

**Szkolenie**



**Przeciwdziałanie praniu pieniędzy  
oraz finansowaniu terroryzmu**

**Opracowanie:  
Departament Compliance  
Warszawa 2025**

**warta.**



## Regulacje prawne

Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu  
z dnia 1 marca 2018 r.

Wejście w życie: 13 lipca 2018 r.

**Dyrektywa 2015/849** Parlamentu Europejskiego i Rady (UE) 2015/849  
z dnia 20 maja 2015 r.

**Rozporządzenie 2015/847** rozporządzenie Parlamentu Europejskiego i Rady (UE)  
z dnia 20 maja 2015 r.

**Dyrektywa 2018/843** Parlamentu Europejskiego i Rady (UE) z dnia 30 maja 2018 r.

**Rozporządzenie Ministra Finansów Funduszy i Polityki z dnia 27 lipca 2021 r.** w sprawie wykazu krajowych stanowisk i funkcji publicznych będących eksponowanymi stanowiskami politycznych (obowiązuje od: 31 października 2021 r.)

## Czym jest pranie pieniędzy?

### Art. 299 § 1 kodeksu karnego.

*Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego,*

- *przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji,*
- *pomaga do przenoszenia ich własności lub posiadania albo*
- *podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępczego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku*

*podlega karze pozbawienia wolności od 6 miesięcy do lat 8*



## Pranie pieniędzy – etapy

proceder prania pieniędzy można podzielić na 3 główne etapy

### LOKOWANIE

**Lokowanie** oznacza wprowadzenie do obrotu finansowego środków finansowych pochodzących z przestępstwa.

Zachowania typowe dla lokowania:

- wprowadzanie do obrotu środków finansowych pochodzących bezpośrednio z przestępstwa,
- dokonywanie transakcji poniżej wartości ponadprogowych np. w formie gotówkowej przez tzw. słupy,
- prostota, jednorodność, powtarzalność i krótkoterminowość dokonywanych transakcji,
- mieszanie pieniędzy legalnych z nielegalnymi.

### MASKOWANIE

**Maskowanie** to proces ukrywania źródła pochodzenia wartości majątkowych z działalności przestępczej przez realizowanie wielu następujących po sobie transakcji finansowych.

Zachowania typowe dla maskowania:

- zlecenie szeregu licznych operacji i transakcji, tak aby uniemożliwić organom kontrolnym dotarcie do osób, które inicjowały wpłacanie “brudnych” pieniędzy,
- fizyczne przemieszczanie gotówki pomiędzy produktami i kontami np. ubezpieczenie z funduszem inwestycyjnym. Środki po zerwaniu polisy są przelewane na rachunki bankowe,
- elektroniczne formy przekazu pieniędzy,

### INTEGRACJA

**Integracja** to proces zapewniający powrót wypranych wartości do systemu gospodarczego w taki sposób, że mają one pozory uzyskania z legalnej działalności, o czym świadczyć mają dokumenty wydane przez banki, instytucje finansowe lub organizacje gospodarcze.



## Pranie pieniędzy – etapy c.d

### LOKOWANIE

- rozdrabnianie/dzielenie wpłat,
- wymiana banknotów,
- mieszanie pieniędzy legalnych z nielegalnymi.

### MASKOWANIE

- realizowanie bardzo dużej liczby transakcji,
- transakcje niemające ekonomicznego uzasadnienia.

### INTEGRACJA

- Fikcyjne transakcje kupna-sprzedaży
- Transakcje pomiędzy członkami rodziny
- Zakup upadających przedsiębiorstw

## Obowiązki wobec klientów

TUnŻ WARTA S.A. zobowiązana jest do stosowania wobec klientów środków bezpieczeństwa finansowego:



## Identyfikacja klienta – osoba fizyczna

### Identyfikacja Ubezpieczającego polega na ustaleniu następujących danych:

W przypadku **osoby fizycznej** ustalić należy:

- imię i nazwisko,
- obywatelstwa,
- serię i numer dokumentu stwierdzającego tożsamość osoby,
- PESEL,
- datę urodzenia oraz państwo urodzenia – w przypadku gdy nie został nadany PESEL,
- adres zamieszkania.

### Identyfikacja osoby upoważnionej do działania w imieniu klienta

- imię i nazwisko,
- obywatelstwa,
- serię i numer dokumentu stwierdzającego tożsamość osoby,
- PESEL,
- datę urodzenia oraz państwo urodzenia – w przypadku gdy nie został nadany PESEL.

### Identyfikacja osoby fizycznej, która prowadzi działalność gospodarczą lub spółki cywilnej

Ustal te same dane jak w przypadku identyfikacji osoby fizycznej oraz dodatkowo ustal:

- nazwę (firmy),
- numer identyfikacji podatkowej (NIP),
- adres głównego miejsca wykonywania działalności gospodarczej.





## Weryfikacja tożsamości – osoba fizyczna

Weryfikacja tożsamości klienta lub osoby upoważnionej do działania w jego imieniu polega na potwierdzeniu danych, o których wspomniałem na poprzednim ekranie.

Teraz dowiesz się **jakie dokumenty musi okazać Tobie klient**, aby prawidłowo przeprowadzić weryfikację jego tożsamości.

### **Osoba fizyczna lub osoba upoważniona do działania w imieniu klienta**

Dokument tożsamości, stwierdzający tożsamość danej osoby. Dla obywateli polskich podstawowym dokumentem tożsamości jest dowód osobisty i paszport, a także mDowód (dostępny w ramach mobilnej aplikacji mObywatel w przypadku fizycznej obecności weryfikowanej osoby). Aby zweryfikować tożsamość obcokrajowca poproś o jego kartę pobytu lub dokument pobytu.

### **Osoba fizyczna prowadząca działalność gospodarczą lub spółka cywilna**

Dokument tożsamości danej osoby prowadzącej działalność gospodarczą/wspólnika(ów) spółki cywilnej oraz dokument zawierający aktualne dane z wyciągu z właściwego rejestru, innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła.



## Sprzedaż zdalna

„Przedstawiciel TUnŻ ”WARTA” S.A. ma obowiązek osobiście zweryfikować tożsamość klienta (ubezpieczającego) na podstawie dokumentu stwierdzającego tożsamość”.

Dokument tożsamości - dokument stwierdzający tożsamość osoby. Podstawowe dane zawarte w dokumencie: nazwisko, imiona osoby, data urodzenia, płeć, numer PESEL, nr dokumentu tożsamości, data ważności dokumentu.

Dla obywateli polskich podstawowym dokumentem tożsamości jest dowód osobisty i paszport, dla obcokrajowców karta pobytu oraz dokument pobytu.

Odznaczenie krzyżyka w AZP oznacza, że wniosek został wystawiony zgodnie z przepisami ustawy AML, tj. m.in. że poprawnie dokonano identyfikacji i weryfikacji klienta

OSOBIŚCIE tzn.

- NIE przez telefon,
- NIE listownie,
- NIE mailem.

**Zachowaj wzmożoną czujność w trakcie weryfikowania tożsamości klienta.**

**warta.**



## Wzmożone ryzyko AML

O wyższym ryzyku prania pieniędzy oraz finansowania terroryzmu może świadczyć:

- nawiązywanie stosunków gospodarczych w nietypowych okolicznościach;
- nietypowa lub nadmiernie złożona struktura własności klienta, biorąc pod uwagę rodzaj i zakres prowadzonej przez niego działalności gospodarczej;
- zlecenie przez nieznaną lub niepowiązaną z klientem podmiot trzeciej transakcji, których beneficjentem rzeczywistym jest klient;
- transakcje związane z ropą naftową, bronią, metalami szlachetnymi, produktami tytoniowymi, artefaktami kulturowymi i innymi przedmiotami o znaczeniu archeologicznym, historycznym, kulturowym i religijnym lub o szczególnej wartości naukowej, a także kością słoniową i gatunkami chronionymi;
- korzystanie przez klienta z usług lub produktów sprzyjających anonimowości lub utrudniających jego identyfikację.

## Ocena ryzyka klienta - kryteria

<p><b>Klient</b></p>	<p>Podczas analizowania czynników oceny ryzyka odnoszących się do klienta można wziąć pod uwagę następujące kwestie:</p> <ul style="list-style-type: none"> <li>• powiązania klienta z sektorami, które są kojarzone z wyższym ryzykiem korupcji: handel bronią, przemysł wydobywczy lub zamówienia publiczne, rynek kryptowalut,</li> <li>• powiązania klienta z sektorami, które są kojarzone z wyższym ryzykiem prania pieniędzy lub finansowania terroryzmu,</li> <li>• charakter działalności i cel powołania osób prawnych bądź podmiotów nieposiadających osobowości prawnej,</li> <li>• fakt zajmowania przez klienta lub beneficjenta rzeczywistego eksponowanego stanowiska politycznego, bądź innej ważnej funkcji, która stwarza mu możliwość nadużywania pozycji do uzyskania korzyści.</li> </ul>
<p><b>Ryzyko geograficzne</b></p>	<p>Przy zarządzaniu ryzykiem geograficznym na etapie oceny ryzyka można uwzględnić poniższe zagadnienia:</p> <ul style="list-style-type: none"> <li>• adres zamieszkania lub siedziby, kraj obywatelstwa, kraj urodzenia występujący na liście państw podwyższonego ryzyka,</li> <li>• informacje z wiarygodnych i rzetelnych źródeł, z których wynika, że jurysdykcja finansuje lub wspiera działalność terrorystyczną albo grupy popełniające przestępstwa terrorystyczne na danym terytorium,</li> <li>• embargo nałożone przez np. ONZ lub UE na kraje powiązane z terroryzmem lub rozprzestrzenianiem broni masowego rażenia,</li> <li>• wypłaty do krajów podwyższonego ryzyka.</li> </ul>
<p><b>Rodzaj produktu, usługi i sposób dystrybucji</b></p>	<p>Brane pod uwagę są następujące kwestie:</p> <ul style="list-style-type: none"> <li>• rodzaj produktu, którym interesuje się klient – ochronny, inwestycyjny czy oszczędnościowy,</li> <li>• sposób zawarcia umowy (osobiście czy na odległość np. online).</li> </ul>
<p><b>Poziom wartości majątkowych</b></p>	<p>W tej kategorii brane są pod uwagę:</p> <ul style="list-style-type: none"> <li>• wysokość transakcji, wpłaconych składek,</li> <li>• ilości zawartych umów.</li> </ul>
<p><b>Cel, regularność, czas trwania</b></p>	<p>Sprawdzana jest szybkość dokonywania wykupów (zysk/strata).</p>
<p><b>Inne okoliczności/zachowanie</b></p>	<p>Należy zwrócić uwagę na inne niepokojące sygnały, takie jak:</p> <ul style="list-style-type: none"> <li>• podejrzane zachowanie (czynniki behawioralne),</li> <li>• obecność osób trzecich (klient nie działa samodzielnie),</li> <li>• negatywne informacje znane z innych źródeł (np. zła reputacja, relacje mediów)</li> </ul>
<p><b>Listy sankcyjne/PEP</b></p>	<p>Dokonywana jest weryfikacja czy klient, reprezentant, pełnomocnik, beneficjent rzeczywisty lub uprawniony jest obecny na listach sankcyjnych bądź posiada status osoby zajmującej eksponowane stanowisko polityczne.</p>

## Sytuacje podejrzone

### Potencjalnie podejrzone elementy podczas zawierania umowy:

- ✓ Klient podaje budzące wątpliwości dane dotyczące tożsamości.
- ✓ Autentyczność przedstawionych dokumentów przez klienta budzi wątpliwość.
- ✓ Klient zamiast pełnego adresu chce podać adres skrytki pocztowej.
- ✓ Niezrozumiałe pod względem ekonomicznym decyzje Klienta, w szczególności brak zainteresowania korzystniejszymi warunkami zawarcia umowy .
- ✓ Zawieranie umów ubezpieczenia w miejscu niemającym związku z miejscem zamieszkania lub siedzibą firmy, np. w innym mieście.
- ✓ Ubezpieczający jest kontrolowany przez inną osobę, szczególnie w sytuacji, w której klient jest osobą nieświadomą, niedołążną lub w podeszłym wieku i towarzyszy mu osoba, która nie jest jego krewnym/krewną.

### Następujące sytuacje mogą budzić uzasadnione podejrzenia:

- ✓ Wykup polis ubezpieczeniowych o relatywnie niskiej wartości wpłaty nieproporcjonalnie wysokich składek/ wpłat nieobowiązkowych,
- ✓ Odbiorcą świadczenia/wykupu ubezpieczenia jest firma,
- ✓ Wypłata świadczeń/wykupu z kilku polis do powtarzających się odbiorców,
- ✓ Wypowiedzenie umowy ubezpieczenia w dość krótkim czasie po jej zawarciu,
- ✓ Częste wpłaty dobrowolne oraz częste wykupy z polisy.



# Postępowanie w sytuacji podejrzenia



**Każda** osoba biorąca udział w obsłudze umowy ubezpieczenia na którymkolwiek etapie zobowiązany jest do bieżącej analizy klienta i dokonywanych transakcji (w szczególności: moment zawarcia umowy, wpłaty składek, wnioski o wykup, realizacja zwrotów)

Co robić, gdy sytuacja wzbudza nasze wątpliwości lub jest nietypowa?

Należy niezwłocznie zgłosić się do Departamentu Compliance  
[compliance@warta.pl](mailto:compliance@warta.pl)

Pracownicy Departamentu Compliance dokonają szczegółowej analizy sytuacji, dokonywanych transakcji, historii klienta i w przypadku potwierdzenia podejrzenia:

- niezwłocznie, ale nie później niż w ciągu 2 dni roboczych, prześlą zawiadomienie do GIIF
- w przypadku planowanej wypłaty środków wstrzymają transakcję na max. 24h

W przypadku powzięcia uzasadnionego podejrzenia, że wartości majątkowe pochodzą z innego przestępstwa niż pranie pieniędzy lub finansowanie terroryzmu lub przestępstwo skarbowe, niezwłocznie zostanie przekazane zawiadomienie do właściwego prokuratora.

## Wstrzymanie transakcji, blokada rachunku, zamrożenie wartości majątkowych

Cel: zapobieganie praniu pieniędzy

W przypadku podejrzenia prania pieniędzy:

- TUnŻ WARTA S.A.** może wstrzymać transakcję na max. 24h i powiadomić GIIF
- Generalny Inspektor Informacji Finansowej** może przekazać instytucji pisemne żądanie:  
wstrzymania transakcji lub blokady rachunku  
maksymalnie na **96 godzin**:
  - ✓ po otrzymaniu zawiadomienia od instytucji, z którego wynika, że transakcja, która ma zostać przeprowadzona, może mieć związek z popełnieniem przestępstwa
  - ✓ z własnej inicjatywy tzn. bez uprzedniego otrzymania zawiadomienia od instytucji obowiązanej

Cel: przeciwdziałanie terroryzmowi

W przypadku podejrzenia finansowania terroryzmu, TUnŻ WARTA S.A. ma obowiązek:

- zamrożenia wartości majątkowych  
będących własnością, posiadanych, kontrolowanych pośrednio lub bezpośrednio przez osoby i podmioty wskazane na podstawie list sankcyjnych UE/MSWiA/GIIF/KNF/ONZ
- nieudostępnienia wartości majątkowych  
bezpośrednio ani pośrednio (weryfikacja stron transakcji na listach sankcyjnych).



## Zasady przetwarzania danych osobowych 1/3

Osoba przetwarzająca w TUnŻ „WARTA” S.A. dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas przetwarzania danych, w tym do:

- ✓ stosowania zabezpieczeń danych osobowych wynikających z innych procedur;
- ✓ zapoznania się z przepisami dot. ochrony danych osobowych oraz dokumentacją obowiązującą w TUnŻ „WARTA” S.A. opisującą sposób przetwarzania danych osobowych;
- ✓ przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
- ✓ przetwarzania danych osobowych wyłącznie w celu i zakresie wynikającym z nałożonych obowiązków służbowych, z wyłączeniem celów prywatnych;



## Zasady przetwarzania danych osobowych 2/3

- ✓ zachowania należytej ostrożności podczas przekazywania informacji drogą telefoniczną, elektroniczną czy faksem;
- ✓ niewysyłania mailem danych osobowych poza TUnŻ „WARTA” S.A. i niekopiowanie danych na inne nośniki bez uzasadnionej potrzeby biznesowej;
- ✓ nieopuszczania stanowiska bez zabezpieczenia dokumentów papierowych zawierających dane osobowe (zasada „czystego biurka”) oraz bez zabezpieczenia dostępu do danych przetwarzanych w systemie informatycznym („zasada czystego ekranu”, „wylogowanie się”);
- ✓ niekopiowania, nieinstalowania i nieużywania oprogramowania pochodzącego z nieznanymi lub niesprawdzonych źródeł;
- ✓ nieujawniania danych osobowych osobom nieupoważnionym lub już nieuprawnionym do ich przetwarzania, również po ustaniu stosunku zatrudnienia/ustaniu umowy.



## Zasady przetwarzania danych osobowych 3/3

Osoby kierujące komórkami/jednostkami organizacyjnymi, którzy są właścicielami: procesów, aplikacji, systemów, zasobów informacyjnych są odpowiedzialni za prawidłową realizację poniższych zasad, aby dane osobowe były:

- ✓ przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
- ✓ prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
- ✓ przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

## Organy kontrolne

- **Kontrole** w ZU przeprowadzają:
  - ❑ Generalny Inspektor Informacji Finansowej
  - ❑ Komisja Nadzoru Finansowego
  - ❑ Naczelnicy urzędów celno-skarbowych
  
- Każdy z ww. organów samodzielnie nakłada w drodze decyzji karę administracyjną za **naruszenie** np.
  - Oceny ryzyka oraz jej aktualizacji,
  - Identyfikacji i weryfikacji klienta, osoby upoważnionej do działania w jego imieniu, beneficjenta rzeczywistego, uprawnionego oraz dokumentowania tych czynności,
  - Stosowania wzmożonych środków bezpieczeństwa finansowego,
  - Zapewnienia udziału osób wykonujących obowiązki AML w programach szkoleniowych (pracownicy i agenci),
  - Opóźnienie w raportowaniu transakcji do GIIF.



## Kary administracyjne

Publikacja informacji o Spółce oraz zakresie naruszenia w Biuletynie Informacji Publicznej

Nakaz zaprzestania podejmowania przez Spółkę określonych czynności

Cofnięcie koncesji lub zezwolenia albo wykreślenie z rejestru działalności regulowanej

Zakaz pełnienia obowiązków na stanowisku kierowniczym osoby odpowiedzialnej za naruszenie do 1 roku

Kara pieniężna: do wysokości równowartości 5 000 000 euro lub do wysokości 10% przychodu wskazanego w ostatnim zatwierdzonym sprawozdaniu finansowym za rok obrotowy lub skonsolidowanym sprawozdaniu finansowym w przypadku instytucji objętych skonsolidowanym sprawozdaniem grupy kapitałowej

Dodatkowo na wyznaczonego członka zarządu odpowiedzialnego za AML można nałożyć karę pieniężną do 1 000 000 PLN



## Przepisy karne

Nieprzestrzeganie zasad może także skutkować karą **pozbawienia wolności od 3 miesięcy do 5 lat**.

Dotyczy to osób działających w imieniu lub na rzecz Instytucji Obowiązanej, które dopuściły się poniższych działań bądź zaniechań.

Brak zawiadomienia o podejrzanej transakcji lub wartościach majątkowych mogących mieć związek z praniem pieniędzy lub finansowaniem terroryzmu

Przekazywanie nieprawdziwych danych, zatajanie danych dotyczących transakcji, rachunków lub osób

Ujawnianie osobom nieuprawnionym, posiadaczom umowy lub osobom, których transakcja dotyczy, informacji wbrew przepisom ustawy.

Jeżeli sprawca jednego z czynów określonych powyżej działa nieumyślnie, podlega grzywnie.



# Zakończenie

Dziękujemy za uczestnictwo w szkoleniu

Wszystkiego rodzaju pytania prosimy kierować do Departamentu Compliance

[compliance@warta.pl](mailto:compliance@warta.pl)

[joanna.dziurzynska-warchol@warta.pl](mailto:joanna.dziurzynska-warchol@warta.pl)

[michal.nowak@warta.pl](mailto:michal.nowak@warta.pl)

[robert.jakimiak@warta.pl](mailto:robert.jakimiak@warta.pl)