WARUNKI ŚWIADCZENIA USŁUG BANKOWOŚCI ELEKTRONICZNEJ IPKO BIZNES

Bank Polski

Obowiązujące od 14.09.2019

§ 1 Postanowienia ogólne

Niniejsze Warunki świadczenia usług Bankowości Elektronicznej iPKO biznes („**Warunki**") określają zasady świadczenia usług Bankowości Elektronicznej iPKO biznes dla klientów rynku korporacyjnego w PKO Banku Polskim SA Niederlassung Deutschland.

§ 2 Definicje

Przez użyte w Warunkach określenia rozumie się:

1) Administrator – Użytkownik działający w imieniu Posiadacza Rachunku zarządzający uprawnieniami Użytkowników, nadanymi przez Posiadacza Rachunku lub w przypadku powierzenia Bankowi funkcji parametryzowania wskazanych przez Posiadacza Rachunku uprawnień Użytkowników, Administratorem jest Użytkownik wskazany przez Posiadacza Rachunku mający podgląd do sekcji administracyjnej Kontekstu iPKO biznes,

2) Aktywacja dostępu – udostępnienie bankowości elektronicznej iPKO biznes, na podstawie wniosku Posiadacza Rachunku,

3) Autoryzacja – udzielenie Bankowi zgody przez Posiadacza Rachunku lub Użytkownika, na realizację Zlecenia płatniczego oraz Dyspozycji, a także innych czynności dokonywanych za pośrednictwem elektronicznych kanałów dostępu, poprzedzone uwierzytelnieniem lub silnym uwierzytelnieniem Użytkownika,

4) Elektroniczny kanał dostępu – udostępnione przez Bank Użytkownikowi rozwiązania techniczne umożliwiające korzystanie z usług przy użyciu urządzeń łączności i komunikacji przewodowej lub bezprzewodowej, w szczególności kanał:

a) internetowy,

b) telefoniczny,

c) mobilny,

(poszczególne kanały dostępu mogą różnić się od siebie zakresem oferowanych opcji i funkcji, a aktualny, szczegółowy opis funkcji udostępnionych za ich pośrednictwem dostępny jest w materiałach informacyjnych na stronie internetowej),

5) Hasło – hasło dostępu; indywidualna dana uwierzytelniająca w postaci alfanumerycznego ciągu znaków służącego do weryfikacji Użytkownika w ramach bankowości elektronicznej iPKO biznes,

6) Identyfikator Użytkownika – indywidualna dana uwierzytelniająca w postaci unikalnego numeru nadawanego Użytkownikowi, wykorzystywanego przy identyfikacji Użytkownika podczas logowania do bankowości elektronicznej iPKO biznes,

7) Indywidualne dane uwierzytelniające - indywidualne dane zapewnione przez Bank w celu uwierzytelnienia, które mogą być wykorzystywane również do wyrażenia zgody w związku ze składaną Dyspozycją, w tym w celu Autoryzacji,

8) Instrument płatniczy – zindywidualizowane urządzenie lub zbiór procedur wykorzystywanych przez Posiadacza Rachunku do złożenia Zlecenia płatniczego,

9) Kod jednorazowy – indywidualna dana uwierzytelniająca, w postaci numerycznego ciągu znaków, służącego do Autoryzacji Dyspozycji; kody jednorazowe są przekazywane w formie karty kodów jednorazowych w formie karty chip lub karty kodów w formie karty chip z cyfrowym certyfikatem klucza publicznego albo są generowane przez token mobilny iPKO biznes albo przez token Vasco DigiPass 270,

10) Kontekst – zbiór rachunków i lista Użytkowników uprawnionych do korzystania z tych rachunków w bankowości elektronicznej iPKO biznes,

11) Powiadomienie – informacje podawane do wiadomości Posiadacza Rachunku, przekazywane za pośrednictwem bankowości elektronicznej oferowanej przez Bank, Centrum Obsługi Klienta Korporacyjnego lub umieszczane w Oddziałach, lub na stronach internetowych Banku lub na wyciągach bankowych,

12) Silne uwierzytelnienie - zapewniające ochronę poufności danych uwierzytelnienie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii wiedza, posiadanie, cecha charakterystyczna Użytkownika,

13) Token Vasco DigiPass 270 – urządzenie kryptograficzne generujące jednorazowe kody służące do weryfikacji tożsamości Użytkownika i do Autoryzacji Dyspozycji podczas korzystania z bankowości elektronicznej iPKO biznes,

14) Umowa – odpowiednio umowa Rachunku,

15) Usługa potwierdzenia dostępności na rachunku kwoty niezbędnej do wykonania transakcji płatniczej – usługa on-line polegająca na dostarczeniu informacji na temat dostępnych środków na co najmniej jednym rachunku Posiadacza Rachunku u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych,

16) Usługa dostępu do informacji o rachunku – usługa on-line polegającą na dostarczaniu skonsolidowanej informacji na temat co najmniej jednego rachunku Posiadacza Rachunku posiadanego przez Posiadacza Rachunku u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych,

17) Usługa inicjowania płatności – usługa polegająca na zainicjowaniu Zlecenia płatniczego przez dostawcę świadczącego usługę inicjowania transakcji płatniczej na wniosek Posiadacza Rachunku z rachunku prowadzonego przez innego dostawcę usług płatniczych,

18) Uwierzytelnienie - weryfikacja tożsamości Użytkownika lub ważności stosowanego instrumentu płatniczego przez Bank dokonywaną przy wykorzystaniu indywidualnych danych uwierzytelniających,

19) Użytkownik – osoba fizyczna posiadająca pełną zdolność do czynności prawnych lub innych czynności w zakresie nadanych jej uprawnień, upoważniona przez Posiadacza Rachunku do korzystania z bankowości elektronicznej iPKO biznes oraz działająca w imieniu i na rzecz Posiadacza Rachunku.

§ 3 Dostęp i korzystanie z bankowości elektronicznej

1. Warunkiem korzystania z dostępu do bankowości elektronicznej jest posiadanie odpowiedniego wyposażenia technicznego i oprogramowania, niezbędnego do współpracy z Bankiem. Bank nie gwarantuje ani nie przejmuje odpowiedzialności za oprogramowanie i urządzenie oferowane przez osoby trzecie pod kątem możliwości ich zastosowania i używania w celu Uwierzytelnienia Użytkownika.

2. Wymagania w zakresie wyposażenia technicznego i oprogramowania Bank podaje do wiadomości Posiadacza Rachunku na stronie internetowej Banku.

3. Bank informuje Posiadacza Rachunku o zasadach poprawnego i bezpiecznego korzystania z bankowości elektronicznej oraz o potencjalnych transakcjach oszukańczych o wystąpieniu podejrzanych zdarzeń i nietypowych ataków.

4. Informacje, o których mowa w ust. 1-3 Bank podaje do wiadomości Posiadacza Rachunku na stronach internetowych Banku lub w Powiadomieniach lub w serwisie telefonicznym.

5. Informacja przekazana innym kanałem (jak np. e-mail) dotycząca poprawnego i bezpiecznego korzystania z bankowości elektronicznej nie jest informacją wiarygodną.

6. W bankowości elektronicznej mogą być udostępnione produkty bankowe i usługi wynikające z zakresu usług świadczonych przez Bank. Posiadacz Rachunku korzystający z bankowości elektronicznej iPKO biznes ma także możliwość zawierania umów w za pośrednictwem elektronicznych kanałów dostępu, o ile taki sposób ich zawierania został udostępniony przez Bank.

7. Informacje dotyczące produktów bankowych i zakresu usług świadczonych przez Bank w ramach bankowości elektronicznej oraz zasady i sposób korzystania z bankowości elektronicznej, w tym w szczególności ustawienia i funkcjonalność serwisu, są dostępne w materiałach informacyjnych na stronie internetowej Banku.

8. Posiadacz Rachunku jest zobowiązany zapoznać się z informacjami, o których mowa w ust. 6-7 przed rozpoczęciem korzystania z bankowości elektronicznej.

9. Zmiana wszelkich informacji oraz zasad i sposobu korzystania z bankowości elektronicznej, o których mowa w ust. 6-7, w tym w szczególności ustawień i funkcjonalności serwisu oraz zamiana wersji bankowości elektronicznej nie wymaga zgody Posiadacza Rachunku.

10. Użytkownik jest zobowiązany do logowania oraz do składania Dyspozycji w elektronicznych kanałach dostępu wyłącznie osobiście przy wykorzystaniu indywidualnych danych uwierzytelniających oraz do:

1) zachowania w tajemnicy informacji zapewniających bezpieczne korzystanie z bankowości elektronicznej i nieprzekazywania oraz nieujawniania innym osobom indywidualnych danych uwierzytelniających, w tym Hasła, kodów jednorazowych oraz informacji przekazanych Bankowi dla celów weryfikacji. Nie dotyczy to korzystania z usługi inicjowania płatności i uzyskania informacji o rachunku zgodnie z § 4.

2) należytego zabezpieczenia wyposażenia technicznego i oprogramowania, za pośrednictwem którego korzysta z bankowości elektronicznej w szczególności poprzez stosowanie:

a) wyłącznie legalnego oprogramowania, jego bieżącą aktualizację i instalację poprawek systemowych zgodnie z zaleceniami producentów,

b) aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall,

c) najnowszych wersji przeglądarek internetowych,

d) haseł zabezpieczających dostęp do komputera, w szczególności, jeśli z urządzenia korzysta więcej osób,

e) innych rekomendowanych przez Bank rozwiązań udostępnionych na stronie internetowej Banku,

3) niezwłocznego zgłoszenia utraty lub zniszczenia indywidualnych danych uwierzytelniających albo stwierdzenia nieautoryzowanych, niewykonanych lub nienależycie wykonanych Dyspozycji, w przypadku pozyskania informacji, o których mowa w ust 5 lub w przypadku podejrzenia nieautoryzowanego lub nielegalnego użycia indywidualnych danych uwierzytelniających

- telefonicznie pod numer podany w materiałach informacyjnych dotyczących bankowości elektronicznej,
- osobiście w Oddziałach Banku.

4) niezwłocznego zgłoszenia odpowiednim organom ścigania utraty lub zniszczenia indywidualnych danych uwierzytelniających lub oprogramowania, używanych do korzystania z bankowości elektronicznej.

5) W odniesieniu do stosowania indywidualnych danych uwierzytelniających Użytkownik jest w szczególności zobowiązany do:

a) zachowywania w tajemnicy danych uwierzytelniających wymagających wiedzy o czymś, o czym wie wyłącznie Użytkownik, w tym nieudostępnienia tych danych ustnie (np. telefonicznie) lub w formie tekstowej (np. przez mail lub komunikatory stosowane na smartfonach), niezapisywania ich w formie elektronicznej bez stosowania zabezpieczeń (np. zapisywania otwartym tekstem na komputerze lub urządzeniu mobilnym) i nieumieszczenia lub niezapisywania tych danych na urządzeniach do identyfikacji Użytkownika wykorzystujących posiadanie czegoś, co posiada wyłącznie Użytkownik lub jego cechy charakterystyczne,

b) w przypadku stosowania indywidualnych danych uwierzytelniających wykorzystujących posiadanie czegoś, co posiada wyłącznie Użytkownik :
   - nieudostępniania tych danych osobom trzecim,
   - uniemożliwienia osobom trzecim dostępu do mobilnego urządzenia końcowego (np. telefonu komórkowego) lub zainstalowanych na nim aplikacji służących do bankowości elektronicznej,
   - usunięcia na mobilnym urządzeniu końcowym aplikacji służących do bankowości elektronicznej przed przekazaniem tego telefon osobom trzecim (np. w drodze sprzedaży),
   - nieudostępniania poza bankowością elektroniczną danych takich jak np. kody jednorazowe ustnie (np. telefonicznie) lub w formie tekstowej (np. przez mail lub komunikatory stosowane na smartfonach,
   - chronienia przed dostępem osób trzecich uzyskanych od Banku danych dostępowych umożliwiających korzystanie z takich danych uwierzytelniających.

c) w przypadku stosowania indywidualnych danych uwierzytelniających zakładających korzystanie z cech charakterystycznych użytkownika - do zapewnienia, że na mobilnym urządzeniu końcowym Użytkownika, służącym do bankowości elektronicznej, nie są zapisane takie elementy należące do innych osób. Jeśli jednak na tym urządzeniu znajdują się już takie elementy należące do osób trzecich, to wtedy należy zastosować elementy indywidualnych danych uwierzytelniających wymagających wiedzy o czymś, o czym wie wyłącznie Użytkownik (np. Hasło),

6) Numer telefonu stosowany do odbioru kodów jednorazowych należy usnąć lub zmienić, jeśli nie jest on już używany przez Użytkownika do korzystania z bankowości elektronicznej,

7) Przed wykonaniem otrzymanej od Użytkownika Dyspozycji Bank informuje go o otrzymanych od niego danych takich jak wysokość kwoty, numer rachunku odbiorcy płatności na ustalonym urządzeniu służącym do bankowości elektronicznej (np. na mobilnym urządzeniu końcowym). Użytkownik jest zobowiązany do sprawdzenia tych danych przed dokonaniem Uwierzytelnienia i w razie gdyby dane otrzymane od Banku różniły się do danych wysłanych wcześniej przez Użytkownika do przerwania realizacji Dyspozycji i niezwłocznego poinformowania

Banku o takiej sytuacji.

11. W celu zapewnienia bezpieczeństwa Dyspozycji złożonych przez Użytkownika Bank stosuje Autoryzację Dyspozycji składanych w bankowości elektronicznej z wykorzystaniem indywidualnych danych uwierzytelniających. Bank zastrzega sobie prawo odmowy wykonania dyspozycji składanych przez serwis internetowy bądź telefoniczny, gdy zaistniałe okoliczności uzasadniają wątpliwości co do tożsamości Użytkownika albo jego autentyczności. W przypadku próby uzyskania dostępu przez Użytkownika do danych szczególnie wrażliwych dotyczących płatności w rozumieniu § 1 ust, 26 zd. 1 ZAG (np. zmiana adresu Posiadacza rachunku) Użytkownik musi skorzystać z dodatkowych danych uwierzytelniających, jeśli uzyskał wcześniej do rachunku korzystając z tylko jednego sposobu uwierzytelnienia, przy czym imię i nazwisko posiadacza rachunku oraz numer rachunku nie są uznawane za dane szczególnie wrażliwe dotyczące płatności

12. Bank nagrywa rozmowy prowadzone za pośrednictwem serwisu telefonicznego oraz dokonuje zapisu Dyspozycji złożonych za pośrednictwem elektronicznych kanałów dostępu. Nagrane Dyspozycje Użytkownika stanowią dowód złożenia danej dyspozycji.

13. Użytkownikowi przysługuje dostęp do informacji stanowiącej tajemnicę bankową w zakresie wynikającym z nadanych uprawnień.

14. Wszelkie Dyspozycje złożone w formie elektronicznej przez osobę, która została prawidłowo zweryfikowana jako Użytkownik, są traktowane jako dyspozycje Użytkownika, działającego w imieniu Posiadacza Rachunku. Bank nie ponosi odpowiedzialności za realizację dyspozycji dokonanych z naruszeniem zasad określonych w ust. 10.

15. Bank może ustanowić limity kwotowe dla transakcji płatniczych, jakie mogą być zlecane w poszczególnych elektronicznych kanałach dostępu.

16. Informacja w tym zakresie udostępniana zostanie na stronie internetowej Banku.

17. Bank zastrzega sobie prawo do zablokowania w całości lub części dostępu do bankowości elektronicznej w tym zablokowaniu poszczególnych indywidualnych danych uwierzytelniających, z uzasadnionych przyczyn związanych z bezpieczeństwem dostępu do tych usług lub w związku z podejrzeniem nieuprawnionego użycia dostępu do bankowości elektronicznej lub umyślnego doprowadzenia do nieautoryzowanej dyspozycji płatniczej z wykorzystaniem dostępu do bankowości elektronicznej lub gdy Bank ma prawo do wypowiedzenia Umowy z ważnego powodu.

18. Bank, za pomocą elektronicznych kanałów dostępu, informuje Posiadacza Rachunku o zablokowaniu dostępu do bankowości elektronicznej w tym zablokowaniu poszczególnych indywidualnych danych uwierzytelniających przed zablokowaniem lub jeśli jest to niemożliwe niezwłocznie po wykonaniu tej czynności, chyba że przekazanie takiej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub jest zabronione na mocy przepisów prawa.

19. Blokada jest utrzymana, a indywidualne dane uwierzytelniające zostaną wymienione, gdy ustanie przyczyna, z powodu której została wykonana. Użytkownik zostanie niezwłocznie poinformowany o usunięciu blokady.

20. Posiadacz Rachunku uzyskuje możliwość korzystania z bankowości elektronicznej iPKO biznes po:

a) zapoznaniu się z materiałami informacyjnymi dotyczącymi bankowości elektronicznej,

b) zawarciu Umowy, aneksu lub załącznika do Umowy,

c) określeniu uprawnień, w tym wskazaniu co najmniej jednego Użytkownika jako Administratora,

d) otrzymaniu indywidualnych danych uwierzytelniających,

e) dokonaniu aktywacji dostępu.

21. Warunkiem korzystania z bankowości elektronicznej iPKO biznes jest posiadanie następujących indywidualnych danych uwierzytelniających:

a) Hasła,

b) Identyfikatora Użytkownika,

c) karty kodów jednorazowych w formie karty chip wraz z czytnikiem albo aplikacji tokena mobilnego iPKO biznes albo tokena Vasco DigiPass 270.

22. Uprawnienia funkcjonalne Użytkownika do korzystania z bankowości elektronicznej ustanawia wskazany przez Posiadacza Rachunku Administrator, wykorzystując funkcje administracyjne systemu albo Bank na podstawie Dyspozycji Posiadacza Rachunku z wykorzystaniem odrębnego wniosku o konfigurację dostępu do iPKO biznes.

23. Bank nie ponosi odpowiedzialności za skutki działania Administratora zarządzającego uprawnieniami Użytkowników po stronie Posiadacza Rachunku i Użytkowników. W przypadku powierzenia Bankowi funkcji parametryzowania wskazanych przez Posiadacza Rachunku uprawnień Użytkowników, Bank nie ponosi odpowiedzialności za zgodne z poleceniem Posiadacza Rachunku skutki ich wykonania.

24. Bank nie ingeruje w zasadność modeli uprawnień, w tym schematów akceptacji Zleceń płatniczych tworzonych przez Administratora zarządzającego uprawnieniami Użytkowników po stronie Posiadacza Rachunku.

25. Zlecenia płatnicze są wykonywane według Warunków szczegółowych obowiązujących dla danego typu zlecenia (na przykład w Warunkach realizacji zleceń przelewów).

§ 4 Korzystanie z usługi inicjowania płatności i uzyskania informacji o rachunku

1. Użytkownik może, zgodnie z § 675f ust.3 BGB, dokonać zlecenia płatności lub uzyskać informację o rachunku przez dostawcę usług inicjowania płatności w myśl § 1 ust.33 ZAG (niemieckiej ustawy o świadczeniu usług płatniczych) lub uzyskiwania informacji o rachunku w myśl § 1 ust.34 ZAG, który nawiąże w tym celu połączenie techniczne z Bankiem.
2. Bank może odmówić dostępu do rachunku dostawcom usług inicjowania płatności lub uzyskiwania informacji o rachunku, jeśli istnieją ku temu obiektywne i dające się odpowiednio wykazać powody, w związku z nieautoryzowanym bądź nielegalnym dostępem takiego dostawcy do rachunku. Bank poinformuje w ustalony sposób Posiadacza rachunku o odmowie dostępu. Udzielenie takiej informacji nastąpi w miarę możliwości przed odmową dostępu, a najpóźniej niezwłocznie po odmowie dostępu. Bank może odmówić powodów odmowy dostępu, jeśli naruszyłby w ten sposób przepisy prawa. Bank przywrócić dostęp, gdy ustaną przyczyny omowy dostępu i poinformuje o tym niezwłocznie Posiadacza rachunku.

§ 5 Odpowiedzialność

1. Odpowiedzialność Banku w razie wykonania nieautoryzowanego zlecenia płatniczego lub w razie gdy zlecenie nie zostało w ogóle wykonane lub zostało wykonane błędnie lub z opóźnieniem jest uregulowana w Warunkach szczegółowych odnoszących się do danego typu zlecenia.

2. Wszelkie roszczenia i uwagi zgłoszone przez Posiadacza Rachunku przeciwko Bankowi w wyniku niewykonania lub nieprawidłowego wykonania zlecenia płatniczego lub w wyniku realizacji nieautoryzowanego zlecenia płatniczego będą wyłączone, jeśli Posiadacz Rachunku nie powiadomi

o nich Banku okresie 13 miesięcy od momentu obciążenia z tytułu nieautoryzowanego lub nieprawidłowo wykonanego zlecenia płatniczego. Okres ten rozpoczyna bieg dopiero od momentu poinformowania Posiadacza Rachunku przez Bank o zaksięgowaniu zlecenia płatniczego w ciężar jego rachunku za pośrednictwem uzgodnionego kanału przekazywania informacji o rachunku, co nastąpi nie później niż w ciągu jednego miesiąca od daty księgowania; w przeciwnym przypadku początek biegu owego okresu określać będzie data poinformowania Posiadacza Rachunku.

3. W przypadku, gdy do wykonania nieautoryzowanych zleceń płatniczych doszło przed zgłoszeniem żądania zablokowania dostępu na skutek użycia zagubionych, skradzionych lub w inny sposób utraconych indywidualnych danych uwierzytelniających lub też ich użycia w inny nieuczciwy sposób, Posiadacz Rachunku odpowiada za ewentualne straty powstałe w ten sposób do wysokości 50,00 Euro włącznie, niezależnie od tego, czy Użytkownik działał w sposób zawiniony.

4. Posiadacz Rachunku nie ponosi odpowiedzialności na podstawie powyższego ustępu 1, gdy:

– nie był on w stanie zauważyć utraty, kradzieży, zagubienia indywidualnych danych uwierzytelniających lub ich użycia do nieuczciwych celów przed dokonaniem nieautoryzowanej płatności lub
– utrata indywidualnych danych uwierzytelniających została spowodowana przez pracownika, agenta, oddział Banku lub inny podmiot wykonujący czynności w imieniu Banku.

5. W przypadku Posiadacza Rachunku niebędącego konsumentem Posiadacz Rachunku ponosi szkodę wynikającą z nieautoryzowanych zleceń płatniczych nawet powyżej maksymalnej kwoty 50,00 Euro, jeżeli Użytkownik naruszył obowiązki nałożone na niego przez niniejsze Warunki poprzez swoje zaniedbanie. Jeżeli Bank przyczynił się do powstania szkody poprzez naruszenie swoich obowiązków, Bank odpowiada za poniesione szkody na zasadach wspólnego zaniedbania w części, za którą ponosi odpowiedzialność.

6. Posiadacz Rachunku nie jest zobowiązany do pokrycia straty, o której mowa w ustępach 3,5,7 jeśli nie mógł on zgłosić żądania zablokowania dostępu, ponieważ Bank nie udostępnił możliwość przyjęcia takiego zgłoszenia. To samo dotyczy sytuacji, w której Bank nie zażądał Silnego Uwierzytelnienia na podstawie § 1 ust. 24 ZAG.

7. W przypadkach, gdy przez zgłoszeniem żądania zablokowania dostępu przeprowadzono nieautoryzowane transakcje, a Użytkownik działał w nieuczciwych zamiarach bądź celowo lub w wyniku rażącego niedbalstwa naruszył obowiązek zachowania należytej staranności, o którym mowa w niniejszych Warunkach, to Posiadacz Rachunku odpowiada za wszelkie straty powstałe w wyniku tego do pełnej wysokości. W szczególności, za rażące niedbalstwo ze strony Użytkownika uważać się będzie naruszenie postanowień § 3 ustęp 10.

8. Odpowiedzialność z tytułu straty powstałej w okresie, w którym obowiązuje limit transakcyjny, jest ograniczona w każdym przypadku do ustalonego limitu transakcyjnego.

9. Powyższe ustępy 4,6,8 nie znajdują zastosowania, gdy Użytkownik działał w nieuczciwych zamiarach.

10. Po otrzymaniu żądania zablokowania dostępu Bank odpowiada za szkody powstałe wskutek wykonywania nieuprawnionych zleceń płatniczych za pomocą bankowości elektronicznej. To postanowienie nie znajduje jednak zastosowania, gdy Użytkownik działał w nieuczciwych zamiarach.

§ 6 Postanowienia końcowe

1. O ile nie ustalono inaczej w Warunkach, współpraca w ramach Warunków będzie regulowana Ogólnymi warunkami współpracy klienta z PKO Bankiem Polskim SA Niederlassung Deutschland („OWW"). Ponadto szczegółowy zakres współpracy regulują Warunki szczegółowe, które zawierają odstępstwa od OWW lub uzupełnienia do nich. Warunki szczegółowe mają w szczególności zastosowanie do przelewów uznaniowych i płatności polecenia zapłaty. Treść wymienionych powyżej warunków jest dostępna w Banku. Uczestnicy mogą również wnioskować o dostarczenie kopii OWW oraz Warunków szczegółowych w terminie późniejszym.

2. Zmiana niniejszych Warunków odbywa się na podstawie pkt 1 ust. 2 OWW.