

NR 321/2019

**UCHWAŁA**  
**ZARZĄDU KRAJOWEGO DEPOZYTU PAPIERÓW WARTOŚCIOWYCH S.A.**  
**Z DNIA 18 CZERWCA 2019 R.**

Na podstawie § 23 ust. 2 Statutu Krajowego Depozytu Papierów Wartościowych, Zarząd Krajowego Depozytu Papierów Wartościowych S.A. postanawia, co następuje:

§ 1

w Regulaminie Systemu Wymiany Informacji, stanowiącym załącznik do uchwały Nr 166/16 Zarządu Krajowego Depozytu Papierów Wartościowych S.A. z dnia 11 marca 2016 r. (z późn. zm.), wprowadza się następujące zmiany:

- 1) w § 4:
  - a) ust. 2 pkt 2 otrzymuje brzmienie:

„2) Klient ESDK - oprogramowanie funkcjonujące w ramach systemu informatycznego Uczestnika SWI, umożliwiające wymianę komunikatów z Serwerem ESDK za pośrednictwem kolejek wejściowych i wyjściowych; Dostęp do kolejek komunikatów z poziomu aplikacji klienckiej zapewnia interfejs programistyczny oprogramowania WebSphere MQ.”;
  - b) ust. 3 pkt 2 skreśla się;
- 2) w § 5 ust. 1 otrzymuje brzmienie:

„1. Zakres zastosowania:

  - 1) system służący do wymiany danych w trybie automatycznym (system – system) lub manualnym (user - system), wykorzystujący zaawansowane usługi operatora sieci SWIFT;
  - 2) System Obsługi Komunikatów SWIFT umożliwia przesyłanie pomiędzy Uczestnikiem SWI a Krajowym Depozytem dokumentów systemowych w postaci komunikatów SWIFT, przekazywanych pomiędzy systemami informatycznymi Uczestnika SWI i Krajowego Depozytu;
  - 3) zakres komunikatów SWIFT, które mogą być przekazywane pomiędzy Uczestnikami SWI oraz Krajowym Depozytem w ramach Systemu Obsługi Komunikatów SWIFT, Krajowy Depozyt określa na swojej witrynie internetowej. Struktura komunikatów SWIFT powinna być zgodna ze standardami stosowanymi w sieci SWIFT, przy czym Krajowy Depozyt może dookreślić zasady ich wypełniania.”;
- 3) w § 12 ust. 1 otrzymuje brzmienie:

„1. Przeznaczone dla stron Porozumienia SWI środki bezpieczeństwa, o których mowa w Załączniku Nr 1 do Regulaminu SWI, to jest:

  - 1) certyfikaty zawierające prywatne klucze kryptograficzne wraz z publicznymi kluczami kryptograficznymi strony (certyfikaty do ESDI/WEB, certyfikaty wykorzystywane do ESDK i zestawienia połączenia TLS w ramach oprogramowania MQ pomiędzy Krajowym Depozytem a Uczestnikiem SWI oraz certyfikat VPN służący do zabezpieczenia w systemie ESDK kanału komunikacyjnego pomiędzy Krajowym Depozytem a Uczestnikiem SWI),
  - 2) certyfikaty Urzędu Certyfikacji zawierające klucze publiczne Urzędu,
  - 3) hasła zabezpieczające,

są generowane przez Głównego Poręczyciela.”;

- 4) w § 13 ust. 3 otrzymuje brzmienie:  
„3. W przypadku, gdy system ESDK wymaga zestawienia połączenia z wykorzystaniem VPN, Główny Poręczyciel generuje certyfikat VPN. Certyfikat VPN wydawany jest jednej z osób upoważnionych przez Uczestnika SWI do odbioru środków bezpieczeństwa przeznaczonych do stosowania w systemie ESDK.”;
- 5) w § 18 ust. 1 pkt 1 otrzymuje brzmienie:  
„1) oprogramowanie klienckie Cisco VPN służące do zestawiania połączeń z Krajowym Depozytem za pośrednictwem sieci Internet wraz z jednostanowiskową licencją na korzystanie z tego oprogramowania udzieloną przez Krajowy Depozyt na podstawie licencji udzielonej przez Cisco Systems, jako podmiot posiadający prawa autorskie do tego oprogramowania, oraz z dokumentacją, w tym m.in. warunkami „License Agreement”,”;
- 6) Załącznik Nr 1 do Regulaminu SWI otrzymuje brzmienie określone w Załączniku Nr 1 do niniejszej uchwały;
- 7) Załącznik Nr 3 do Regulaminu SWI otrzymuje brzmienie określone w Załączniku Nr 2 do niniejszej uchwały;
- 8) Załącznik Nr 5 do Regulaminu SWI otrzymuje brzmienie określone w Załączniku Nr 3 do niniejszej uchwały.

## § 2

1. Uchwała wchodzi w życie z dniem podjęcia.
2. Zmiany Regulaminu SWI, o których mowa w § 1, zostają wprowadzone z dniem 1 lipca 2019 r., z zastrzeżeniem postanowień § 21 ust. 4 Regulaminu SWI.

Maciej Trybuchowski  
Prezes Zarządu

dr Paweł Górecki  
Wiceprezes Zarządu

Sławomir Panasiuk  
Wiceprezes Zarządu

Michał Stępniewski  
Wiceprezes Zarządu

Załącznik Nr 1  
do Uchwały Nr 321/2019  
Zarządu KDPW S.A. z dnia 18 czerwca 2019 r.

„Załącznik Nr 1  
do Regulaminu SWI

### **Środki bezpieczeństwa**

Podstawą funkcjonowania systemów komunikacji elektronicznej są usługi oparte na kryptografii asymetrycznej (zwanej kryptografią klucza publicznego). W zależności od aktywowanego przez Uczestnika SWI systemu komunikacji elektronicznej, Uczestnik SWI będzie posiadać unikalny zestaw środków bezpieczeństwa, na który składają się:

- 1) certyfikaty zawierające prywatne klucze kryptograficzne wraz z publicznymi kluczami kryptograficznymi strony (certyfikaty do ESDI/WEB, certyfikaty do ESDK i zestawienia połączenia TLS w ramach oprogramowania MQ pomiędzy Krajowym Depozytem a Uczestnikiem SWI oraz certyfikat VPN służący do zabezpieczenia w systemie ESDK kanału komunikacyjnego pomiędzy Krajowym Depozytem a Uczestnikiem SWI),
- 2) certyfikaty Urzędu Certyfikacji zawierające klucze publiczne Urzędu,
- 3) hasła zabezpieczające.

Krajowy Depozyt udostępnia również repozytoria list certyfikatów unieważnionych (CRL) niezbędne do weryfikacji ważności certyfikatów. Certyfikaty Urzędu Certyfikacji udostępnione będą w postaci plików w formacie binarnym CER.

### **System ESDI/WEB**

Na potrzeby systemu ESDI/WEB, Krajowy Depozyt wystawia certyfikaty służące do uwierzytelniania stron Porozumienia SWI i podpisywania dokumentów. Certyfikaty wraz z prywatnymi kluczami kryptograficznymi wystawiane dla systemu ESDI/WEB przekazywane są Uczestnikom SWI na nośnikach zewnętrznych w postaci plików PKCS12, natomiast w przypadku internetowych środków bezpieczeństwa certyfikaty wraz z prywatnymi kluczami kryptograficznymi udostępniane są Uczestnikom SWI za pośrednictwem witryny internetowej Krajowego Depozytu.

Dla zapewnienia wiarygodności komunikatów przesyłanych za pośrednictwem systemu ESDI/WEB zastosowano metody kryptograficzne oparte na rozwiązaniach PKI oraz certyfikatach. Umieszczenie w strukturze komunikatu podpisu elektronicznego zapewnia możliwość weryfikacji integralności komunikatu oraz niezaprzeczalności nadawcy. Podpis elektroniczny generowany jest dla bufora danych obejmującego komunikat merytoryczny oraz dane identyfikujące nadawcę, odbiorcę, numer i typ komunikatu oraz datę i czas utworzenia komunikatu. Do dalszego przetwarzania przyjmowane są tylko komunikaty, których podpis elektroniczny został pozytywnie zweryfikowany. Do wydawania i zarządzania certyfikatami jest wykorzystywana istniejąca w Krajowym Depozycie infrastruktura PKI (Urząd Certyfikacji). Certyfikaty wystawiane przez Urząd Certyfikacji zgodne są ze standardem X.509 v.3, a podpis elektroniczny tworzony będzie zgodnie ze standardem PKCS7 z wykorzystaniem algorytmu asymetrycznego RSA, stosującego klucze o długości co najmniej 1024 bity.

Uwierzytelnienie i autoryzacja użytkowników do systemu ESDI/WEB realizowane są w oparciu o protokół TLS oraz certyfikaty identyfikujące użytkownika w systemie. Protokół TLS zapewnia poufność i integralność danych na poziomie warstwy transportowej. Uwierzytelnienie i autoryzacja użytkownika w systemie są realizowane poprzez wykorzystanie środków bezpieczeństwa wydanych przez Krajowy Depozyt.

### **System ESDK**

Na potrzeby systemu ESDK, Krajowy Depozyt wystawia certyfikaty dla następujących zastosowań:

- certyfikaty do zestawienia połączenia TLS w ramach oprogramowania MQ, uwierzytelniania Uczestników SWI w systemie ESDK i podpisywania komunikatów;
- certyfikaty do uwierzytelniania i szyfrowania tuneli VPN.

Certyfikaty wraz z prywatnymi kluczami kryptograficznymi wystawiane dla systemu ESDK przekazywane są Uczestnikom SWI na nośnikach zewnętrznych w postaci plików PKCS12. W uzasadnionych przypadkach możliwe jest wystawianie certyfikatów na podstawie plików PKCS10 (certyfikaty dla MQ Servera lub urządzeń wspierających protokół IPSec).

Dla zapewnienia wiarygodności komunikatów przesyłanych za pośrednictwem systemu ESDK zastosowano metody kryptograficzne oparte na rozwiązaniach PKI oraz certyfikatach. Umieszczenie w strukturze komunikatu podpisu elektronicznego zapewnia możliwość weryfikacji integralności komunikatu oraz niezaprzeczalności nadawcy. Podpis elektroniczny generowany jest dla bufora danych obejmującego komunikat merytoryczny oraz dane identyfikujące nadawcę, odbiorcę, numer i typ komunikatu oraz datę i czas utworzenia komunikatu. Do dalszego przetwarzania przyjmowane są tylko komunikaty, których podpis elektroniczny został pozytywnie zweryfikowany. Do wydawania i zarządzania certyfikatami jest wykorzystywana istniejąca w Krajowym Depozycie infrastruktura PKI (Urząd Certyfikacji). Certyfikaty wystawiane przez Urząd Certyfikacji zgodne są ze standardem X.509 v.3, a podpis elektroniczny tworzony będzie zgodnie ze standardem PKCS7 z wykorzystaniem algorytmu asymetrycznego RSA, stosującego klucze o długości co najmniej 1024 bity. Uwierzytelnienie i autoryzacja Uczestników SWI do kolejek komunikatów w systemie ESDK realizowane jest w oparciu o protokół TLS oraz certyfikaty identyfikujące użytkownika w systemie. W celu zapewnienia bezpieczeństwa transmisji danych, komunikacja w ramach ESDK pomiędzy systemami Uczestników SWI a Krajowym Depozytem realizowana jest za pośrednictwem kanałów VPN (protokołu IPSec) i/lub kanału TLS w ramach oprogramowania MQ pomiędzy Krajowym Depozytem a Uczestnikiem SWI. Protokół IPSec zapewnia uwierzytelnienie Uczestników SWI oraz gwarantuje zachowanie poufności i integralności danych na poziomie warstwy transportowej. Po stronie Krajowego Depozytu kanały VPN terminowane są na koncentratorze VPN, pełniącym rolę węzła dostępowego, natomiast po stronie Uczestnika SWI na dowolnym urządzeniu sieciowym wspierającym protokół IPSec (router, VPN box, firewall) lub bezpośrednio na komputerze PC wyposażonym w odpowiednie oprogramowanie klienckie VPN, udostępniane Uczestnikowi SWI nieodpłatnie.”;

Załącznik Nr 2  
do Uchwały Nr 321/2019  
Zarządu KDPW S.A. z dnia 18 czerwca 2019 r.

„Załącznik Nr 3  
do Regulaminu SWI

### FORMULARZ CERTYFIKACYJNY

SUBSKRYBENT	
<b>A</b>	<b>DANE OSOBOWE</b>
	A1. Imię
	A2. Nazwisko
	A3. Kod kraju
	A4. Obywatelstwo
	A5. PESEL <sup>1</sup> / Data urodzenia <sup>2</sup>
	A6. Dokument tożsamości <input type="checkbox"/> dowód osobisty <sup>1</sup> <input type="checkbox"/> paszport <sup>2</sup>
	A7. Seria i numer
	<b>ADRES ZAMIESZKANIA</b>
	A8. Miejscowość
A9. Kod pocztowy	
A10. Ulica i nr domu /mieszkania	
<b>DANE KONTAKTOWE</b>	
A11. e-mail	
A12. Nr telefonu	
<b>DANE CERTYFIKACYJNE</b>	
<b>B</b>	B1. Środowisko pracy: <input type="checkbox"/> produkcyjne <input type="checkbox"/> testowe
	B2. Zastosowanie certyfikatu <input type="checkbox"/> certyfikat do systemu ESDI/WEB <input type="checkbox"/> certyfikat do systemu ESDK <input type="checkbox"/> certyfikat dla połączeń VPN
B3. Kod instytucji	
B4. Nazwa Uczestnika SWI	
<b>OŚWIADCZENIE I PODPIS</b>	
<b>C</b>	1. Subskrybent oświadcza, że dane zawarte w formularzu są zgodne z prawdą.
	<p>_____</p> <p>Podpis</p>

<sup>1</sup> PESEL - dotyczy obywateli polskich,

<sup>2</sup> Data urodzenia i paszport – dotyczy obcokrajowców,

**Administratorem Pani/Pana danych osobowych jest Krajowy Depozyt Papierów Wartościowych S.A. z siedzibą w Warszawie (00-498) przy ul. Książęcej 4.** Z KDPW S.A. można skontaktować się poprzez adres e-mail: [kdpw@kdpw.pl](mailto:kdpw@kdpw.pl) lub pisemnie, pod adresem wskazanym powyżej.

Podstawa prawna oraz cel przetwarzania:

- wykonywania prawnie uzasadnionych interesów realizowanych przez KDPW S.A. polegających na potrzebie identyfikacji Pani/Pana jako osoby przesyłającej wiadomość do KDPW S.A. w imieniu podmiotu, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB lub ESDK, funkcjonujących zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej oraz w celu zapewnienia bezpieczeństwa transakcji i innych czynności wykonywanych przez KDPW S.A., dochodzenia lub obrony ewentualnych roszczeń lub praw KDPW S.A. lub podmiotu, z którym KDPW S.A. łączy umowa, bądź inny stosunek prawny;
- wykonywania obowiązku prawnego – obowiązki takie wynikają z przepisów o przeciwdziałaniu praniu pieniędzy lub ustawy o obrocie instrumentami finansowymi.

Dotyczące Pani/Pana dane osobowe możemy przekazywać do podmiotów lub organów, które są upoważnione do ich otrzymania na podstawie przepisów prawa.

Dotyczące Pani/Pana dane osobowe będą przechowywane przez okres nie dłuższy niż 10 lat od zakończenia uczestnictwa w systemie SWI podmiotu, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB lub ESDK funkcjonujących zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej. Jeżeli toczy się spór, proces sądowy lub trwa inne postępowanie, okres przechowywania danych osobowych będzie liczony od dnia prawomocnego zakończenia sporu, a w przypadku wielu postępowań – prawomocnego zakończenia ostatniego z nich, bez względu na sposób jego zakończenia, chyba że przepisy prawa przewidują dłuższy okres przechowywania danych lub dłuższy okres przedawnienia dla roszczeń lub prawa, których/ego dotyczy postępowanie.

Przysługuje Pani/Panu prawo do żądania od KDPW S.A. dostępu do dotyczących Pani/Pana danych osobowych, prawo do ich sprostowania, gdy są niezgodne ze stanem rzeczywistym, a nadto, w przypadkach przewidzianych prawem, prawo do żądania ich usunięcia lub ograniczenia ich przetwarzania. Przysługuje Pani/Panu prawo do wniesienia sprzeciwu do przetwarzania danych osobowych. Przysługuje Pani/Panu prawo do przenoszenia danych.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego w zakresie przetwarzania Pani/Pana danych osobowych.

Podanie przez Panią/Pana danych osobowych jest dobrowolne i wynika ze stosunku prawnego pomiędzy KDPW S.A. a podmiotem, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB lub ESDK funkcjonujących zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej. Niepodanie danych osobowych uniemożliwi wydanie Pani/Panu certyfikatu umożliwiającego przesyłanie wiadomości z wykorzystaniem systemów ESDI/WEB i ESDK.

Pani/Pana dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji, w tym do profilowania, za wyjątkiem sytuacji, w których profilowanie może być związane z realizacją wymogów wynikających z przepisów prawa, np.: z koniecznością dokonania oceny ryzyka prania pieniędzy oraz finansowania terroryzmu.

---

Podpis";

Załącznik Nr 3  
do Uchwały Nr 321/2019  
Zarządu KDPW S.A. z dnia 18 czerwca 2019 r.

„Załącznik Nr 5  
do Regulaminu SWI

**Dane identyfikujące osobę upoważnioną do przesyłania informacji  
za pomocą Systemu Obsługi Komunikatów SWIFT.**

W związku z treścią § 19 ust. 1 Regulaminu SWI oraz Porozumieniem w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej, z Krajowym Depozytem, niżej podpisany/i, działając w imieniu ..... z siedzibą w ..... pod adresem ....., numer właściwego rejestru urzędowego: ..... kod instytucji: .....(dalej „**Uczestnik SWI**”), oświadczamy niniejszym iż wskazana poniżej osoba:

<b>DANE OSOBOWE</b>		
1. Imię		2. Nazwisko
3. Kod kraju	4. Obywatelstwo	5. PESEL <sup>3</sup> / Data urodzenia <sup>4</sup>
6. Notarialnie poświadczona kopia dokumentu tożsamości <input type="checkbox"/> dowód osobisty <sup>1</sup> <input type="checkbox"/> paszport <sup>2</sup>		7. Seria i numer
<b>ADRES ZAMIESZKANIA</b>		
8. Miejscowość		9. Kod pocztowy
10. Ulica i nr domu/mieszkania		
<b>DANE KONTAKTOWE</b>		
11. e-mail		12. Nr telefonu

jest osobą upoważnioną do składania w naszym imieniu oświadczeń woli za pośrednictwem Systemu Obsługi Komunikatów SWIFT, która będzie przysyłała do Krajowego Depozytu wszystkie dokumenty oznaczone kodem BIC ..... identyfikującym Uczestnika SWI w sieci SWIFT.

W przypadku odwołania lub wygaśnięcia upoważnienia udzielonego wskazanej wyżej osobie lub zmiany osoby, poprzez którą za pośrednictwem Systemu Obsługi Komunikatów SWIFT będziemy składać oświadczenia i przysyłać dokumenty do Krajowego Depozytu, zobowiązujemy się niezwłocznie złożyć w Krajowym Depozycie oświadczenie o treści jak wyżej, wskazujące nową osobę, poprzez którą będziemy działać w Systemie Obsługi Komunikatów SWIFT.

.....  
.....  
*imiona i nazwiska osób uprawnionych  
do reprezentowania Uczestnika SWI*

<sup>1 3</sup> Dotyczy obywateli polskich

<sup>1 4</sup> Dotyczy obcokrajowców



**Administratorem Pani/Pana danych osobowych jest Krajowy Depozyt Papierów Wartościowych S.A. z siedzibą w Warszawie (00-498) przy ul. Książęcej 4.** Z KDPW S.A. można skontaktować się poprzez adres e-mail: [kdpw@kdpw.pl](mailto:kdpw@kdpw.pl) lub pisemnie, pod adresem wskazanym powyżej.

Podstawa prawna oraz cel przetwarzania:

- wykonywania prawnie uzasadnionych interesów realizowanych przez KDPW S.A. polegających na potrzebie identyfikacji Pani/Pana jako osoby przesyłającej wiadomość do KDPW S.A. w imieniu podmiotu, który wskazał Panią/Pana jako osobę upoważnioną do składania w jego imieniu oświadczeń za pośrednictwem Systemu Obsługi Komunikatów SWIFT funkcjonującego zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej oraz w celu zapewnienia bezpieczeństwa transakcji i innych czynności wykonywanych przez KDPW S.A., dochodzenia lub obrony ewentualnych roszczeń lub praw KDPW S.A. lub podmiotu, z którym KDPW S.A. łączy umowa, bądź inny stosunek prawny;
- wykonywania obowiązku prawnego – obowiązki takie wynikają z przepisów o przeciwdziałaniu praniu pieniędzy lub ustawy o obrocie instrumentami finansowymi.

Dotyczące Pani/Pana dane osobowe możemy przekazywać do podmiotów lub organów, które są upoważnione do ich otrzymania na podstawie przepisów prawa.

Dotyczące Pani/Pana dane osobowe będą przechowywane przez okres nie dłuższy niż 10 lat od zakończenia uczestnictwa w systemie SWI podmiotu, który ustanowił Panią/Pana pełnomocnikiem/dalszym pełnomocnikiem do składania w jego imieniu oświadczeń za pośrednictwem ESDI/WEB lub ESDK funkcjonujących zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej. Jeżeli toczy się spór, proces sądowy lub trwa inne postępowanie, okres przechowywania danych osobowych będzie liczony od dnia prawomocnego zakończenia sporu, a w przypadku wielu postępowań – prawomocnego zakończenia ostatniego z nich, bez względu na sposób jego zakończenia, chyba że przepisy prawa przewidują dłuższy okres przechowywania danych lub dłuższy okres przedawnienia dla roszczeń lub prawa, których/ego dotyczy postępowanie.

Przysługuje Pani/Panu prawo do żądania od KDPW S.A. dostępu do dotyczących Pani/Pana danych osobowych, prawo do ich sprostowania, gdy są niezgodne ze stanem rzeczywistym, a nadto, w przypadkach przewidzianych prawem, prawo do żądania ich usunięcia lub ograniczenia ich przetwarzania. Przysługuje Pani/Panu prawo do wniesienia sprzeciwu do przetwarzania danych osobowych. Przysługuje Pani/Panu prawo do przenoszenia danych.

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego w zakresie przetwarzania Pani/Pana danych osobowych.

Podanie przez Panią/Pana danych osobowych jest dobrowolne i wynika ze stosunku prawnego pomiędzy KDPW S.A. a podmiotem, który wskazał Panią/Pana jako osobę upoważnioną do składania w jego imieniu oświadczeń za pośrednictwem Systemu Obsługi Komunikatów SWIFT funkcjonującego zgodnie z postanowieniami Porozumienia w sprawie składania oświadczeń i przesyłania dokumentów w postaci elektronicznej. Niepodanie danych osobowych uniemożliwi przesyłanie Pani/Panu wiadomości z wykorzystaniem Systemu Obsługi Komunikatów SWIFT w imieniu w/w podmiotu.

Pani/Pana dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji, w tym do profilowania, za wyjątkiem sytuacji, w których profilowanie może być związane z realizacją wymogów wynikających z przepisów prawa, np.: z koniecznością dokonania oceny ryzyka prania pieniędzy oraz finansowania terroryzmu.

.....  
*Podpis osoby wskazanej przez Uczestnika SWI*”.