Krajowy Depozyt
Papierów Wartościowych S.A.
ul. Książęca 4
00-498 Warszawa

T 22 537 93 43
F 22 627 31 11
E kdpw@kdpw.pl
www.kdpw.pl

NR 228/2020

UCHWAŁA
ZARZĄDU KRAJOWEGO DEPOZYTU PAPIERÓW WARTOŚCIOWYCH S.A.
Z DNIA 17 MARCA 2020 r.

W SPRAWIE PRZYJĘCIA
REGULAMINU DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH KRAJOWEGO DEPOZYTU PAPIERÓW WARTOŚCIOWYCH

§ 1

Na podstawie § 23 ust. 2 Statutu Krajowego Depozytu Papierów Wartościowych, Zarząd Krajowego Depozytu Papierów Wartościowych S.A., Zarząd Krajowego Depozytu przyjmuje *Regulamin dostępu do systemów informatycznych Krajowego Depozytu Papierów Wartościowych*, stanowiący załącznik do niniejszej uchwały.

§ 2

Uchwala wchodzi w życie z dniem podjęcia.

Maciej Trybuchowski
Prezes Zarządu

Sławomir Panasiuk
Wiceprezes Zarządu

REGULAMIN DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH KRAJOWEGO DEPOZYTU PAPIERÓW WARTOŚCIOWYCH

Rozdział 1

Postanowienia ogólne

§ 1

1. Regulamin dostępu do systemów informatycznych Krajowego Depozytu Papierów Wartościowych, zwany dalej „Regulaminem", określa zasady dostępu oraz autoryzacji do aplikacji KDPW przeznaczonych do elektronicznego komunikowania się z KDPW oraz zasady wymagane do zestawiania połączenia systemowego z aplikacjami KDPW.
2. Regulamin stosuje się w stosunkach prawnych wynikających z umów zawieranych przez KDPW z uczestnikami lub innymi podmiotami będącymi odbiorcami świadczonych przez KDPW usług, które są udostępnianie z wykorzystaniem systemów informatycznych KDPW.

§ 2

Ilekroć w przepisach regulaminu mowa jest o:

1) aplikacji KDPW – rozumie się przez to system informatyczny, wykorzystywany w ramach danej usługi świadczonej przez KDPW, umożliwiający wymianę informacji lub komunikatów pomiędzy uczestnikiem a KDPW, przy wykorzystaniu transmisji danych;
2) aplikacji dostępowej – rozumie się przez to aplikację umożliwiającą dostęp do aplikacji GK KDPW na zasadzie jednolitego punktu dostępowego (SSO), dostępną na stronie internetowej KDPW oraz spółki zależnej KDPW;
3) usłudze – rozumie się przez to świadczoną przez KDPW usługę albo funkcjonalności, udostępniane uczestnikom z wykorzystaniem aplikacji KDPW;
4) uczestniku – rozumie się przez to podmiot, który jest stroną umowy o uczestnictwo zawartej na podstawie regulaminu usługi KDPW, albo stroną innej umowy zawartej zgodnie z regulaminem usługi, albo podmiot uzyskujący dostęp do innych niż usługi funkcjonalności udostępnianych przez KDPW;
5) regulaminie usługi – rozumie się przez to wzorzec umowny kształtujący treść stosunku prawnego pomiędzy KDPW a uczestnikiem, obowiązujący w ramach danej usługi, albo inną umowę zawartą przez KDPW z uczestnikiem o świadczenie danej usługi;
6) komunikacie - rozumie się przez to informację, która zgodnie z postanowieniami regulaminu usługi, w relacji pomiędzy uczestnikiem a KDPW, może albo powinna być przekazana z wykorzystaniem środków komunikacji elektronicznej;
7) komunikacji elektronicznej – rozumie się przez to wymianę komunikatów pomiędzy uczestnikiem a KDPW lub uzyskanie przez uczestnika dostępu do informacji, z wykorzystaniem aplikacji KDPW;
8) KDPW – rozumie się przez to spółkę Krajowy Depozyt Papierów Wartościowych S.A.;
9) GK KDPW – rozumie się przez to KDPW oraz spółki zależne od KDPW;
10) dniu roboczym – rozumie się przez to każdy dzień tygodnia, który nie jest dniem ustawowo wolnym od pracy oraz sobotą.

§ 3

1. Komunikacja elektroniczna z aplikacjami KDPW dostępna jest poprzez następujące interfejsy

komunikacyjne:

1) interfejs U2A, będący interfejsem graficznym, wspierającym manualną wymianę danych z aplikacją KDPW, lub
2) interfejs A2A, będący interfejsem wspierającym automatyczną wymianę danych pomiędzy aplikacją KDPW a aplikacją uczestnika.

2. Interfejsy komunikacyjne określone są dla każdej z usług odrębnie zgodnie z przyjętymi w danej usłudze zasadami dotyczącymi komunikacji.

3. Dane przekazane do KDPW z wykorzystaniem interfejsu U2A należy uważać za doręczone z chwilą potwierdzenia przez aplikację KDPW skutecznego ich zapisania.

4. Dane przekazane do KDPW z wykorzystaniem interfejsu A2A należy uważać za doręczone z chwilą przekazania przez uczestnika komunikatu zawierającego te dane, o ile nie nastąpi jego odrzucenie po przeprowadzonej kontroli. Komunikat uważa się za przekazany z chwilą jego umieszczenia w kolejce wejściowej dla komunikatów, utworzonej w ramach kanału komunikacyjnego dla danej usługi.

5. Przyjęte dla danej usługi zasady komunikacji mogą wprowadzać dodatkowe obowiązki uczestnika związane z przekazywaniem komunikatów, w szczególności mogą wymagać opatrzenia komunikatu podpisem elektronicznym.

Rozdział 2

Komunikacja elektroniczna z wykorzystaniem interfejsu U2A

Oddział 1

Konto dostępowe

§ 4

1. Komunikacja elektroniczna z KDPW z wykorzystaniem interfejsu U2A wymaga otwarcia konta dostępowego w aplikacji dostępowej.

2. Konto dostępowe w aplikacji dostępowej otwiera osoba fizyczna działając we własnym imieniu, poprzez wypełnienie dedykowanego formularza dostępowego, wymaganymi w tym formularzu danymi tej osoby. Przy wypełnianiu formularza osoba ta składa oświadczenie wyrażające zgodę na przetwarzanie przez KDPW jej danych osobowych zawartych w formularzu. Nieudzielenie takiej zgody uniemożliwia złożenie wniosku o uzyskanie dostępu do aplikacji KDPW, a jej cofnięcie skutkuje zamknięciem konta dostępowego. Otwarcie konta dostępowego możliwe jest po weryfikacji adresu poczty elektronicznej podanego w formularzu, która dokonywana jest przez osobę otwierającą konto, przy użyciu wygenerowanego przez aplikację i przekazanego na ten adres kodu weryfikacyjnego.

3. Adres poczty elektronicznej podany w formularzu jest identyfikatorem konta dostępowego (loginem).

4. Szczegółowe informacje dotyczące otwarcia konta dostępowego oraz sposobu korzystania z konta dostępowego przez jego posiadacza, znajdują się w instrukcji użytkownika konta, zamieszczonej na stronie internetowej KDPW.

5. W przypadku konta dostępowego osoby, która uzyskała dostęp do aplikacji KDPW w imieniu uczestnika, uczestnik zobowiązany jest niezwłocznie powiadomić KDPW o każdym przypadku naruszenia ochrony danych wykorzystywanych do logowania się przez tą osobę do aplikacji KDPW, i w razie potrzeby, zgłosić KDPW wniosek o zablokowanie konta dostępowego tej osoby.

6. Uczestnik zobowiązany jest niezwłocznie zgłosić KDPW każde podejrzenie możliwości wykorzystania konta dostępowego osoby, która uzyskała dostęp do aplikacji KDPW w jego imieniu, przez osobę nieuprawnioną.

7. KDPW dokonuje blokady konta dostępowego:
1) w przypadku zgłoszenia przez uczestnika podejrzenia uzyskania dostępu do aplikacji KDPW, przy użyciu tego konta, przez osobę nieuprawnioną,
2) w razie zgłoszenia przez uczestnika wniosku o zablokowanie tego konta zgodnie z ust.**5**,
3) gdy utrzymywanie tego konta zagraża bezpieczeństwu systemów informatycznych KDPW,
4) gdy jest to wymagane przepisami prawa.

8. KDPW może przeprowadzać weryfikację aktywności kont dostępowych, polegającą na zweryfikowaniu dostępu osób będących posiadaczami kont dostępowych do adresów poczty elektronicznej, będących identyfikatorami tych kont. W przypadku braku uzyskania przez KDPW potwierdzenia aktywności danego konta, KDPW może zarówno zablokować jak i usunąć konto z aplikacji dostępowej, odbierając jednocześnie dostęp do aplikacji KDPW.

9. KDPW niezwłocznie informuje uczestnika o zablokowaniu konta dostępowego i przyczynie jego zablokowania.

Oddział 2

Autoryzacja do aplikacji KDPW

§ 5

1. Uzyskanie dostępu do aplikacji KDPW przez osobę będącą posiadaczem konta dostępowego następuje na podstawie wniosku.

2. Złożenie wniosku polega na:
1) wypełnieniu przez osobę upoważnioną przez uczestnika dedykowanego formularza internetowego udostępnionego w ramach otwartego przez tę osobę konta dostępowego w aplikacji dostępowej, oraz
2) dostarczeniu do KDPW oświadczenia złożonego przez uczestnika w sprawie udzielenia tej osobie upoważnienia do działania w jego imieniu w zakresie wskazanym w tym oświadczeniu oraz potwierdzającego dane osobowe tej osoby wskazane przez nią w formularzu, o którym mowa w pkt 1.

3. Oświadczenie, o którym mowa w ust. 2 pkt 2, uczestnik dostarcza do KDPW w formie pisemnej w oryginale, albo w postaci skanu, w zależności od rodzaju usługi. Szczegółowe informacje dotyczące formy i sposobu dostarczenia oświadczenia, osoba upoważniona przez uczestnika otrzymuje po wypełnieniu formularza, o którym mowa w ust. 2 pkt 2, w wiadomości mailowej wygenerowanej z aplikacji dostępowej.

4. Uzyskanie dostępu do danej aplikacji KDPW, może również nastąpić na podstawie już posiadanych uprawnień dostępowych, w przypadku:

1) tworzenia nowej aplikacji KDPW, która zastępuje aplikację dotychczas wykorzystywaną w obsłudze danej usługi - poprzez umożliwienie uzyskania dostępu do takiej aplikacji w wyniku transferu (migracji) dotychczasowych uprawnień osoby upoważnionej przez uczestnika do działania w tej usłudze**;**
2) rozpoczęcia świadczenia nowej usługi przez KDPW - poprzez przyznanie dostępu do nowej aplikacji KDPW w sposób automatyczny osobie, która posiada już uprawnienia do działania w innej usłudze; w takim przypadku osoba składająca wniosek o uzyskanie dostępu do aplikacji KDPW zostanie poinformowana o przyznaniu jej dostępu w sposób automatyczny w wiadomości mailowej wygenerowanej z aplikacji dostępowej.

5. Wniosek, o którym mowa w ust. 2, powinien zostać złożony nie później niż na 5 dni roboczych przed dniem, w którym osoba upoważniona przez uczestnika, zamierza przekazać albo otrzymać komunikat za pośrednictwem aplikacji KDPW.

6. Wniosek może dotyczyć uzyskania przez osobę upoważnioną przez uczestnika uprawnienia do:
1) bezpośredniej komunikacji z KDPW w imieniu uczestnika (rola użytkownika), albo
2) udzielania innym osobom, które poprzez wypełnienie formularza, o którym mowa w ust.2 pkt 1, wystąpią o uzyskanie dostępu do aplikacji KDPW, w zakresie określonym w pkt 1, dalszych pełnomocnictw do bezpośredniej komunikacji z KDPW w imieniu uczestnika a także do odwoływania takich dalszych pełnomocnictw, poprzez, odpowiednio, udzielanie albo odbieranie im dostępu do aplikacji KDPW (rola administratora).

7. Z zastrzeżeniem § 6, KDPW akceptuje albo odrzuca wniosek po przeprowadzeniu weryfikacji formalnej i merytorycznej oświadczenia, o którym mowa w ust. 2 pkt 2.

8. Wniosek może również zostać odrzucony po upływie terminu nie krótszego niż 30 dni od dnia wypełnienia formularza, o którym mowa w ust. 2 pkt 1, jeżeli w tym terminie nie uzyska on akceptacji KDPW.

9. W przypadku odrzucenia wniosku, uzyskanie uprawnień do dostępu do aplikacji KDPW wymaga ponownego złożenia wniosku.

§ 6

Określone dla danej usługi zasady dotyczące komunikacji, mogą przewidywać, że KDPW akceptuje albo odrzuca wyłącznie wnioski dotyczące uzyskania uprawnień, o których mowa w § 5 ust. 6 pkt 2 (rola administratora). W takim przypadku, uczestnik zobowiązany jest upoważnić przynajmniej jedną osobę do działania w jego imieniu w roli administratora. Uzyskanie dostępu do aplikacji KDPW przez osobę działającą w imieniu uczestnika w roli użytkownika, albo odebranie dostępu do aplikacji KDPW takiej osobie, może nastąpić wyłącznie przez osobę działającą w imieniu tego uczestnika, która uzyskała dostęp do tej aplikacji w roli administratora.

§ 7

1. W momencie logowania do aplikacji dostępowej posiadacz konta dostępowego dokonuje uwierzytelnienia do wszystkich aplikacji GK KDPW, do których uzyskał dostęp, dostępnych w ramach aplikacji dostępowej. Uwierzytelnienie dokonywane jest na podstawie podanego loginu i hasła do konta dostępowego.

2. Lista usług dostępnych posiadaczowi konta dostępowego jest uaktualniania w momencie każdego logowania do aplikacji dostępowej.

3. W przypadku, gdy uprawnienia dostępu do aplikacji KDPW zostały nadane w trakcie aktywnej sesji użytkownika, uprawnienia te mogą być realizowane przez posiadacza konta dostępowego po zamknięciu tej sesji i powtórnym zalogowaniu się.

4. Weryfikacja posiadanych przez użytkownika uprawnień dostępu do usług przeprowadzana jest w czasie trwania sesji dostępowej. Brak możliwości potwierdzenia uprawnień skutkuje utratą dostępu do usługi.

§ 8

1. Osobę, która uzyskała dostęp do aplikacji KDPW w roli użytkownika, w związku z dostarczeniem przez uczestnika oświadczenia, o którym mowa w § 5 ust.2 pkt 2, albo na podstawie dalszego pełnomocnictwa udzielonego jej zgodnie z § 5 ust.6 pkt 2, uważa się za osobę upoważnioną do bezpośredniej komunikacji z KDPW, a czynności dokonane przez taką osobę uznaje się za czynności dokonane przez tego uczestnika. Postanowienie zdania poprzedzającego stosuje się także w przypadku, gdy formularz lub oświadczenie, o których mowa w § 5 ust.2, zawierają nieprawidłowe dane osobowe osoby, której dotyczą.

2. Osobę, która uzyskała dostęp do aplikacji KDPW w roli administratora, w związku z dostarczeniem przez uczestnika oświadczenia, o którym mowa w § 5 ust.2 pkt 2, uważa się za osobę upoważnioną do udzielania dalszych pełnomocnictw uprawniających do bezpośredniej komunikacji z KDPW. Postanowienie ust.1 zd. drugie stosuje się odpowiednio.

3. Uczestnik zobowiązany jest, odpowiednio:
1) zapewnić należytą ochronę danych wykorzystywanych do logowania się przez osobę upoważnioną do aplikacji KDPW a także zapewnić tej osobie warunki do właściwego zabezpieczenia urządzeń, z wykorzystaniem których osoba ta loguje się do tej aplikacji, oraz ochrony tych urządzeń przed złośliwym oprogramowaniem lub dostępem osób nieuprawnionych, albo
2) na bieżąco weryfikować, czy stosowane przez osobę upoważnioną, metody i środki mające zapewnić ochronę danych wykorzystywanych przez nią do logowania się do aplikacji KDPW oraz mające chronić urządzenia, z wykorzystaniem których osoba ta loguje się do tej aplikacji, przed złośliwym oprogramowaniem lub dostępem osób nieuprawnionych, są adekwatne i zapewniają należyty poziom tej ochrony**.**

4. Ryzyko związane z doborem stosowanych środków ochrony lub metod zabezpieczenia danych lub urządzeń, o których mowa w ust.3 pkt 1 lub 2, obciąża wyłącznie uczestnika. Jeżeli środki ochrony lub metody zabezpieczenia danych lub urządzeń, o których mowa w ust.3 pkt 1 lub 2, okażą się z jakichkolwiek powodów niewystarczające lub zawodne, wyłączną odpowiedzialność za skutki takiego stanu ponosi uczestnik. Odpowiedzialność ta jest niezależna od winy uczestnika.

5. Uczestnik zobowiązany jest dokonywać cyklicznej weryfikacji uprawnień osób posiadających w jego imieniu dostęp do aplikacji KDPW.

§ 9

1. Odebranie dostępu do aplikacji KDPW może zostać dokonane:
1) przez KDPW – w wyniku odwołania przez uczestnika upoważnienia udzielonego osobie, o której mowa w § 5 ust. 6 pkt 1 lub 2;
2) przez KDPW – w wyniku dokonania blokady konta dostępowego w trybie określonym w § 4 ust. 5, 7 lub 8;

3) przez osobę upoważnioną przez uczestnika, występującą w roli administratora - w wyniku odwołania przez uczestnika upoważnienia osobie, o której mowa w § 5 ust.6 pkt 1.

2. Odwołanie upoważnienia, o którym mowa w ust. 1 pkt 1, staje się skuteczne względem KDPW z upływem drugiego dnia roboczego po dniu dostarczenia do KDPW pisemnego oświadczenia uczestnika w tej sprawie.

Rozdział 3

Komunikacja elektroniczna z wykorzystaniem interfejsu A2A

§ 10

1. Interfejs A2A jest systemem komunikacji elektronicznej dedykowanym do obsługi komunikacji zautomatyzowanej, przeznaczonym do wymiany komunikatów w czasie rzeczywistym, z zastosowaniem środków technicznych umożliwiających zachowanie poufności i integralności przesyłanych informacji przy zapewnieniu niezaprzeczalności nadawcy.

2. Komunikacja z wykorzystaniem interfejsu A2A działa w oparciu o kolejki służące przekazywaniu komunikatów, utworzone w ramach poszczególnych kanałów komunikacyjnych.

3. Kanały komunikacyjne mogą być powoływane niezależnie dla każdej aplikacji KDPW. Dopuszcza się również wykorzystanie kanału komunikacyjnego do dostępu do więcej niż jednej aplikacji KDPW, poprzez tworzenie dedykowanych im kolejek.

4. Wszystkie kolejki udostępniane w ramach interfejsu A2A tworzone są na zasadach zgodnych z regulaminami usług oraz przyjętymi w danej usłudze zasadami komunikacji. W ramach ustanawianej komunikacji, przewiduje się tworzenie par kolejek, odrębnie dla każdego kierunku komunikacji.

5. Dostęp do kolejek komunikacyjnych realizowany jest po uwierzytelnieniu dostępu do kanału komunikacyjnego, w ramach którego są one utworzone, z wykorzystaniem pobranego przez uczestnika certyfikatu elektronicznego. Komunikacja wewnątrz kanałów komunikacyjnych zabezpieczona jest protokołem szyfrowania TLS.

6. Połączenie do infrastruktury KDPW może być realizowane zarówno w modelu klient-serwer jak również serwer-serwer. Wymagane jest wykorzystanie połączenia opartego o VPN z uwierzytelnianiem opartym o mechanizm współdzielonego klucza (pre-shared key).

§ 11

1. Z zastrzeżeniem ust. 2, komunikacja z wykorzystaniem interfejsu A2A dostępna jest dla uczestnika w trybie 24/7.

2. Przerwa w dostępności kolejek komunikacyjnych może zostać spowodowana:

1) planowanymi przerwami w działaniu poszczególnych usług, ogłaszanymi zgodnie z regulaminami usług lub przyjętymi w danej usłudze zasadami komunikacji,
2) kilkuminutowymi przerwami technicznymi spowodowanymi zmianą konfiguracji ustawień kolejek komunikacyjnych.

3. Uczestnik zobowiązany jest do skonfigurowania w swoim systemie automatycznego wznowienia połączenia do kolejek komunikacyjnych.

4. KDPW zastrzega sobie prawo do usuwania z kolejek komunikacyjnych komunikatów, które nie zostały odebrane przez adresata, po upływie 30 dni od dnia przekazania komunikatu, albo w terminie krótszym, jeżeli został uzgodniony z uczestnikiem.

§ 12

1. Ustanowienie komunikacji elektronicznej z wykorzystaniem interfejsu A2A, wymaga pobrania przez uczestnika certyfikatu elektronicznego.

2. Pobranie certyfikatu elektronicznego wymaga wypełnienia przez osobę upoważnioną przez uczestnika, dedykowanego formularza zamieszczonego na stronie internetowej KDPW, wymaganymi w tym formularzu danymi, oraz dostarczenia do KDPW pisemnego oświadczenia uczestnika w sprawie uznania skuteczności doręczeń komunikantów dokonywanych z wykorzystaniem tego certyfikatu. KDPW doręcza certyfikat uczestnikowi na adres poczty elektronicznej wskazany w formularzu oraz potwierdzony przez uczestnika w dostarczonym oświadczeniu.

3. Certyfikat elektroniczny służy do uwierzytelnienia uczestnika składającego komunikat z wykorzystaniem tego certyfikatu do dedykowanego kanału komunikacyjnego.

4. KDPW oraz uczestnik uznają skuteczność doręczeń komunikatów, uwierzytelnionych przy użyciu certyfikatów elektronicznych, o których mowa w ust. 1, oraz wyrażają zgodę na przeprowadzenie wszelkich dowodów na fakt dokonania tych czynności.

5. Uczestnik zobowiązany jest przechowywać pobrany certyfikat elektroniczny w sposób zapewniający dostęp do certyfikatu wyłącznie osobom upoważnionym. Od chwili pobrania certyfikatu do chwili unieważnienia tego certyfikatu ryzyko jego utraty lub ujawnienia obciąża wyłącznie uczestnika.

§ 13

1. Z zastrzeżeniem ust. 4, certyfikaty elektroniczne zachowują ważność przez okres wskazany w treści certyfikatu.

2. Uczestnicy zobowiązani są do stałego monitorowania okresu ważności pobranych certyfikatów elektronicznych. Uczestnik powinien wystąpić do KDPW o wydanie nowego certyfikatu elektronicznego nie później niż na 10 dni roboczych przed dniem, utraty ważności tego certyfikatu.

3. KDPW może przed upływem terminu, o którym mowa w ust. 1, unieważnić certyfikat elektroniczny, z własnej inicjatywy z przyczyn technicznych, na wniosek uczestnika albo w związku z podejrzeniem, że certyfikatem elektronicznym posługuje się osoba nieupoważniona przez uczestnika.

4. KDPW udostępnia uczestnikom, na swojej stronie internetowej, listy certyfikatów unieważnionych (CRL) niezbędne do weryfikacji ważności certyfikatów. Udostępnienie informacji o unieważnieniu certyfikatu na liście, następuje niezwłocznie po unieważnieniu tego certyfikatu elektronicznego.

5. W przypadku unieważnienia certyfikatu elektronicznego, KDPW niezwłocznie informuje o tym fakcie uczestnika, na adres poczty elektronicznej wskazany w formularzu, o którym mowa w § 12 ust. 2.

§ 14

1. W razie utraty certyfikatu elektronicznego albo powstania uzasadnionego podejrzenia udostępnienia certyfikatu elektronicznego osobie nieupoważnionej, uczestnik, który pobrał certyfikat elektroniczny, niezwłocznie zwraca się do KDPW o unieważnienie certyfikatu elektronicznego, wskazując przyczyny jego unieważnienia.

2. Unieważnienie certyfikatu elektronicznego z przyczyn, o których mowa w ust. 1, następuje niezwłocznie po otrzymaniu żądania unieważnienia tego certyfikatu.

3. KDPW nie ponosi odpowiedzialności za szkody wyrządzone uczestnikowi w związku z utratą certyfikatu elektronicznego, w okresie jego ważności.

§ 15

KDPW nie jest kwalifikowanym dostawcą usług zaufania w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L Nr 257, str. 73). W związku z powyższym, certyfikat, o którym mowa w § 12, nie jest kwalifikowanym certyfikatem podpisu elektronicznego w rozumieniu tego rozporządzenia. Oznacza to w szczególności, że uwierzytelnieniu komunikatów z wykorzystaniem tych certyfikatów, w myśl przepisów w/w rozporządzenia oraz w myśl postanowień art. 78^1 ust. 2 Kodeksu cywilnego, nie można przypisać skutków prawnych równoważnych podpisowi własnoręcznemu.

Rozdział 4

Przepisy końcowe

§ 16

1. KDPW jest uprawniony do dokonywania zmian niniejszego regulaminu.

2. Treść zmian regulaminu, KDPW udostępnia uczestnikom na swojej stronie internetowej, nie później niż na 14 dni przed dniem ich wejścia w życie.

3. Dokonanie zmiany regulaminu wymaga powiadomienia uczestnika o treści zmian oraz dacie ich wejścia w życie.

4. Przekazanie informacji o dokonanej zmianie regulaminu, przy wykorzystaniu poczty elektronicznej, na adres poczty elektronicznej osoby upoważnionej przez uczestnika do uzyskania dostępu do aplikacji KDPW, uznaje się za skutecznie doręczone temu uczestnikowi.

5. W przypadku, gdy uczestnik nie wyraża zgody na dokonanie zmiany regulaminu, przysługuje mu prawo wypowiedzenia umowy z KDPW o świadczenie usługi, z zachowaniem warunków wypowiedzenia przewidzianych w regulaminie usługi.

6. Jeżeli uczestnik nie wypowiedział umowy o uczestnictwo zgodnie z ust. 5, oznacza to, że uczestnik wyraził zgodę na zmiany regulaminu, o których został powiadomiony zgodnie z postanowieniami ust. 3 - 4.