PROCRYPTIC SP. Z O.O.

Polityka przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu

(“Procryptic Polityka AML/CTF”)

Wersja:	1
Wyprodukowano	czerwiec 2023

1. WSTĘP

Celem niniejszej Polityki AML/CTF Procryptic jest określenie i opisanie procedur, polityk, regulacji i mechanizmów, które zostały ustanowione, wdrożone i utrzymywane przez Procryptic sp. z o.o. zgodnie z obowiązującym prawem. Procedury te zostały opracowane w celu ustanowienia, wdrożenia i utrzymania polityk, kontroli i procedur umożliwiających wykrywanie, zarządzanie oraz skuteczne przeciwdziałanie i łagodzenie prania pieniędzy i finansowania terroryzmu (dalej "**ML/TF**").

Procryptic sp. z o.o. z siedzibą w Warszawie (dalej "**Firma**") została założona przez Metafortune Limited w celu świadczenia usług związanych z wirtualnymi walutami zgodnie z wpisem w rejestrze działalności związanej z wirtualnymi walutami (nr RDWW-83).

Firma jest zobowiązana działać zgodnie z polskimi przepisami prawnymi dotyczącymi ML/TF.

Ten dokument jest przeznaczony wyłącznie do użytku wewnętrznego Firmy i jej zainteresowanych osób. Ten dokument lub jakakolwiek jego część może być ujawniona i/lub udostępniona innym osobom, w tym audytorom i organom nadzorczym, tylko w przypadkach i na warunkach, które są przewidziane w tym dokumencie lub przez prawo.

Każdy pracownik jest zobowiązany potwierdzić na piśmie, że zapoznał się z tą Polityką AML/CTF Procryptic. Szablon potwierdzenia jest załączony jako Załącznik 1 do tej Polityki AML/CTF Procryptic.

Istotne przepisy i odniesienia:

- Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (dalej **„Ustawa o AML")**
- Dyrektywa (UE) 2015/849 Parlamentu Europejskiego i Rady z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do celów prania pieniędzy i finansowania terroryzmu, zmieniająca rozporządzenie (UE) nr 648/2012 Parlamentu Europejskiego i Rady, uchylająca dyrektywę 2005/60/WE Parlamentu Europejskiego i Rady oraz dyrektywę Komisji 2006/70/WE (dalej „**Dyrektywa**")

Osoba ds. ML/TF (MLRO) działa jako osoba wskazana w artykule 8 Ustawy o AML - pracownik odpowiedzialny za nadzór nad zgodnością działania Firmy z przepisami prawa dotyczącymi ML/TF. MLRO jest również odpowiedzialny za nadzór nad przestrzeganiem wewnętrznych procedur i raportowania dotyczących ML/TF przez Firmę.

2. OCENA RYZYKA

2.1. Firma identyfikuje i ocenia ryzyko ML/TF związane z jej działalnością, biorąc pod uwagę czynniki ryzyka dotyczące klientów, krajów lub obszarów geograficznych, produktów, usług, transakcji lub ich kanałów dostarczania zgodnie z niniejszą Polityką AML/CTF Procryptic, zwracając szczególną uwagę na:

2.1.1. Informacje o ML/TF udostępniane Firmie przez właściwe organy regulacyjne i rządowe (jeśli dotyczy) oraz

2.1.2. W odniesieniu do każdego czynnika ryzyka klienta określonego w punkcie 2.5 - prawdopodobieństwo jego wystąpienia, konsekwencje jego wystąpienia oraz prawdopodobieństwo zwiększenia tego ryzyka.

2.2. Ocena ryzyka, o której mowa w punkcie 2.1, jest przygotowywana i przechowywana w formie elektronicznej. Ocena ryzyka jest aktualizowana w razie potrzeby, ale co najmniej co 2 lata, przez MLRO. Aktualizacje powinny być przeprowadzane zwłaszcza w przypadku zmian czynników ryzyka dotyczących klientów, krajów lub obszarów geograficznych, produktów, usług, transakcji lub ich kanałów dostarczania lub zmiany oceny ryzyka na szczeblu krajowym i raportu Komisji Europejskiej, o którym mowa w art. 6 ust. 1 do 3 Dyrektywy. MLRO przedstawia wyniki oceny ryzyka Zarządowi wraz z rekomendacjami dotyczącymi ewentualnych wymaganych zmian w środkach lub procedurach Firmy.

2.3. Na żądanie Generalnego Inspektora Informacji Finansowej ("GIIF"), Firma jest zobowiązana dostarczyć swoją ocenę ryzyka oraz inne informacje, które mogą wpływać na ocenę ryzyka na szczeblu krajowym..

2.4. Firma identyfikuje i ocenia ryzyko ML/TF związane z jej klientami.

2.5. Firma w szczególności bierze pod uwagę następujące czynniki podczas oceny ryzyka ML/TF klientów:

a) typ klienta,

b) obszar geograficzny,

c) cel konta,

d) typ produktów, usług i metod dystrybucji,

e) kwota wartości majątkowych wpłaconych przez klienta lub wartość przeprowadzanych transakcji,

f) cel, regularność lub czas trwania relacji biznesowej.

2.6. Firma bierze pod uwagę powyższe i kategoryzuje Klientów zgodnie z niniejszą Polityką AML/CTF Procryptic (jako Klientów o wysokim, standardowym lub niskim ryzyku), biorąc pod uwagę okoliczności, które mogą wskazywać na wyższe lub niższe ryzyko ML/TF określone w art. 42 i 43 Ustawy o AML oraz w punktach 5 i 6 niniejszej Polityki AML/CTF Procryptic. Biorąc pod uwagę ocenione ryzyko, Firma określa rodzaj i zakres środków, które przyjmuje, aby skutecznie zarządzać i łagodzić zidentyfikowane ryzyka zgodnie z Polityką AML/CTF Procryptic.

2.7. Firma stosuje następujące środki zabezpieczenia finansowego, które obejmują:

a) identyfikację klienta i weryfikację jego tożsamości (zgodnie z pkt 3);
b) identyfikację właściciela rzeczywistego i podjęcie rozsądnych działań w celu:
    i. weryfikacji jego/jej tożsamości;
    ii. ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną, jednostką organizacyjną nieposiadającą osobowości prawnej lub trustem;
        - zgodnie z pkt. 3.
c) ocena relacji biznesowych i, w razie potrzeby, uzyskanie informacji o celu i zamierzonej naturze tych relacji – zgodnie z procedurami onboardingu w Firmie oraz formularzem KYC;
d) bieżące monitorowanie relacji biznesowych klienta, w tym:

i. analiza transakcji podejmowanych w trakcie trwania relacji biznesowych, aby upewnić się, że są one zgodne z wiedzą Firmy na temat klienta, jego rodzaju działalności i zakresu oraz z ryzykiem ML/TF związanym z tym klientem – zgodnie z Załącznikiem 2;
ii. badanie źródła pochodzenia wartości majątkowych będących w dyspozycji Klienta - w uzasadnionych przypadkach – zgodnie z Załącznikiem 3;
iii. zapewnienie, że dokumenty, dane lub informacje dotyczące relacji biznesowych są aktualne – zgodnie z Załącznikiem 3.

2.8. Firma nie akceptuje następujących kategorii Klientów, którym zabrania się nawiązywania jakichkolwiek relacji biznesowych z Firmą:

a) Klientów, którzy nie dostarczają wystarczających dokumentów i/lub informacji do założenia i weryfikacji swojej tożsamości, struktury własności i właścicieli rzeczywistych,
b) Klientów, którzy podlegają sankcjom na podstawie decyzji właściwych organów Unii Europejskiej, OFAC lub innych organizacji międzynarodowych,
c) Obywateli niektórych krajów, w których działalność Firmy jest zabroniona.

3. AKCEPTACJA KLIENTA & DOCHODZENIE PRAWA (CDD)

3.1. Firma przeprowadza proces dochodzenia prawa klienta (CDD).

3.2. Celem dochodzenia prawa klienta jest identyfikacja, w szczególności w przypadku:

3.2.1. osoby fizycznej:

a. imię i nazwisko,

b. narodowość,

c. numer PESEL lub w przypadkach, gdy osoba nie posiada PESEL - data i miejsce urodzenia,

d. seria i nr dokumentu potwierdzającego tożsamość (ID),

e. adres zamieszkania - jeżeli Firma posiada takie informacje,

f. nazwa (nazwa handlowa), Numer Identyfikacji Podatkowej (NIP) i adres głównego miejsca prowadzenia działalności – dotyczy przedsiębiorców.

3.2.2. osoby prawnej:

a. nazwa (nazwa handlowa)

b. typ jednostki prawnej,

c. adres siedziby lub biura,

d. Numer Identyfikacji Podatkowej (NIP), a jeśli klient nie posiada NIP - kraj rejestracji, nazwa rejestru handlowego, w którym klient jest zarejestrowany, numer i data rejestracji,

e. dane identyfikacyjne odnoszące się do pkt 3.2.1 dotyczące osoby działającej w imieniu klienta.

3.3. Identyfikacja rzeczywistego właściciela obejmuje ustalenie danych, o których mowa w punkcie 3.2.1(a) i (b), a gdy Firma posiada takie informacje - także danych, o których mowa w punkcie 3.2.1 (c)-(e) niniejszej Polityki AML/CTF Procryptic.

Identyfikacja osoby uprawnionej do działania w imieniu klienta obejmuje identyfikację danych, o których mowa w punkcie 3.2.1(a)-(d) niniejszej Polityki AML/CTF Procryptic.

Identyfikacja (1) klienta będącego osobą fizyczną, (2) rzeczywistego właściciela lub (3) osoby uprawnionej do działania w imieniu klienta – wymagane dokumenty

3.4. Weryfikacja dokumentu tożsamości polega na sprawdzeniu rodzaju prezentowanego dokumentu i sprawdzeniu, czy dane dostarczone przez klienta są takie same jak dane w dokumencie. Następujące dokumenty (ID) są akceptowalne jako dokumenty tożsamości:

   a. Dowód osobisty;

   b. Paszport;

   c. Karta pobytu,

3.5. pod warunkiem, że w przypadku klienta będącego obywatelem kraju spoza EOG, Firma powinna uzyskać od tego klienta kartę pobytu lub paszport.

3.6. Przy weryfikacji ID, pracownicy sprawdzają w szczególności:

   a. czy dokument jest ważny,

   b. czy nie ma wątpliwości co do jego autentyczności,

   c. czy dane osobowe widoczne na ID są takie same jak dane podane w umowie (imię, nazwisko, data urodzenia, numer PESEL [jeśli dotyczy]),

   d. czy dokument jest czytelny i czy dostarczona kopia nie była poddawana modyfikacji, w szczególności czy dane identyfikacyjne pozostają niezmienione.

3.7. Weryfikacja dodatkowego dokumentu potwierdzającego tożsamość polega na sprawdzeniu rodzaju prezentowanego dokumentu. Akceptowane są następujące dodatkowe dokumenty:

   a. Dowód osobisty (jeśli nie został odebrany na podstawie klauzuli 3.5 jako dokument tożsamości);

   b. Paszport (jeśli nie został odebrany na podstawie klauzuli 3.5 jako dokument tożsamości);

   c. Karta pobytu (jeśli nie została odebrana na podstawie klauzuli 3.5 jako dokument tożsamości);

   d. wyciąg bankowy lub inny dokument związany z działalnością bankową (wydany nie wcześniej niż 3 miesiące przed dniem zawarcia umowy);

   e. prawo jazdy;

   f. rachunek telefoniczny (wydany nie wcześniej niż 3 miesiące przed dniem zawarcia umowy);

   g. rachunek za usługi komunalne dotyczące usług świadczonych okresowo na miejsce zamieszkania (wydany nie wcześniej niż 3 miesiące przed dniem zawarcia umowy);

   h. decyzja podatkowa (wydana nie wcześniej niż 12 miesięcy przed dniem zawarcia umowy);

i. dokument rządowy (wydany nie wcześniej niż 12 miesięcy przed dniem zawarcia umowy);

j. legitymacja studencka lub doktorancka (ważna w dniu zawarcia umowy);

k. certyfikat rejestracyjny (ważny w dniu zawarcia umowy).

3.8. Firma ma obowiązek zbierania i weryfikacji przynajmniej jednego dokumentu tożsamości (paragraf 3.5) dodatkowo do co najmniej jednego dodatkowego dokumentu tożsamości, jak określono powyżej w paragrafie 3.7.

<u>Identyfikacja osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej - wymagane dokumenty</u>

3.9. Właściwa identyfikacja osoby prawnej lub jednostki organizacyjnej, w szczególności w przypadku jednostki wpisanej do Krajowego Rejestru Sądowego (KRS), wymaga uzyskania:

a. oryginału lub kopii aktualnego wyciągu z odpowiedniego rejestru - jeżeli dane przedsiębiorcy są dostępne w eKRS lub innych publicznych rejestrach przedsiębiorców, pracownik może dołączyć wydruki z powyższych rejestrów do dokumentacji klienta,

b. oryginału lub kopii zaświadczenia o przyznaniu statystycznego numeru REGON w przypadku polskich przedsiębiorców. Jeżeli numer REGON jest zawarty w powyższym wyciągu, nie jest konieczne dostarczanie zaświadczenia o REGON. Jeżeli numer REGON nie jest zawarty w wyciągu z odpowiedniego rejestru firm, pracownik może pobrać zaświadczenie z Internetu na własną rękę i dołączyć je do dokumentacji klienta,

c. oryginału lub kopii zaświadczenia o przyznaniu odpowiedniego numeru identyfikacji podatkowej. Jeżeli, w przypadku polskich przedsiębiorców, numer NIP jest zawarty w wyciągu z KRS, wówczas wydruk wspomniany w punkcie a) jest wystarczający. Jeżeli numer NIP nie jest zawarty, pracownik może pobrać zaświadczenie z Internetu na własną rękę i dołączyć je do dokumentacji klienta,

d. listy beneficjentów rzeczywistych zawierającej ich imiona, nazwiska, adresy zamieszkania, numery PESEL lub daty urodzenia - jeżeli numer PESEL nie został przyznany, oraz kraje urodzenia, kopii dowodów tożsamości lub paszportów takich beneficjentów rzeczywistych,

e. wydruku z Centralnego Rejestru Beneficjentów Rzeczywistych, jeżeli to dotyczy,

f. imienia, nazwiska, obywatelstwa, numeru PESEL lub daty urodzenia (jeżeli numer PESEL nie został przyznany), i kraju urodzenia, kopii dowodu tożsamości lub paszportu osób upoważnionych do reprezentowania klienta,

g. kopii zaświadczenia wydanego przez bank lub wyciągu z konta bankowego zawierającego dane korporacyjne i szczegóły adresu zgodne z danymi podanymi w umowie.

3.10. W przypadku gdy dostarczone dokumenty nie są w języku polskim lub angielskim, musi być dostarczone ich prawdziwe tłumaczenie.

3.11. Firma może zażądać dodatkowych informacji i dokumentów zgodnie z Polityką AML/CTF.

3.12. Weryfikacja tożsamości klienta/beneficjenta rzeczywistego musi zostać zakończona przed nawiązaniem relacji handlowej, w szczególności przed zaakceptowaniem klienta i przed przeprowadzeniem sporadycznej transakcji.

3.13. Weryfikacja klienta (CDD) powinna być również przeprowadzana, gdy Firma przeprowadza sporadyczną transakcję:

a. o wartości równoważnej 15 000 EUR lub więcej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy jako kilka operacji, które wydają się być powiązane, lub

b. która stanowi transfer funduszy na kwotę przekraczającą 1 000 EUR,

c. korzystając z walut wirtualnych o równowartości 1 000 EUR lub więcej,

d. i kiedy Firma podejrzewa ML/TF lub ma wątpliwości co do prawdziwości lub adekwatności dokumentów lub informacji wcześniej uzyskanych do celów identyfikacji lub weryfikacji.

3.14. Weryfikacja tożsamości klienta i właściciela korzyści może być zakończona przez Firmę na początku relacji biznesowej, jeśli jest to konieczne, aby zapewnić ciągłość biznesu i istnieje niskie ryzyko ML/TF. W takich przypadkach weryfikacja powinna być przeprowadzona jak najszybciej po rozpoczęciu relacji biznesowej.

3.15. Firma może zawrzeć umowę z klientem i otworzyć konto klienta, umożliwiając klientowi handel, pod warunkiem zastosowania opisanych tutaj środków bezpieczeństwa finansowego.

3.16. Przed rozpoczęciem relacji biznesowych lub wykonaniem sporadycznej transakcji, Firma poinformuje klienta o przetwarzaniu jego danych osobowych, w szczególności o obowiązkach Firmy określonych w ustawie o przeciwdziałaniu praniu pieniędzy do zakresu przetwarzania danych.

4. CENTRALNY REJESTR BENEFICJENTÓW RZECZYWISTYCH (CRBR)

4.1. Różnice między informacjami zebranymi podczas procesu CDD a informacjami z Centralnego Rejestru Beneficjentów Rzeczywistych (CRBR), a także przeszkody zidentyfikowane w związku z weryfikacją tożsamości właściciela korzyści i działaniami podjętymi w związku z identyfikacją osoby na stanowisku kierowniczym jako właściciela korzyści, powinny być zgłaszane do MLRO.

4.2. Każda niezgodność wymieniona w punkcie 4.1 powinna być udokumentowana w systemie CRM Firmy w formie krótkiej notatki.

4.3. Firma podejmuje kroki w celu rozwiązania przyczyn niezgodności poprzez kontakt z klientem za pomocą e-maila i/lub telefonu. Jeśli niezgodności są potwierdzone, Firma powinna dostarczyć właściwemu organowi zarządzającemu CRBR zweryfikowane informacje na temat tych niezgodności, wraz z uzasadnieniem i dokumentacją zidentyfikowanych niezgodności.

4.4. Ten punkt 4 dotyczy tylko klientów podlegających rejestracji w CRBR (tj. polskich spółek handlowych).

5. UPOROSZCZONE ŚRODKI BEZPIECZEŃSTWA FINANSOWEGO

5.1. Firma może stosować uproszczone środki bezpieczeństwa finansowego w przypadkach, w których ocena ryzyka, o której mowa w punkcie 2.4, potwierdziła niższe ryzyko ML/TF.

5.2. Niższe ryzyko ML/TF może wskazywać w szczególności:

5.2.1. fakt, że Klient jest:

a) podmiotem sektora finansów publicznych, o którym mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznyce;
b) przedsiębiorstwem państwowym lub spółką z większościowym udziałem Skarbu Państwa, jednostkami samorządu terytorialnego lub ich związkami;
c) spółka, której papiery wartościowe są dopuszczone do obrotu na rynku regulowanym podlegającym wymogom ujawniania informacji o jej beneficjentach rzeczywistych wynikającym z przepisów prawa Unii Europejskiej lub przepisów kraju trzeciego odpowiadających tym przepisom, lub spółka z większościowym udziałem takiej spółki;
d) rezydent państwa członkowskiego;
e) rezydent kraju trzeciego określonego przez wiarygodne źródła jako kraj o niskim poziomie korupcji lub innej działalności przestępczej;
f) rezydent kraju trzeciego, w którym, według danych z wiarygodnych źródeł, mają zastosowanie przepisy dotyczące AML/CTF, które przepisy odpowiadają wymogom wynikającym z przepisów Unii Europejskiej w dziedzinie AML/CTF;

5.2.2. fakt oferowania produktów lub usług w celu zapewnienia odpowiednio zdefiniowanego i ograniczonego dostępu do systemu finansowego dla klientów mających ograniczony dostęp do produktów lub usług oferowanych w ramach tego systemu;

5.2.3. fakt oferowania produktów lub usług związanych z klientem, w przypadku których produktów lub usług ryzyko ML/TF jest ograniczane przez inne czynniki, w tym przez jednostki uczestnictwa w otwartych funduszach inwestycyjnych lub specjalistycznych otwartych funduszach inwestycyjnych lub określone typy elektronicznych pieniędzy;

5.2.4. fakt nawiązania relacji biznesowych lub przeprowadzenia transakcji okazjonalnej z:

a) państwem członkowskim;
b) krajem trzecim określonym przez wiarygodne źródła jako kraj o niskim poziomie korupcji lub innej działalności przestępczej;
c) krajem trzecim, w którym, według danych z wiarygodnych źródeł, mają zastosowanie przepisy dotyczące zwalczania prania pieniędzy lub finansowania terroryzmu, które przepisy odpowiadają wymogom wynikającym z przepisów Unii Europejskiej w dziedzinie zwalczania prania pieniędzy i finansowania terroryzmu.

5.3. Uproszczone środki zabezpieczające finansowo nie mają zastosowania w przypadkach określonych w punkcie 3.13.

6. WZMOCNIONE ŚRODKI ZABEZPIECZAJĄCE FINANSOWO

6.1. Spółka stosuje wzmocnione środki zabezpieczające finansowo w następujących przypadkach:

6.1.1. Spółka zidentyfikowała dowolne z wskaźników wyższego ryzyka ML/TF zgodnie z punktem 6.2,

6.1.2. rozpoczęcie relacji biznesowych lub przeprowadzenie transakcji związanych z krajem trzecim o wysokim ryzyku, zidentyfikowanym przez Komisję Europejską w akcie delegowanym przyjętym na mocy artykułu 9 dyrektywy 2015/849,

6.1.3. Spółka zidentyfikowała klienta lub beneficjenta rzeczywistego jako PEP.

6.2. Wyższe ryzyko ML/TF można wskazać w szczególności poprzez:

a) nawiązanie relacji biznesowych w nietypowych okolicznościach;
b) fakt, że klientem jest:
    i. osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której działalność służy do przechowywania środków osobistych;
    ii. spółka, w której wyemitowano akcje na okaziciela, której papiery wartościowe nie są dopuszczone do obrotu zorganizowanego, lub spółka, w której prawa przysługujące z akcji lub udziałów są wykonywane przez podmioty inne niż akcjonariusze lub udziałowcy;
    iii. rezydent państwa wymienionego w punkcie g;
c) przedmiot działalności gospodarczej prowadzonej przez klienta obejmujący przeprowadzanie znacznej liczby transakcji gotówkowych lub transakcji gotówkowych o wysokich kwotach;
d) nietypowa lub nadmiernie skomplikowana struktura własnościowa klienta, biorąc pod uwagę rodzaj i zakres prowadzonej przez niego działalności gospodarczej;
e) fakt korzystania przez klienta z usług lub produktów oferowanych w ramach bankowości prywatnej;
f) fakt korzystania przez klienta z usług lub produktów przyczyniających się do anonimowości lub utrudniających identyfikację klienta;
g) fakt nawiązania lub utrzymania relacji biznesowych lub przeprowadzenia sporadycznej transakcji bez fizycznej obecności klienta - w przypadku, gdy wyższe ryzyko związane z praniem pieniędzy/finansowaniem terroryzmu nie zostało ograniczone w inny sposób;
h) fakt zlecenia transakcji przez trzecie osoby nieznane lub niepowiązane z klientem, którego transakcje są beneficjentem;
i) fakt obejmowania nowymi produktami lub usługami lub oferowanie produktów lub usług za pomocą nowych kanałów dystrybucji lub nowych rozwiązań technologicznych w ramach relacji biznesowych lub transakcji;
j) powiązanie relacji biznesowych lub sporadycznej transakcji z:
    i. krajem o wysokim ryzyku;
    ii. krajem zdefiniowanym przez wiarygodne źródła jako kraj o wysokim poziomie korupcji lub innej przestępczości, krajem finansującym lub wspierającym działania o charakterze terrorystycznym, lub z którym wiąże się działalność organizacji o charakterze terrorystycznym;
    iii. krajem, w stosunku do którego Organizacja Narodów Zjednoczonych lub Unia Europejska podjęły decyzję o nałożeniu sankcji lub specyficznych środków restrykcyjnych;
k) k) fakt, że relacje biznesowe lub sporadyczne transakcje są związane z ropą naftową, bronią, szlachetnymi kruszcami, wyrobami tytoniowymi, artefaktami kultury, kością słoniową, chronionymi gatunkami lub innymi przedmiotami o wartości archeologicznej, historycznej, kulturalnej i religijnej, lub o rzadkiej wartości naukowej;
l) fakt, że relacje biznesowe lub sporadyczne transakcje są związane z klientem, który jest obywatelem kraju trzeciego i ubiega się o prawo pobytu lub obywatelstwo w państwie członkowskim w zamian za transfery kapitału, nabycie nieruchomości lub obligacje skarbowe lub, w zależności od przypadku, inwestycje w podmioty korporacyjne w danym państwie członkowskim.

6.3. Firma prowadzi ciągłą analizę przeprowadzanych transakcji.

6.4. W przypadku ujawnienia następujących transakcji:

a) złożonych lub

b) o wysokich kwotach, które nie są uzasadnione okolicznościami przeprowadzania transakcji; lub

c) przeprowadzanych w nietypowy sposób; lub

d) które wydają się nie mieć podstaw prawnych lub biznesowych

– Firma podejmuje działania w celu wyjaśnienia okoliczności, w jakich przeprowadzono te transakcje, a w przypadku transakcji przeprowadzanych w ramach relacji biznesowych, Firma zwiększa stosowanie środka zabezpieczającego finansowo, o którym mowa w klauzuli 3, w odniesieniu do relacji biznesowych, w ramach których przeprowadzono te transakcje.

6.5. W przypadku, gdy transakcja Klienta wiąże się z wysokim ryzykiem ML/TF, oprócz stosowania zaostrzonych środków bezpieczeństwa finansowego, Firma:

a. podejmuje dodatkowe działania w ramach zaostrzonych środków bezpieczeństwa finansowego;
b. wprowadza zaostrzone obowiązki dotyczące raportowania informacji lub raportowania transakcji;
c. ogranicza zakres relacji biznesowych lub transakcji.

6.6. MLRO powinien być poinformowany o transakcji opisanej w klauzuli 6.5. MLRO decyduje, które z działań opisanych w klauzuli 6.5 powinno być zastosowane, i daje precyzyjne wytyczne, jakie środki należy podjąć.

6.7. Firma przestrzega decyzji GIIF nakazującej zmianę zakresu lub zakończenie relacji korespondencyjnych lub przegląd relacji korespondencyjnych z instytucją respondentem zlokalizowaną w kraju o wysokim ryzyku.

7. EWIDENCJA I RAPORTOWANIE ML/TF DO WŁADZ PUBLICZNYCH

7.1. Działania opisane w tej Polityce AML/CTF Procryptic powinny być odpowiednio udokumentowane przez Firmę.

7.2. Firma przechowuje dokumenty i zapisy w formie elektronicznej za pomocą Systemu CRM oraz w postaci papierowych kopii w zamykanych szafkach. MLRO nadzoruje proces przechowywania dokumentów. Dokumenty i zapisy powinny być dostępne bez opóźnienia dla GIIF.

7.3. Firma ma obowiązek dostarczyć GIIF informacje wymienione w art. 72, 86 i 90 PL AML Act, tj.:

a. W ciągu 7 dni od wystąpienia zdarzenia, Firma wysyła informacje na temat:

i. przyjętej płatności lub wypłaty środków gotówkowych, których wartość przekracza równowartość 15 000 EUR;

ii. transakcji kupna lub sprzedaży waluty obcej, gdy taka transakcja przekracza równowartość 15 000 EUR, lub informacje o byciu pośrednikiem takiej transakcji.

b. Natychmiast - informacje o uzasadnionym podejrzeniu, że dana transakcja lub aktywa mogą być związane z ML/TF.

c. Natychmiast - informacje o wykonaniu transakcji wymienionej w punkcie b - w przypadku, gdy GIIF nie mógł zostać powiadomiony przed jej wykonaniem. W powiadomieniu Firma powinna uzasadnić przyczyny, dla których informacje nie zostały udzielone przed wykonaniem, oraz informacje dostępne dla Firmy uzasadniające podejrzenie ML/TF.

7.4. Raporty wymienione w punkcie 7.3(a) będą przygotowane w formacie .xml, używając schematów opublikowanych w Centralnym Repozytorium Dokumentów Elektronicznych (http://crd.gov.pl/). Numer odpowiednich schematów można sprawdzić pod adresem: https://www.gov.pl/web/finanse/komunikaty-giif Raporty będą wysyłane za pośrednictwem systemu GIIF - https://www.giif.mofnet.gov.pl/ .

7.5. Raporty wymienione w punkcie 7.3(b) i (c) będą wysyłane za pomocą e-maila lub ePUAP.

7.6. Spółka powiadamia odpowiedniego prokuratora bez zwłoki, jeśli ma uzasadnione podejrzenie, że wartości majątkowe będące przedmiotem transakcji lub przechowywane na koncie pochodzą lub mają związek z przestępstwem fiskalnym lub jakimkolwiek innym przestępstwem niż ML/TF (SAR). Powiadomienie powinno być zgodne z art. 89 ustawy o PPL AML, tj. powinno zawierać informacje dostępne dla Spółki, które wzbudziły podejrzenie, oraz informacje o przewidywanym czasie transakcji. Do momentu otrzymania decyzji prokuratora o wszczęciu lub odmowie wszczęcia postępowania, czas nie powinien przekraczać 96 godzin od momentu wysłania zawiadomienia, Spółka powinna powstrzymać się od przeprowadzenia zgłoszonej transakcji lub jakiejkolwiek innej transakcji, która mogłaby obciążyć konto klienta.

7.7. W przypadku, gdy nie można było złożyć zawiadomienia przed wykonaniem transakcji, o której mowa w punkcie 7.6, Spółka natychmiast powiadamia odpowiedniego prokuratora, że transakcja została wykonana. W swoim zawiadomieniu Spółka uzasadni powody, dla których transakcja nie została zgłoszona wcześniej, oraz informacje dostępne dla Spółki uzasadniające podejrzenie ML/TF.

7.8. Spółka powiadomi GIIF o okolicznościach, które mogą wskazywać na podejrzenie ML/TF.

7.9. Spółka powiadomi GIIF o wszelkich okolicznościach, które mogą wskazywać na podejrzenie, że zostało popełnione przestępstwo ML/TF.

7.10. Na żądanie GIIF lub prokuratora Spółka zablokuje środki, wstrzyma transakcję lub zablokuje konto klienta.

7.11. Zamrożone środki na mocy ustawodawstwa dotyczącego sankcji finansowych oraz każdy przypadek, w którym Spółka ma wiedzę lub uzasadnione podejrzenie, że środki sankcji finansowych zostały lub są naruszane, lub że klient jest osobą lub podmiotem wymienionym, lub osobą działającą w imieniu osoby lub podmiotu podlegającego sankcjom finansowym, muszą być zgłoszone odpowiedniej władzy.

7.12. W żadnym momencie klient, którekolwiek z jego przedstawicieli, ani żadne strony trzecie (z wyłączeniem stron, do których ma być skierowany raport na mocy tej części lub jakiegokolwiek obowiązującego prawa), nie będą informowane o podejrzeniu powstałym na mocy niniejszego, ani o żadnym zgłoszeniu z tym związane.

7.13. SAR zostaną przygotowane i przechowywane w podfolderze Raportów o podejrzanej aktywności (Suspicious Activity Reporting) w folderze Compliance. Dodatkowy podfolder będzie przechowywać Złożone SAR. Ten plik będzie zawierać plik transakcji w formacie csv i opis SAR opisany poniżej, oraz kopię potwierdzenia e-mailowego od GIIF.

8. KONTROLA WEWNĘTRZNA I WEWNĘTRZNE ZGŁASZANIE NARUSZEŃ ML/TF

8.1. Zgodność działalności Firmy z przepisami dotyczącymi ML/TF, a także z niniejszą Polityką AML/CTF Procryptic, podlega kontroli wewnętrznej prowadzonej przez Inspektora ds. Zgodności działalności firmy z prawem. Kontrola ta powinna być przeprowadzana co najmniej raz do roku.

8.2. Każdy pracownik ma prawo zgłosić rzeczywiste lub potencjalne naruszenia ML/TF. Zgłoszenie powinno być przesłane zgodnie z Procedurą Whistleblowing, dołączoną jako Załącznik 5 do tej Polityki AML/CTF Procryptic.

8.3. Fakt zawiadomienia GIIF lub innych właściwych władz zgodnie z ustawą PL AML i informacje na temat przeprowadzonych analiz dotyczących ML/TF muszą być utrzymane w tajemnicy.

9. OSOBA POLITYCZNIE NARAŻONA (PEP)

9.1. Firma przyjęła i przestrzega Procedury dotyczącej Osób Politycznie Narażonych, dołączonej jako Załącznik 4 do tej Polityki AML/CTF Procryptic ("**Procedura PEP**")

9.2. Lista krajowych stanowisk publicznych i funkcji, które są stanowiskami politycznie narażonymi, jest wprowadzana w regulaminie Ministerstwa Finansów oraz w Załączniku A do Procedury PEP.

9.3. W przypadku relacji biznesowych z PEP, Firma stosuje następujące środki CDD i podejmuje następujące działania w stosunku do takich osób: 1) uzyskuje zgodę Rady Dyrektorów na nawiązanie lub kontynuowanie relacji biznesowych z PEP; 2) stosuje odpowiednie środki w celu ustalenia źródła bogactwa klienta i źródeł środków dostępnych dla klienta w ramach relacji biznesowych lub okazjonalnej transakcji - zgodnie z procedurami EDD.

10. WPROWADZENIE POLITYKI AML/CTF PROCRYPTIC I SZKOLENIA

10.1. MLRO przeprowadzi co najmniej raz do roku szkolenie z ML/TF dla wszystkich pracowników Firmy. Ponadto, każdy nowy pracownik Firmy powinien otrzymać szkolenie w pierwszych dniach swojej pracy.

10.2. Ta Polityka AML/CTF Procryptic, przed jej wdrożeniem, musi być zatwierdzona przez Radę Dyrektorów Firmy.

ZAŁĄCZNIK 1
Wzór potwierdzenia – procedury

OŚWIADCZENIE **o zapoznaniu się z procedurami obowiązującymi w Procryptic Spółka z ograniczoną odpowiedzialnością w Warszawie („Spółka")**	***STATEMENT*** ***on familiarizing with the procedures implemented in Procryptic Spółka z ograniczoną odpowiedzialnością w Warszawie ("Company")***
Ja niżej podpisany/a oświadczam, że zapoznałem/am się z następującymi procedurami obowiązującymi w Spółce: 1. Anti-Money Laundering and Counter-Terrorist Financing Policy	*I, the undersigned, hereby declare that I have familiarized myself with the following procedures implemented in the Company:* *1. Anti-Money Laundering and Counter-Terrorist Financing Policy*
Oświadczam też, że zrozumiałem wyżej wymienione procedury i zobowiązuję się ich przestrzegać.	*I also declare that I have understood the above-mentioned procedures and undertake to follow them.*

Imię i nazwisko*/Name and Surname*	
Dział*/Department*	

Warszawa, data*/date*: _____/_____/_____

Podpis*/Signature*:

ZAŁĄCZNIK 2
Analiza transakcji przeprowadzanych w trakcie trwania relacji biznesowych

Bieżące monitorowanie to okresowy przegląd relacji z Klientem. Częstotliwość tego okresowego przeglądu będzie określana zgodnie z Profilem Ryzyka Klienta, który jest identyfikowany podczas procesu onboardingu.

Klienci przekierowani do Bieżącego Monitorowania zostaną dodani do Dziennika Bieżącego Monitorowania w oddzielnej zakładce odpowiadającej ich początkowemu Profilowi Ryzyka. Gdy Klient jest przeglądany, wyniki każdej kontroli będą zapisywane w Dzienniku Bieżącego Monitorowania.

Wszelka zebrana dokumentacja zostanie przechowywana w odpowiednim pliku w odpowiednim podfolderze folderu Zgodności. Firma analizuje transakcje przeprowadzane przez Klientów w trakcie trwania relacji biznesowych, korzystając z FUGU do transakcji FIAT i Chainanalysis do transakcji kryptowalutowych.

- Aktualizowanie danych Klienta i powtarzanie procesu CDD:

W staraniach o utrzymanie aktualności i dokładności danych, informacji i dokumentacji Klientów, MLRO będzie powtarzać proces Due Diligence Klienta (CDD) w okresach monitorowania wymienionych poniżej. Jeśli w trakcie trwania relacji biznesowej pojawią się wątpliwości co do jakichkolwiek szczegółów uzyskanych podczas onboardingu, odpowiednie zapytania i przeglądy będą powtarzane, a odpowiednie dane zostaną zaktualizowane.

Klienci o niskim ryzyku (co 24 miesiące)
- Sprawdzenie danych klienta
- Sprawdzenie całkowitej aktywności transakcyjnej

Klienci o standardowym ryzyku (co 18 miesięcy)
- Sprawdzenie danych klienta

Sprawdzenie całkowitej aktywności transakcyjnej

Klienci o wysokim ryzyku (co 12 miesięcy)
- Sprawdzenie danych klienta
- Sprawdzenie całkowitej aktywności transakcyjnej
- Dodanie streszczenia do rocznego raportu dla Głównego Oficera ds. Zgodności

Jak wspomniano powyżej, wyniki wszystkich przeglądów będą zapisywane w Dzienniku Bieżącego Monitorowania dla każdego przeglądanego Klienta. Każdy Klient, który potrzebuje zmiany w swoim Profilu Ryzyka, zostanie przekazany do Zarządu do zatwierdzenia z pisemnym zaleceniem. Jakakolwiek dokumentacja zebrana od Klienta będzie przechowywana w podfolderze odpowiadającym ich okresowi przeglądu.

DODATEK 3

Badanie źródła pochodzenia wartości majątkowych na dyspozycji Klienta

Przegląd źródła funduszy będzie polegał na:

- Pierwszym kroku, którym jest rozważenie prima facie legalności źródła funduszy Klienta.
- Następnie, przegląd ryzyka jurysdykcyjnego klienta oraz profilu ryzyka klienta.
- Po trzecie, przeprowadzenie analizy blockchain portfeli Klienta, jeżeli to jest odpowiednie, lub korzystanie z usług zewnętrznych dostawców do przeglądu transakcji fiat (włącznie z monitorowaniem i przesiewem).
- Na koniec, dla bardzo dużych sum (wszystko powyżej 1000 EUR) prosić o dodatkowe informacje od Klienta, jeżeli zauważone są dodatkowe, wysokie wskaźniki ryzyka.

Recenzent powinien być w stanie zidentyfikować, jaki jest adres docelowy dla wychodzących środków (blockchain) za pomocą eksploratora bloków lub Chainalysis Reactor.

Recenzent powinien zauważyć, z czego składa się portfel dla przychodzących środków, tzn. środki z giełdy, rynek wysokiego ryzyka, hazard itp., korzystając z Chainalysis Reactor.

Przeglądnij konto użytkownika w systemie CRM firmy:

- Historia transakcji i testowych transakcji.
- Adres IP (w dziennikach aktywności użytkownika)/historia lokalizacji i urządzeń.
- Źródło polecania, lub konta polecone, jeżeli takie istnieją.
- Dokumenty i notatki dotyczące procesu onboardingu.
- Na koniec, przegląd wszelkich notatek dodanych do systemu CRM.

ZAŁĄCZNIK 4

Procedura PEP

I. PODSUMOWANIE

Celem tego dokumentu jest zarysowanie procedury dotyczącej akceptacji, zarządzania i monitorowania klientów, którzy są uważani za osoby pełniące lub pełniące istotne funkcje publiczne **("PEP")**. Jest to robione w celu zmniejszenia ryzyka reputacyjnego, operacyjnego, regulacyjnego i prawnych, opartego na międzynarodowo akceptowanych najlepszych praktykach, standardach i wytycznych dotyczących zarządzania PEP.

II. DEFINICJE

Osoby pełniące lub pełniące istotne funkcje publiczne (PEP)

PEP to osoby powierzone ważną funkcją publiczną (a także ich rodziny i osoby znane jako bliscy współpracownicy) inaczej niż średniego szczebla lub bardziej juniorów.

Lista krajowych stanowisk i funkcji publicznych, które są PEP, jest wprowadzana w regulaminie Ministerstwa Finansów i w Załączniku A do tej Procedury PEP.

Do członków rodziny PEP należą:

- ich małżonek lub partner;
- ich dzieci i dzieci ich małżonka lub partnera; oraz
- ich rodzice.

nane bliscy współpracownicy PEP to:

- osoba, która ma wspólne korzystne prawo własności do podmiotu prawnego lub układu prawnego, lub jakiekolwiek inne bliskie stosunki biznesowe z PEP; oraz
- osoba, która ma wyłączne korzystne prawo własności do podmiotu prawnego lub układu prawnego, który jest znany z tego, że został ustanowiony na korzyść PEP.

PEP, ich rodziny i wszyscy bliscy współpracownicy, są poddawani zwiększonej kontroli, ponieważ mogą być w stanie wykorzystać swój publiczny urząd dla prywatnych korzyści, poprzez niewłaściwe wykorzystanie publicznych funduszy lub akceptowanie łapówkarstwa i korupcji.

W związku z tym, Firma powinna przeprowadzić kontrolę wszystkich klientów Firmy podczas onboardingu w oparciu o znane listy PEP, aby zweryfikować ich status PEP.

Klienci, którzy są PEP, są klasyfikowani jako Klient Specjalnej Kategorii ("**SCC**") (wysoki profil ryzyka), i są poddawani specjalnym zwiększonym środkom Due Diligence ("**EDD**"), w tym zwiększonemu monitorowaniu i niższym limitom. Konta Firmy dla PEP mogą być otwarte tylko za zgodą Compliance Officer Firmy, oprócz innych zatwierdzeń wymaganych w ramach tej procedury.

III. IDENTYFIKACJA PEP

Firma nie jest wykluczona z prowadzenia biznesu z PEP, a więc identyfikacja PEP nie stanowi sama w sobie automatycznego powodu do odrzucenia lub odrzutu wniosku o konto/portfel cyfrowy.

Jednakże, gdy PEP jest identyfikowany, powinno być przeprowadzone zwiększone Due Diligence (EDD) przed podjęciem decyzji o nawiązaniu relacji biznesowej czy nie.

Identyfikacja PEP

Firma identyfikuje PEP poprzez:

- Kontrolę klientów w odniesieniu do zidentyfikowanych list PEP
- Profilowanie ryzyka klienta jako PEP na podstawie komunikacji z klientem

Rozważanie innych wiarygodnych źródeł informacji, takich jak publikacje branżowe, publikacje rządowe lub komunikaty prasowe

W celu zidentyfikowania klienta lub beneficjenta jako PEP, Firma może zaakceptować pisemne lub dokumentalne oświadczenie od klienta, że jest lub nie jest osobą politycznie narażoną. Oświadczenie musi być złożone pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia. Oświadczenie powinno zawierać następujące stwierdzenie: "Jestem świadom odpowiedzialności karnej za złożenie fałszywego oświadczenia" - które zastępuje pouczenie o odpowiedzialności karnej za złożenie fałszywego oświadczenia.

Podmioty, w których PEP ma udział korzyściowy lub kontrolę

W przypadku, gdy PEP jest stroną powiązaną z podmiotem i posiada więcej niż 25% praw głosu w podmiotie, sam podmiot będzie uznawany za podmiot o wysokim ryzyku z powodu powiązania z PEP. Określenie PEP wynika z beneficjenta, akcjonariusza lub kontrolera i nie jest podyktowane przez sam podmiot.

Podmiot powinien być również uznawany za podmiot o wysokim ryzyku, jeżeli znaczący wpływ na politykę, biznes i strategię tego podmiotu wywiera PEP. Aby określić, czy PEP ma znaczący wpływ na politykę, biznes i strategię podmiotu, należy rozważyć charakter stanowiska zajmowanego przez daną osobę.

IV. WYMAGANIA ZNAJOMOŚCI KLIENTA (KYC)

Identyfikacja i proces identyfikacji

Dla każdego nowego związku biznesowego, informacje KYC powinny być pozyskiwane podczas procesu wdrażania oraz podczas oceny potencjalnych możliwości. Te informacje będą wykorzystywane przez Firmę do przeprowadzenia kontroli tła klienta.

Od pracowników obsługi klienta wymaga się, aby upewnili się, że uzyskane od klientów informacje są zgodne z obowiązującymi listami kontrolnymi KYC.

Przedzatwierdzenie – Due Diligence Klienta (CDD)

CDD jest kluczowym i podstawowym źródłem informacji wykorzystywanych do określania, czy klient jest PEP, czy nie. CDD musi być przeprowadzone, gdy:

- Zawierany jest związek biznesowy z klientem
- W regularnych odstępach czasu w trakcie cyklu życia klienta, w zależności od oceny ryzyka

- Jest uzasadniony powód do wątpliwości co do autentyczności informacji lub dokumentacji lub danych lub innych informacji wcześniej uzyskanych w celu KYC
- W innych przypadkach wymaganych w procedurach Firmy

Podczas prowadzenia CDD na PEP, mogą zostać odkryci beneficjenci rzeczywiści, którzy następnie zostaną odpowiednio zweryfikowani przez Funkcję Zgodności.

Gdy nastąpi pozytywna identyfikacja PEP, Funkcja Zgodności zapewni przeprowadzenie EDD.

Odkrycie po zatwierdzeniu - CDD

Jeśli którykolwiek pracownik odkryje, że klient jest PEP podczas codziennych czynności, kiedy wykonuje jakąkolwiek aktywność na koncie klienta, pracownik jest zobowiązany poinformować Funkcję Zgodności.

Jeżeli nastąpią jakiekolwiek zmiany w strukturze udziałów klienta, nowi akcjonariusze muszą zostać przesłani do Funkcji Zgodności w celu przeprowadzenia CDD i EDD w razie potrzeby, a rejestr PEP zostanie odpowiednio zaktualizowany.

V. TRAKTOWANIE PEP

Decydując o zatwierdzeniu lub niezatwierdzeniu wniosku, gdy zostanie zidentyfikowany PEP, przegląd uwzględni wszystkie informacje odkryte podczas odkrywania PEP.

VI. PROCES ODKRYWANIA PRZED ZATWIERDZENIEM

Poniżej przedstawiono krok po kroku proces, który należy przestrzegać, gdy PEP zostanie zidentyfikowany w procesie CDD przed zatwierdzeniem:

1) Kiedy PEP, członek rodziny lub współpracownik zostanie odkryty/zidentyfikowany podczas etapu CDD, odpowiedzialny pracownik musi przesłać informacje do Funkcji Zgodności.
2) MLRO powinien przeprowadzić ocenę ryzyka proponowanego związku z PEP. Ocenę ryzyka powinny stanowić wszystkie czynniki ryzyka, aby określić, czy proponowany związek z PEP wiąże się z wyższym ryzykiem.
3) Podczas oceny należy uwzględnić:
   a) Czynniki ryzyka klienta, w tym geograficzne;
   b) Naturę PEP; oraz
   c) Produkty, do których PEP szuka dostępu.
4) Jeżeli ocena ryzyka stwierdzi, że proponowany związek niesie niskie ryzyko, MLRO sklasyfikuje go odpowiednio, a mniej rygorystyczne EDD zostanie przeprowadzone.
5) Jeżeli ocena ryzyka sugeruje, że proponowany związek z PEP będzie wiązał się z wysokim ryzykiem, MLRO musi zapewnić ciągłe monitorowanie tego konta.
6) EDD będzie zawierało następujące elementy:
   a) Wyszukiwanie więcej informacji od PEP w celu identyfikacji i weryfikacji, czy są inni beneficjenci rzeczywiści;
   b) Wyszukiwanie więcej informacji na temat proponowanego użytkowania konta;
   c) Weryfikacja źródła funduszy, źródła majątku.

7) Po zakończeniu EDD, MLRO sporządzi podsumowanie zawierające wszystkie istotne informacje odkryte na temat zidentyfikowanego PEP. Takie podsumowanie zostanie dostarczone do Zarządu.
8) Zgodnie z rekomendacjami FATF i obowiązującymi przepisami w Polsce, wymagana jest zgoda Zarządu na nawiązanie lub prowadzenie istniejącego związku biznesowego z PEP.
9) MLRO przeanalizuje PEP i, jeśli to konieczne, zwróci uwagę Zarządu, aby uzyskać zgodęl:
10) Jeżeli Zarząd zatwierdzi, jednostka biznesowa zostanie poinformowana, a klient będzie mógł nawiązać relację z firmą;
11) Jeżeli Zarząd odrzuci, jednostka biznesowa zostanie poinformowana, a odpowiednie procesy będą przestrzegane dla wszystkich odrzuconych wniosków.

Załącznik A do procedury PEP
Lista krajowych (polskich) stanowisk publicznych i funkcji, które są politycznie narażone

2. Prezydent Rzeczypospolitej Polskiej;
3. Przewodniczący Rady Ministrów;
4. Wiceprezydent Rady Ministrów;
5. minister;
6. sekretarz stanu;
7. podsekretarz stanu;
8. poseł;
9. senator;
10. poseł do Parlamentu Europejskiego;
11. członek organu reprezentującego zewnętrznie partię polityczną, wpisanej do rejestru partii politycznych prowadzonego przez Sąd Okręgowy w Warszawie;
12. członek organu kierowniczego partii politycznej wpisanej do rejestru partii politycznych prowadzonego przez Sąd Okręgowy w Warszawie, upoważniony do zaciągania zobowiązań finansowych;
13. sędzia Trybunału Stanu;
14. sędzia Sądu Najwyższego;
15. sędzia Trybunału Konstytucyjnego;
16. sędzia Naczelnego Sądu Administracyjnego;
17. sędzia Sądu Apelacyjnego;
18. Prezes Narodowego Banku Polskiego;
19. członek Zarządu Narodowego Banku Polskiego;
20. członek Rady Polityki Pieniężnej;
21. upoważniony przedstawiciel Rzeczypospolitej Polskiej w innym kraju lub przy organizacji międzynarodowej;
22. chargé d'affaires;
23. oficer zajmujący stanowisko urzędowe w Siłach Zbrojnych Rzeczypospolitej Polskiej do rangi generała (admirała);
24. przedstawiciel Ministra Obrony Narodowej wyznaczony na podstawie odrębnej decyzji Ministra Obrony Narodowej;
25. dyrektor, prezes przedsiębiorstwa państwowego lub inne równorzędne stanowisko;
26. przewodniczący rady nadzorczej przedsiębiorstwa państwowego;
27. członek rady nadzorczej przedsiębiorstwa państwowego;
28. prezes zarządu spółki z udziałem Skarbu Państwa, w której więcej niż połowa akcji należy do Skarbu Państwa lub innych państwowych osób prawnych;
29. członek zarządu spółki z udziałem Skarbu Państwa, w której więcej niż połowa akcji należy do Skarbu Państwa lub innych państwowych osób prawnych;
30. przewodniczący rady nadzorczej spółki z udziałem Skarbu Państwa, w której więcej niż połowa akcji należy do Skarbu Państwa lub innych państwowych osób prawnych;
31. członek rady nadzorczej spółki z udziałem Skarbu Państwa, w której więcej niż połowa akcji należy do Skarbu Państwa lub innych państwowych osób prawnych;
32. dyrektor generalny urzędu głównego organu władzy państwowej;

33. dyrektor generalny urzędu centralnego organu władzy państwowej;
34. dyrektor generalny urzędu wojewódzkiego;
35. Szef Kancelarii Prezydenta Rzeczypospolitej Polskiej;
36. Szef Kancelarii Prezesa Rady Ministrów;
37. Szef Kancelarii Sejmu;
38. Szef Kancelarii Senatu;
39. wojewoda;
40. zastępca wojewody;
41. marszałek województwa;
42. członek zarządu województwa inny niż marszałek województwa;
43. wójt, burmistrz, prezydent miasta;
44. zastępca wójta, burmistrza lub prezydenta miasta;
45. starosta;
46. członek zarządu powiatu inny niż starosta;
47. Dyrektor Generalny Krajowego Ośrodka Wsparcia Rolnictwa;
48. Zastępca Dyrektora Generalnego Krajowego Ośrodka Wsparcia Rolnictwa;
49. Dyrektor Generalny Lasów Państwowych;
50. Zastępca Dyrektora Generalnego Lasów Państwowych;
51. Dyrektor Generalny Służby Więziennej;
52. Zastępca Dyrektora Generalnego Służby Więziennej;
53. Dyrektor Generalny Służby Zagranicznej;
54. Dyrektor Generalny Urzędu Przewodniczącego Komitetu stanowiącego Radę Ministrów;
55. Dyrektor Krajowej Szkoły Administracji Publicznej;
56. Zastępca Dyrektora Krajowej Szkoły Administracji Publicznej;
57. Dyrektor Polskiego Centrum Akredytacji;
58. Zastępca Dyrektora Polskiego Centrum Akredytacji;
59. Dyrektor Rządowego Centrum Bezpieczeństwa;
60. Zastępca Dyrektora Rządowego Centrum Bezpieczeństwa;
61. Dyrektor Transportowego Dozoru Technicznego;
62. Zastępca Dyrektora Transportowego Dozoru Technicznego;
63. Generalny Dyrektor Dróg Krajowych i Autostrad;
64. Zastępca Generalnego Dyrektora Dróg Krajowych i Autostrad;
65. Generalny Dyrektor Ochrony Środowiska;
66. Zastępca Generalnego Dyrektora Ochrony Środowiska;
67. Generalny Inspektor Informacji Finansowej;
68. Główny Geodeta Kraju;
69. Zastępca Głównego Geodety Kraju;
70. Główny Inspektor Farmaceutyczny;
71. Zastępca Głównego Inspektora Farmaceutycznego;
72. Główny Inspektor Jakości Handlowej Artykułów Rolno-Spożywczych;
73. Zastępca Głównego Inspektora Jakości Handlowej Artykułów Rolno-Spożywczych;
74. Główny Inspektor Nadzoru Budowlanego;
75. Zastępca Głównego Inspektora Nadzoru Budowlanego;
76. Główny Inspektor Ochrony Roślin i Nasiennictwa;
77. Zastępca Głównego Inspektora Ochrony Roślin i Nasiennictwa;
78. Główny Inspektor Ochrony Środowiska;
79. Zastępca Głównego Inspektora Ochrony Środowiska;
80. Główny Inspektor Pracy;
81. Zastępca Głównego Inspektora Pracy;
82. Główny Inspektor Sanitarny;
83. Zastępca Głównego Inspektora Sanitarnego;
84. Główny Inspektor Transportu Drogowego;
85. Zastępca Głównego Inspektora Transportu Drogowego;
86. Główny Lekarz Weterynarii;
87. Zastępca Głównego Lekarza Weterynarii;
88. Główny Rzecznik Dyscypliny Finansowej;
89. Zastępca Głównego Rzecznika Dyscypliny Finansowej;

90. Komendant Główny Państwowej Straży Pożarnej;
91. Zastępca Komendanta Głównego Państwowej Straży Pożarnej;
92. Komendant Główny Policji;
93. Zastępca Komendanta Głównego Policji;
94. Komendant Główny Straży Granicznej;
95. Zastępca Komendanta Głównego Straży Granicznej;
96. Szef Służby Ochrony Państwa;
97. Zastępca Szefa Służby Ochrony Państwa;
98. Naczelny Dyrektor Archiwów Państwowych;
99. Zastępca Naczelnego Dyrektora Archiwów Państwowych;
100. Prezes Agencji Mienia Wojskowego;
101. Zastępca Prezesa Agencji Mienia Wojskowego;
102. Prezes Agencji Restrukturyzacji i Modernizacji Rolnictwa;
103. Zastępca Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa;
104. Prezes Biura Substancji Chemicznych;
105. Prezes Głównego Urzędu Miar;
106. Wiceprezes Głównego Urzędu Miar;
107. Prezes Głównego Urzędu Statystycznego;
108. Wiceprezes Głównego Urzędu Statystycznego;
109. Prezes Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
110. Zastępca Prezesa Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
111. Prezes Funduszu Ubezpieczeń Społecznych Rolników;
112. Zastępca Prezesa Funduszu Ubezpieczeń Społecznych Rolników;
113. Prezes Narodowego Funduszu Zasobów;
114. Zastępca Prezesa Narodowego Funduszu Zasobów;
115. Prezes Najwyższej Izby Kontroli;
116. Wiceprezes Najwyższej Izby Kontroli;
117. Członek Kolegium Najwyższej Izby Kontroli;
118. Prezes Narodowego Funduszu Zdrowia;
119. Zastępca Prezesa Narodowego Funduszu Zdrowia;
120. Prezes Państwowego Gospodarstwa Wodnego Wody Polskie;
121. Zastępca Prezesa Państwowego Gospodarstwa Wodnego Wody Polskie;
122. Prezes Państwowej Agencji Atomistyki;
123. Wiceprezes Państwowej Agencji Atomistyki;
124. Prezes Polskiej Agencji Kosmicznej;
125. Wiceprezes Polskiej Agencji Kosmicznej;
126. Prezes Polskiego Urzędu Nadzoru Audytowego;
127. Zastępca Prezesa Polskiego Urzędu Nadzoru Audytowego;
128. Prezes Polskiej Agencji Rozwoju Przedsiębiorczości;
129. Zastępca Prezesa Polskiej Agencji Rozwoju Przedsiębiorczości;
130. Prezes Polskiej Organizacji Turystycznej;
131. Wiceprezes Polskiej Organizacji Turystycznej;
132. Prokurator Generalny Rzeczypospolitej Polskiej;
133. Zastępca Prokuratora Generalnego Rzeczypospolitej Polskiej;
134. Prezes Rządowego Centrum Legislacji;
135. Wiceprezes Rządowego Centrum Legislacji;
136. Prezes Rządowego Agencji Rezerw Strategicznych;
137. Zastępca Przewodniczącego Rządowej Agencji Rezerw Strategicznych;
138. Prezes Urzędu Dozoru Technicznego;
139. Wiceprezes Urzędu Dozoru Technicznego;
140. Prezes Urzędu Komunikacji Elektronicznej;
141. Zastępca Prezesa Urzędu Komunikacji Elektronicznej;
142. Prezes Urzędu Lotnictwa Cywilnego;
143. Wiceprezes Urzędu Lotnictwa Cywilnego;
144. Prezes Urzędu Ochrony Danych Osobowych;
145. Zastępca Prezesa Urzędu Ochrony Danych Osobowych;

146. Prezes Urzędu Ochrony Konkurencji i Konsumentów.
147. Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów;
148. Prezes Urzędu Patentowego Rzeczypospolitej Polskiej;
149. Wiceprezes Urzędu Patentowego Rzeczypospolitej Polskiej;
150. Prezes Urzędu Regulacji Energetyki;
151. Wiceprezes Urzędu Regulacji Energetyki;
152. Prezes Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych;
153. Wiceprezes Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych;
154. Prezes Urzędu Transportu Kolejowego;
155. Wiceprezes Urzędu Transportu Kolejowego;
156. Prezes Urzędu Zamówień Publicznych;
157. Wiceprezes Urzędu Zamówień Publicznych;
158. Prezes Wyższego Urzędu Górniczego;
159. Wiceprezes Państwowego Górniczego Zakładu Górniczego;
160. Prezes Zakładu Ubezpieczeń Społecznych;
161. Członek Zarządu Zakładu Ubezpieczeń Społecznych;
162. Prezes Zarządu Banku Gospodarstwa Krajowego;
163. Wiceprezes Zarządu Banku Gospodarstwa Krajowego;
164. Członek Zarządu Banku Gospodarstwa Krajowego;
165. Prezes Zarządu Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej;
166. Wiceprezes Zarządu Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej;
167. Prezes Zarządu Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych;
168. Wiceprezes Zarządu Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych;
169. Prokurator Generalny;
170. Zastępca Prokuratora Generalnego;
171. Prokurator Krajowy;
172. Przewodniczący Komisji Nadzoru Finansowego;
173. Zastępca Przewodniczącego Komisji Nadzoru Finansowego;
174. Członek Komisji Nadzoru Finansowego;
175. Przewodniczący Państwowej Komisji do spraw wyjaśniania przypadków czynów przeciwko wolności seksualnej i obyczajności wobec małoletniego poniżej 15 roku życia;
176. Członek Państwowej Komisji do spraw wyjaśniania przypadków czynów przeciwko wolności seksualnej i obyczajności wobec małoletniego poniżej 15 roku życia;
177. Przewodniczący Krajowej Rady Radiofonii i Telewizji;
178. Zastępca Przewodniczącego Krajowej Rady Radiofonii i Telewizji;
179. Członek Krajowej Rady Radiofonii i Telewizji;
180. Przewodniczący Państwowej Komisji Wyborczej;
181. Zastępca Przewodniczącego Państwowej Komisji Wyborczej;
182. Członek Państwowej Komisji Wyborczej;
183. Przewodniczący Rady do spraw Uchodźców;
184. Wiceprzewodniczący Rady do spraw Uchodźców;
185. Przewodniczący Krajowej Rady Mediów;
186. Członek Krajowej Rady Mediów;
187. Rzecznik Finansowy;
188. Zastępca Rzecznika Finansowego;
189. Rzecznik Małych i Średnich Przedsiębiorców;
190. Zastępca Rzecznika Małych i Średnich Przedsiębiorców;
191. Rzecznik Praw Dziecka;
192. Zastępca Rzecznika Praw Dziecka;
193. Rzecznik Praw Obywatelskich;
194. Zastępca Rzecznika Praw Obywatelskich;
195. Rzecznik Praw Pacjenta;
196. Zastępca Rzecznika Praw Pacjenta;
197. Szef Agencji Bezpieczeństwa Wewnętrznego;
198. Zastępca Szefa Agencji Bezpieczeństwa Wewnętrznego;
199. Szef Agencji Wywiadu.

200. Zastępca Szefa Agencji Wywiadu;
201. Szef Biura Bezpieczeństwa Narodowego;
202. Zastępca Szefa Biura Bezpieczeństwa Narodowego;
203. Szef Centralnego Biura Antykorupcyjnego;
204. Szef Krajowego Biura Wyborczego;
205. Szef Krajowej Administracji Skarbowej;
206. Zastępca Szefa Krajowej Administracji Skarbowej;
207. Szef Służby Cywilnej;
208. Szef Służby Kontrwywiadu Wojskowego;
209. Zastępca Szefa Służby Kontrwywiadu Wojskowego;
210. Szef Służby Wywiadu Wojskowego;
211. Zastępca Szefa Służby Wywiadu Wojskowego;
212. Szef Służby Zagranicznej;
213. Szef Urzędu do Spraw Cudzoziemców;
214. Zastępca Szefa Urzędu do Spraw Cudzoziemców;
215. Szef Urzędu do Spraw Kombatantów i Osób Represjonowanych;
216. Zastępca Szefa Urzędu do Spraw Kombatantów i Osób Represjonowanych.

ZAŁĄCZNIK 5

Procedura sygnalizacji naruszeń

1. Każdy Pracownik ma prawo anonimowo zgłosić potencjalne lub faktyczne naruszenie praw (w szczególności ML/TF), przepisów, procedur wewnętrznych lub standardów etycznych ("**Zgłoszenie Naruszenia**").
2. Firma chroni Sygnalizującego przed ujawnieniem jego tożsamości oraz wszelkimi działaniami represyjnymi i/lub dyskryminacyjnymi czy innymi formami niesprawiedliwego traktowania.
3. Anonimowość jest zapewniana przez wprowadzenie mechanizmu uniemożliwiającego weryfikację danych osobowych Sygnalizującego. Dlatego Zgłoszenia Naruszeń mogą być przesyłane w następujący sposób:
    a. Złożone w zamkniętej skrzynce na listy w biurze, lub;
    b. Wysłane e-mailem do inspektora ds. zgodności lub członków zarządu (jeśli nastąpi punkt 9 poniżej).
4. Wszystkie Zgłoszenia Naruszeń powinny być przekazywane w wyznaczonej formie elektronicznej, zapewniającej anonimowość. Zgłoszenia Naruszeń są kierowane do inspektora ds. zgodności w Firmie.
5. Sygnalizujący musi:
    a. działać w dobrej wierze;
    b. dostarczyć precyzyjne informacje na temat naruszenia;
    c. przestrzegać poufności;
6. Sygnalizujący są proszeni o podanie następujących informacji:
    a. data(y) zdarzenia;
    b. charakter zdarzenia;
    c. nazwisko osób zaangażowanych w zdarzenie;
    d. nazwiska ewentualnych świadków zdarzenia;
    e. dowody zdarzenia, np. dokumenty, e-maile, inne.
7. Zgłoszenia Naruszeń, które nie zawierają wystarczających informacji, mogą nie być badane.
8. Zgłoszenia Naruszeń są badane przez Inspektora ds. Zgodności i Zarząd lub inne osoby wyznaczone przez Zarząd.
9. W przypadku, gdy Zgłoszenie Naruszenia dotyczy Inspektora ds. Zgodności, Zgłoszenie to będzie badane przez Zarząd lub inną upoważnioną osobę.
10. W przypadku, gdy Zgłoszenie Naruszenia dotyczy członka Zarządu, Zgłoszenie będzie badane przez cały Zarząd z wyjątkiem zainteresowanego członka.
11. Wstępne śledztwo w sprawie Zgłoszenia Naruszenia powinno z zasady zakończyć się w ciągu 1 miesiąca od otrzymania Zgłoszenia.
12. Jeżeli w wyniku wstępnego śledztwa stwierdzono, że istnieją uzasadnione fakty i/lub okoliczności dowodzące, że zgłoszone Zgłoszenie Naruszenia jest wystarczająco uzasadnione, przeprowadza się pełne śledztwo.
13. Po zakończeniu śledztwa, organ prowadzący je określa dalsze działania, w szczególności ich rodzaj i charakter, które powinny być podjęte.
14. W przypadku, gdy dane osobowe Sygnalizującego są znane, powinien on zostać poinformowany o wynikach zakończonego śledztwa.
15. Osoby prowadzące śledztwo w sprawie Zgłoszenia Naruszenia nie mogą próbować odkryć tożsamości Sygnalizującego, który zdecydował się działać anonimowo.
16. W przypadku, gdy dane osobowe Sygnalizującego są znane, osoby lub organy prowadzące śledztwo nie mogą przekazywać tych danych innym osobom i powinny starać się ograniczyć do minimum krąg osób, które mogą mieć dostęp do tych danych. Ujawnienie może nastąpić, ale nie jest ograniczone do przypadku, gdy Firma jest prawnie zobowiązana do ujawnienia tożsamości Sygnalizującego; i/lub ujawnienie takich informacji jest wymagane, jeśli i kiedy Firma zdecyduje się zgłosić sprawę odpowiednim władzom.

17. Sygnalizujący powinien zastosować się do wszelkich uzasadnionych żądań wyjaśnienia faktów i/lub okoliczności, dostarczenia (dodatkowych) informacji i współpracy przy śledztwie.
18. Brak dodatkowych żądanych informacji może być powodem do podjęcia decyzji o niewykonywaniu śledztwa i/lub do wniosku, że Zgłoszenie Naruszenia nie ma podstaw faktycznych.
19. Ani Sygnalizujący, ani żaden inny pracownik, który dostarcza informacje, sprawia, że informacje są dostarczane lub w inny sposób pomaga w śledztwie, nie mogą dyskutować na temat szczegółów zgłoszonego Zgłoszenia Naruszenia lub jakiegokolwiek związanego z nim śledztwa z nikim poza osobami prowadzącymi śledztwo, chyba że jest to wymagane przez prawo.
20. Po zakończeniu śledztwa ewentualne dane osobowe powinny zostać zanonimizowane w Zgłoszeniu Naruszenia.
21. Inspektor ds. Zgodności w Firmie prowadzi szkolenia początkowe i okresowe dotyczące tej Procedury. Szkolenia mogą być przeprowadzane poprzez dystrybucję prezentacji elektronicznej.
22. Inspektor ds. Zgodności w Firmie co najmniej raz do roku informuje Zarząd o zgłoszonych Zgłoszeniach Naruszeń.
23. Zarząd Firmy co najmniej raz do roku ocenia adekwatność i skuteczność tego procesu.