

WARUNKI SZCZEGÓLNE DOTYCZĄCE BANKOWOŚCI ELEKTRONICZNEJ ZA POŚREDNICTWEM APLIKACJI WESTERN UNION DIGITAL BANKING

Mając na względzie łatwość zapoznania się z tekstem niniejsze Warunki Szczególne Dotyczące Bankowości Elektronicznej z Wykorzystaniem Aplikacji Western Union Digital Banking nie są sformułowane w sposób odnoszący się do konkretnej poci i mają równorzędne zastosowanie do wszystkich poci.

Dla potrzeb niniejszych Warunków Szczólnych termin „Dokumenty Rachunku” oznacza w dalszej części niniejszych Warunków Szczólnych wszystkie dokumenty związane z pozyskaniem klienta za pośrednictwem Aplikacji Western Union Digital Banking, w tym, między innymi, Informacje przekazywane przed zawarciem umowy przekazane przez Western Union International Bank GmbH, Ogólne warunki świadczenia usług przez Western Union International Bank GmbH, Warunki szczególne dotyczące kart debetowych i wirtualnych kart debetowych, niniejsze Warunki Szczególne, Warunki szczególne dotyczące płatności natychmiastowych w ramach Jednolitego Obszaru Płatności w Euro (Single Euro Payment Area, SEPA) oraz powiązane taryfy, jakie mogą mieć zastosowanie zależnie od przypadku, w zależności od usług, jakie Bank ma świadczyć na rzecz klienta, razem z wszelką inną dokumentacją pomocniczą niezbędną do sfinalizowania lub wdrożenia procesu pozyskania klienta za pośrednictwem Aplikacji Western Union Digital Banking, wyraźnie i z osobna zaakceptowane przez klienta, z każdorazowymi zmianami.

1. Postanowienia ogólne

1.1. Korzystanie z bankowości elektronicznej za pośrednictwem Aplikacji Western Union Digital Banking (zwanej dalej „e-bankowością”)

(1) Niniejsze Warunki Szczólnie regulują korzystanie przez klienta z e-bankowości Western Union International Bank GmbH (zwanego dalej „Bankiem”).

(2) Aplikacja Western Union Digital Banking (zwanej dalej „Aplikacja”) jest aplikacją Banku umożliwiającą klientowi, z zastrzeżeniem spełnienia wymogów uzgodnionych w niniejszych Warunkach Szczólnych, korzystania z urządzenia mobilnego terminala (np. smartfona) w celu składania zapytań (np. o saldo rachunku, obroty na rachunku) oraz do składania zleceń (np. zleceń płatniczych), a także do składania prawnie wiążących oświadczeń woli i innych oświadczeń.

(3) e-bankowość jest formą bankowości internetowej w rozumieniu aneksu do Rozporządzenia o Usługach Dotyczących Rachunków Płatniczych Konsumentów (Verbraucherzahlungskonto-Diensteverordnung) opublikowanego w Federalnym Dzienniku Ustaw II nr 60 z 2018 r. (BGBl II No. 60/2018).

1.2. Warunek korzystania z Aplikacji

Warunkiem korzystania z Aplikacji jest istnienie stosunku gospodarczego pomiędzy Bankiem i klientem oraz zawarcie umowy o korzystanie z e-bankowości pomiędzy klientem i Bankiem. Stosunek gospodarczy podlega Dokumentom Rachunku oraz ich warunkom; w szczególności niniejsze Warunki Szczólnie regulują korzystanie przez klienta z e-bankowości za pośrednictwem Aplikacji.

1.3. Rejestracja w Aplikacji

Rejestracja w Aplikacji przebiega w kolejnych etapach w Aplikacji. Pierwszym etapem jest podanie adresu poczty elektronicznej oraz Hasła (i) z którego klient korzysta logując się do swojego profilu wu.com lub (ii) stworzonego przez klienta podczas rejestracji w Aplikacji. Po stworzeniu Nazwy Użytkownika i Hasła klient może uruchomić wykorzystywanie danych biometrycznych lub Kodu Dostępu.

1.4. Definicje

Hasło

Hasło to poufne słowo (kombinacja 8-16 znaków z co najmniej 1 wielką literą, 1 małą literą i 1 cyfrą lub znakiem specjalnym) (i) z

którego klient korzysta logując się do swojego profilu wu.com lub (ii) które klient podał podczas rejestracji w Aplikacji. Hasło jest osobistą cechą identyfikacyjną klienta, która służy do identyfikacji klienta w e-bankowości, jeśli podany jest również adres poczty elektronicznej. Klient może zmienić hasło w Aplikacji.

Kod Dostępu

Kod dostępu to sześciocyfrowy numer, który może być stworzony przez klienta i używany do logowania zamiast Hasła. Za pomocą Kodu Dostępu można składać zlecenia oraz prawnie wiążące oświadczenia woli lub inne oświadczenia. Dla potrzeb kontroli przez klienta wyświetlane są w tym celu szczegóły dotyczące autoryzowanego zlecenia (np. Międzynarodowy Numer Rachunku Bankowego (International Bank Account Number, IBAN) odbiorcy i kwota transakcji płatniczej) lub prawnie wiążącego oświadczenia woli lub innego oświadczenia.

Kod Dostępu musi być podany w celu uzyskania dostępu do Aplikacji również, gdy zgodnie z austriacką Ustawą o Usługach Płatniczych (Zahlungsdienstegesetz, ZaDiG) z 2018 r. lub Rozporządzeniem delegowanym Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji wymagane jest silne uwierzytelnienie. Klient może zmienić Kod Dostępu w Aplikacji.

Rozpoznawanie Odcisku Palca

Rozpoznawanie Odcisku Palca jest osobistą cechą identyfikacyjną klienta umożliwiającą identyfikację w e-bankowości poprzez rozpoznanie odcisku palca i musi zostać aktywowane przez klienta w Aplikacji. Rozpoznawanie Odcisku Palca stanowi alternatywę dla identyfikacji klienta na podstawie adresu poczty elektronicznej i Hasła. Za pomocą Rozpoznawania Odcisku Palca można składać zlecenia oraz prawnie wiążące oświadczenia woli lub inne oświadczenia. Dla potrzeb kontroli przez klienta wyświetlane są w tym celu szczegóły dotyczące autoryzowanego zlecenia (np. Międzynarodowy Numer Rachunku Bankowego (International Bank Account Number, IBAN) odbiorcy i kwota transakcji płatniczej) lub prawnie wiążącego oświadczenia woli lub innego oświadczenia. Aby korzystać z Rozpoznawania Odcisku Palca, klient musi posiadać urządzenie z funkcją Rozpoznawania Odcisku Palca i musi aktywować Rozpoznawanie Odcisku Palca.

Rozpoznawanie Twarzy

Rozpoznawanie Twarzy jest osobistą cechą identyfikacyjną klienta umożliwiającą identyfikację w e-bankowości poprzez rozpoznanie twarzy musi zostać aktywowane przez klienta w Aplikacji. Rozpoznawanie Twarzy stanowi alternatywę dla identyfikacji klienta na podstawie adresu poczty elektronicznej i Hasła. Za pomocą Rozpoznawania Twarzy można składać zlecenia oraz prawnie wiążące oświadczenia woli lub inne oświadczenia. Dla potrzeb kontroli przez klienta wyświetlane są w tym celu szczegóły dotyczące autoryzowanego zlecenia (np. Międzynarodowy Numer Rachunku Bankowego (International Bank Account Number, IBAN) odbiorcy i kwota transakcji płatniczej) lub prawnie wiążącego oświadczenia woli lub innego oświadczenia. Aby korzystać z Rozpoznawania Twarzy, klient musi posiadać urządzenie z funkcją Rozpoznawania Twarzy i musi aktywować Rozpoznawanie Odcisku Palca.

e-Skrzynka Poczтовая

e-Skrzynka Poczтовая jest dostępną dla klienta skrzynką pocztową na potrzeby wysyłania Bankowi zawiadomień, gdyby klient miał pytania lub potrzebował wsparcia oraz odbierania zawiadomień z Banku.

Kod Uwierzytelniający

Kod uwierzytelniający jest kodem generowanym podczas silnego uwierzytelnienia klienta w rozumieniu austriackiej Ustawy o Usługach Płatniczych (Zahlungsdienstegesetz, ZaDiG) z 2018 r. Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji i jest dynamicznie związany z etapem podlegającym autoryzacji (np. autoryzowane zlecenie lub składane oświadczenie woli klienta). Przy każdym podaniu Kodu Dostępu generowany jest unikalny kod uwierzytelniający.

Silne Uwierzytelnienie Klienta

Silne uwierzytelnienie klienta jest procedurą silnego uwierzytelnienia klienta uregulowaną w austriackiej Ustawie o Usługach Płatniczych (*Zahlungsdienstegesetz, ZaDiG*) z 2018 r. i Rozporządzeniu delegowanym Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji.

2. Dostęp – zlecenia i oświadczenia

(1) Dostęp do e-bankowości jest przyznawany wyłącznie klientom, którzy potwierdzili swoją tożsamość podając swój adres poczty elektronicznej i Hasło bądź też za pomocą Rozpoznawania Odcisku Palca lub Rozpoznawania Twarzy lub podając Kod Dostępu. Podanie Kodu Dostępu w celu uzyskania dostępu do Aplikacji będzie dodatkowo wymagane, gdy od ostatniego Silnego Uwierzytelnienia Klienta minęło ponad 30 dni lub gdy klient uzyskuje dostęp do swojego rachunku płatniczego po raz pierwszy.

(2) Klient może składać zlecenia oraz prawnie wiążące oświadczenia woli lub inne oświadczenia podając Kod Dostępu lub za pomocą Rozpoznawania Odcisku Palca lub Rozpoznawania Twarzy.

(3) Klient może ponadto składać zlecenia oraz prawnie wiążące oświadczenia woli lub inne oświadczenia przyjmując ofertę wyraźnie złożoną mu przez Bank w e-bankowości składając oświadczenie o przyjęciu oferty (np. dotycząc pola zawierającego jego oświadczenie o przyjęciu oferty), a następnie potwierdzając jej przyjęcie (np. naciskając przycisk); klient może w ten sposób składać także inne oświadczenia.

(4) Bank jest uprawniony, lecz nie zobowiązany, do wykonywania przelewów zleconych przez klienta na warunkach określonych w Art. 20 do Art. 21 Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji również bez autoryzacji w drodze podania Kodu Dostępu lub za pomocą Rozpoznawania Odcisku Palca lub Rozpoznawania Twarzy.

(5) Przyjęcie zlecenia przez Bank nie będzie uważane za potwierdzenie jego wykonania.

3. Działanie z należytą starannością i zalecane środki bezpieczeństwa

3.1. Zobowiązanie do przestrzegania przepisów

Każdy klient jest zobowiązany do przestrzegania obowiązków dochowania należytej staranności uzgodnionych w Punkcie 3.2. Klienci będący przedsiębiorcami są ponadto zobowiązani do przestrzegania zalecanych środków bezpieczeństwa zgodnie z Punktem 3.3. W przypadku klientów będących konsumentami, Bank jedynie zaleca przestrzeganie zalecanych środków bezpieczeństwa tzn. że konsumenci nie są zobowiązani do ich przestrzegania. Naruszenie tych zobowiązań może, zgodnie z Punktem 7 (w przypadku konsumentów) lub Punktem 8 (w przypadku przedsiębiorców) skutkować odpowiedzialnością odszkodowawczą klienta bądź też anulowaniem lub obniżeniem jego roszczeń odszkodowawczych wobec Banku.

3.2. Obowiązki dochowania należytej staranności

3.2.1. Obowiązek zachowania poufności i blokowania

(1) Klient zachowuje swoje Hasło i Kod Dostępu w poufności; nie ujawni Hasła ani Kodu Dostępu osobom trzecim ani nie przekaze Hasła ani Kodu Dostępu osobom trzecim w żaden inny sposób. Jednakże ujawnienie Hasła i Kodu Dostępu dostawcom świadczącym usługę inicjowania płatności oraz dostawcom świadczącym usługę dostępu do informacji o rachunku jest dozwolone, o ile jest to konieczne, aby mogli oni świadczyć swoje usługi klientowi.

(2) Klient jest zobowiązany do zachowania najwyższej staranności przy przechowywaniu i korzystaniu ze swojego Hasła i Kodu Dostępu w celu uniknięcia ich niewłaściwego wykorzystania. W szczególności klient powinien zadbać o to, aby jego Hasło i Kod Dostępu nie zostało podejrzanie podczas ich używania; klient nie

powinien również przechowywać Hasła i Kodu Dostępu w swoim urządzeniu mobilnym, na którym zainstalował Aplikację, ani zapisywać ich w formie elektronicznej, np. w aplikacji do tworzenia notatek, chyba że takie przechowywanie lub taka aplikacja są zabezpieczone przed dostępem osób trzecich.

(3) W przypadku utraty Hasła i/lub Kodu Dostępu, jak również w przypadku, gdy klient dowiedział się o jakimkolwiek niewłaściwym użyciu lub innym nieuprawnionym użyciu e-bankowości, klient niezwłocznie spowoduje zablokowanie dostępu do swojej e-bankowości.

(4) W przypadku zgubienia lub kradzieży urządzenia mobilnego klienta, na którym zainstalowana jest Aplikacja, klient niezwłocznie spowoduje zablokowanie dostępu klienta do e-bankowości; dotyczy to również sytuacji, gdy klient zainstalował Aplikację na kilku urządzeniach mobilnych i jedno z nich zostało skradzione lub zgubione.

3.2.2. Obowiązek dochowania należytej staranności w zakresie blokowania dostępu do urządzenia i w trakcie instalacji

(1) Klient jest zobowiązany do zablokowania dostępu do urządzenia mobilnego, na którym została zainstalowana Aplikacja, lub dostępu do danych w nim przechowywanych osobom nieuprawnionym, jeżeli klient nie korzysta z urządzenia.

(2) Klient może zainstalować Aplikację wyłącznie ze Sklepu Apple App lub Sklepu Google Play.

3.2.3. Obowiązek dochowania należytej staranności przy składaniu zleceń i oświadczeń

Klient musi zweryfikować dane wprowadzone przez siebie i wyświetlane w Aplikacji pod względem ich poprawności przed skorzystaniem z Kodu Dostępu, Rozpoznawania Odcisku Palca lub Rozpoznawania Twarzy. Kod Dostępu, Rozpoznawanie Odcisku Palca lub Rozpoznawanie Twarzy mogą zostać wykorzystane do składania zleceń lub oświadczeń tylko, gdy dane wyświetlane w Aplikacji są zgodne z danym zleceniem lub danym prawnie wiążącym oświadczeniem woli lub innym oświadczeniem.

3.3. Zalecane środki bezpieczeństwa przy korzystaniu z e-bankowości

(1) Zaleca się, aby klient samodzielnie zmieniał Hasło i Kod Dostępu w regularnych odstępach czasu, co najmniej co dwa miesiące.

(2) Zaleca się, aby klient niezwłocznie zablokował dostęp do e-bankowości, jeżeli istnieją przesłanki, aby obawiać się, że nieuprawnione osoby trzecie weszły w posiadanie Hasła i/lub Kodu Dostępu lub jeżeli istnieją inne okoliczności, które mogłyby umożliwić nieuprawnionej osobie trzeciej niewłaściwe wykorzystanie Hasła i/lub Kodu Dostępu.

(3) Zaleca się, aby klient zabezpieczył swoje urządzenie mobilne, na którym została zainstalowana Aplikacja, przed zagrożeniami internetowymi, w szczególności, aby utrzymywał je w stanie aktualnym, jak również przeprowadzał aktualizacje zabezpieczeń systemu operacyjnego urządzenia przenośnego oraz stosował aktualną ochronę antywirusową.

4. Blokowanie

4.1. Automatyczne blokowanie

(1) Dostęp do e-bankowości zostanie automatycznie zablokowany tymczasowo, jeśli podczas dostępu Hasło zostanie błędnie wprowadzone trzy razy z rzędu. Po automatycznym zniesieniu pierwszej blokady tymczasowej, jeśli Hasło zostanie błędnie wprowadzone dwa razy z rzędu, nastąpi druga blokada tymczasowa. Po zniesieniu drugiej blokady tymczasowej, każde kolejne błędne wprowadzenie Hasła spowoduje nową blokadę tymczasową. Maksymalna łączna liczba błędnych wprowadzeń Hasła, które spowodują blokadę tymczasową, wynosi dziewięć. Po dziesiątym błędnym wprowadzeniu Hasła dostęp do e-bankowości zostanie automatycznie zablokowany na stałe. Bank niezwłocznie zawiadomi klienta o czasie trwania danej blokady tymczasowej.

(2) Dostęp do e-bankowości zostanie automatycznie zablokowany na stałe, jeśli Kod Dostępu zostanie błędnie wprowadzony pięć razy z rzędu.

4.2. Blokowanie przez klienta

Klient może w każdym czasie zablokować dostęp do e-bankowości błędnie wprowadzając Kod Dostępu pięć razy z rzędu samodzielnie lub dzwoniąc pod numer +48221520541.

4.3. Blokowanie przez Bank

(1) Bank może zablokować klientowi dostęp do e-bankowości, jeśli zablokowanie dostępu uzasadniają obiektywne przyczyny związane z bezpieczeństwem lub jeśli istnieje podejrzenie nieuprawnionego lub oszukańczego użycia.

(2) Bank zawiadomi klienta o zablokowaniu dostępu do e-bankowości i przyczynach zablokowania o ile to możliwe przed zablokowaniem, a najpóźniej bez zbędnej zwłoki po jego dokonaniu, pod warunkiem że ujawnienie zablokowania lub jego przyczyn nie naruszyłoby orzeczenia sądu lub nakazu wydanego przez organ administracyjny bądź nie byłoby sprzeczne z prawem krajowym lub europejskim albo obiektywnymi względami bezpieczeństwa

4.4. Ogłoszenie i zniesienie blokady

(1) Klient otrzyma ostrzeżenie zanim blokada tymczasowa przekształci się w blokadę stałą.

(2) Bank zniesie blokadę zgodnie z Punktem 4.3. niezwłocznie po ustaniu przyczyn, które ją spowodowały. Bank poinformuje klienta o zniesieniu blokady bez zbędnej zwłoki.

(3) Klient może w każdym czasie wystąpić o zniesienie blokady dzwoniąc pod numer +48221520541.

5. Zlecenia i prawnie wiążące oświadczenia klienta

(1) Zlecenia i prawnie wiążące zlecenia i oświadczenia woli oraz inne oświadczenia złożone przez klienta w e-bankowości będą uważane za złożone przez klienta, jeśli wydał jest podając Kod Dostępu bądź stosując Rozpoznawanie Odcisku Palca lub Rozpoznawanie Twarzy. Klient może również składać oświadczenia woli w sposób określony w Punkcie 2 Ustęp (3).

(2) Bank nie będzie zobowiązany do uzyskania potwierdzenia zlecenia bądź prawnie wiążącego oświadczenia woli lub innego oświadczenia. Nie plynie to jednakże na prawo Banku do uzyskania potwierdzenia zlecenia uzgodnione w Punkcie 4 Ogólnych warunków świadczenia usług przez Western Union International Bank GmbH (zwanych dalej „OW”).

(3) Zlecenia i prawnie wiążące zlecenia i oświadczenia woli oraz inne oświadczenia klienta mogą być składane za pośrednictwem Aplikacji, o ile są one objęte uprawnieniem do dysponowania zgodnie z Punktem 31 OW.

6. Moment otrzymania / Wykonywanie zleceń płatniczych

(1) Moment otrzymania zleceń płatniczych: Moment, w którym Bank otrzyma zlecenie płatnicze w e-bankowości będzie uważany za moment otrzymania. Jeśli zlecenie płatnicze zostanie otrzymane w dniu roboczym po nieprzekraczalnym terminie lub w dniu niebędącym dniem roboczym Banku, zalecenie będzie traktowane, jak gdyby Bank otrzymał je w następnym dniu roboczym.

(2) Nieprzekraczalny termin dla zleceń płatniczych w dniu roboczym jest określony w Punkcie II.5.2 „Informacji przekazywanych przed zawarciem umowy przekazanych przez Western Union International Bank GmbH”.

(3) Zlecenia płatnicze: Jeśli klient nie poda przyszłej daty wykonania, zlecenie płatnicze zostanie wykonane w tym samym dniu, jeśli dane dotyczące transakcji płatniczej będą dostępne do przetwarzania najpóźniej do terminu akceptacji przez Bank. W przeciwnym razie wykonanie nastąpi nie później niż w dniu roboczym następującym po dniu przekazania danych przez zlecającego. Warunkiem wykonania jest wystarczające pokrycie rachunku (saldo kredytowe lub kredyt w rachunku bieżącym).

(4) Ponadto w przypadku uregulowania poleceń przelewu zastosowanie mają Punkt 39 i Punkt 39a OW.

7. Odpowiedzialność klienta będącego konsumentem

(1) Klient będący konsumentem będzie odpowiedzialny za całkowitą utratę przez Bank nieautoryzowanej transakcji płatniczej (i) na następstwie winy umyślnej lub rażącego niedbalstwa klienta

skutkujących naruszeniem obowiązków dochowania należytej staranności zgodnie z Punktem 3.2 lub (ii) w zamiarze oszustwa.

(2) Jeśli naruszenie obowiązków dochowania należytej staranności zgodnie z Punktem 3.2 zostało spowodowane lekkim niedbalstwem klienta, wówczas odpowiedzialność klienta będzie ograniczona do maksymalnej kwoty 50 EUR. Jeżeli klient naruszył obowiązki dochowania należytej staranności zgodnie z Punktem 3.2 bez zamiaru oszustwa i bez winy umyślnej, przy ustalaniu podziału odszkodowania pomiędzy klientem i Bankiem uwzględnione zostaną rodzaj indywidualnych zabezpieczeń i szczególne okoliczności towarzyszące niewłaściwemu użyciu e-bankowości.

(3) Jeżeli klient nie zauważył utraty lub kradzieży urządzenia mobilnego, na którym została zainstalowana Aplikacja, bądź niewłaściwego użycia e-bankowości przed dokonaniem płatności, klient nie ponosi odpowiedzialności w przypadku naruszenia obowiązków dochowania należytej staranności zgodnie z Punktem 3.2 spowodowanego lekkim niedbalstwem klienta. Klient nie ponosi również odpowiedzialności w przypadku naruszenia obowiązków dochowania należytej staranności zgodnie z Punktem 3.2 spowodowanego lekkim niedbalstwem klienta, jeżeli utrata osobistych cech identyfikacyjnych klienta została spowodowana działaniami lub zaniechaniami Banku (w tym jego pracowników i agentów oraz innych podmiotów, którym zlecono wykonywanie tych usług na zasadzie outsourcingu).

(4) Niezależnie od Punktu 7 Ustęp (2), klient nie poniesie odpowiedzialności, jeśli Bank nie zażądał Silnego Uwierzytelnienia Klienta w przypadku niewłaściwego użycia e-bankowości lub w przypadku nieautoryzowanej płatności w e-bankowości. Jeśli klient przyczynił się w zamiarze oszustwa do wykonania nieautoryzowanej transakcji płatniczej, klient poniesie odpowiedzialność niezależnie od tego, czy Bank zażądał Silnego Uwierzytelnienia Klienta, czy nie.

(5) Klient nie poniesie odpowiedzialności, jeśli szkody wynikły z nieautoryzowanego użycia e-bankowości po zawiadomieniu Banku przez klienta o utracie, kradzieży lub niewłaściwym wykorzystaniu zgodnie z Punktem 3.2.1(3) lub Punktem 4, chyba że klient działał w zamiarze oszustwa.

8. Odpowiedzialność wobec przedsiębiorców / Odpowiedzialność klienta będącego przedsiębiorcą

W przypadku przedsiębiorców art. 68 austriackiej Ustawy o Usługach Płatniczych (*Zahlungsdiensteegesetz, ZaDiG*) z 2018 r. nie będzie miał zastosowania w całości; odpowiedzialność Banku z szkody wynikłe z jego lekkiego niedbalstwa będzie wyłączona. Bank nie poniesie odpowiedzialności, bez względu na stopień winy, za jakiegokolwiek szkody powstałe w związku ze sprzętem lub oprogramowaniem klienta lub spowodowane brakiem możliwości nawiązania połączenia z centrum przetwarzania danych Banku lub spowodowane czasową awarią urządzeń Banku służących do przetwarzania e-bankowości, lub jeśli przedsiębiorca naruszył obowiązki dochowania należytej staranności określone w Punkcie 3 lub jeśli przedsiębiorca nie zastosował się do zalecanych środków bezpieczeństwa określonych w Punkcie 3. W przypadku naruszenia przez przedsiębiorcę obowiązków dochowania należytej staranności określonych w Punkcie 3 lub niezastosowania się do zalecanych środków bezpieczeństwa zawartych w Punkcie 3, przedsiębiorca poniesie odpowiedzialność wobec Banku za wynikłą z tego tytułu szkodę.

9. Oświadczenia i komunikacja

(1) Klient będzie otrzymywał od Banku oświadczenia prawne, zawiadomienia i informacje (zwane dalej łącznie „Oświadczeniami”) w formie komunikacji uzgodnionej z klientem. Uzgodnione formy komunikacji to list elektroniczny, wiadomość tekstowa (SMS), powiadomienia wypychane (*push*) oraz przesyłka na e-Skrzynkę Pocztową klienta z powiadomieniem klienta. Jeżeli klient i Bank zawrą umowy dotyczące innych form komunikacji, niniejsze postanowienie nie wpłynie na ich skuteczność; dotyczy to również komunikacji za pośrednictwem Aplikacji. Niniejsze postanowienie nie wpłynie również na skuteczność oświadczeń pisemnych (w tym przesyłanych listownie).

(2) Bank może przekazywać oświadczenia skierowane do klienta na adres poczty elektronicznej podany Bankowi przez klienta. Oświadczenia złożone klientowi przez Bank za pośrednictwem poczty elektronicznej na ten adres poczty elektronicznej będą zatem skuteczne. Klient może również komunikować się z Bankiem

za pośrednictwem poczty elektronicznej i składać skuteczne oświadczenia za pośrednictwem poczty elektronicznej oraz e-Skrzynki Pocztovej w Aplikacji. Klient nie może komunikować się z Bankiem i składać skutecznych oświadczeń, jeżeli zostanie poinformowany w liście elektronicznym, że nie ma możliwości udzielenia odpowiedzi na wiadomości z tego adresu poczty elektronicznej („adresy bez możliwości udzielenia odpowiedzi”).

(3) W przypadku zmiany swojego adresu poczty elektronicznej, klient bez zbędnej zwłoki zawiadomi Bank o nowym adresie poczty elektronicznej dzwoniąc pod numer +48221520541 lub w Aplikacji. Jeżeli klient nie zawiadomił Banku o zmianie adresu poczty elektronicznej i jeżeli Bank otrzyma informację, że adres poczty elektronicznej nie jest już aktualny, oświadczenia Banku będą uważane za otrzymane przez klienta, jeżeli Bank zarówno wysłał je na ostatni podany przez klienta adres poczty elektronicznej, jak i przekazał je na e-Skrzynkę Pocztovej klienta z powiadomieniem klienta; w przypadku nieotrzymania przez Bank takiej informacji, oświadczenia Banku będą uważane za otrzymane przez klienta, jeżeli Bank przesłał je na ostatni adres poczty elektronicznej podany przez klienta.

10. Zmiany do niniejszych Warunków Szczególnych Dotyczących Bankowości Elektronicznej za Pośrednictwem Aplikacji Western Union Digital Banking

(1) Bank zaproponuje klientowi zmiany do niniejszych Warunków Szczególnych co najmniej dwa miesiące przed ich proponowaną datą wejścia w życie; postanowienia, których dotyczy propozycja wprowadzenia zmian i proponowane zmiany do niniejszych Warunków Szczególnych zostaną przedstawione w porównaniu załączonym do propozycji wprowadzenia zmian (w dalszej części niniejszych Warunków Szczególnych zwanym „**Porównaniem**”).

Propozycja wprowadzenia zmian zostanie przekazana klientowi. Uważać się będzie, że klient wyraził zgodę na wprowadzenie zmian, jeśli Bank nie otrzyma sprzeciwu klienta na piśmie lub w formie elektronicznej uzgodnionej z klientem (np. w formie listu elektronicznego lub za pośrednictwem Aplikacji) przed proponowaną datą wejścia w życie. W propozycji wprowadzenia zmian Bank zwróci uwagę klienta na fakt, że brak odpowiedzi klienta tj. brak sprzeciwu klienta na piśmie lub w formie elektronicznej uzgodnionej z klientem będzie uważany za zgodę na zmiany i klientowi będącemu konsumentem będzie przysługiwać prawo do rozwiązania umowy o korzystanie z e-bankowości i Dokumentów Rachunku, dla których została uzgodniona e-bankowość, bez wypowiedzenia i bezpłatnie przed wejściem zmian w życie. Ponadto Bank opublikuje Porównanie oraz pełną wersję nowych Warunków Szczególnych Dotyczących Bankowości Elektronicznej za Pośrednictwem Aplikacji Western Union Digital Banking na swojej stronie internetowej oraz wyśle klientowi pocztą elektroniczną pełną wersję nowych Warunków Szczególnych Dotyczących Bankowości Elektronicznej za Pośrednictwem Aplikacji na żądanie klienta; ponadto Bank nawiąże do tego w propozycji wprowadzenia zmian.

(2) Zawiadomienie i propozycja wprowadzenia zmian, o których mowa w Ustępie (1) Punktu 10, zostaną dostarczone klientowi w drodze przesłania propozycji wprowadzenia zmian razem z Porównaniem pocztą elektroniczną. Zawiadomienie zostanie złożone w taki sposób, aby Bank nie mógł jednostronnie zmienić propozycji wprowadzenia zmian, a klient miał ponadto możliwość przechowywania i wydrukowania zawiadomienia dla siebie. Propozycję wprowadzenia zmian uważać się będzie za otrzymaną przez klienta w momencie, gdy klient otrzyma list elektroniczny i będzie w stanie uzyskać te informacje w zwykłych okolicznościach.

(3) Zmiana dotycząca usług Banku w drodze zmiany niniejszych Warunków Szczególnych zgodnie z Ustępem (1) Punktu 10 będzie ograniczona do obiektywnie uzasadnionych przypadków; zmiana będzie obiektywnie uzasadniona, jeśli:

- (i) zmiana jest konieczna z uwagi na zmiany przepisów ustawowych dotyczących usług płatniczych i ich rozrachunku lub na zmiany wymogów austriackiego Urzędu Nadzoru nad Rynkami Finansowymi (*Finanzmarktaufsicht*), Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Banku Centralnego, Austriackiego Banku Narodowego (*Oesterreichische Nationalbank, OeNB*) lub innego właściwego urzędu regulacyjnego;
- (ii) zmiana jest konieczna ze względu na powstanie nowego orzecznictwa dotyczącego usług płatniczych i ich rozrachunku;

- (iii) zmiana podnosi bezpieczeństwo operacji bankowych lub przetwarzania stosunku gospodarczego z klientem dotyczącego e-bankowości;
- (iv) zmiana jest konieczna w celu uwzględnienia rozwoju technologicznego lub dostosowania nowego oprogramowania do korzystania z urządzeń mobilnych lub Aplikacji;
- (v) zmiana jest konieczna z uwagi na zmianę wymogów prawnych dotyczących składania zleceń i oświadczeń w Aplikacji;
- (vi) zmiana jest konieczna z uwagi na zmianę przepisów prawa dotyczących transakcji bankowych, które klient może przeprowadzić w Aplikacji.

Wprowadzanie opłat i prowizji oraz zmienianie uzgodnionych opłat i prowizji w drodze wprowadzania zmian do niniejszych Warunków Szczególnych jest wyłączone.