant for Business is considered with higher risk than customers who already is known for the company. During Ongoing monitoring AML Officer should conduct AML Risk Score Matrix again and change duration of business relationships.

Possible Answers:

- *Applicant for Business*
- *Less than 1 Year*

- *More than 1 Year*
- *More than 5 years*

1.8. Is there PEP involvement?

Politically Exposed Persons (PEP's) present a higher risk for involvement in money laundering and/or terrorist financing because of the position they hold. Each PEP should be reviewed and approved by Head of Compliance.

Possible Answers:

- *Yes*
- *No*

1.9. Is Source of Wealth/Source of Funds known ?

Source of Wealth (SOW) refers to the origin of the customer's entire body of wealth (for example, ownership of a business, employment, inheritance, investments), while Source of Funds (SOF) refers to the origin of the funds or any other monetary instrument which are the subject of the transaction between a Financial Institution and the customer. SOF is the origin and means of transfer of monies that are accepted for the account. (for example, funds from a saving account owned by individual, funds from Germany bank account owned by a company)

Possible Answers:

- *Known (Supported with documents)* – provided SOF document, for example, bank statement from saving account, loan agreement etc. All High-Risk merchants is required to provide SOF.
- *Known (From Application form)* – SOW is outlined in the application, fill in this section in Customer Application Form is mandatory.
- *Unknown* – if customer SOW/SOF is unknown AML Risk Score Matrix should result with Very High Risk - it is prohibited to establish business relationships if customer SOW/SOF is unknown.

Interface

Risk:

2.1. What is the Delivery Channel ?

Transactions with persons identified in a non-face-to-face identification process are characterised by a higher risk of money laundering and terrorism financing.

Possible Answers:

- *Face-to-face* – onboarding via customers physical presence;

- *Non-face-to-face* – to mitigate the non-face-to-face risk the company is using electronic identification and verification vendor. Customers from non-EU countries has to go through Liveness checks.

2.2. What is Customers Interface with TSIRADU SOLUTIONS Sp. z.o.o. ?

Customers interface with TSIRADU SOLUTIONS Sp. z.o.o., means what products/services customer will use from

Possible Answers:

- *IBAN Accounts;*
- *Other* – TSIRADU SOLUTIONS Sp. z.o.o. might offer other services in the future

2.3. What is TSIRADU SOLUTIONS Sp. z.o.o. interface with the Customer ?

TSIRADU SOLUTIONS Sp. z.o.o. Interface with Customer means the way how TSIRADU SOLUTIONS Sp. z.o.o. reached out Customer, or how customer reached out TSIRADU SOLUTIONS Sp. z.o.o.

Possible Answers:

- *Direct (Customer reached out TSIRADU SOLUTIONS Sp. z.o.o.)* – we consider if merchant reached out TSIRADU SOLUTIONS Sp. z.o.o. by themselves and TSIRADU SOLUTIONS Sp. z.o.o. do not know this merchant it represents higher risk.
- *Direct (TSIRADU SOLUTIONS Sp. z.o.o. Sales Agent reached out Customer)* –we consider that if TSIRADU SOLUTIONS Sp. z.o.o. Sales Agent reached out this customer, Sales Agent might have some information about the customer or is known from other personal activities.
- *Referral (Referrer, Intermediary)* – refers to cases when our existing customer introduced to TSIRADU SOLUTIONS Sp. z.o.o. other entity with the same business model and that might be within the customers structure, or might not be within the structure.
- *Referral (Reputable, Trustable Referrer or Intermediary)* - refers to cases when our well-known customer introduced to TSIRADU SOLUTIONS Sp. z.o.o. other entity with the same business model, or different business model and is considered as trustable referral or intermediary.

Geographical Risk

Geographical Risk is the vulnerability to money laundering threats that countries face at a national level. A crucial step in devising a risk-scoring model involves jurisdictional risk.

When looking specifically at money laundering risk, the terrorism and sanctions lists published by governments and international organizations is being used as starting point. These include lists published by the:

- United Kingdom's Financial Conduct Authority (FCA),
- U.S. Office of Foreign Assets Control (OFAC), the
- U.S. Financial Crimes Enforcement Network (FinCEN), the

- European Union (EU),
- the World Bank,
- the United Nations Security Council
- etc.

AML Officer might also consider the overall reputation of the countries in question. In some countries, cash may be a standard mean of exchange. Others may have politically unstable regimes and high levels of public or private sector corruption. Some may have a reputation as bank secrecy havens. Still, others may be widely known to have high levels of internal drug production or to be in drug transit regions.

3.1. Country of incorporation of the Customer ?

Please refer to the Tab “Country Risk Assessment” in the Customer AML Risk Score Matrix, where each country has assigned with AML Score as per Knowyourcountry.com July 2021 update (hereinafter it should be considered, that risk rate from Knowyourcountry.com will be updated regularly upon availability on new data).

Country	Score	Incorp Country	UBO Residence Country	UBO Nationality country	UBO Citizenship country	Comment									
BLANK		3	3	3	3		Last update 29 June 2021								
Afghanistan	52,1	20	20	20	20	NON-REPUTABLE	Lower	Lower - Med	Medium	Med-Higher	High	Adjustments			
Åland Islands	86,64	1	1	1	1		80 - 100	70 - 80	60 - 70	50-60	<50	NON-REPUTABLE		20	
Albania	53,61	20	20	20	20	NON-REPUTABLE	Rating	1	2	5	8	15	BLOCKED		30

3.2. The main market where the Customer is operating ?

Merchants who operate in jurisdictions outside of Europe Economic Area are considered with greater risk than customers who operates only in EU.

Possible Answers:

- EU and EEA countries
- Non-EU countries (CIS countries)
- Other (US, Latin America, Africa, Asia, Arabic)

3.3. Nationality of UBO ?

Ultimate Beneficial Owner might be Afghanistan nationality, however, can hold EU Identification document, therefore it is required to identify nationality of UBO. Please refer to the Tab “Country Risk Assessment” in the Customer AML Risk Score Matrix, where each country has assigned with AML Score as per Knowyourcountry.com July 2021 update.

Country	Score	Incorp Country	UBO Residence Country	UBO Nationality country	UBO Citizenship country	Comment	Last update 29 June 2021					Adjustments	
BLANK		3	3	3	3		Lower	Lower-Med	Medium	Med-Higher	High		
Afghanistan	52.1	20	20	20	20	NON-REPUTABLE	80 - 100	70 - 80	60 - 70	50-60	<50	NON-Repeatable	20
Åland Islands	86.64	1	1	1	1								
Albania	53.63	20	20	20	20	NON-REPUTABLE	Rating	1	2	5	8	15	

3.4. Country of citizenship of UBO ?

Country where UBO's identification document is issued. Please refer to the Tab "Country Risk Assessment" in the Customer AML Risk Score Matrix, where each country has assigned with AML Score as per Knowyourcountry.com July 2021 update.

Country	Score	Incorp Country	UBO Residence Country	UBO Nationality country	UBO Citizenship country	Comment	Last update 29 June 2021					Adjustments	
BLANK		3	3	3	3		Lower	Lower - Med	Medium	Med-Higher	High		
Afghanistan	10,1	20	20	20	20	NON-REPUTABLE	80 - 100	70 - 80	60 - 70	50-60	>50	NON- Reputable	20
Aland Islands	86,04	1	1	1	1								
Albania	53,03	20	20	20	20	NON-REPUTABLE	Rating	1	2	3	4	5	

3.5. Country of residence of UBO ?

Country where UBO is residing and Proof of Residence is provided. Please refer to the Tab "Country Risk Assessment" in the Customer AML Risk Score Matrix, where each country has assigned with AML Score as per Knowyourcountry.com July 2021 update.

Country	Score	Incorp Country	UBO Residence Country	UBO Nationality country	UBO Citizenship country	Comment	Last update 29 June 2021					Adjustments	
BLANK		3	3	3	3		Lower	Lower - Med	Medium	Med-Higher	High		
Afghanistan	10,1	20	20	20	20	NON-REPUTABLE	80 - 100	70 - 80	60 - 70	50-60	>50	NON- Reputable	20
Aland Islands	86,04	1	1	1	1								
Albania	53,03	20	20	20	20	NON-REPUTABLE	Rating	1	2	3	4	5	

AML Risk Score

Results:

Score 1-40 – **Low Risk**

Score 41-50 – **Medium Risk**

Score 51-60 – **High Risk** => Additional Enhanced Due Diligence is mandatory + MLRO and/or Senior Management Approval required

Score 61 < - **Very High Risk** => Prohibited to establish Business Relationships

AML Risk Score can be overridden to High Risk based on the following reasons:

- *PEP* – if score card resulted Low or Medium Risk, however within the structure it has been noticed PEP involvement, and it's approved by Head of Compliance, final AML Risk Score should be overridden to High Risk.
- *Request for information (Law Enforcements, Regulators etc.)* – if TSIRADU SOLUTIONS Sp. z.o.o. receives any requests for information from Law Enforcements, Regulators or Supervisors with regards customer, final AML Risk Score should be overridden to High Risk
- *MLRO or Senior Management Request* – if there have been multiple internal investigations, suspicious activities are being noticed, filled STR's/SAR's etc. MLRO and/or Senior Management should request to override final AML Risk Score to High Risk.
- *Other* – other cases, that are not included above, can override final AML Risk Score to High Risk. In case of chosen answer "Other" additional comment is required by AML Officer.

4. CUSTOMER DUE DILIGENCE

4.1. Know Your Business (KYB)

Know Your Business refers to corporate customers. Documents that must be obtained depends on the 2 factors:

- 1) The Business model of the customer.
- 2) AML Risk Level

Initial KYC pack request that is being send to the corporate customers email is the following:

- 1) *Copy of Certificate of Incorporation*
- 2) *Copy of Register of Directors (latest version)*
- 3) *Copy of Register of Shareholders (latest version)*
- 4) *Copies of Identification document and Proof of Residence for all Directors (issued within the last 3 months)*
- 5) *Copies of Identification document + Proof of Residence for all UBO's (issued within the last 3 months)*
- 6) *Detailed Company structure showing shareholders >= 25%*
- 7) *Completed Application Form*

4.1.1. Corporate Documents

Documents that must be requested based on the customers Business model is described in the *APPENDIX 1* of this policy.

When the Customer is a corporate entity, the following KYC documents are required based on the AML Risk Level:

Documents for Low-Risk Corporate Customers:

- Certificate of Incorporation or a search in the official company registry of the jurisdiction of incorporation of customer, which contains the company's official full name, registration number, date of incorporation and registered address, or principal place of business of the customer. Entry should reflect that company is Active.
- Register of Directors, or an official document that would contain the list of directors, such as an Annual Return, where applicable.
- Register of Shareholders, or an official document that would contain the list of shareholders, such as an Annual Return, where applicable.

Documents for Medium Risk Corporate Customers:

- Certificate of Incorporation or a search in the official company registry of the jurisdiction of incorporation of customer, which contains the company's official full

name, registration number, date of incorporation and registered address, or principal place of business of the customer. Entry should reflect that company is Active.

- Memorandum of Association or equivalent document.
- Register of Directors, or an official document that would contain the list of directors, such as an Annual Return, where applicable.
- Register of Shareholders, or an official document that would contain the list of shareholders, such as an Annual Return, where applicable

Documents for High-Risk Corporate Customers:

- Certificate of Incorporation or a search in the official company registry of the jurisdiction of incorporation of customer, which contains the company's official full name, registration number, date of incorporation and registered address, or principal place of business of the customer. Entry should reflect that company is Active.
- Memorandum of Association or equivalent document.
- Register of Directors, or an official document that would contain the list of directors, such as an Annual Return, where applicable.
- Register of Shareholders, or an official document that would contain the list of shareholders, such as an Annual Return, where applicable.
- Corporate Structure showing shareholders >=25% – Organogram.
- Source of Wealth (SOW)/Source of Funds (SOF) supported with documents.

When the customer is a corporate entity, the following information must be derived from the corporate documents:

- Company registration Full Legal name;
- Company registration number;
- Country of Incorporation;
- Date of Incorporation;
- Registered address.

If the shareholder is a corporate shareholder, the company documents of that shareholder should be obtained until a UBO (described below) is ultimately reached. Note that the UBO is always a natural person. When the Customer is a Sole Trader that must register with its local jurisdiction, the Sole Trader must submit a copy of the official registration.

4.1.2. Identification of Directors

In the case of directors who are natural persons, identification should be carried out by:

1. referring to the list of directors contained in the most recent version of the Memorandum and Articles of Association; or
2. performing a company registry search (provided that the officers of the company are listed therein); or

3. by obtaining a copy of the directors' register of the company.

In the case of corporate directors, the details of the corporate director's official full name, registration number, date of incorporation or registration and registered address or principal place of business must be obtained.

4.1.3. KYC for Ultimate Beneficial Owners (UBO's)

In the case of a body corporate or a body of persons, an Ultimate Beneficial Owner (UBO) is defined as a natural person who has:

- via ownership or other type of control, has the final dominant influence over a natural or legal person;
- in whose interests, for the benefit of whom or in whose name a transaction or operation is made;
- Direct/indirect ownership or control of 25% or more (including bearer shares); or
- Direct/indirect ownership or control of 25% or more voting rights
- Any natural person who otherwise exercises control over the management of that body corporate (even if such person owns less than 25% of the shares).

In the case of a legal entity or legal arrangement (e.g. foundation, association, fund or trust) which administers and distributes funds, the UBO is considered to be:

- A natural person who is the beneficiary of at least 25% of the property;
- The class of persons in whose main interest the legal entity or arrangement is set up or operates;
- A natural person who controls at least 25% of the property of the legal entity or arrangements.

Where the beneficial owner of a company is a trustee, the following persons is considered as beneficial owners:

- the settlor of the trust or the establisher of the arrangement;
- the trustee;
- the person ensuring and controlling the preservation of property, where such person has been appointed;
- the beneficiary, or where the beneficiary or beneficiaries are yet to be determined, the class of persons in whose main interest such trust or arrangement has been set up or operates;
- any other person who in any way exercises ultimate control over the property of the trust or arrangement.

Required
Information

UBO

The following information is required and must be recorded for UBOs:

- Official full name;
- Place and date of birth;
- Permanent residential address;
- The expiry date of the identity document and its place of issue
- Nationality.

4.1. Know Your Client (KYC)

Know Your Customer refers to Individual customers. Documents that must be obtained: Collect necessary identification documents (e.g., government-issued ID, proof of address).

Verify the authenticity of the documents.

Initial Contact: Engage with the client to gather basic information.

Provide an overview of the onboarding process.

Pre-Screening: Perform a preliminary risk assessment based on the client's profile.

Determine if the client falls within acceptable risk parameters.

Application Submission: Collect detailed information through application forms.

Obtain consent for background checks and verification.

KYC (Know Your Customer) Process: Conduct thorough KYC checks to verify the client's identity.

Assess the client's risk profile and categorize as low, medium, or high risk.

AML (Anti-Money Laundering) Checks: Screen the client against global sanctions lists.

Assess the potential risk of money laundering or other financial crimes.

Regulatory Compliance Checks: Ensure compliance with relevant regulatory requirements.

Confirm that the client meets legal and industry-specific standards.

Risk Assessment: Evaluate the overall risk associated with the client based on various factors.

Assign a risk rating and determine the level of due diligence required.

Approval Process: Submit the client's information and risk assessment for internal review and approval. Obtain necessary approvals from compliance or risk management teams.

Account Setup: Create the client's account in the system. Provide necessary credentials and account details.

Welcome Package: Send a welcome package to the client, including relevant information about the services, terms, and conditions.

Client Education: Educate the client about the organization's products, services, and policies.

Provide information on how to use and access services. Ongoing Monitoring: Implement

continuous monitoring of the client's transactions and behavior. Update client information

regularly and conduct periodic reviews. Record Keeping: Maintain detailed records of the client's onboarding process, communications, and transactions. Ensure compliance with record-keeping

requirements. Feedback and Improvement: Collect feedback from the client regarding the onboarding process. Use feedback to improve and refine the onboarding process.

5. ENHANCED DUE DILIGENCE

TSIRADU SOLUTIONS Sp. z.o.o. applies Enhanced Due Diligence measures to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing.

Enhanced Due Diligence measures are applied always when:

- 1) there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
- 2) the customer is PEP, or for corporate clients – PEP is involved in the corporate structure;
- 3) AML Risk Level represents High Risk;
- 4) Customer is from High Risk Third country (place of residence or seat)

AML Officer may apply one or several of the following due diligence measures:

- Requiring additional documentation and information not already provided by the applicant. The documents required need to cover both the identity and residential address of each UBO. One document (e.g. a bank statement) may be relied on where it confirms both the identity and the address. If a copy of the utility bill and a copy of the passport have already been utilised as part of Initial CDD, then different documents would need to be provided in order to satisfy this requirement. (Bank Statement)
- Require certified true copies of the documentation provided. This measure consists in the certification/Apostille of the documentation used in the due diligence process by a lawyer, accountant, a notary, a senior official of a financial or credit institution on behalf of same.
- Require certified confirmation of the documentation through a written statement supplied by a person carrying out relevant financial business. E.g. a letter from a bank confirming that customer due diligence has been performed on the customer and its UBOs and certifying the details of the corporate and UBOs, names, ID numbers, place and date of birth, nationality and address. (Banking Reference, Proof of Good Standing).
- Request the customer to transfer a minimal amount of money from an account held in its name into an account in the name of TSIRADU SOLUTIONS Sp. z.o.o. This procedure would require the customer to affect a minimal payment to one of the TSIRADU SOLUTIONS Sp. z.o.o. accounts and it is intended to verify that a

reputable banking institution has conducted KYC checks on the customer. (Bank-to-Bank transfer)

- Source of Wealth/Source of Funds. This measure refer to High Risk customers and customers where noticed PEP involvment. Source of Wealth (SOW) refers to the origin

of the customer's entire body of wealth (Ownership of a business, employment, inheritance, investments) while Source of Funds (SOF) refers to the origin of the particular funds or any other monetary instrument which are the subject of the transaction between a Financial Institution and the customer (Funds are from a saving account owned by parents, funds are from X Bank account owned by a company).

- Enhanced Ongoing Monitoring. For High Risk customers must be applied enhanced KYC and Transaction monitoring, meaning, that High Risk customers should be reviewed for KYC documents every six months. Transaction Analysis has to be conducted and AML Risk Level Reassessed.

For High-Risk customers AML Officer must obtain the approval of Senior Management and/or MLRO to continue the business relationship.

Original Documents, Apostille and Certified True Copies

Corporate documents provided by the customer must be original or downloaded copies which are signed and dated by the company director, company secretary, company registrar in that jurisdiction, or a lawyer, notary, accountant or financial or credit institution.

When we require a certified true copy of any other document, the document must be signed by a lawyer, notary, accountant or financial institution. Such certification should contain the following:

- Statement that the document is a true copy of the original document;
- In the case of a photo, that such photo is the true likeness of the person;
- The certifier must sign and date the document;
- The certifier must clearly state his name and designation or capacity;

The AML Officer should run searches on the certifier to ensure that such person exists and has the capacity of a lawyer, notary public or accountant. Where the AML Officer cannot find any confirmation about the existence and the capacity of the certifier and/or such certifier is from a country that is considered high risk, the AML Officer may request a copy of the document apostilled by the competent authority.

5. SIMPLIFIED DUE DILIGENCE

Entities and/ or Individuals can qualify for Simplified Due Diligence if following criteria are met:

- Ø Low-transaction- value customer
- Ø EU/EEA and/or FATFA members states Licensed Payment Institutions (PI)
- Ø Credit institutions;
- Ø Insurance companies (long-term);
- Ø Publicly listed entities.
- Ø Customers with Low AML Risk Level.

To qualify for SDD on the basis of its license, the entity in question must be fully licensed and the license must be active. In the event that any of the above category of applicants are involved in the customer corporate structure, the customer may qualify for Simplified Due Diligence (SDD), unless other risk factors indicate that SDD should not be applied in such circumstances.

In the case of publicly listed entities, it is not necessary that the entire shareholding be listed for SDD to be applicable as long as all the other criteria are met. Where SDD may be applied, TSIRADU SOLUTIONS Sp. z.o.o. is not required to identify or verify the applicant for business or UBO, need not obtain information relating to the purpose or intended nature of the business relationship. When an entity qualifies for SDD, TSIRADU SOLUTIONS Sp. z.o.o. verifies the following (usually through information publicly available online):

- Ø The public listed company is in good standing;
- Ø The stock exchange is in a reputable jurisdiction;

6. PEP/SANCTION SCREENING

Sanctions are the withdrawal of customary trade and financial relations for foreign and security policy purposes and are utilized by national governments as well as international organizations. Sanctions may be comprehensive, prohibiting commercial activity regarding an entire country or region, or they may be targeted, blocking transactions of and with particular businesses, groups, or individuals.

Sanctions have been used to advance a range of foreign policy goals, including counterterrorism, counter-narcotics, non-proliferation, democracy and human rights promotion, conflict resolution, and, more recently, cyber security.

Before the Company starts doing business with a new customer, AML Officer should review the various country sanction program requirements as well as published lists of known or suspected terrorists, narcotics traffickers, and other criminal actors for potential matches.

There are 3 main types of financial sanctions that TSIRADU SOLUTIONS Sp. z.o.o. should take in consideration:

- Ø Designated – usually, they are focused on specific persons or corporate bodies. The sanctions targets are determined in specific lists and usually are subject of assets freezing;
- Ø Geographical – they are related to imposed sanctions on entire countries or geographical areas;
- Ø Sectoral – imposed on specific business sectors, goods and/or services. Sometimes persons or corporate bodies could be also objects of sectoral sanctions, for example some goods or services are not permitted to be provided to them

To identify designated persons and entities, TSIRADU SOLUTIONS Sp. z.o.o. via Jumio screening solution provides screening in various watchlists and global and national sanctions lists, including:

- OFAC sanctions list,
- UN sanctions list (equal to EU sanctions lists),
- HMT sanctions list,
- global PEP database for 220+ countries and territories
- others.

TSIRADU SOLUTIONS Sp. z.o.o. position is not to accept business relationships with Sanctions targets and not to provide services within some countries and jurisdictions, subject of imposed sanctions – please refer to *Appendix 2 – Prohibited List of Countries*

Any potential matches are immediately verified prior to onboarding if confirmed as false matches. If a true match is detected, the onboarding is unsuccessful, and the relationship is declined. Further actions (such as reporting to the authorities) may be taken on case-by-case basis and if required.

TSIRADU SOLUTIONS Sp. z.o.o. is a subject to sanctions compliance and are required to screen customers and transaction records against periodically updated lists that include individuals and entities designated or identified by governmental bodies. Sanctions lists identify terrorists, terrorist organizations and supporters of terrorism etc.

In order to meet requirements TSIRADU SOLUTIONS Sp. z.o.o. conduct Adverse Media, PEP and Sanction screening using trustable and reliable system - Comply Advantage, that is implemented in our vendor Jumio. TSIRADU SOLUTIONS Sp. z.o.o. signed Agreement with Jumio, that provided screening services. Screening Service is provided from Comply Advantage system.

6.1. PEP's

A corporate customer with UBO(s) or director(s), or Individual who are Politically Exposed Persons (PEPs) include:

- Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries, Members of Parliament;
- Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors, Audit Committees or the boards of central banks;
- Ambassadors, chargés d'affaires and other high ranking officers in the armed forces;
- Members of the a TSIRADU SOLUTIONS Sp. z.o.o. inistration, management or boards of State-owned corporations.

In addition to the above, a spouse, child or parent of any of the above individuals is also classified as a PEP. Where a PEP is involved, such cases must:

- Have authorized senior management approval for establishing a business relationship with such a person;
- Take risk based and adequate measures to establish the source of wealth of the PEPs and source of funds involved;
- Conduct enhanced ongoing monitoring of the business relationship.

Similar requirements are to be met, within a reasonable time frame, in the event that an individual or UBO, during the course of the business relationship, turns out to be or

becomes a PEP. By virtue of the position and the influence that a PEP may hold, such person generally

presents a higher risk for potential involvement in bribery and corruption. This is why extra diligence should be exercised when dealing with PEPs.

The AML Officer should also consider requesting further documentation where adequate. Should the AML Officer not be entirely certain whether the person in question is a PEP or not, the AML Officer should request a declaration entitled “PEP Declaration” from the potential PEP, confirming or otherwise.

For politically exposed persons, the following follow-up measures might be applied:

- Requesting additional information from the customer in order to identify sources of assets and funds used in business relationships or transactions;
- Checking the data or making inquiries into the databases of state authorities of the respective country and the search and verification of data on the Internet;
- Making inquiries or verifying data from websites of the relevant supervisory authorities or institutions of the customer’s or persons home country.

Regarding a politically exposed person, additional vigilance measures shall be taken at least 12 months after the politically exposed person has ceased to fulfil significant public duties.

6.2. Sanction Screening

TSIRADU SOLUTIONS Sp. z.o.o. shall use Comply Advantage or other system that might be changed in the future) for sanction screening, that uses the information from dozens of publicly available and proprietary databases to help customers meet their AML requirements, eliminate fraud, and protect business and reputation. An effective screening system relies on both ‘exact’ and ‘inexact’ name matching for accurate identification as fraudsters often transpose names and other data trying to conceal their identity. Therefore, Comply Advantage screening system is using fuzzy match that is a technology that identifies spelling variations of the names and other search terms in case a character was omitted, inserted, or replaced either occasionally or on purpose.

Frequency of screening

Type of data (source)	When the data gets to Sumsb
Adverse media (negative news)	within 48 hours after publication on the referral website
Sanctions and watchlists	within 15 minutes after publication on the source website
Politically exposed persons (PEPs)	within 1 month after the source database update
National warning lists (e.g. EU Most Wanted warnings)	within 1 month after the source database update
Fitness and probity (senior employees competence) watchlists	within 1 month after the source database update

Findings

:

Ø Adverse Media (Negative news)

Alerts with regards of Adverse Media must be reviewed by AML Officer. AML Officer must conduct research and identify if there is a true connection between our customer and provided Adverse Media Match. Adverse Media Articles older than 5 years can be disregarded if they are not related to ML/TF, unless the content of the findings is of such a concerning nature that in the opinion of the AML Officer, they should be taken into account, despite the lapse of time. In case of doubt, the AML Officer may refer the matter to Head of Compliance for further guidance. Adverse Media must be published in trustable, reliable, and independent sources. AML Officer should use critical thinking when reviewing online reviews and identify trustable source from scam or competitors created websites. Positive Adverse Media should be outlined in AML Risk Score Tool as soon as positive Adverse Media is identified, even if Adverse Media noticed after business relationships has been established.

Ø Sanction and watchlists

Alerts with regards of Sanctions and/or watchlists must be reviewed by AML Officer. TSIRADU SOLUTIONS Sp. z.o.o. will not conduct business relationships with sanctioned entities and/or individuals. Each case should be reviewed case by case base.

Ø Politically exposed persons (PEP)

Please refer to 6.1. section.

Ø National Warning lists (EU Most Wanted warnings)

Alerts with regards of National Warning lists must be reviewed AML Officer and is case by case based.

7. RECORD KEEPING

Copies of all documents related to TSIRADU SOLUTIONS Sp. z.o.o. Customers Identification Procedures will be retained for an appropriate period of time and, at a minimum, the period of time required by applicable law or regulation. The documents the Company retains are copies of documents reviewed in connection with Customers Identification Procedures or enhanced due diligence procedures.

TSIRADU SOLUTIONS Sp. z.o.o. will retain documents for so long as a Customer is a Customer of the Company and for a minimum of 5 (five) years after this relationship ends. TSIRADU SOLUTIONS Sp. z.o.o. shall, however, retain those records for a longer period where transactions, customers or accounts involved litigation, or it is required by court or other competent Authority. The Company shall satisfy, on a timely basis, any enquiry or order from the relevant competent authorities.

All records must be kept in a form which is immediately accessible upon request. Records do not have to be kept in hard copy. Retention may be by way of original documents, or by way of copies in any machine-readable or electronic form from which a paper copy can be readily produced.

During onboarding AML Officer creates Corporate customers folders named as per customers Legal Name. All documents provided by customers must be saved in the folder. During Onboarding process folders must be saved in “Corporate Customer in Onboarding Process” folder:

Ø Compliance - General\05 Clients files\Corporate Clients\2. Corporate Customers in Onboarding Process

Once Corporate customer is Approved the folder must be moved to “All Active Customers” folder:

Ø Compliance - General\05 Clients files\Corporate Clients

Once Corporate customer is Terminated folder must be removed to “Inactive Customers”:

Ø Compliance - General\05 Clients files\Corporate Clients\5. INACTIVE Customers

Corporate Customers folder is made the following way:

1. CAF/Agreement – Customer Application Form and Agreement
2. Corporate – Corporate KYC documents for all involved entities
3. UBO, Directors – Full KYC pack on UBO’s and Directors
4. Licenses and LO – If applicable license must be saved here, or if applicable Legal Opinion
5. Screening – Adverse Media Checks, PEP, Sanction Screening checks, Website Checks
6. AML, KYC policies – if applicable AML policy and/or KYC/Onboarding policy must be saved here
7. AML Risk Assessment – AML Risk Score Matrix and AML Risk Assessment doc. must be saved here

8. Monitoring – KYC, Transaction Monitoring, Internal Investigations must be saved here.

9. Emails, Escalations, Approvals – all relevant emails, escalations to MLRO and/or Senior

Management and Approvals from MLRO and/or Senior Management must be saved here.

Documents

- 1. CAF, Agreement
- 2. Corporate
- 3. UBO, Directors
- 4. Licenses and LO
- 5. Screening
- 6. AML, KYC policies
- 7. AML Risk Assessment
- 8. Monitoring
- 9. Emails, Escalations, Approvals

AML Officers conducted internal reports, adverse media checks, transaction analysis, internal approvals and any other information related to corporate customer must be documented and saved in the corporate customer folder.

For individuals all documents will remain in Jumio platform, however in cases where AML Officer conducts internal investigation, transaction analysis, applies additional scrutiny for individual, or company received request for information from the regulators, authorities or Law Enforcements, folder must be created, and supporting/additional documents must be saved on the folder. Folders must be named as per individuals NAME and SURNAME. Individuals folders must be saved in “Individuals” folder:

Compliance - General\05 Clients files\Individuals

8. STAFF TRAINING

A supervisor shall be assigned to create training program for new employees. Supervisor's duties are to teach employees in relation to all policies, procedures, customer documentary forms and requirements. A training for every new employee must be provided within first month.

The Company provides AML training to \employees who will be dealing with customers or will be involved in any AML tasks - identification, verification, or monitoring processes. The Company will conduct its training internally once every year to employees to whom AML/CFT is relevant. Training will be conducted in form of presentation and afterwards test. Training results must be documented and saved in the personnel folders.

Compliance - General\07 Personnel

The Company's AML training programs are aimed to ensure its employees to get an appropriate training level with regards to any possible ML/TF risks.

Training that will be provided for employees is:

- Relevant to today's challenging working environment.
- Practical so everyone can apply his learning to the role immediately.
- Global with an emphasis on international best practice but using local expertise.
- Interactive with a combination of first-class online materials and face to face teaching.

APPENDIX 1 – ACCEPTED/PROHIBITED INDUSTRIES

1) Financial Services



Requirements:

- The customer must be the entity that holds the licence. Licences of a parent company are accepted;
- Customers involved in the following currency exchange fields – Forex, e-wallets and MSBs – are considered on a case-by-case basis.
- The customer is required to be licensed within the EU in the country where their main business is located and, in the jurisdictions, where they offer their services. Without these licences, the customer may not actively target these countries. Russia, the USA, Canada, Japan and China.
- The customer must be well-established, must have been processing for at least two years, must have adequate fraud and AML/CFT processes and provide their last 6- months processing history.
- The customer must have and provide a copy of the following documents:
 - ü AML and KYC policies
 - ü Full EMI, PI licence for MSBs
 - ü the completed questionnaire
- Customers involved in the following activities must provide a business plan:
 - ü buying, selling, or brokering securities, stocks, bonds, commodities, and mutual funds
 - ü third party payment service providers
 - ü payday loan providers (subject to a clean processing history and full liability of the partner) pre-paid debit cards



Prohibited List

- Corporates selling e-vouchers where we do not have visibility of the end retailer or where the e-voucher is redeemed.

2) Gambling

Requirements:

- Allowed activities: gambling, gambling advice and forecasting, sports betting, odds- making.
- The corporates website must have age-restriction measures.
- The corporates must be licensed in the country in which they are incorporated, which must be in the EEA.
- Should the customer want to offer online gambling activities in EEA states other than their country of incorporation, they may have to present a local licence in such country (depending on the national laws of that country). If this is not available and the targeted country requires such a licence, the customer may not actively target that country. The only EEA states where online gambling may be targeted and advertised without requiring a local licence are:
 - ü Bulgaria
 - ü Cyprus ü
 - Malta
- The customer must provide:
 - ü KYC & AML policies
 - ü last 6-months' processing history
 - ü the latest audited financial statement (for customers with expected turnover more than Euro 500K per month)
 - ü the completed questionnaire



Prohibited List:

- Lottery syndicates
- Unlicensed activities
- Gambling customers registered in the USA and Turkey where online gambling is prohibited.
- For customers targeting Germany, Finland, Greece, Norway and the Netherlands, a legal opinion is required confirming that the customers activities follow applicable rules in these countries.

3) Gaming

Requirements

- Where the winner of a game receives cash and/or a prize of monetary value in relation to the game, the customer is requested to provide the following information:
 - ü copy of their licence (where applicable) or a legal opinion issued by a reputable law firm from their country of incorporation, confirming that they do not require a licence to operate and/or offer services in that jurisdiction;
 - ü customers targeting the USA must obtain a legal opinion by a reputable US law firm, addressed to the TSIRADU SOLUTIONS Sp. z.o.o.
- If the customers gaming platform is linked to a third-party platform, the customer must provide a copy of the agreement/authorisation to link to the third-party platform (i.e., evidence that the linking is explicitly authorised by the third party).
- Skill games customers must provide certification from a qualified independent third party demonstrating that the customers systems ensure that the skill games business remains within legal limits where USA traffic is targeted and includes:
 - ü age and location verification, as applicable; and
 - ü all screenshots relevant to the certification (for example, age verification process)



Prohibited List:

- Sale of in-game currency in a virtual environment where the merchant is not the operator.

4) Marketing

Requirements:

Permitted marketing activities:

- direct marketing.
- outbound telemarketing services, non-recurring billing (as evidenced in processing history and financial statements)

Multi-level marketing customers must:

- be well established and in operation for a minimum of 5 years
- have an AML policy.
- provide a description of the type of products sold
- have a compensation model that allows compensation for sales but not for introduction of other participants.
- have a compensation model that allows compensation for sales but not for introduction of other participants.
- be enrolled with an MLM or direct selling association (ensuring a consumer protection/code of ethics to which members must adhere).

Prohibited



List:

- Pyramid sales.
- Bulk marketing tools.
- Direct marketing of questionable products, such as dieting cures and other get-rich-quick schemes.
- Programs that offer compensation for the introduction of new participants.

5) Weapons

Prohibited



List:

- Weapons, including, without limitation, knives, guns, firearms or ammunition.

6) Travel & Cruise Line Offerings

Travel-related services are considered high-risk because of a longer period of chargeback probability due to the long period of service fulfilment. This risk may be mitigated through a clean processing history. Cruise line offerings also fall under this category.

Requirements:

- Customer must provide a clean processing history for the last 6 months.
- Customer providing holiday packages/deals directly as travel agencies or tour operators must be licensed/authorised by the relevant authority in the country in which they are offering holiday packages (Except for Germany and the Netherlands. However, merchants in Germany and the Netherlands must be licensed/authorised if they are directly selling railway tickets and flight tickets).
- Customers offering intermediary services, whereby a database of travel agents is provided to consumers, do not have to be licensed as travel agents/tour operators
- Customers offering flight bookings must be licensed. Customers offering flight bookings on behalf of another entity (a licensed entity), as an agent, must provide a copy of their agency agreement.
- Customers must provide proof of cooperation agreements with hotels, airlines or travel operators.
- Customers offering flights must be members of IATA.
- Customers must provide an audited financial statement.
- In the event that licensing is not available in their jurisdiction, the customers must provide proof of insurance coverage.



Prohibited List:

- Customer selling timeshares.

7) Drugs, Medical Devices, Nutra & Pharma



Requirements:

Medical and dental devices:

- must be approved by the relevant regulatory entity.
- must be manufactured by the original manufacturer (not counterfeit) and sold before their expiry date.

Note: Examples of medical devices include condoms, contact lenses (prescription and coloured), test kits and instruments used by medical professionals Nutraceuticals and diet control substances:

- business model should be based on single sales (no recurring billing).
- the merchant must have been in operation for at least two years.
- the merchant must provide his last 6-months' processing history
- chargeback rate must be under 1%.

Cosmetics merchants must provide:

- proof of notification of products on CPNP.
- authorisation or certification from a competent authority.
- a copy of an invoice or reseller agreement



Prohibited List:

- Drugs and marijuana dispensaries (and affiliated services);
- Pharmaceuticals and transactions involving narcotics, steroids, certain controlled substances or other products that present a risk to consumer safety;
- Any illegal substances (including Spanish Fly) or substances that can be used to produce illegal substances (such as seeds and plants).
- Miracle cures.
- Male enhancements.
- Substances designed to imitate illegal drugs, also known as legal highs (herbal smoking blends, herbal incense, bath salts, etc.).
- Merchants who offer subscriptions with automatic renewal, following a free or low-cost purchase for the following industries:
 - ü nutraceuticals (Acai berry or health related drinks or tea.)
 - ü pseudo-pharmaceuticals (weight loss, anti-aging, muscle building, sexual stimulant supplements, colon cleansers, detox products, HCG, of HGH-like substances).
 - ü beauty cosmetics products (teeth whitening, anti-wrinkle, tanning).
 - ü medical devices and products (glucose strips)
 - ü dental devices

8) Computer Equipment and IT Support



Requirements:

The merchant must provide documentation showing that they are an authorised reseller or a well-established company for the following:

- sale of computer software; or
- provision of computer programming services, system design and data processing services on a contract or fee basis.

Computer hardware and software services merchants must show that they are an authorised reseller or well-known brands.

Merchants offering VoIP services: VoIP calls and VoIP minutes must:

- be a well-established company that has been in operation for at least two years; and
- provide their last 6-months processing history, even if VoIP is only part of the services offered by the merchant.



Prohibited List:

- Remote technical, desktop support and repairs.
- Unauthorised resellers

9) Government Related



Prohibited List:

- Government IDs and/or licences, and other no-value-added services.
- Official documents or uniforms
- Involvement in sale of activities that are identified by government agencies as being potentially fraudulent
- Governmental Application Support Services

APPENDIX 2 – PROHIBITED LIST OF COUNTRIES

Afghanistan
Albania
Barbados
Botswana
Burkina Faso
Burma
Burundi
Cambodia
Cayman Islands
Central African Republic
Crimea
Cuba
Democratic People's Republic of Korea(DPRK)
Democratic Republic of the Congo
Ghana
Haiti
Iran
Iraq
Jamaica
Lebanon
Libya
Mali
Malta
Mauritius
Morocco
Myanmar
Nicaragua
Pakistan
Palestine
Panama
Philippines
Senegal
Somalia
South Sudan
Sudan
Syria
The Bahamas
Trinidad and Tobago
Uganda
United States of America
Vanuatu
Venezuela
Yemen
Zimbabwe