Regulamin

świadczenia usług Systemu bankowości internetowej ING Banku Śląskiego S.A. dla posiadaczy Konta dla Uchodźców

obowiązuje od 15 marca 2025 r.

Spis treści

1. Postanowienia ogólne

§ 1

1. System bankowości internetowej ING Banku Śląskiego S.A. dla posiadaczy Konta dla Uchodźców jest nazwą handlową usługi bankowości elektronicznej, o której mowa w Rozporządzeniu Ministra Rozwoju i Finansów w sprawie wykazu usług reprezentatywnych powiązanych z rachunkiem płatniczym z dnia 14 lipca 2017 r. (dalej: Rozporządzenie). Zgodnie z Rozporządzeniem usługa bankowości elektronicznej polega na dostępie do rachunku płatniczego przez Internet, która umożliwia sprawdzenie salda rachunku płatniczego, zmianę limitów dla płatności bezgotówkowych i transakcji dokonywanych przy użyciu karty debetowej lub złożenie innego rodzaju dyspozycji do rachunku. System bankowości internetowej ING Banku Śląskiego S.A. dla posiadaczy Konta dla Uchodźców może obejmować także usługi nie powiązane z rachunkami płatniczymi. Dalej w Regulaminie będą używane nazwy handlowe (tj. System bankowości internetowej, System) na określenie usługi bankowości elektronicznej.
2. Użyte w Regulaminie terminy i skróty oznaczają:
   1) **adres do doręczeń elektronicznych** - adres elektroniczny podmiotu korzystającego z publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej albo z kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, opisany w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, umożliwiający jednoznaczną identyfikację nadawcy lub adresata danych przesyłanych w ramach tych usług;
   2) **aplikacja mobilna** – aplikacja Banku przeznaczona na urządzenia mobilne. Jest ona częścią Systemu bankowości internetowej i umożliwia także dostęp do niego po jej zainstalowaniu na urządzeniu mobilnym użytkownika. Aplikacja mobilna może być dostępna w różnych wersjach i pod różnymi nazwami handlowymi m.in.: „Aplikacja Moje ING" lub „Moje ING mobile" lub inne nazwy. Wykaz aplikacji mobilnych przeznaczonych dla danego typu urządzeń mobilnych, wymogi techniczne, zakres ich funkcjonalności, w tym rodzaje dyspozycji, jakie mogą zostać złożone przy ich pomocy opisuje Komunikat.;
   3) **Bank** – ING Bank Śląski Spółka Akcyjna z siedzibą w Katowicach, przy ul. Sokolskiej 34, 40-086 Katowice, wpisany do Rejestru Przedsiębiorców w Sądzie Rejonowym Katowice-Wschód Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000005459, o kapitale zakładowym w kwocie 130 100 000 zł oraz kapitale wpłaconym w kwocie 130 100 000 zł, NIP 634-013-54-75, o międzynarodowym kodzie identyfikacyjnym w systemie SWIFT (BIC) - INGBPLPW i adresie poczty elektronicznej: info@ing.pl podlegający nadzorowi Komisji Nadzoru Finansowego z siedzibą w Warszawie, ul. Piękna 20, 00-549 Warszawa, prowadzący na podstawie zezwoleń Komisji Nadzoru Finansowego, działalność maklerską w wyodrębnionym organizacyjnie Biurze Maklerskim ING Banku Śląskiego S.A.;
   4) **czytnik cech biometrycznych** – funkcja urządzenia mobilnego udostępniona przez jego producenta lub producenta zainstalowanego na nim oprogramowania. Służy on do odczytywania cech biometrycznych i ich zapisania w urządzeniu w celu utworzenia odpowiadającego im cyfrowego klucza użytkownika;
   5) **identyfikator biometryczny** – utworzony w urządzeniu mobilnym i zapisany w nim cyfrowo klucz użytkownika, generowany dla jednej, określonej cechy biometrycznej użytkownika i odpowiadający unikatowemu kodowi, który tworzy Bank. Dla przykładu cechą biometryczną może być odcisk palca lub indywidualne cechy twarzy. Unikatowy kod jest stale powiązany z loginem użytkownika. Kod ten tworzony jest po akceptacji przez użytkownika metody uwierzytelniania lub autoryzacji dyspozycji za pomocą identyfikatora biometrycznego. Użytkownik może cofnąć zgodę na jego uwierzytelnianie lub autoryzację dyspozycji za pomocą identyfikatora biometrycznego wyłączając tę metodę w aplikacji mobilnej. Cecha biometryczna i ww. klucz użytkownika nie są przekazywane Bankowi ani przez niego zapisywane

6) **dyspozycja** – każde oświadczenie, które złożył użytkownik, zlecenie płatnicze jest też dyspozycją;
7) **dzień roboczy** – dzień inny niż sobota lub inny niż dzień ustawowo wolny od pracy;
8) **hasło** – ciąg znaków, który ustala użytkownik. Służy ono do logowania się do Systemu bankowości internetowej oraz do nadania kodu PIN do aplikacji mobilnej. Liczbę i typ znaków hasła wskazuje system w chwili jego ustalania;
9) **identyfikator użytkownika (zwany także loginem)** – indywidualny ciąg znaków nadawany użytkownikowi przez Bank, który służy do logowania się użytkownika do Systemu bankowości internetowej. Składa się on z sześciu liter oraz czterech cyfr losowych i może być konieczny do uwierzytelnienia użytkownika;
10) **jednorazowy kod aktywacyjny** – ciąg liter i cyfr generowany losowo przez Bank. Służy on do nadania hasła do Systemu bankowości internetowej i ustalenia telefonu do autoryzacji;
11) **infolinia** – linia telefoniczna przeznaczona do udzielania informacji, prowadzenia akcji marketingowych, sprzedaży i obsługi wybranych produktów i usług bankowych, a także ofert handlowych innych podmiotów, których usługi lub produkty są oferowane przez Bank lub są związane z działalnością Banku. Wykaz czynności realizowanych na infolinii jest udostępniany na tablicy ogłoszeń w placówkach bankowych oraz na stronie internetowej Banku;
12) **klucz zabezpieczeń** - urządzenie zgodne ze standardem opisanym w Komunikacie, podłączane do komputera lub urządzenia mobilnego, używane w procesie uwierzytelniania lub autoryzacji w Systemie bankowości internetowej. Uwierzytelnianie oraz autoryzacja za pomocą tego klucza zabezpieczeń jest możliwa, gdy Bank udostępnia taką funkcjonalność**;**
13) **kod autoryzacyjny, kod do autoryzacji (kod)** – ciąg cyfr lub liter lub innych znaków, który służy do uwierzytelnienia użytkownika, w tym podczas aktywacji Systemu lub aplikacji mobilnej, lub jednorazowej autoryzacji dyspozycji składanych przez użytkownika, w tym dyspozycji płatniczych. Kod ten może być wymagany także do dostępu do Systemu, w tym aplikacji mobilnej lub urządzenia lub złożenia dyspozycji. Kod ten jest generowany przez Bank chyba, że dany rodzaj kodu ustala użytkownik. Rodzajem kodu autoryzacyjnego może być np. kod SMS, kod PIN, kod przekazywany głosowo podczas automatycznego połączenia telefonicznego. Za każdym razem, gdy Regulamin pozwala na uwierzytelnianie lub autoryzację za pomocą identyfikatora biometrycznego, a użytkownik włączył metodę uwierzytelniania lub autoryzacji za pomocą identyfikatora biometrycznego, jest on kodem autoryzacyjnym w rozumieniu Regulaminu;
14) **kod PIN** – wielocyfrowy kod do logowania się do aplikacji mobilnej, autoryzacji dyspozycji lub zleceń płatniczych. Ustala go i zmienia użytkownik. W chwili jego ustalania lub zmiany Bank informuje użytkownika o wymaganej ilości cyfr w kodzie PIN;
15) **Komunikat** – wydany przez Bank Komunikat dla użytkowników Systemu bankowości internetowej dla posiadacza Konta dla Uchodźców
16) **Konwencja** – konwencja z 5 października 1961 r. znosząca wymóg legalizacji zagranicznych dokumentów urzędowych;
17) **lista kluczy zabezpieczeń** – zawiera wszystkie klucze, które użytkownik uznaje za bezpieczne i które spełniają wymogi techniczne określone w Komunikacie. Użytkownik może modyfikować listę aktywowanych kluczy przez dodawanie lub usuwanie z niej poszczególnych kluczy. Lista może zawierać jeden lub więcej kluczy;
18) **lista zaufanych przeglądarek (dalej lista przeglądarek)**– zawiera wszystkie przeglądarki, które użytkownik uznaje za bezpieczne i które spełniają wymogi techniczne określone w Komunikacie i za pomocą których decyduje się korzystać z bankowości internetowej. Użytkownik może modyfikować listę przeglądarek przez dodawanie lub usuwanie z niej poszczególnych przeglądarek. Lista przeglądarek może zawierać jedną lub więcej przeglądarek (maksymalnie 5). Przeglądarka wpisywana jest na listę w momencie logowania do bankowości internetowej za pomocą przeglądarki internetowej. Przed zapisaniem danej przeglądarki internetowej jako zaufanej przeglądarki Bank może wymagać podania lub potwierdzenia danych lub informacji w celu potwierdzenia tożsamości-użytkownika. Mogą to być także takie informacje, które, według wiedzy Banku, są znane wyłącznie użytkownikowi. Taka przeglądarka internetowa nazywana jest dalej zaufaną przeglądarką;
19) **lista zaufanych urządzeń mobilnych (dalej lista)** – zawiera wszystkie urządzenia mobilne, które użytkownik uznaje za bezpieczne i które spełniają wymogi dotyczące zasad bezpieczeństwa określone Regulaminem

i za pomocą których decyduje się korzystać z aplikacji mobilnej. Lista może zawierać jedno lub więcej urządzeń. Urządzenie mobilne wpisywane jest na listę w momencie aktywacji na nim aplikacji mobilnej. Przed zapisaniem danego urządzenia jako zaufanego urządzenia mobilnego, Bank może wymagać podania lub potwierdzenia danych lub informacji w celu zidentyfikowania tożsamości użytkownika. Mogą to być także takie informacje, które, według wiedzy Banku, są znane wyłącznie użytkownikowi. Takie urządzenie nazywane jest dalej zaufanym urządzeniem mobilnym;

20) **NFC** – Near Field Communication (skrót NFC – [ang.] komunikacja bliskiego zasięgu) – krótkozasięgowy, wysokoczęstotliwościowy, radiowy standard komunikacji pozwalający na bezprzewodową wymianę danych na odległość do 20 centymetrów;

21) **odbiorca** – osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, będąca odbiorcą środków pieniężnych stanowiących przedmiot transakcji płatniczej;

22) **oddział** - zgrupowanie jednostek lub placówek zajmujących się bezpośrednią obsługą klienta lub obsługą operacyjną w Banku;

23) **placówka bankowa** – miejsce, w którym klient obsługiwany jest przez specjalistę albo pracownika partnera Banku. Placówką bankową jest miejsce spotkań, punkt obsługi kasowej, punkt sprzedaży. Placówki bankowe są zlokalizowane w oddziale albo poza nim. Informacja o zakresie obsługi w danej placówce bankowej znajduje się w Wykazie czynności realizowanych w placówkach i na infolinii Banku. Wykaz jest dostępny na tablicy ogłoszeń w placówkach bankowych oraz na stronie internetowej Banku;

24) **płatnik** – osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, której przepisy przyznają zdolność prawną, składająca zlecenie płatnicze;

25) **powiadomienie PUSH/ push** – rodzaj komunikatu, który wyświetlany jest na zaufanym urządzeniu mobilnym z zainstalowaną aplikacją mobilną. Aby użytkownik mógł otrzymywać push-e, musi mieć włączoną tę funkcję w urządzeniu mobilnym, na którym aplikacja mobilna jest zainstalowana oraz wyrazić zgodę na ich otrzymywanie. Systemy operacyjne, dla których Bank udostępnia push-e podane są w Komunikacie;

26) **przycisk akceptacji** – przycisk, którym użytkownik potwierdza złożenie dyspozycji. Może być oznaczony znakami graficznymi lub nazwami, np. „Wyślij", „Zatwierdź", „Potwierdź", „Zamów", „Akceptuj". W zależności od dyspozycji może być zamieszczony w różnym miejscu Systemu bankowości internetowej;

27) **punkt sprzedaży** – placówka bankowa, w której klient obsługiwany jest przez pracownika partnera Banku. W punkcie sprzedaży wykonywane są czynności bankowe lub czynności faktyczne, które są związane z działalnością bankową na rzecz Banku przez partnera Banku lub jego pracowników;

28) **rachunek płatniczy** – to rachunek płatniczy w rozumieniu ustawy o usługach o płatniczych. Wiążące klienta regulacje umowne, które dotyczą danego rachunku zawierają informację, czy dany typ rachunku prowadzonego przez Bank jest rachunkiem płatniczym;

29) **rachunek oszczędnościowo-rozliczeniowy** – rachunek płatniczy w rozumieniu Regulaminu posiadaczy Konta dla Uchodźców,

30) **Regulamin** – niniejszy Regulamin

31) **Regulamin rachunków dla klientów indywidualnych** – Regulamin świadczenia przez ING Bank Śląski S.A. usług w ramach prowadzenia Konta dla Uchodźców;

32) **silne uwierzytelnianie użytkownika (zwane silnym uwierzytelnianiem)** - oznacza stosowaną przez Bank i wymaganą przepisami prawa procedurę uwierzytelniania, która zapewnia ochronę poufności danych i wymaga potwierdzenia, co najmniej dwóch spośród elementów należących do kategorii:

a) wyłącznej wiedzy użytkownika b) posiadania wyłącznie przez użytkownika określonej rzeczy lub urządzenia lub c) cechy użytkownika. Potwierdzenie to musi być niezależne w taki sposób, że naruszenie jednego z jej elementów nie osłabia wiarygodności pozostałych. Przy zachowaniu powyższej reguły potwierdzenie tych okoliczności wymagać będzie podania przez użytkownika takich elementów jak np:
a) hasła, lub
b) karty płatniczej niezależnie od jej postaci, w tym dane karty takie, jak numer karty, data ważności lub
c) kodu identyfikacyjnego lub autoryzacyjnego, lub
d) cech biometrycznych, także podawanych na urządzeniach zawierających ich czytnik jak np. telefon lub

inne urządzenie posiadające czytnik odcisku palca lub cech biometrycznych twarzy,
e) użycia kluczy zabezpieczeń, lub
innych informacji potwierdzających posiadanie przez użytkownika określonej rzeczy, urządzenia bądź cechy. Element ten uznaje się za spełniony także wówczas, gdy urządzenie należące do użytkownika zostaje uznane za zweryfikowane. Weryfikacji można dokonać przez zdalne ustalenie przez Bank cech sprzętowych lub oprogramowania urządzenia. Urządzeniami zweryfikowanymi są np. zaufane urządzenie mobilne, inne urządzenia lub rzeczy, na których zainstalowano kartę płatniczą wydaną przez Bank;

33) siła wyższa – niezależne od Banku zdarzenie zewnętrzne, któremu Bank nie mógł zapobiec lub którego nie mógł przewidzieć i które bezpośrednio lub pośrednio doprowadziło do niewykonania lub nienależytego wykonania Umowy przez Bank. Za siłę wyższą uznajemy zdarzenia spełniające powyższe przesłanki takie jak:

a) powódź, trzęsienie ziemi, wyładowania atmosferyczne, huragan, trąby powietrzne, wybuch wulkanu lub inne podobne zjawiska atmosferyczne,

b) wyłączenie dostaw prądu przez dostawcę energii elektrycznej, z przyczyn pozostających poza wpływem Banku.

Postanowienia o sile wyższej stosuje się także w przypadku działania będącego aktem władczym państwa (takiego jak umowa międzynarodowa, ustawa, rozporządzenie, zarządzenie, uchwała uprawnionego organu władzy/administracji), na mocy którego dana transakcja lub transakcje określonego typu/rodzaju lub z określonymi podmiotami, lub transakcje w określonym czasie nie mogą być przeprowadzane przez Bank. Bank poda do wiadomości publicznej fakt wystąpienia siły wyższej i - o ile jest to możliwe - przewidywany czas jej trwania;

34) System bankowości internetowej, bankowość internetowa, System – nazwy handlowe, które użyte w Umowie, Regulaminie i Komunikacie oznaczają usługę bankowości elektronicznej dla posiadaczy Konta dla Uchodźców. System bankowości internetowej dla posiadaczy Konta dla Uchodźców przeznaczony jest wyłącznie dla jego użytkowników i dostępny przez urządzenie z przeglądarką internetową i łącza internetowe lub aplikację mobilną. Może on występować w różnych wersjach, które mogą mieć różne nazwy handlowe, np.: „Moje ING" lub inne. Poszczególne, oznaczone innymi nazwami, wersje Systemu mogą się różnić wymogami technicznymi;

35) telefon do autoryzacji – numer telefonu komórkowego użytkownika przeznaczony do otrzymywania kodów autoryzacyjnych lub wykonywania usług objętych Umową lub Regulaminem. Telefon ten może służyć także do otrzymywania z Banku informacji lub zawiadomień. Mogą one dotyczyć m.in. bezpieczeństwa transakcji lub zmian Regulaminu lub innych warunków umownych. Telefon do autoryzacji wskazywany jest przez użytkownika podczas wnioskowania o udostępnienie Systemu lub zawierania Umowy lub nadawania hasła do Systemu. Użytkownik może w trybie określonym przez Bank zmienić numer telefonu do autoryzacji;

36) transakcja płatnicza/ transakcja – zainicjowana przez płatnika lub odbiorcę wpłata, transfer lub wypłata środków pieniężnych, powodująca zmianę stanu środków na rachunku;

37) transakcja zbliżeniowa – rodzaj transakcji, która jest wykonana przy użyciu technologii zbliżeniowej w terminalu akceptanta (terminalu w Punkcie Obsługi Sprzedaży) lub bankomacie wyposażonym w czytnik zbliżeniowy;

38) Umowa – zawarta pomiędzy użytkownikiem a Bankiem *Umowa o korzystanie z systemów bankowości elektronicznej* dla posiadacza Konta dla Uchodźców , której przedmiotem jest świadczenie usługi Systemu bankowości internetowej. Taką umową jest *Umowa o korzystanie z systemów bankowości elektronicznej* dla posiadaczy Konta dla Uchodźców

Za każdym razem, gdy w innych dokumentach, w tym umowach lub aneksach mowa o *umowie o korzystanie z systemów bankowości elektronicznej dla posiadacza Konta dla Uchodźców*, rozumie się Umowę;

39) unikatowy identyfikator – kombinacja liter, liczb lub symboli określona przez Bank, która jest dostarczana przez płatnika/ odbiorcę w celu jednoznacznej identyfikacji drugiego biorącego udział w transakcji płatniczej płatnika/ odbiorcy lub jego rachunku. Regulamin opisuje unikatowy identyfikator dla poszczególnych typów transakcji. Jeśli Umowa lub Regulamin nie stanowi inaczej unikatowym identyfikatorem jest numer rachunku bankowego odbiorcy lub numer telefonu komórkowego. Aby numer telefonu komórkowego odbiorcy lub osoby upoważnionej do działania w jego imieniu był unikatowym identyfikatorem musi on być uprzednio

powiązany z jednym numerem rachunku bankowego odbiorcy albo powiązany z odbiorcą w sposób umożliwiający jednoznaczną identyfikację tego odbiorcy. Zasady tego powiązania opisuje Regulamin;

40) **ustawa o usługach płatniczych, ustawa** - ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych;

41) **uwierzytelnianie** – procedura, która umożliwia Bankowi zweryfikowanie tożsamości użytkownika lub ważności stosowania danego instrumentu płatniczego, w tym jego indywidualnych danych uwierzytelniających. Regulamin określa jakie dane lub informacje mają zostać podane w celu weryfikacji tożsamości;

42) **urządzenie mobilne** – wielofunkcyjne urządzenie przenośne z dostępem do internetu, integrujące w sobie funkcje komputera i/lub telefonu komórkowego. Lista systemów operacyjnych dla urządzeń mobilnych przeznaczonych do korzystania z aplikacji mobilnej wskazana jest w § 28 ust. 3 Regulaminu, w Komunikacie oraz na stronie internetowej Banku;

43) **użytkownik** – to osoba, która jest stroną Umowy;

44) **Wykaz** - wykaz czynności realizowanych w placówkach i na infolinii Banku, zawierający informacje o zakresie obsługi wykonywanej w danej placówce bankowej. Wykaz jest udostępniany na tablicy ogłoszeń w placówkach bankowych oraz na stronie internetowej Banku i ma charakter informacyjny;

45) **zlecenie płatnicze** – oświadczenie woli płatnika lub odbiorcy skierowane do Banku, zawierające polecenie wykonania transakcji płatniczej.

3. Ilekroć w Umowie jest mowa o oddziale/placówce bankowej w odniesieniu do danej czynności, należy przez to rozumieć tę placówkę bankową, w której dana czynność jest realizowana. Informacja, w jakiej placówce bankowej ta czynność jest realizowana znajduje się w Wykazie. Wykaz jest udostępniany na tablicy ogłoszeń w placówkach bankowych oraz na stronie internetowej Banku.

4. Ilekroć w Regulaminie jest mowa o placówce bankowej w odniesieniu do danej czynności, informacja, w jakiej placówce bankowej ta czynność jest realizowana, znajduje się w Wykazie. Wykaz jest udostępniany na tablicy ogłoszeń w placówkach bankowych oraz na stronie internetowej Banku.

§ 2

1. Regulamin określa warunki, na jakich Bank świadczy usługi Systemu bankowości internetowej dla posiadaczy Konta dla Uchodźców.

2. Przedmiotem świadczenia są opisane w Regulaminie usługi Systemu bankowości internetowej umożliwiające wykonywanie, za pomocą tego Systemu, usług finansowych przez Bank.

3. Za pomocą Systemu użytkownik ma dostęp wyłącznie do usług, w tym rachunków, do których jest uprawniony. Przez osobę uprawnioną rozumie się osobę umocowaną do złożenia określonej dyspozycji zgodnie z odrębną umową.

4. Jeśli określone usługi finansowe dostępne w systemie, będą wiązać się z ryzykiem wynikającym z ich szczególnych cech lub charakteru czynności lub wynagrodzenia zależnego od ruchu cen na rynku finansowym, opis tego ryzyka znajduje się w umowach lub regulaminach (ogólnych warunkach umów) dotyczących danej usługi. Ryzyka związane z usługami Systemu bankowości internetowej mogą polegać na naruszeniu opisanych w Regulaminie zasad bezpieczeństwa, w szczególności opisanych zasad bezpiecznego korzystania z Systemu w rozdziale 16, lub ryzyka udostępnienia urządzeń lub aplikacji osobom nieupoważnionym.

5. System bankowości internetowej jest dostępny przez 24 godziny na dobę, przez 7 dni w tygodniu. Czasem właściwym dla wykonania zleceń płatniczych i innych dyspozycji składanych przez System jest czas środkowoeuropejski (CET) albo czas letni środkowoeuropejski w okresie jego wprowadzenia do odwołania.

6. Propozycja zawarcia Umowy, której treść obejmuje Regulamin nie ma charakteru wiążącego, chyba, że taki charakter wyraźnie jest przewidziany w propozycji Banku.

7. Istnieje Bankowy Fundusz Gwarancyjny, który działa na zasadach określonych w ustawie o tym Funduszu. Arkusz informacyjny dotyczący tego Funduszu Bank przekazuje posiadaczowi rachunku, zgodnie z odrębną umową rachunku. Przesłanie arkusza informacyjnego oraz potwierdzenie jego otrzymania przez użytkownika, będącego posiadaczem rachunku, może nastąpić przez System.

8. Językiem stosowanym w relacjach Banku z klientem, także wówczas, gdy Bank działa w imieniu innego podmiotu, jako pośrednik, agent lub pełnomocnik jest język polski.

9. Prawem właściwym, które stanowi podstawę stosunków Banku z klientem przed zawarciem Umowy oraz prawem właściwym do zawarcia i wykonania Umowy jest prawo polskie (prawo Rzeczypospolitej Polskiej).

10. W przypadku, gdy użytkownik będący stroną Umowy jest także stroną umowy o określony rachunek bankowy lub stroną innych umów zawartych z Bankiem lub za pośrednictwem Banku a dostęp do tych rachunków, usług lub produktów odbywa się za pomocą Systemu bankowości internetowej, w sprawach nieuregulowanych Regulaminem stosuje się postanowienia zawartych przez klienta umów, w tym regulaminów
11. Użytkownik za pośrednictwem Systemu może, o ile przepisy prawa dają taką możliwość dokonać: identyfikacji i uwierzytelniania w elektronicznej platformie usług administracji publicznej, autoryzacji związanych z wykorzystaniem profilu zaufanego oraz potwierdzania profilu zaufanego.
12. Użycie w innych regulacjach obowiązujących dla produktów i usług Banku nazwy Regulamin świadczenia usług Systemu bankowości internetowej ING Banku Śląskiego S.A. oznacza niniejszy Regulamin.
13. Komunikat nie jest integralną częścią Regulaminu i ma charakter informacyjny. Zmiana treści Komunikatu nie skutkuje zmianą Regulaminu i nie powoduje konieczności wypowiedzenia Regulaminu.
14. Bank udostępnia pełną treść Komunikatu:
    1) w placówkach bankowych - na tablicy ogłoszeń,
    2) na stronie internetowej Banku.
15. Zmiana treści Wykazu nie skutkuje zmianą Regulaminu i nie powoduje konieczności wypowiedzenia Wykazu. Aktualna treść Wykazu jest udostępniania na tablicy ogłoszeń w placówkach bankowych oraz na stronie internetowej Banku.

2. Zawarcie umowy

§ 3

1. Umowa zawierana jest na czas określony.
2. Umowa może być zawarta w placówce bankowej realizującej tę czynność, przy czym Bank zastrzega sobie prawo wyłączenia możliwości zawierania Umów w poszczególnych placówkach bankowych,
3. Umowę może zawrzeć klient będący osobą fizyczną o pełnej zdolności do czynności prawnych,
4. Bank nie udostępnia Systemu bankowości internetowej osobom ubezwłasnowolnionym częściowo i osobom ubezwłasnowolnionym całkowicie.
5. Bank, w przypadku gdy przepisy prawa tego wymagają, przed udostępnieniem użytkownikowi niektórych wskazanych w Komunikacie funkcjonalności/ usług dokonuje weryfikacji tożsamości użytkownika z przedłożonym przez niego dokumentem tożsamości podczas jego fizycznej obecności w placówce bankowej. Postanowienie to nie ma zastosowania w przypadku, gdy weryfikacja taka została dokonana w procesie zawierania Umowy.

3. Udostępnianie systemu

§ 4

1. W trakcie wnioskowania o udostępnienie Systemu lub najpóźniej po zawarciu Umowy Bank nadaje każdemu użytkownikowi login oraz przekazuje jednorazowy kod aktywacyjny lub kod autoryzacyjny.
2. Użytkownik, aby korzystać z Systemu bankowości internetowej musi go najpierw aktywować. Aktywacja Systemu oznacza nadanie ustalonego przez siebie hasła, którym użytkownik będzie logował się do Systemu.
3. Do nadania hasła do Systemu niezbędny jest kod autoryzacyjny, przekazywany w wiadomości SMS wysłanej przez Bank na podany przez użytkownika telefon do autoryzacji lub jednorazowy kod aktywacyjny przekazywany w placówce bankowej realizującej tę czynność lub przesyłką pocztową na wskazany przez użytkownika adres do korespondencji. Kod autoryzacyjny oraz jednorazowy kod aktywacyjny może być przekazany w innej formie uzgodnionej przez Bank i użytkownika.
4. Czas ważności kodu autoryzacyjnego może zostać ograniczony ze względów bezpieczeństwa Systemu. Standardowy czas ważności jest ograniczony do czasu trwania sesji tj. czasu połączenia użytkownika z Bankiem. Jednorazowy kod aktywacyjny jest ważny 30 dni liczonych od daty zamówienia go przez użytkownika.

5. Jeśli użytkownik otrzymał jednorazowy kod aktywacyjny przesyłką pocztową zobowiązany jest zadzwonić na infolinię celem potwierdzenia jej dostarczenia. Jeśli użytkownik nie potwierdzi telefonicznie faktu doręczenia jednorazowego kodu aktywacyjnego nie będzie mógł nadać hasła i korzystać z Systemu.
6. Jeśli przesyłka z jednorazowym kodem aktywacyjnym jest uszkodzona lub gdy jednorazowy kod aktywacyjny jest nieczytelny, użytkownik powinien niezwłocznie złożyć reklamację.

§ 5

1. Bank powiadamia użytkownika o sposobie przekazania loginu podczas zawierania Umowy lub podczas wnioskowania o udostępnienie Systemu bankowości internetowej.

§ 6

1. W celu nadania hasła do Systemu użytkownik zobowiązany jest wypełnić odpowiedni wniosek, znajdujący się na stronie internetowej Banku. Użytkownik może również zostać poproszony o ustalenie hasła do Systemu podczas wnioskowania o udostępnienie Systemu bankowości internetowej.

2. Ze względu na bezpieczeństwo informatyczne Systemu lub bezpieczeństwo zdeponowanych środków, Bank może uzależnić złożenie wniosków od podania przez użytkownika określonych danych osobowych lub informacji dotyczących danej usługi.
3. Jeżeli użytkownik nie wykorzystał jednorazowego kodu aktywacyjnego/ kodu autoryzacyjnego w okresie jego ważności, powinien zwrócić się o jego powtórne nadanie przez Bank.

4. Uwierzytelnianie użytkownika

§ 7

1. Użytkownik loguje się do Systemu bankowości internetowej osobiście, używając wyłącznie własnych danych, które go uwierzytelniają (np. loginu, który nadał mu Bank).
2. Uwierzytelnienie użytkownika jest wymagane zarówno podczas logowania się do Systemu, jak i podczas inicjowania elektronicznej dyspozycji płatniczej. Z zastrzeżeniem ust. 3,4 i 5 uwierzytelnianie użytkownika podczas logowania do Systemu bankowości internetowej obejmuje następujące czynności:
   1) podanie poprawnego loginu,
   2) podanie hasła w formie maskowanej, co oznacza podanie przez użytkownika losowo wskazanych przez System znaków składających się na hasło,
   3) a w przypadku, gdy jest to wymagane prawem lub wynika ze względów bezpieczeństwa dodatkowo także – podanie odpowiedniego kodu autoryzacyjnego lub potwierdzenia w aplikacji mobilnej, gdy użytkownik posiada aplikację mobilną lub użycia klucza zabezpieczeń, gdy użytkownik posiada aktywny klucz na liście kluczy zabezpieczeń

   Jeżeli podczas logowania się użytkownika do Systemu, Bank wymaga podania wszystkich informacji, o których mowa w pkt 1) - 3) nazywa się to silnym uwierzytelnianiem. Bank stosuje silne uwierzytelnianie, gdy jest to wymagane przepisami prawa.
3. Uwierzytelnianie użytkownika podczas logowania do aplikacji mobilnej wymaga wykonania następujących czynności na zaufanym urządzeniu mobilnym:
   1) podania poprawnego loginu - przy pierwszym logowaniu,
   2) podania hasła w formie maskowanej - przy pierwszym logowaniu, a przy kolejnych logowaniach - podania kodu PIN,
   3) w przypadku, gdy aplikacja mobilna zainstalowana jest na urządzeniu mobilnym wyposażonym w czytnik cech biometrycznych, kolejne logowania mogą odbywać się za pomocą:
      a) identyfikatora biometrycznego, o ile użytkownik wybrał taką metodę uwierzytelniania,
      b) a w przypadku, gdy jest to wymagane prawem lub wynika ze względów bezpieczeństwa dodatkowo także może być wymagane podanie odpowiedniego kodu autoryzacyjnego, nie będącego identyfikatorem biometrycznym (np. kodu SMS lub kodu PIN).

4) w przypadku, gdy jest to wymagane prawem lub wynika ze względów bezpieczeństwa dodatkowo także użycia klucza zabezpieczeń, gdy użytkownik posiada aktywny klucz na liście kluczy zabezpieczeń.

Uwierzytelnianie nazywa się silnym uwierzytelnianiem, jeśli, podczas logowania do aplikacji mobilnej, Bank wymaga posiadania zaufanego urządzenia mobilnego, a nadto podania, wszystkich informacji, o których mowa w pkt 1) i 2) albo informacji, o których mowach w pkt 3). W celu przeciwdziałania nieuprawionym logowaniom Bank ma prawo wprowadzić dodatkowe środki lub sposoby uwierzytelniania użytkownika podczas logowania do Systemu. Bank może wprowadzić dodatkowe środki uwierzytelniania, również gdy będzie to wynikało z przepisów prawa.

4. Uwierzytelnienie użytkownika za pomocą klucza zabezpieczeń wymaga od użytkownika:

1) rejestracji klucza zabezpieczeń w systemie bankowości internetowej,

2) aktywacji klucza zabezpieczeń w placówce banku, infolinii banku, lub w systemie bankowości internetowej, o ile bank udostępnia taką możliwość oraz wyrażenia zgody na taką metodę uwierzytelnienia.

5. Z zastrzeżeniem ust. 7, w celu wyboru metody uwierzytelniania za pomocą identyfikatora biometrycznego użytkownik zobowiązany jest najpierw:

1) aktywować lub skonfigurować funkcję czytnika cech biometrycznych na urządzeniu mobilnym zgodnie z zaleceniami producenta urządzenia lub zainstalowanego na nim oprogramowania,
2) wprowadzić do pamięci tego urządzenia jedną, własną cechę biometryczną, która będzie podstawą utworzenia identyfikatora biometrycznego użytkownika,
3) wyrazić zgodę na metodę uwierzytelniania w oparciu o identyfikator biometryczny.

6. Jeśli Bank uzna, że stosowane przez producenta urządzenia mobilnego techniczne lub technologiczne rozwiązanie korzystania z czytnika cech biometrycznych stanowi ryzyko zagrażające bezpieczeństwu informatycznemu Banku lub jego klientów, zastrzega on sobie prawo odmowy uwierzytelniania użytkownika na podstawie identyfikatora biometrycznego. Wówczas uwierzytelnienie użytkownika odbywa się na zasadach opisanych w ust. 3 pkt 1) i pkt 2).

7. W przypadku, gdy użytkownik korzysta z zaufanego urządzenia mobilnego Bank przyjmuje, że każda dyspozycja wydana za pomocą tego urządzenia została wydana przez użytkownika, przy wykonaniu czynności uproszczonego uwierzytelnienia. Wobec powyższego z chwilą dodania urządzenia do listy, użytkownik jest zobowiązany do szczególnej, podwyższonej staranności w przechowywaniu takiego urządzenia i nieudostępnianiu go osobom trzecim. Wykaz rodzajów dyspozycji, które są realizowane przez Bank w oparciu o uwierzytelnienie użytkownika dokonywane przez powiązanie jego osoby z urządzeniem mobilnym, które dodał do listy zawiera Komunikat.

8. Poprawne uwierzytelnienie użytkownika, dokonane zgodnie z ust. 2 i 3, umożliwia użytkownikowi dostęp do informacji o rachunkach lub innych usługach udostępnionych w ramach Systemu i umożliwia składanie dyspozycji w zakresie tych rachunków oraz produktów lub usług.

9. Błędne uwierzytelnienie użytkownika podczas logowania do Systemu, polegające na pięciokrotnym z rzędu wprowadzeniu błędnego hasła, powoduje automatyczne zablokowanie dostępu do Systemu. Licznik prób błędnego logowania jest zerowany po poprawnym zalogowaniu się.

10. Błędne uwierzytelnienie użytkownika podczas logowania do aplikacji mobilnej przez trzykrotne z rzędu wprowadzenie błędnego kodu PIN powoduje jego zablokowanie oraz może powodować zablokowanie dostępu do Systemu. Licznik prób błędnego podania kodu PIN jest zerowany po poprawnym zalogowaniu się. Ponowne nadanie kodu PIN jest możliwe po poprawnym podaniu hasła w formie maskowanej.

11. W przypadku gdy użytkownik podczas logowania do aplikacji mobilnej użył czytnika cech biometrycznych i nie doszło do jego uwierzytelnienia w oparciu o identyfikator biometryczny, zalogowanie do aplikacji mobilnej będzie możliwe po podaniu prawidłowego kodu PIN lub innego kodu autoryzacyjnego.

5. Składanie oświadczeń woli i wiedzy w postaci elektronicznej

§ 8

1. Na podstawie zawartej Umowy użytkownik i Bank mogą przez System bankowości internetowej składać oświadczenia woli lub wiedzy w postaci elektronicznej związane z dokonywaniem:

1) czynności bankowych, lub

2) innych czynności zgodnie z statutem Banku.

Oświadczenia te mogą być składane z tym zastrzeżeniem, iż z uwagi na stały rozwój technologii informatycznej poszczególne funkcjonalności udostępniane za pomocą Systemu bankowości internetowej mogą ulegać zmianie albo też zostać udostępniane w różnych terminach. Informacje dotyczące możliwości złożenia w danym czasie, określonych oświadczeń woli lub wiedzy opisane są w Komunikacie.

2. Za oświadczenia woli w postaci elektronicznej związane z dokonywaniem czynności, o których mowa w ust. 1 pkt 1) i pkt 2) uznaje się takie oświadczenia, które są związane z powstaniem, wykonywaniem, zmianą, wypowiedzeniem, rozwiązaniem lub wygaśnięciem stosunków prawnych dotyczących tych czynności. Oświadczeniem takim jest także udzielenie, zmiana lub odwołanie pełnomocnictwa związanego z dokonywaniem czynności, o których mowa w ust. 1 pkt 1) i pkt 2).

3. O ile złożone w postaci elektronicznej oświadczenia woli spełniają wymogi przepisów prawa przewidziane dla uznania ich za złożone w formie pisemnej, przyjmuje się, że zostały złożone w formie pisemnej, także wtedy, gdy jest ona zastrzeżona pod rygorem nieważności. W przypadku dyspozycji, w tym także wymagających formy pisemnej, podpis może być złożony w postaci elektronicznej, gdy spełnia on wymagania postaci elektronicznej równoważnej formie pisemnej, stosownie do odpowiednich przepisów prawa. Podpis taki w postaci elektronicznej może zostać złożony jako kwalifikowany podpis elektroniczny, zaawansowany podpis elektroniczny lub inny podpis elektroniczny w rozumieniu przepisów prawa powszechnie obowiązującego, w tym:

1) w postaci przesłania drugiej stronie danych identyfikujących użytkownika lub Bank, lub

2) inny sposób dopuszczalny przez przepisy prawa.

4. O ile przepisy prawa pozwalają na uznanie danego sposobu autoryzacji dyspozycji za podpis w postaci elektronicznej, użytkownik może złożyć taki podpis dokonując autoryzacji. W przypadku, gdy Bank składa podpis w postaci elektronicznej poprzez przesłanie drugiej stronie danych identyfikujących, podpis przesłany za pomocą Systemu zawiera dane identyfikujące osobę reprezentującą Bank. Bank i użytkownik w drodze oświadczeń woli złożonych za pomocą Systemu bankowości internetowej mogą, w drodze aneksu do umowy zawartego w postaci elektronicznej, wprowadzić inny sposób składania podpisu w postaci elektronicznej, o ile przepisy prawa będą uznawać, że złożenie podpisu w danej postaci spełnia wymogi formy pisemnej.

5. Bank oraz użytkownik mogą dokonać czynności lub zawrzeć umowy/ aneksy do umów lub złożyć oświadczenie wymagające formy pisemnej w postaci elektronicznej równoważnej formie pisemnej. O ile przepisy prawa będą na to zezwalać Bank oraz użytkownik mogą za pomocą Systemu składać inne oświadczenia wymagające formy pisemnej w postaci elektronicznej równoważnej formie pisemnej.

6. W przypadku, gdy z dostępnej w Systemie informacji, oświadczenia lub dokumentu wynika, że oświadczenie woli lub wiedzy Banku lub użytkownika odnosi się do więcej niż jednej dyspozycji lub więcej niż jednego oświadczenia lub dokumentu, przyjmuje się, że jeden podpis złożony w postaci elektronicznej dotyczy wszystkich przesłanych dyspozycji lub wszystkich oświadczeń lub dokumentów.

7. Bank przesyła użytkownikowi korespondencję, w tym wszelkie oświadczenia woli lub wiedzy, wzory dokumentów, a także zawarte przez użytkownika umowy wraz z regulaminami, oraz innymi dokumentami za pomocą Systemu bankowości internetowej, o ile przepisy prawa powszechnie obowiązującego nie stanowią inaczej. Korespondencja, w tym oświadczenia woli lub wiedzy przesyłane przez Bank mogą być opatrywane kwalifikowaną pieczęcią elektroniczną, zaawansowaną pieczęcią elektroniczną lub inną pieczęcią elektroniczną o jakiej mowa w przepisach prawa powszechnie obowiązującego.

8. Bank może umożliwić użytkownikowi doręczanie Bankowi korespondencji drogą elektroniczną przez System. Ze względu na rozwój technologii informatycznej poszczególne rodzaje oświadczeń (korespondencji) udostępniane za pomocą Systemu mogą ulegać zmianie albo też zostać udostępniane w różnych terminach. Informacje dotyczące możliwości złożenia w danym czasie określonych rodzajów oświadczeń (korespondencji) opisane są w Komunikacie.

9. Bank będzie przesyłał użytkownikowi elektronicznie, w tym za pomocą Systemu, komunikaty potwierdzające fakt zawarcia określonej umowy lub przyjęcie dyspozycji do wykonania.

6. Elektroniczne doręczanie korespondencji

§ 9

1. W ramach Systemu bankowości internetowej Bank udostępnia użytkownikowi:

1) skrzynkę „wiadomości", która służy do kontaktu Banku z użytkownikiem,
2) Elektroniczny system doręczania korespondencji, w którym Bank umieszczać będzie zmiany regulacji umownych, które zgodnie z prawem mają być dostarczone na trwałym nośniku informacji. Użycie w innych regulacjach obowiązujących dla produktów i usług Banku nazwy Elektroniczny system doręczania korespondencji oznacza niniejszą usługę. Użytkownikom w Elektronicznym systemie doręczania korespondencji Bank będzie umieszczać również wyciąg z rachunku, zestawienie transakcji z karty kredytowej oraz inne dokumenty, które zgodnie z prawem mają być dostarczane na trwałym nośniku informacji.

2. Bank nie ponosi odpowiedzialności za skutki niezapoznania się z dokumentami/ wiadomościami/ korespondencją przesłaną za pomocą Systemu bankowości internetowej. Użytkownik jest zobowiązany do zapoznawania się z wiadomościami przesyłanymi mu przez Bank za pomocą Systemu. Powyższe nie narusza prawa Banku do wysłania użytkownikowi korespondencji pocztą na podany przez użytkownika adres lub doręczenia mu korespondencji osobiście w placówce bankowej realizującej tę czynność.

3. Od dnia udostępnienia przez Bank Elektronicznego systemu doręczania korespondencji zmiany regulacji umownych, które zgodnie z prawem muszą być wysłane na trwałym nośniku informacji, Bank będzie doręczał użytkownikom będącym stroną Umowy, w Elektronicznym systemie doręczania korespondencji. Umożliwia on użytkownikowi przechowywanie adresowanych do niego informacji od Banku w sposób umożliwiający dostęp do nich przez okres odpowiedni do celów sporządzenia tych informacji i pozwalający na odtworzenie przechowywanych informacji w niezmienionej postaci. Przestrzeń ta jest integralną częścią Systemu i może występować pod różną nazwą handlową. Dostęp do niej nie wymaga zawarcia odrębnej umowy.

4. Użytkownik będzie miał dostęp do Elektronicznego systemu doręczania korespondencji do czasu rozwiązania Umowy. Przed rozwiązaniem Umowy klient może wydrukować lub zapisać na innym trwałym nośniku informacji dokumenty, które doręczył mu Bank w Elektronicznym systemie doręczania korespondencji.

5. Po rozwiązaniu Umowy Bank zapewni użytkownikowi dostęp do zawartości Elektronicznego systemu doręczania korespondencji przez archiwum dokumentów (dalej: Archiwum), o ile Bank udostępnia taką możliwość, lub przekaże takiemu użytkownikowi zawartość tego systemu na innym trwałym nośniku informacji.

6. Logowanie do Archiwum wymaga podania Bankowi przez użytkownika jego adresu e-mail oraz numeru telefonu do autoryzacji. Dane te są konieczne do zalogowania się przez klienta do Archiwum.

7. Korzystając z Archiwum użytkownik powinien przestrzegać zasad bezpieczeństwa przewidzianych Regulaminem. W przypadku podejrzenia, że osoba nieuprawniona uzyskała dostęp do jego Archiwum, użytkownik jest zobowiązany niezwłocznie zablokować dostęp do swojego Archiwum lub zmienić dane konieczne do korzystania z Archiwum (e-mail, telefon do autoryzacji).

8. Bank ma prawo zablokować dostęp do Archiwum zgodnie z przesłankami do zablokowania Systemu. Użytkownik również może sam zablokować dostęp do Archiwum.

9. Użytkownik może złożyć dyspozycję odblokowania Archiwum lub zmiany danych do logowania do Archiwum wyłącznie w placówce bankowej realizującej tę czynność.

10. Szczegóły związane z korzystaniem przez użytkownika z Archiwum znajdują się w Komunikacie.

7. Składanie dyspozycji, ich autoryzacja i wykonywanie

§ 10

1. Bank wykonuje dyspozycje tylko takiego użytkownika, któremu nadał login.

2. Użytkownik nie może składać za pomocą Systemu dyspozycji związanych z uczestnictwem w grach hazardowych, których przedmiotem byłoby wykonywanie przez Bank usług płatniczych, chyba że gra jest prowadzona zgodnie z ustawą o grach hazardowych. Bank ma prawo odmówić realizacji takich dyspozycji.

3. Złożenie dyspozycji w aplikacji mobilnej będzie możliwe, o ile w chwili jej złożenia urządzenie mobilne jest na liście zaufanych urządzeń mobilnych.

4. Bank ma prawo ustalić limity kwotowe i ilościowe dla transakcji płatniczych realizowanych na podstawie zleceń płatniczych, które są wykonywane za pomocą Systemu bankowości internetowej.

5. W przypadku, gdy jest to wymagane przepisami prawa Bank uzależnia wykonanie dyspozycji, w tym zleceń płatniczych, od silnego uwierzytelniania użytkownika. W przypadku, gdy Bank wymaga, aby silne uwierzytelnianie użytkownika nastąpiło przez aplikację mobilną użytkownik zobowiązany jest podczas wykonywania danej czynności posiadać zaufane urządzenie mobilne.

§ 11

1. Bank wykonuje transakcje płatnicze po ich autoryzacji przez użytkownika. Autoryzacja zlecenia płatniczego przez użytkownika oznacza jego zgodę na wykonanie transakcji płatniczej. Zgody na wykonanie transakcji płatniczej użytkownik może również udzielić za pośrednictwem odbiorcy, dostawcy odbiorcy albo dostawcy świadczącego usługę inicjowania transakcji płatniczej.
2. Autoryzacja dyspozycji, w tym zleceń płatniczych składanych przez użytkownika za pomocą Systemu bankowości internetowej obejmuje:
   1) wybranie przycisku akceptacji – gdy Bank uzna, że dana dyspozycja, ze względu na zasady bezpieczeństwa może zostać w ten sposób autoryzowana, albo
   2) wybranie przycisku akceptacji w aplikacji mobilnej (autoryzacja mobilna) – gdy Bank uzna, że dana dyspozycja powinna zostać autoryzowana w aplikacji mobilnej. Ten sposób autoryzacji wymaga jednocześnie fizycznego posiadania przez użytkownika zaufanego urządzenia mobilnego, na którym jest zainstalowana i aktywowana aplikacja mobilna, lub
   3) podanie poprawnego kodu lub kodów autoryzacyjnych, w tym identyfikatora biometrycznego i wybranie przycisku akceptacji – gdy Bank uzna, że dana dyspozycja płatnicza, ze względu na przepisy prawa lub zasady bezpieczeństwa, wymaga autoryzacji przez podanie kodu lub kodów autoryzacyjnych, lub
   4) podanie poprawnego kodu lub kodów autoryzacyjnych, w tym identyfikatora biometrycznego oraz zbliżenie urządzenia mobilnego do terminalu, lub
   5) użycie klucza zabezpieczeń, gdy użytkownik posiada aktywny klucz na liście kluczy zabezpieczeń oraz gdy Bank uzna, że dana dyspozycja, ze względu na zasady bezpieczeństwa może zostać w ten sposób autoryzowana, lub
   6) użycie karty płatniczej w postaci materialnej, z włączoną funkcją płatności zbliżeniowych, poprzez zbliżenie do urządzenia mobilnego z zainstalowaną aplikacją mobilną oraz włączoną funkcją NFC.
3. Autoryzacja dyspozycji za pomocą identyfikatora biometrycznego wymaga najpierw od użytkownika:
   1) aktywacji lub konfiguracji funkcji czytnika cech biometrycznych na urządzeniu mobilnym zgodnie z zaleceniami producenta urządzenia lub zainstalowanego na nim oprogramowania,
   2) wprowadzenia do pamięci tego urządzenia określonej cechy biometrycznej użytkownika, która będzie podstawą utworzenia jego identyfikatora biometrycznego, oraz wyrażenia zgody na dodatkową metodę uwierzytelniania i metodę autoryzacji dyspozycji za pomocą identyfikatora biometrycznego.
4. Ze względów bezpieczeństwa Bank zastrzega sobie prawo odmowy autoryzacji dyspozycji dokonywanej na podstawie identyfikatora biometrycznego. Powodem tego może być uznanie przez Bank, że stosowane przez producenta urządzenia mobilnego techniczne lub technologiczne rozwiązanie korzystania z czytnika cech biometrycznych stanowi ryzyko zagrażające bezpieczeństwu informatycznemu Banku lub jego klientów. Wówczas autoryzacja dyspozycji odbywa się na zasadach opisanych w ust. 2, z wyłączeniem możliwości wykorzystania w tym celu identyfikatora biometrycznego.
5. Każda dyspozycja składana przez użytkownika, która ma zostać wykonana przez System, a która powodować będzie zmianę w stanie środków pieniężnych na rachunkach, lub będzie wnioskiem o zawarcie przez Bank nowej umowy lub wykonanie usługi, lub będzie z takim wnioskiem związana, wymaga autoryzacji przez użytkownika zgodnie z ust. 2.
6. Autoryzacja dyspozycji za pomocą klucza zabezpieczeń wymaga od użytkownika:
   1) rejestracji klucza zabezpieczeń w systemie bankowości internetowej,
   2) aktywacji klucza zabezpieczeń w placówce bankowej, infolinii banku, lub w systemie bankowości internetowej, gdy bank udostępnia taką możliwość oraz wyrażenia zgody na taką metodę autoryzacji dyspozycji.
7. Stosując zasady bezpieczeństwa Bank weryfikuje fakt autoryzacji użytkownika podczas składania dyspozycji przez:

1) sprawdzenie poprawności danych podanych przez użytkownika podczas logowania do Systemu, o których mowa w § 7 ust. 2 i 3,

2) sprawdzenie czy użytkownik wybrał przycisk akceptacji dyspozycji, która została uznana przez Bank, jako niewymagająca autoryzacji przez podanie kodu autoryzacyjnego,

3) weryfikację poprawności kodu lub kodów autoryzacyjnych udostępnionych przez Bank i podanych przez użytkownika, w tym identyfikatora biometrycznego lub weryfikację użycia klucza zabezpieczeń, gdy użytkownik posiada aktywny klucz na liście kluczy zabezpieczeń.

Jeśli wynik weryfikacji, o której mowa powyżej jest negatywny, Bank uznaje, że dyspozycja nie jest autoryzowana przez użytkownika i odmawia jej wykonania.

8. Bank dostarcza użytkownikowi kody autoryzacyjne, które są kodami SMS, w wiadomości SMS na wskazany wcześniej przez użytkownika telefon do autoryzacji.

9. Czas ważności przekazanego przez Bank kodu autoryzacyjnego może zostać ograniczony ze względów bezpieczeństwa Systemu. Standardowy czas ważności jest ograniczony do czasu trwania sesji tj. czasu połączenia użytkownika z Bankiem przez System. Kod autoryzacyjny jest generowany do złożonej dyspozycji i może posłużyć do autoryzacji wyłącznie tej dyspozycji. Wraz z kodem autoryzacyjnym użytkownik otrzymuje informacje o szczegółach dyspozycji.

10. W przypadku pięciokrotnego podania błędnego kodu autoryzacyjnego, który przekazał Bank do zatwierdzenia danej dyspozycji, dostęp do Systemu bankowości internetowej zostaje zablokowany. W przypadku trzykrotnego podania błędnego kodu PIN w celu zatwierdzenia dyspozycji w aplikacji mobilnej, Bank może zablokować dostęp do Systemu bankowości internetowej.

11. Dyspozycję odblokowania dostępu do Systemu można złożyć w placówce bankowej realizującej tę czynność, przez stronę internetową Banku lub w Systemie, o ile Bank dopuszcza taką funkcjonalność. W każdym przypadku do odblokowania konieczne jest ponowne ustalenie hasła lub kodu PIN do aplikacji mobilnej przez użytkownika.

12. Mając na uwadze względy bezpieczeństwa, Bank zastrzega sobie, w stosunku do każdej dyspozycji, prawo żądania jej dodatkowej autoryzacji, np. za pomocą kodów autoryzacyjnych, kluczy zabezpieczeń, gdy użytkownik posiada aktywny klucz na liście kluczy zabezpieczeń.

§ 12

1. Dyspozycja złożona przez użytkownika w Systemie bankowości internetowej jest nieodwołalnym i ostatecznym wyrażeniem woli użytkownika, z zastrzeżeniem ust. 5.

2. Dyspozycje składane przez System mogą dotyczyć wyłącznie rachunków oraz produktów lub usług bankowych, którymi dany użytkownik dysponuje za pomocą tego Systemu.

3. Informacja w sprawie trybu realizacji poszczególnych dyspozycji złożonych za pomocą Systemu bankowości internetowej dostępna jest w załączniku 1 oraz na stronie internetowej Banku, w części dotyczącej Systemu.

4. Za moment otrzymania przez Bank zlecenia płatniczego złożonego przez System bankowości internetowej

1) w dniu roboczym lub w sobotę do godziny granicznej określonej w załączniku 1, z zastrzeżeniem pkt 3), uznaje się moment dokonania autoryzacji zlecenia płatniczego, o której mowa w § 11 ust. 2,

2) w dniu roboczym lub w sobotę po godzinie granicznej określonej w załączniku 1 lub w dniu ustawowo wolnym od pracy, z zastrzeżeniem pkt 3), uznaje się pierwszy dzień roboczy następujący po dniu złożenia zlecenia płatniczego, z zastrzeżeniem zleceń płatniczych wskazanych w załączniku 1, dla których brak jest godzin granicznych przyjmowania zleceń płatniczych, w przypadku których za moment otrzymania zlecenia płatniczego uznaje moment określony w pkt 1),

3) z odroczoną datą płatności (przelew, którego wykonanie rozpoczyna się w innym dniu niż dzień złożenia zlecenia płatniczego):

a) uznaje się dzień wskazany przez użytkownika do obciążenia rachunku,

b) jeżeli wskazany przez użytkownika dzień do obciążenia rachunku nie jest dniem roboczym (z wyjątkiem soboty) uznaje się, że zlecenie płatnicze zostało otrzymane w pierwszym dniu roboczym następującym po dniu wskazanym przez użytkownika do obciążenia jego rachunku, z zastrzeżeniem zleceń określonych w pkt c),

c) jeżeli wskazany przez użytkownika dzień do obciążenia rachunku nie jest dniem roboczym (z wyjątkiem soboty) to w przypadku zleceń płatniczych określonych w załączniku 1 , dla których brak jest godzin granicznych przyjmowania zleceń płatniczych, za moment otrzymania tych zleceń płatniczych przez Bank, uznaje się dzień wskazany przez użytkownika do obciążenia jego rachunku,

d) jeżeli wskazany przez użytkownika dzień do obciążenia rachunku przypada w sobotę uznaje się, że zlecenie płatnicze zostało otrzymane w tym dniu, z zastrzeżeniem zleceń określonych w pkt e),

e) jeżeli wskazany przez użytkownika dzień do obciążenia rachunku przypada w sobotę, to w przypadku zleceń płatniczych określonych w załączniku 1 , dla których występują godziny graniczne przyjmowania zleceń płatniczych, za moment otrzymania tych zleceń płatniczych przez Bank, uznaje się pierwszy dzień roboczy następujący po dniu wskazanym przez użytkownika do obciążenia jego rachunku.

5. Z zastrzeżeniem ust. 6 użytkownik nie może odwołać zlecenia płatniczego od momentu jego otrzymania przez Bank, chyba że inne regulaminy lub odrębnie zawarte umowy stanowią inaczej.

6. W przypadku zlecenia płatniczego wychodzącego wskazanego w załączniku 1 , użytkownik może je odwołać do dnia i godziny określonych w załączniku 1 .

7. W przypadku gdy transakcja płatnicza jest inicjowana przez dostawcę świadczącego usługę inicjowania transakcji płatniczej lub przez odbiorcę lub za jego pośrednictwem, za wyjątkiem zlecenia płatniczego z odroczoną datą płatności określonego w ust. 4 pkt 3), płatnik nie może odwołać zlecenia płatniczego po udzieleniu dostawcy świadczącemu usługę inicjowania transakcji płatniczej zgody na zainicjowanie transakcji płatniczej albo po udzieleniu odbiorcy zgody na wykonanie transakcji płatniczej.

§ 13

1. Bank realizuje dyspozycje, w tym zlecenia płatnicze składane przez System bankowości internetowej na zasadach przewidzianych Regulaminem, a w sprawach nieuregulowanych w nim, na zasadach przewidzianych odrębnymi i wiążącymi użytkownika regulacjami dotyczącymi właściwych rachunków, lub innych usług, których dana dyspozycja dotyczy.

2. W przypadku rozwiązania Umowy, złożone wcześniej przez System zlecenie płatnicze z odroczoną datą płatności zostanie wykonane zgodnie ze złożoną przez użytkownika dyspozycją.

3. Z zastrzeżeniem ust. 5, Bank odmawia wykonania dyspozycji, w tym zlecenia płatniczego z przyczyn wskazanych w umowie lub regulaminie, który wiąże użytkownika i dotyczy właściwego rachunku, a nadto dyspozycji, która jest:

1) niekompletna lub niepoprawna z powodu podania błędnego unikatowego identyfikatora lub innych błędnych informacji, które są niezbędne do wykonania danej dyspozycji,

2) sprzeczna z inną złożoną już dyspozycją,

3) nie może zostać zrealizowana z powodu niewystarczających środków na rachunku właściwym dla jej wykonania,

4) nieautoryzowana w sposób opisany w Regulaminie,

5) z innych przyczyn wyraźnie przewidzianych Regulaminem, Umową lub powszechnie obowiązującymi przepisami prawa.

Powyższe dotyczy wszystkich zleceń płatniczych, w tym zainicjowanych przez odbiorcę lub za pośrednictwem odbiorcy.

4. Użytkownik niezwłocznie otrzyma powiadomienie o odmowie wykonania dyspozycji przez System. Jeżeli będzie to możliwe, otrzyma on również informację o przyczynach odmowy lub procedurze sprostowania błędów, które spowodowały odmowę, chyba że powiadomienie takie jest niedopuszczalne z mocy odrębnych przepisów.

5. W przypadku braku aktualizacji w Banku dokumentu tożsamości przez osobę składającą zlecenie w Systemie bankowości internetowej Bank ma prawo odmówić wykonania zlecenia płatniczego.

6. Bank wykonuje transakcje płatnicze na tych samych zasadach bez względu na to czy zlecenie płatnicze zostało złożone przez użytkownika bezpośrednio w Banku, czy zostało zainicjowane przez dostawcę świadczącego usługę inicjowania transakcji płatniczej, chyba że postanowienia Regulaminu stanowią inaczej.

§ 14

Informacje wymagane na podstawie ustaw udostępniane są okresowo, co najmniej raz w miesiącu, bezpłatnie w Systemie - chyba, że inaczej przewidziano w odrębnie wiążącej użytkownika regulacji lub Regulaminie.

§ 15

1. W przypadku, gdy użytkownik składa dyspozycję będącą zleceniem płatniczym w placówce bankowej realizującej tę czynność lub przez infolinię może, o ile Bank udostępnia taką możliwość, autoryzować taką dyspozycję, podając w tej placówce lub przez infolinię kod autoryzacyjny otrzymany za pomocą wiadomości SMS wysłanej przez Bank na jego numer telefonu do autoryzacji.
2. W przypadku, gdy użytkownik składa dyspozycję niebędącą zleceniem płatniczym w placówce bankowej realizującej tę czynność lub przez infolinię, może, o ile Bank udostępnia taką możliwość, złożyć taką dyspozycję, z zastrzeżeniem dyspozycji, dla których Regulamin przewiduje złożenie wyłącznie w formie pisemnej lub poprzez System bankowości internetowej, podając w tej placówce lub przez infolinię kod autoryzacyjny otrzymany za pomocą wiadomości SMS wysłanej przez Bank na jego numer telefonu do autoryzacji. Wykaz dyspozycji określa Komunikat.
3. W przypadku, gdy Bank udostępnia taką możliwość, użytkownik może złożyć dyspozycję będącą zleceniem płatniczym lub dyspozycję niebędącą zleceniem płatniczym oraz dokonać ich autoryzacji składając w placówce bankowej realizującej tę czynność podpis na urządzeniu elektronicznym, zgodnie z art. 7 ust. 1 Prawa bankowego, po uprzednim podaniu Bankowi swoich danych identyfikacyjnych oraz potwierdzeniu przez pracownika Banku tożsamości składającego oświadczenie. Dokumenty, na podstawie których Bank potwierdza tożsamość określone są w Komunikacie dla posiadaczy rachunków określonych w Regulaminie świadczenia przez ING Bank Śląski S.A. usług w ramach prowadzenia Konta dla Uchodźców. Urządzenie elektroniczne zapewnia utrwalenie i integralność treści oświadczenia, złożonego podpisu oraz daty i czasu złożenia oświadczenia. W przypadku, gdy oświadczenie woli klienta związane jest z powstaniem, wykonywaniem, zmianą, wypowiedzeniem, rozwiązaniem lub wygaśnięciem stosunków prawnych łączących go z Bankiem i wymaga złożenia oświadczenia woli przez Bank, Bank składa podpis w postaci elektronicznej poprzez umieszczenie w jego treści danych identyfikujących swojego reprezentanta tj. imienia i nazwiska oraz numeru identyfikacyjnego pracownika.

8. Usługi wspierające zarządzanie finansami

§ 16

1. W ramach Systemu Bank świadczy usługi wspierające zarządzanie finansami (dalej: zarządzanie finansami). Usługi te mają charakter usług konsultacyjno-doradczych i są związane w szczególności z płatnościami.
2. Bank, w celu świadczenia tych usług, udostępnia funkcjonalności Systemu, które dostosowane są do indywidualnych potrzeb użytkownika. Aby Bank mógł wykonywać zarządzanie finansami niezbędne jest kategoryzowanie informacji finansowych oraz profilowanie danych osobowych dotyczących użytkownika w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. – ogólne rozporządzenie o ochronie danych. Profilowanie może następować tylko w zakresie koniecznym do wykonania zarządzania finansami. Bank wykonując zarządzanie finansami nie podejmuje decyzji w sprawach finansowych za użytkownika.
3. Zarządzanie finansami nie obejmuje usług doradztwa, zarządzania portfelami, sporządzania analiz inwestycyjnych, finansowych oraz innych rekomendacji w rozumieniu art. 69 ust. 2 oraz ust. 4 ustawy o obrocie instrumentami finansowymi, które mogą być świadczone przez Bank na podstawie innych umów/ regulacji, nawet gdy są one świadczone zdalnie przez System.
4. Zarządzanie finansami jest wykonywane w postaci:

   1) informacji lub powiadomień o:

   a) terminologii finansowej oraz wiedzy z tych dziedzin,

   b) przyszłych płatnościach, w tym realizowanych okresowo przez użytkownika oraz przyszłych zdarzeniach lub terminach,

   c) możliwych do złożenia przez użytkownika przyszłych płatnościach, w tym realizowanych okresowo,

2) prezentacji sytuacji finansowej użytkownika przez wskazywanie:

a) rodzaju transakcji przez niego wykonywanych lub przynależności transakcji do określonej grupy lub typu transakcji,

b) rodzaju lub kategorii wpływów, wydatków lub kontrahentów biznesowych.

5. Informacje, prezentacje i konsultacje, o których mowa w ust. 4 mogą mieć różne formy graficzne lub tekstowe.

6. Zarządzanie finansami będzie wykonywane zgodnie z następującymi zasadami:

1) informacje o terminologii przekazywane są w Systemie na bieżąco, natomiast powiadomienia o przyszłych transakcjach/ zdarzeniach lub terminach nie później niż 48 godzin przed wskazaną w Systemie transakcją/ zdarzeniem lub terminem,

2) prezentacje sytuacji finansowej przygotowane są w ujęciu miesięcznym lub rocznym na podstawie dokonanych lub przewidywanych płatności. Prezentacje te mogą także uwzględniać informacje podane przez użytkownika w Systemie lub inne podmioty działające z upoważnienia użytkownika. System może umożliwić inne ustawienie okresu danej prezentacji.

7. Zarządzanie finansami jest integralną częścią Systemu, z tym, że w ramach tych usług poszczególne ich funkcjonalności mogą wymagać samodzielnego uruchomienia przez użytkownika.

§ 17

1. Za należyte wykonywanie zarządzania finansami Bank ponosi odpowiedzialność za udowodnione straty użytkownika, z zastrzeżeniem ust. 2.

2. Bank nie odpowiada za ustalony przez użytkownika cel, przedsięwzięcie lub limit wydatków, ani za ich realizację czy poziom wykonania.

3. Bank nie ponosi odpowiedzialności za podejmowane przez użytkownika decyzje związane z zarządzaniem finansami, w tym za decyzje dotyczące nabycia poszczególnych usług lub dotyczące lokowania środków. Wyłączenie odpowiedzialności nie obejmuje sytuacji naruszenia przez Bank obowiązku działania z należytą starannością ani nie narusza bezwzględnie wiążących przepisów prawa.

4. Bank przygotowuje konsultacje według swojej najlepszej woli i wiedzy i z dochowaniem należytej staranności, w oparciu o znany Bankowi stan faktyczny istniejący w chwili jej udzielania, w szczególności o informacje podane przez użytkownika. Bank nie weryfikuje czy informacje podane przez użytkownika są prawdziwe. W celu otrzymania wiarygodnej konsultacji użytkownika zobowiązany jest podawać prawdziwe informacje, w szczególności dotyczące sytuacji finansowej.

5. W przypadku, gdy w ramach zarządzania finansami dana funkcjonalność jest uruchamiana przez użytkownika samodzielnie, Bank - niezależnie od obowiązków informacyjnych wynikających z przepisów prawa - może przekazać dodatkową informację o ryzykach związanych z usługami. Użytkownik jest zobowiązany zapoznać się z taką informacją i rozsądnie podejmować decyzje dotyczące lokowania środków.

6. Z uwagi na stały rozwój technologii informatycznej, poszczególne funkcjonalności udostępniane w ramach zarządzania finansami mogą ulegać zmianie lub mogą być uruchamiane w Systemie w różnych terminach. Informacje dotyczące ich dostępności znajdują się w Komunikacie. Funkcjonalności te mogą mieć różne oznaczenia i nazwy.

7. Zarządzanie finansami jest świadczone do chwili wygaśnięcia lub rozwiązania Umowy. Po tej chwili użytkownik nie ma dostępu do przygotowanych przez Bank rezultatów świadczenia usług wspierających zarządzanie finansami, w szczególności informacji, prezentacji, konsultacji oraz celów lub przedsięwzięć finansowych, które użytkownik ustalił. Przed dniem wygaśnięcia lub rozwiązania Umowy użytkownik może wydrukować rezultaty konsultacji finansowej lub zapisać je i przechowywać na nośniku elektronicznym - o ile System umożliwia przygotowanie konsultacji w formie pliku tekstowego.

9. Elektroniczny sejf w systemie bankowości internetowej

§ 18

1. Elektroniczny sejf (dalej: sejf) to usługa, która polega na przechowywaniu, zapisanych przez użytkownika, elektronicznych dokumentów (nazywanych także: plikami), w specjalnie wydzielonej przestrzeni Systemu

bankowości internetowej. Przestrzeń ta jest integralną częścią Systemu i może występować pod różną nazwą handlową.

2. Bank udostępnia usługę sejfu użytkownikom, którzy zawarli Umowę. Korzystanie z tej usługi nie wymaga zawarcia odrębnej umowy. W przestrzeni sejfu użytkownik może zapisać pliki, pobrać albo usunąć uprzednio zapisane przez niego pliki. Użytkownik nie ma możliwości edycji zapisanych plików ani zmiany ich formatów.
3. Katalog formatów plików, które można zapisywać w Systemie podany jest w Komunikacie.
4. Użytkownik uzyskuje dostęp do sejfu z chwilą zalogowania się do Systemu. Użytkownik może korzystać z sejfu wówczas, gdy jest zalogowany do Systemu.
5. Sejf jest powiązany z loginem użytkownika. Jeśli użytkownik posiada kilka loginów, usługa dostępna jest osobno dla każdego loginu. Nie ma możliwości korzystania z jednego, tego samego sejfu w ramach kilku loginów.
6. Informacja o dostępnej pojemności sejfu jest podana w Systemie.
7. Użytkownik jest odpowiedzialny za treść zapisanych plików oraz ich format. Użytkownik może zapisywać w sejfie jedynie takie pliki do których posiada stosowne uprawnienia, które nie naruszają przepisów powszechnie obowiązującego prawa, zostały utworzone lub pozyskane zgodnie z prawem i nie naruszają praw osób trzecich, w tym dóbr osobistych, praw autorskich, praw własności przemysłowej, ani tajemnic handlowych tych osób. Użytkownik może zapisywać tylko takie pliki, które nie zawierają jakichkolwiek wirusów elektronicznych ani jakichkolwiek części niebezpiecznego oprogramowania.
8. Bank ma prawo odmówić użytkownikowi zapisania w sejfie dokumentu, który nie spełnia wymogów technicznych, zagrażałby bezpieczeństwu Banku, systemów elektronicznych Banku lub innych użytkowników, lub środków gromadzonych w Banku. Z chwilą powzięcia wiadomości o naruszeniu postanowień § 27 ust. 7 Bank odmówi użytkownikowi umieszczenia plików. W przypadku, gdyby naruszenie bezpieczeństwa lub naruszenie obowiązków wskazanych w ust. 7 mogło doprowadzić do poważnej straty dla Banku lub innych użytkowników, Bank ma prawo wdrożyć działanie odpowiedniego oprogramowania zabezpieczającego, a w przypadkach nagłego ryzyka odizolować, a gdyby to było niemożliwe - skasować przechowywane pliki.
9. Bank nie ma dostępu do plików i dokumentów umieszczonych przez użytkownika w sejfie, nie sprawdza i nie weryfikuje danych i treści w nich zawartych. Bank ponosi odpowiedzialność przewidzianą Regulaminem od chwili zapisania danego pliku w sejfie.
10. Przechowując pliki, zapisane przez użytkownika, przy dochowaniu należytej staranności Bank nie ponosi odpowiedzialności za:
    1) treści i dane zawarte w plikach i dokumentach umieszczonych w Systemie,
    2) zmianę nazwy pliku, którą dokonał użytkownik,
    3) pliki pobrane z sejfu z chwilą złożenia dyspozycji,
    4) konsekwencje spowodowane naruszeniem przez użytkownika praw opisanych w ust. 7 lub ust. 8,
    5) pozostawienie w sejfie pliku z chwilą wygaśnięcia lub rozwiązania umowy o System,
    6) straty i koszty poniesione w wyniku jakichkolwiek uszkodzeń pliku, całkowitego jego uszkodzenia lub przechwycenia pliku w czasie transferu do Systemu, chyba, że wynikły one z funkcjonowania systemu informatycznego Banku,
    7) nie wykrycie przez Bank, w momencie zapisywania pliku w Systemie, czy ma jakiekolwiek elementy zawirusowane,
    8) opóźnienia w wykonaniu lub niewykonaniu dyspozycji użytkownika w ramach sejfu, gdy było to spowodowane siłą wyższą.
11. Organom uprawnionym na mocy przepisów prawa Bank udostępni zawartość sejfu bez analizy znajdujących się w nim plików, w trybie przewidzianym właściwymi przepisami prawa bankowego.
12. Bank nie ponosi odpowiedzialności za szkodę wynikającą z ujawnienia zawartości sejfu osobom lub instytucjom upoważnionym do żądania od Banku udzielania tych informacji.
13. Użytkownik traci dostęp do sejfu i zapisanych w nim plików/ dokumentów, z chwilą wygaśnięcia lub rozwiązania Umowy. W momencie zamknięcia Systemu, pliki/ dokumenty przechowywane w sejfie są automatycznie i trwale usuwane przez Bank. Bank nie przechowuje kopii tych plików/ dokumentów. Przed wypowiedzeniem / rozwiązaniem Umowy Bank powiadomi użytkownika o konieczności pobrania zapisanych plików. Powiadomienie

może nastąpić w dowolny sposób także za pomocą komunikatu, który zostanie wyświetlony użytkownikowi w Systemie.

14. Ze względów technicznych, rozwoju technologii oraz oprogramowania stosowanego w obsłudze sejfu lub ze względów bezpieczeństwa, Bank ma prawo ograniczyć możliwość korzystania z zapisywania określonych formatów plików w przestrzeni sejfu lub ograniczyć funkcjonalności sejfu. W takim przypadku, przed dokonaniem określonej czynności, użytkownik otrzyma w Systemie stosowną informację.

10. Korzystanie z usług płatniczych świadczonych przez uprawnione podmioty trzecie

§ 19

1. Użytkownik może, w zakresie posiadanych uprawnień, korzystać z usług płatniczych podmiotów trzecich takich, które świadczą usługę dostępu do informacji o rachunku lub usługę inicjowania transakcji płatniczej:

1) usługa dostępu do informacji o rachunku - wykonywana przez dostawcę świadczącego usługę dostępu do informacji o rachunku, polega na przesłaniu przez Bank - na żądanie tego dostawcy - informacji o rachunku prowadzonym w Banku,

2) usługa inicjowania transakcji płatniczej – wykonywana przez dostawcę świadczącego usługę inicjowania transakcji płatniczej, polega na zainicjowaniu przez tego dostawcę, działającego na wniosek użytkownika, zlecenia płatniczego z rachunku płatniczego prowadzonego w Banku, do którego użytkownik jest uprawniony.

2. Korzystanie z usługi dostępu do informacji o rachunku jest możliwe pod warunkiem, że prowadzony przez Bank rachunek jest rachunkiem płatniczym dostępnym on-line i użytkownik zostanie uwierzytelniony przez Bank, zgodnie z wymogami prawa i postanowieniami Regulaminu.

3. Korzystanie z usługi inicjowania transakcji płatniczej jest możliwe pod warunkiem, że zgodnie z wiążącą użytkownika regulacją jest to elektroniczna transakcja bezgotówkowa dotycząca rachunku płatniczego dostępnego on-line, jej inicjowanie następuje wyłącznie wskutek dyspozycji użytkownika, a nadto użytkownik zostanie uwierzytelniony przez Bank, zgodnie z wymogami prawa i postanowieniami Regulaminu.

4. Dostawcy świadczącemu usługę dostępu do informacji o rachunku Bank udostępnia informacje o wyznaczonych rachunkach i związanych z nimi transakcjach, w tym historii tych rachunków - z tym, że okres za który Bank dostarcza historię rachunków może być ograniczony ze względów technologicznych.

5. Bank nie odpowiada za należyte wykonywanie usług, o których mowa w ust. 1, przez uprawnione podmioty trzecie.

6. Użytkownik może w Systemie wyrazić zgodę na udzielanie przez Bank odpowiedzi na wnioski dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej, że kwota odpowiadająca określonej transakcji płatniczej realizowanej w oparciu o tę kartę jest dostępna na rachunku płatniczym.

7. Rachunek płatniczy jest dostępny on-line, gdy spełnione są łącznie następujące warunki:

1) użytkownik jest stroną Umowy,

2) użytkownik ma aktywny dostęp do Systemu bankowości internetowej,

3) dany rachunek płatniczy jest dostępny przez System w chwili otrzymania przez Bank stosownego wniosku lub żądania właściwego dostawcy, w sprawie wykonania czynności w celu realizacji usługi wskazanej w ust. 1.

8. Rachunek płatniczy nie jest dostępny on–line, gdy w chwili otrzymania przez Bank stosownego wniosku lub żądania wykonania czynności:

1) użytkownik nie ma aktywnego Systemu bankowości internetowej, lub

2) gdy dostęp do Systemu jest zablokowany, lub

3) gdy użytkownik skorzystał z funkcji ukrycia danego rachunku w Systemie i nie cofnął tej dyspozycji.

9. Bank może odmówić dostawcy świadczącemu usługę dostępu do informacji o rachunku lub dostawcy świadczącemu usługę inicjowania transakcji płatniczej - dostępu do danego rachunku płatniczego z obiektywnie uzasadnionych i należycie udokumentowanych przyczyn związanych z nieuprawnionym lub nielegalnym

dostępem do rachunku płatniczego przez takiego dostawcę, w tym nieuprawnionym zainicjowaniem transakcji płatniczej. W takim przypadku Bank poinformuje użytkownika przez System o odmowie dostępu do rachunku płatniczego i jej przyczynach. Informacja ta, o ile jest to możliwe, jest przekazywana użytkownikowi przed odmową dostępu, a najpóźniej bezzwłocznie po takiej odmowie, nie później jednak niż w dniu roboczym następującym po dniu takiej odmowy, chyba że jej przekazanie nie byłoby wskazane z obiektywnie uzasadnionych względów bezpieczeństwa lub jest sprzeczne z odrębnymi przepisami.

11. Odpowiedzialność banku

§ 20

1. Bank zobowiązuje się do:

1) zachowania poufności wszystkich danych służących do uwierzytelniania i autoryzacji, którymi posługuje się użytkownik,

2) zapewnienia użytkownikowi dostępu za pomocą Systemu bankowości internetowej do bieżących informacji o rachunkach, do których jest uprawniony, w sposób umożliwiający stałe monitorowanie transakcji dokonywanych na tych rachunkach.

2. Bank odpowiada za udowodnione straty użytkownika, spowodowane przez niezrealizowanie dyspozycji lub jej nieprawidłowe lub nieterminowe realizowanie, chyba że są następstwem okoliczności, za które Bank nie ponosi odpowiedzialności.

3. Bank ponosi odpowiedzialność za ewentualne skutki wykonania transakcji przez osoby trzecie, po dokonaniu zgłoszenia, o jakim mowa w § 22a ust. 4 i 5 pkt 1) i złożeniu przez użytkownika dyspozycji blokady dostępu do Systemu, począwszy od:

1) wpłynięcia dyspozycji do Banku - w przypadku, gdy dyspozycję złożono przez System,

2) pisemnego potwierdzenia przez Bank faktu złożenia takiej dyspozycji - w przypadku, gdy dyspozycję złożono w placówce bankowej realizującej tę czynność,

3) uzyskania przez użytkownika ustnego potwierdzenia ze strony infolinii blokady dostępu do Systemu – w przypadku, gdy dyspozycję złożono przez infolinię,

- chyba że użytkownik doprowadził umyślnie do nieautoryzowanej transakcji.

4. Bank ponosi odpowiedzialność za ochronę poufności danych użytkownika służących do uwierzytelniania i autoryzacji za pomocą Systemu bankowości internetowej tylko wówczas, gdy użytkownik posługuje się tymi danymi zgodnie z zasadami określonymi w Regulaminie chyba, że poufność została naruszona z winy Banku.

5. Bank nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy, w przypadku, gdy powodem niewykonania lub nienależytego wykonania Umowy, w tym transakcji, jest siła wyższa.

6. Bank nie ponosi odpowiedzialności za niewykonanie Umowy, w przypadku, gdy odmowa wykonania zobowiązań wynikających z Umowy, następuje na podstawie przepisów powszechnie obowiązującego prawa, upoważniających lub zobowiązujących Bank do odmowy wykonania takich zobowiązań lub dyspozycji.

7. Bank nie ponosi odpowiedzialności za:

1) niezrealizowane dyspozycje - w przypadku nieprawidłowych lub niepełnych informacji dotyczących unikatowego identyfikatora, albo niepodania przez płatnika lub odbiorcę informacji niezbędnych dla wykonania danej dyspozycji lub transakcji, w zakresie w jakim niezrealizowanie dyspozycji wynika z niepodania informacji niezbędnych do jej wykonania,

2) skutki wynikłe z funkcjonowania urządzeń telekomunikacyjnych użytkownika w związku z otrzymywaniem wiadomości SMS, o ile opóźnienie w otrzymaniu wiadomości nie nastąpiło z winy Banku,

3) szkody użytkownika powstałe wskutek nieprzestrzegania przez użytkownika zasad bezpieczeństwa Systemu bankowości internetowej.

8. W stosunku do użytkowników będących stroną umowy o rachunek płatniczy w rozumieniu ustawy, Bank ponosi odpowiedzialność za niewykonanie lub nienależyte wykonanie prawidłowo zleconej transakcji, chyba że udowodni, że rachunek odbiorcy został uznany w terminie wymaganym przepisami prawa lub gdy:

1) roszczenia użytkownika wygasły wskutek braku zgłoszenia w wymaganym w Regulaminie 13 miesięcznym terminie o nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach, lub

2) niewykonanie lub nienależycie wykonanie transakcji było skutkiem siły wyższej lub wynikało z przepisów prawa.

9. Jeśli zgodnie z Regulaminem Bank ponosi odpowiedzialność wobec płatnika lub odbiorcy będącego użytkownikiem- zobowiązuje się zwrócić mu kwotę niewykonanej lub nienależycie wykonanej transakcji, a gdy taki użytkownik jest posiadaczem rachunku płatniczego w rozumieniu ustawy - przywrócić rachunek do stanu, jaki istniałby, gdyby nie miało miejsce nienależyte wykonanie lub niewykonanie transakcji. Powyższe dotyczy także opłat lub odsetek, którymi użytkownik został obciążony w razie niewykonania lub nienależytego, w tym opóźnionego, wykonania transakcji płatniczej.

10. W przypadku niewykonanej lub nienależycie wykonanej transakcji płatniczej zainicjowanej przez płatnika lub przez odbiorcę lub za jego pośrednictwem, Bank na wniosek płatnika lub odbiorcy podejmuje niezwłocznie działania w celu bezpłatnego prześledzenia transakcji płatniczej i - o ile przepisy prawa na to zezwalają - powiadamia płatnika o ich wyniku.

11. W sprawach nieuregulowanych w Regulaminie, a dotyczących odpowiedzialności Banku z tytułu wykonywania zleceń płatniczych, w tym transakcji płatniczych inicjowanych za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej oraz żądań zwrotu kwot nieautoryzowanych transakcji, w stosunku do posiadaczy rachunków oszczędnościowo – rozliczeniowych oraz rachunków oszczędnościowych stosuje się postanowienia Regulaminu świadczenia przez ING Bank Śląski S.A. usług w ramach prowadzenia Konta dla Uchodźców.

12. Bank w świadczeniu usługi Systemu bankowości internetowej zgodnie z niniejszym Regulaminem, zachowuje należytą staranność w rozumieniu Kodeksu cywilnego.

13. Bank nie ponosi odpowiedzialności za bezpieczeństwo i działanie zaufanego urządzenia mobilnego, w tym wszystkich jego funkcji.

§ 21

Wszystkie dyspozycje złożone przez użytkownika w Systemie bankowości internetowej są zabezpieczone w sposób trwały przez Bank i stanowią dowody w przypadku sytuacji spornych.

12. Odpowiedzialność użytkownika

§ 22

1. Bank w świadczeniu usługi Systemu bankowości internetowej zgodnie z niniejszym Regulaminem, zachowuje należytą staranność w rozumieniu Kodeksu cywilnego.

2. Bank nie ponosi odpowiedzialności za bezpieczeństwo i działanie zaufanego urządzenia mobilnego, w tym wszystkich jego funkcji.

§ 22a

1. Użytkownik zobowiązuje się nie podejmować działań, które spowodowałyby otrzymanie dostępu do Systemu przez osoby trzecie, nawet jeśli jest to osoba będąca innym użytkownikiem.

2. Użytkownik jest zobowiązany przestrzegać następujących zasad korzystania z Systemu:

1) zachować w poufności wszystkie dane i informacje służące do:

a) uwierzytelnienia i autoryzacji wszelkich dyspozycji (płatniczych albo nie płatniczych) (np. login, kody, hasło, PIN), które służą do korzystania z Systemu lub jego części,

b) korzystania z Systemu, z aplikacji Moje ING lub z ich funkcji lub funkcjonalności.

Tych danych i informacji nie wolno użytkownikowi ujawniać osobie trzeciej, nawet jeśli ta osoba jest inną uprawnioną do korzystania z usług za pomocą Systemu,

2) zapamiętać hasło lub inne dane służące do uwierzytelniania i autoryzacji, a w przypadku niemożności ich zapamiętania, przechowywać to hasło i dane w wybrany przez siebie bezpieczny sposób i w bezpiecznym miejscu, które nie jest dostępne dla osób trzecich. Użytkownik zobowiązany jest w taki sam sposób przechowywać urządzenia służące do logowania, uwierzytelniania lub autoryzacji (np. klucz U2F). Niedopuszczalne jest przechowywanie w jednym miejscu razem hasła oraz danych, które umożliwiają uwierzytelnienie lub autoryzację (np. przechowywanie hasła wraz z innymi danymi,

3) użytkownik zobowiązuje się nie udostępniać osobom trzecim zaufanego urządzenia mobilnego, którego skutkiem byłoby umożliwienie osobie trzeciej uzyskania danych do uwierzytelnienia lub autoryzacji lub złożenie dyspozycji w Systemie,

4) użytkownik zobowiązuje się:

a) nie instalować ani nie zezwalać na instalowanie oprogramowania ani narzędzia w urządzeniu zaufanym lub innym urządzeniu, z którego użytkownik korzysta, aby łączyć się z Systemem, które umożliwi osobie trzeciej uzyskanie dostępu do Systemu, oraz

b) nie łączyć urządzenia zaufanego lub innego urządzenia, z którego użytkownik korzysta, aby łączyć się z Systemem z oprogramowaniem, które umożliwi innym osobom/ podmiotom uzyskanie dostępu do Systemu, w tym przejęcia kontroli nad urządzeniem użytkownika lub kierowaniem jego funkcjami (wszelkie sposoby podszywania się pod użytkownika),

5) użytkownik zobowiązuje się zabezpieczać urządzenie zaufane oraz urządzenia, z których użytkownik korzysta, aby łączyć się z Systemem (np. komputer, telefon komórkowy, inne urządzenia mobilne) przed złośliwym oprogramowaniem lub dostępem osób trzecich poprzez:

a) instalowanie wyłącznie legalnego oprogramowania na urządzeniu zaufanym oraz innych urządzeniach, z których łączy się z Systemem,

b) zainstalowanie oprogramowania antywirusowego, z tym, że może być ono bezpłatne na urządzeniu zaufanym oraz innych urządzeniach, z których łączy się z Systemem,

c) ustalenie kodu, hasła lub PINu lub innego zabezpieczenia dostępu do urządzenia zaufanego lub innego urządzenia, z którego użytkownik łączy się z Systemem,

d) niedopuszczanie do zapisania - na urządzeniu zaufanym lub innym urządzeniu wykorzystywanym do uwierzytelnienia lub autoryzacji - cech biometrycznych osób trzecich, np. zapisania cech twarzy (funkcja face ID) lub linii papilarnych, obrazu naczyń krwionośnych (funkcja touch ID), albowiem rodzi to ryzyko zakwalifikowania przez urządzenie danych osoby trzeciej jako danych użytkownika,

6) użytkownik jest zobowiązany regularnie instalować aktualizacje (w tym nowe wersje i poprawki) aplikacji mobilnej – nie później niż w terminach określonych przez Bank. W przypadku, gdy aktualizacja, nowa wersja lub poprawka jest krytyczna, Bank powiadamia użytkownika o konieczności jej zainstalowania, wdrożenia bezpośrednio przed zalogowaniem. Ponadto w przypadku, gdy użytkownik zainstalował aplikację mobilną lub stale używa tego samego urządzenia, korzystając z Systemu to użytkownik jest zobowiązany regularnie aktualizować oraz instalować poprawki i nowe wersje, co najmniej oprogramowania systemu operacyjnego (np. Android, iOS), które są zalecane przez producentów urządzeń lub oprogramowania, o ile dany producent przewiduje takie wsparcie. Brak instalacji aktualnych wersji lub poprawek w powyższym zakresie może mieć wpływ na bezpieczeństwo Systemu.

3. Użytkownik jest zobowiązany przestrzegać następujących zasad związanych z uwierzytelnieniem i autoryzacją dyspozycji:

1) przed każdą autoryzacją użytkownik zobowiązany jest sprawdzić czy dyspozycja jest zgodna z zamiarem użytkownika, a w przypadku, gdy użytkownik przed autoryzacją otrzymuje informacje od Banku, zobowiązany jest zapoznać się z tą informacją. W przypadku, gdy dyspozycja dotyczy dodania urządzenia do listy urządzeń zaufanych, użytkownik przed złożeniem dyspozycji powinien się upewnić, że faktycznie je posiada (rzeczywiście włada urządzeniem),

2) użytkownik zobowiązany jest niezwłocznie zawiadomić Bank o przypadkach nieautoryzowanych, nieprawidłowo zainicjowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych wskutek dyspozycji złożonych za pomocą Systemu. Zawiadomienie to użytkownik może złożyć przez System, telefonicznie przez infolinię lub w placówce bankowej,

3) w przypadku, gdy użytkownik zamierza korzystać z metody uwierzytelniania lub autoryzacji opartej na identyfikatorze biometrycznym, zobowiązany jest używać jednej, wyłącznie własnej cechy biometrycznej, która stanowi podstawę do utworzenia identyfikatora biometrycznego. W przypadku, gdy urządzenie mobilne umożliwia zapis kilku egzemplarzy danej cechy biometrycznej (np. linii papilarnych kilku palców) użytkownik zobowiązany jest zapisać wyłącznie jedną własną cechę biometryczną, albowiem ta cecha zostanie następnie przyporządkowana do klucza użytkownika, o którym mowa w § 1 ust. 2 pkt 5).

4. Użytkownik zobowiązany jest także do niezwłocznego zgłoszenia Bankowi utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia danych służących do uwierzytelnienia lub autoryzacji przez System, jak również nieuprawnionego dostępu do Systemu.

5. Użytkownik zobowiązany jest także do niezwłocznego powiadomienia Banku w przypadku stwierdzenia:

1) utraty kradzieży, przywłaszczenia lub stwierdzenia nieuprawnionego użycia urządzenia zaufanego lub telefonu komórkowego lub innego urządzenia, które jest powiązane z numerem telefonu oznaczonym, jako telefon do autoryzacji lub urządzenia służącego do logowania, uwierzytelniania lub autoryzacji (np. klucz U2F),

2) jakiegokolwiek incydentu technicznego lub innej awarii związanej z korzystaniem z Systemu, która może w ocenie użytkownika zagrozić bezpieczeństwu Systemu lub bezpiecznemu korzystaniu przez użytkownika z Systemu,

3) że osoby trzecie podjęły próbę logowania do Systemu. Obowiązek niezwłocznego zawiadomienia Banku istnieje także w przypadku uzasadnionego, w opinii użytkownika, podejrzenia, że nastąpiło naruszenie zabezpieczeń lub naruszenie poufności stosowanych przez użytkownika indywidualnych danych uwierzytelniających takich jak np. kody, kody autoryzacyjny lub identyfikatory biometryczny.

6. W przypadkach, o których mowa w ust. 4 lub ust. 5 oraz w przypadku ujawnienia lub podejrzenia, że nastąpiło ujawnienie osobom trzecim danych służących do uwierzytelnienia lub autoryzacji dyspozycji lub dostępu do Systemu przez inne osoby, użytkownik powinien niezwłocznie:

1) powiadomić Bank i dokonać blokady dostępu do Systemu lub zlecić Bankowi dokonanie blokady dostępu do Systemu. Dyspozycję blokady Systemu można złożyć w placówce bankowej realizującej tę czynność, przez System albo infolinię,

2) zmienić wszystkie dane służące do uwierzytelnienia lub autoryzacji, które są możliwe do zmiany.

7. W przypadku, gdy użytkownik stwierdzi, że:

1) doszło do popełnienia przestępstwa, w tym kradzieży tożsamości, lub działania skutkującego dostępem do Systemu przez osobę nieuprawnioną, lub

2) doszło do użycia przez osobę trzecią innych instrumentów płatniczych lub danych, do których dostęp umożliwia System lub jakakolwiek jego część, lub

3) pozyskanie przez osoby trzecie cech biometrycznych lub identyfikatorów biometrycznych zarejestrowanych na zaufanym urządzeniu mobilnym może prowadzić do nieuprawnionego dostępu tych osób do aplikacji mobilnej i nieuprawnionej autoryzacji dyspozycji - użytkownik zobowiązany jest niezwłocznie podjąć działania przewidziane w ust. 5 oraz zastrzec w odpowiednich instytucjach określone dane lub numery instrumentów płatniczych. Ponadto w przypadku podejrzenia przestępstwa, użytkownik zobowiązany jest zawiadomić właściwy organ, w szczególności Prokuraturę lub Policję.

8. Postanowienia dotyczące dostępu do Systemu osób trzecich nie dotyczą sytuacji:

1) gdy w imieniu użytkownika występują dostawca świadczący usługę inicjowania transakcji płatniczej lub dostawca świadczący usługę dostępu do informacji o rachunku, o ile dostawcy ci działają za zgodą użytkownika w celu i w zakresie wykonywania tych usług,

2) gdy innym użytkownikiem systemu jest osoba małoletnia, w imieniu której użytkownik będący przedstawicielem ustawowym tej osoby małoletniej zawarł umowę o System. Powyższe nie narusza zasady, że każdy z użytkowników może składać tylko własne dyspozycja, a osoba małoletnia może składać

dyspozycje jedynie w takim zakresie w jakim jest do tego upoważniona przez przedstawiciela ustawowego lub uprawniona na mocy przepisów prawa.

9. W celu ograniczenia ryzyka skorzystania przez użytkownika ze stron internetowych podobnych do strony Banku użytkownik podczas logowania zobowiązany jest sprawdzić czy strona, która została wyświetlona posiada certyfikat strony Banku. Sposób weryfikacji tego certyfikatu jest informacją ogólnie dostępną i jest podany na stronie internetowej Banku oraz na stronie logowania do Systemu Banku. Informacyjnie podajemy obecną nazwę strony Banku – www.ing.pl. Nazwa strony może ulec zmianie, Bank podaje ją w Komunikacie.

10. Użytkownik nie powinien:

1) logować się z urządzenia zaufanego lub innego urządzenia, którego stale używa podczas korzystania z Systemu do stron internetowych, które są oznaczane jako niezabezpieczone lub niebezpieczne (w takich przypadkach producenci oprogramowana stosują także praktykę wyświetlania na urządzeniu użytkownika komunikatu przy nazwie wyszukanej strony internetowej np. „połączenie nie jest bezpieczne" lub oznaczenia/ znaku „!"),

2) bezkrytycznie zezwalać aplikacjom instalowanym na urządzeniu zaufanym lub urządzeniu, którego stale używa podczas korzystania z Systemu na dostęp do innych aplikacji, a także posiadanych zdjęć, filmów lub kontaktów, - albowiem takie praktyki zwiększają ryzyko dostępu osób nieuprawnionych do urządzenia zaufanego lub urządzenia, które użytkownik stale używa podczas korzystania z Systemu.

11. Użytkownik może przekazać zgłoszenia lub powiadomienia, o których mowa w Regulaminie przez System, telefonicznie przez infolinię lub w placówce bankowej.

§ 22b

1. Bank rozpoznaje zgłoszenie użytkownika dotyczące nieautoryzowanej transakcji przeprowadzając wszechstronne badanie okoliczności związanych z transakcją. Celem badania jest ustalenie czy dyspozycja użytkownika została prawidłowo złożona i przez niego autoryzowana. Badanie obejmuje także ustalenie czy dyspozycja jest dyspozycją użytkownika, czy też została złożona przez osobę trzecią, złożoną także za pomocą oprogramowania lub innego urządzenia.

2. W przypadku, gdy okaże się, że zgoda na wykonanie transakcji nie została złożona przez płatnika uznaje się, że taka dyspozycja nie była autoryzowana. Powyższe nie narusza zasad odpowiedzialności opisanych niniejszym Regulaminem.

§ 22c

1. W przypadku, gdy użytkownik naruszy, co najmniej jedno zobowiązanie opisane w § 22a przyjmuje się, że użytkownik nie korzysta z Systemu zgodnie z Regulaminem.

2. Użytkownik jest odpowiedzialny za nieautoryzowane transakcje w pełnej wysokości, jeżeli były następstwem umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia przynajmniej jednego z zobowiązań użytkownika wskazanych w § 22a ust. 1-9.

3. Za wyjątkiem ust. 2, odpowiedzialność użytkownika za nieautoryzowane transakcje ogranicza się do równowartości w walucie polskiej kwoty 50 euro przeliczonej według średniego kursu euro ogłaszanego przez NBP, który obowiązywał w dniu dokonania transakcji, jeżeli transakcja nieautoryzowana jest skutkiem:

1) posłużenia się utraconymi przez użytkownika albo skradzionymi mu danymi służącymi do uwierzytelnienia lub autoryzacji,

2) przywłaszczenia przez osobę trzecią danych służących do uwierzytelniania lub autoryzacji.

Użytkownik nie odpowiada za nieautoryzowane transakcje, w przypadku gdy:

3) nie miał możliwości stwierdzenia utraty, kradzieży lub przywłaszczenia danych służących do uwierzytelniania lub autoryzacji przed wykonaniem transakcji płatniczej, z wyjątkiem przypadku gdy użytkownik działał umyślnie, lub

4) utrata danych służących do uwierzytelniania lub autoryzacji przed wykonaniem transakcji została spowodowana działaniem lub zaniechaniem ze strony Banku lub podmiotów wskazanych w art. 6 pkt 10) w ustawie o usługach płatniczych.

4. Za wyjątkiem sytuacji opisanych w ust. 2 i ust. 3 w przypadku wystąpienia nieautoryzowanej transakcji Bank zwróci płatnikowi kwotę nieautoryzowanej transakcji niezwłocznie - nie później jednak niż do końca dnia

roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji lub po dniu otrzymania zgłoszenia - z wyjątkiem przypadku, gdy Bank ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo i poinformuje, o tym w formie pisemnej organy powołane do ścigania przestępstw. W przypadku, gdy płatnik korzysta z rachunku płatniczego a zwrot według powyższej zasady jest należny Bank przywróci obciążony rachunek do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

5. Płatnik nie odpowiada za nieautoryzowane transakcje po dokonaniu zgłoszenia Bankowi utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia danych służących do uwierzytelniania lub autoryzacji przez System, jak również nieuprawnionego dostępu do Systemu o którym mowa w § 22a ust. 4 chyba, że działał umyślnie.
6. W przypadku, gdy transakcja była nieautoryzowana, a Bank nie wymagał od użytkownika silnego uwierzytelniania, użytkownik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że działał umyślnie. Powyższe nie dotyczy sytuacji, gdy zgodnie z przepisami prawa Bank był uprawiony do rezygnacji z wymogu silnego uwierzytelniania. W przypadku, gdy odbiorca lub dostawca odbiorcy nie akceptują silnego uwierzytelniania użytkownika odpowiadają oni za szkodę poniesioną przez Bank.
7. Niezależnie od postanowień powyższych jeżeli użytkownik nie powiadomi o nieautoryzowanych, nieprawidłowo zainicjowanych, niewykonanych, lub nienależycie wykonanych transakcjach płatniczych, w terminie 13 miesięcy od dnia obciążenia rachunku albo od dnia, w którym transakcja miała być wykonana, wygasają roszczenia użytkownika z tytułu nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcji płatniczych.

§ 22d

1. W przypadku, gdy użytkownik naruszy, co najmniej jedno z zobowiązań określonych w § 22 lub § 22a oraz gdy w związku z tym naruszeniem okaże się, że:
   1) osoba trzecia - korzystając z całości lub części danych do uwierzytelnienia lub autoryzacji użytkownika - złożyła lub autoryzowała dyspozycję nie płatniczą, a Bank wykonał tę dyspozycję lub złożył odpowiadające jej oświadczenie (np. o zawarciu umowy), oraz
   2) Bank poniósł szkodę wskutek wykonania dyspozycji lub złożenia odpowiadającego jej oświadczenia, bowiem dyspozycja ta nie pochodziła od użytkownika,

   to użytkownik będzie odpowiedziany za naprawienie szkody wyrządzonej Bankowi z tytułu naruszenia zobowiązań przewidzianych w § 22 oraz § 22a odpowiednio do stopnia naruszenia tych zobowiązań.
2. Odpowiedzialność użytkownika ogranicza się do szkody rzeczywistej Banku powstałej wskutek naruszenia zobowiązań przewidzianych w § 22 oraz 22a. Odpowiedzialność użytkownika nie wyłącza dochodzenia przez Bank odszkodowania wobec osoby trzeciej aż do całkowitego pokrycia szkody

13. Pozostałe zasady i rekomendacje bezpiecznego korzystania z systemu

§ 23

1. Bank powiadamia użytkownika o bieżących zagrożeniach tj. wystąpieniu oszustwa lub podejrzeniu jego wystąpienia lub innych zagrożeń dla bezpieczeństwa korzystania z Systemu. Powiadomienia te mogą być:
   1) przekazywane użytkownikowi przed logowaniem do Systemu,
   2) przekazywane użytkownikowi wewnątrz Systemu (np. po zalogowaniu, w wiadomościach),
   3) przekazywane innym bezpiecznym kanałem komunikacji uzgodnionym pomiędzy użytkownikiem i Bankiem.

   Dodatkowo informacje w tej sprawie są publikowane na stronie internetowej Banku.
2. Użytkownik powinien zapoznać się z powiadomieniami dot. zagrożeń, o których mowa w ust. 1 oraz przestrzegać rekomendacji w nich wskazanych. Niezapoznanie się z powiadomieniami o zagrożeniach i nieprzestrzeganie rekomendacji może wiązać się m.in. z ryzykiem:
   1) wystąpienia ataków socjotechnicznych, podczas których osoby trzecie mogą – podszywając się pod Bank lub inną instytucję – nakłaniać użytkownika do udostępnienia danych identyfikacyjnych, kodów autoryzacyjnych lub kodu PIN,
   2) autoryzacji przez użytkownika dyspozycji, której nie przygotował,

3) wykorzystania urządzeń, nad którymi kontrolę przejęły osoby trzecie.

3. Zaleca się, aby użytkownik upewnił się, czy jego środowisko komputerowe i środowisko urządzenia mobilnego jest bezpieczne. Użytkownik zobowiązany jest do stosowania aktualnych rekomendacji Banku w zakresie bezpieczeństwa transakcji internetowych w celu ochrony przed szczególnymi zagrożeniami powodowanymi przez łączenie się z siecią internetową. Rekomendacje te prezentowane są przez Bank na stronie internetowej Banku.

Informacje o kolejnych aktualizacjach tych rekomendacji są wysyłane przez System.

4. Bank stosuje środki bezpieczeństwa, które zmniejszają ryzyko korzystania z aplikacji mobilnej w sposób nieuprawniony. W związku z tym, Bank ma prawo stosować elektroniczne mechanizmy sprawdzające czy użytkownik lub osoba trzecia dokonali zmian w zaufanym urządzeniu mobilnym lub w oryginalnym, wymaganym przez producenta oprogramowaniu, które zostało zainstalowane na danym urządzeniu. Uznaje się, że dokonanie zmian, o których mowa powyżej może skutkować ryzykiem przejęcia kontroli nad urządzeniem przez osobę nieuprawnioną.

5. Jeśli Bank ustali, że występuje ryzyko przejęcia kontroli nad urządzeniem zaufanym przez osobę nieuprawnioną, może obniżyć limit transakcyjny dla zleceń płatniczych w aplikacji mobilnej dokonywanych z tego urządzenia - najniżej do 5% kwoty maksymalnego limitu dziennego dla tej aplikacji ustalonego w Regulaminie. Bank niezwłocznie powiadomi o tym użytkownika. Bank ma prawo zablokować System zgodnie z § 27 ust. 2 jeśli ryzyko, o którym mowa wyżej stanie się wysokie lub Bank ustali, że z urządzenia, nad którym najprawdopodobniej przejęła kontrolę osoba nieuprawniona, są składane kolejne dyspozycje płatnicze lub inne dyspozycje, które prowadziłyby do nieuprawnionego dostępu osób trzecich do rachunków, produktów lub usług bankowych za pomocą Systemu.

§ 24

1. Bank na stronach internetowych banku i wewnątrz Systemu, publikuje informacje z zakresu bezpiecznego korzystania z Systemu. Szczegółowe informacje dot. miejsca publikacji informacji i rekomendacji z zakresu bezpieczeństwa znajdują się w Komunikacie.

2. Zalogowanie się do Systemu bankowości internetowej i korzystanie z tego Systemu na żądanie użytkownika wymaga plików cookies lub innych technologii które pochodzą z tego Systemu. Bank stosuje pliki cookies i inne technologie zgodnie z Polityką cookies (zwana Polityką cookies). W Systemie bankowości internetowej pliki cookies i inne technologie wykorzystywane są w celu ustanowienia i utrzymania sesji użytkownika w tym Systemie, wsparcia ochrony integralności transakcji oraz identyfikacji cech technicznych i technologicznych urządzenia używanego podczas korzystania z usług Systemu, w związku z wymogami bezpieczeństwa Systemu i dokonywanych transakcji. W przypadku, gdy użytkownik korzysta ze strony internetowej Banku ale nie z Systemu bankowości internetowej, może, zgodnie z Polityką Banku dotyczącą plików cookies, ustawić własną przeglądarkę internetową tak, aby nie akceptować plików cookies innych niż używane w Systemie. Stosowana przez Bank Polityka cookies jest dostępna na stronie internetowej Banku.

3. Użytkownik jest obowiązany niezwłocznie powiadamiać Bank o wszelkich zmianach dotyczących danych personalnych, oraz danych kontaktowych użytkownika. Zmiana danych może zostać złożona za pomocą Systemu bankowości internetowej, o ile w Systemie istnieje techniczna funkcjonalność umożliwiająca taki sposób zmiany danych. Za wyjątkiem gdy użytkownik doręcza dokument w formie aktu notarialnego, własnoręczność podpisu użytkownika musi być potwierdzona:

1) przez notariusza – w przypadku dokumentów podpisanych na terenie Rzeczypospolitej Polskiej,

2) przez polską placówkę dyplomatyczną, konsularną lub notariusza kraju, z którym Rzeczpospolita Polska podpisała umowę o pomocy prawnej w sprawach cywilnych, lub potwierdzone urzędowo lub notarialnie wraz z dołączoną apostille w rozumieniu konwencji – w przypadku dokumentów podpisanych za granicą.

4. Za wyjątkiem ust. 5 dyspozycje składane drogą korespondencyjną muszą być składne w formie wskazanej w ust. 3.

5. Oświadczenia użytkownika, o których mowa w § 29 ust. 1, § 31 ust. 3, mogą być nadesłane drogą korespondencyjną bez spełnienia warunków określonych w ust. 3. Bank zastrzega sobie jednak prawo dokonania dodatkowej weryfikacji nadesłanych oświadczeń.

§ 25

1. System bankowości internetowej można odblokować składając dyspozycję w placówce bankowej realizującej tę czynność, wypełniając odpowiedni wniosek na stronie internetowej Banku lub w aplikacji mobilnej, o ile Bank dopuszcza taką funkcjonalność. Korzystanie z Systemu będzie możliwe po powtórnym nadaniu hasła lub kodu PIN do aplikacji mobilnej.
2. Użytkownik może zmienić dotychczasowe dane niezbędne do otrzymywania uwierzytelnienia lub autoryzacji:
   1) za pomocą Systemu - jeżeli jest w posiadaniu dotychczasowego telefonu do autoryzacji,
   2) składając odpowiedni wniosek na stronie internetowej lub w placówce banku - jeżeli nie posiada dotychczasowego numeru telefonu do autoryzacji.

§ 26

1. W celu zapewnienia bezpieczeństwa, urządzenie mobilne przeznaczone do korzystania ze wszystkich funkcji aplikacji mobilnej musi zostać dodane do listy zaufanych urządzeń mobilnych. W przypadku gdy jedno urządzenie mobilne został wskazane, jako zaufane przez kilku użytkowników, każdy z tych użytkowników jest zobowiązany spełniać wymogi dotyczące bezpieczeństwa przewidziane Regulaminem, w tym do bezpiecznego zakończenia używania aplikacji.
2. Lista zaufanych urządzeń mobilnych jest dostępna w Systemie,
3. Urządzenie mobilne można usunąć z listy w Systemie bankowości internetowej lub w aplikacji mobilnej. Bank ma prawo usunąć urządzenie mobilne z listy, gdy powziął uzasadnioną wątpliwość, że użytkownik nie korzysta z tego urządzenia lub dostęp do urządzenia uzyskała osoba nieuprawniona. Przyjmuje się, że użytkownik nie korzysta z urządzenia mobilnego, o ile nie logował się z tego urządzenia do aplikacji mobilnej przez 90 dni. Użytkownik może ponownie wpisać dane urządzenie na listę. Ze względów bezpieczeństwa usuwanie z listy - w zależności od wersji aplikacji mobilnej - może też następować automatycznie wskutek aktywacji aplikacji na innym urządzeniu.
4. Zaufaną przeglądarkę można usunąć z listy w Systemie bankowości internetowej. Bank ma prawo usunąć zaufaną przeglądarkę z listy, gdy powziął uzasadnioną wątpliwość, że użytkownik nie korzysta z tego urządzenia lub dostęp do urządzenia uzyskała osoba nieuprawniona. Ze względów bezpieczeństwa zaufana przeglądarka będzie usuwana z listy po 90 dniach od daty jej dodania do listy zaufanych przeglądarek. Użytkownik może ponownie dodać daną przeglądarkę na listę.
5. Usuwanie klucza zabezpieczeń z listy kluczy jest możliwe w Systemie bankowości, gdy uprzednio nastąpiło uwierzytelnienie z użyciem klucza zabezpieczeń bądź w placówce lub na infolinii banku.
6. W przypadku utraty, kradzieży, przywłaszczenia lub stwierdzenia nieuprawnionego użycia zaufanego urządzenia mobilnego użytkownik zobowiązany jest najszybciej jako to możliwe usunąć urządzenie, którego dotyczy podejrzenie, z listy zgodnie z ust. 3.
7. W przypadku podejrzenia nieuprawnionego użycia Systemu lub kradzieży, przywłaszczenia urządzenia, z którym jest powiązany telefon do autoryzacji lub podejrzenia umyślnego doprowadzenia do nieautoryzowanej transakcji użytkownik jest zobowiązany do niezwłocznego zawiadomienia Banku za pomocą Systemu bankowości internetowej lub przez infolinię.

§ 27

1. Bank zastrzega sobie prawo do przeprowadzania modernizacji, aktualizacji oraz regularnych konserwacji technicznych Systemu bankowości internetowej skutkujących okresowymi przerwami w dostępie do Systemu lub do wybranych jego funkcjonalności. O powyższych okolicznościach Bank poinformuje, podając szacunkowy czas braku lub ograniczenia dostępu:
   1) za pomocą opcji wiadomości w Systemie bankowości internetowej, i/ lub
   2) na stronie internetowej Banku, i/ lub
   3) przez infolinię.
2. Bank zastrzega sobie prawo do dokonania blokady dostępu do Systemu bankowości internetowej ze względów bezpieczeństwa. Przez względy bezpieczeństwa należy rozumieć sytuacje nieuprawnionego dostępu osób trzecich do rachunków, produktów lub usług bankowych za pomocą Systemu, lub też zagrożenie taką sytuacją, a także w przypadkach przewidzianych przepisami prawa.

3. W przypadku podejrzenia próby nieuprawnionego dostępu do Systemu, Bank może na określony czas wstrzymać możliwość zalogowania się do Systemu. O sposobie ponownego zalogowania się do Systemu Bank poinformuje w wiadomości przesłanej na telefon do autoryzacji.
4. Bank zastrzega sobie prawo odmowy wykonania dyspozycji lub wprowadzenia dodatkowych ograniczeń i zabezpieczeń w stosunku do dyspozycji składanych przez System bankowości internetowej, w przypadku wystąpienia ważnych okoliczności uniemożliwiających wykonanie tych dyspozycji, tj. przeszkód natury technologicznej, względów bezpieczeństwa lub sprzeczności treści dyspozycji z wiążącymi użytkownika regulacjami obowiązującymi w Banku, a także w przypadku niestosowania się przez użytkownika do ogólnie obowiązujących przepisów prawa.
5. Bank może wprowadzić ograniczenia w korzystaniu z Systemu bankowości internetowej w przypadku, gdy w oparciu o lokalizację adresu IP ustali, że Użytkownik loguje się do systemu w kraju, który znajduje się w wykazie krajów wysokiego ryzyka. Wykaz takich krajów i zakres ograniczeń został szczegółowo określony na stronie internetowej Banku.
6. Bank zastrzega sobie możliwość wdrożenia ograniczeń w korzystaniu z pełnej funkcjonalności Systemu bankowości internetowej wobec określonej grupy użytkowników znajdujących się w takiej samej sytuacji prawnej lub faktycznej. Ograniczenia te mogą wynikać z wymogów bezpieczeństwa. O wprowadzonych ograniczeniach Bank poinformuje użytkowników w Systemie co najmniej 14 dni kalendarzowych przed datą wdrożenia przedmiotowych ograniczeń.
7. Z uwagi na zasady bezpieczeństwa, Bank ma prawo żądać od użytkownika aktualnych danych osobowych lub potwierdzenia tych danych.
8. Użytkownik nie ma prawa wpisywać ani przesyłać do Systemu treści bezprawnych, ani też używać programów, które zagrażają innym użytkownikom Systemu lub zagrażają integralności Systemu, w tym danych w nim zawartych lub aplikacji informatycznych z nim współpracujących. Jeśli dana usługa Systemu, w tym aplikacji mobilnej umożliwia wyświetlanie danych innych osób, użytkownik nie ma prawa do zbierania tych danych, a może je użyć jedynie w celu zlecenia transakcji.
9. Podczas korzystania z Systemu Bank może przekazywać użytkownikowi instrukcje dotyczące techniczno-organizacyjnych narzędzi Systemu lub ogłoszenia o udostępnionych w jego ramach usługach lub funkcjonalnościach. Instrukcje i ogłoszenia mają wyłącznie charakter informacyjny i nie są reklamą. Mogą być przekazywane za pomocą dostępnych w Systemie środków komunikacji lub mogą być przedstawiane w postaci m.in. graficznej, tekstowej, prezentacji lub animacji.
10. Pozyskanie przez osoby trzecie cech biometrycznych lub identyfikatorów biometrycznych zarejestrowanych na zaufanym urządzeniu mobilnym może prowadzić do nieuprawnionego dostępu tych osób do aplikacji mobilnej i nieuprawnionej autoryzacji dyspozycji.
11. Zalogowanie się do Systemu bankowości internetowej i korzystanie z tego Systemu na żądanie użytkownika wymaga plików cookies lub innych technologii które pochodzą z tego Systemu. Bank stosuje pliki cookies i inne technologie zgodnie z Polityką cookies (zwana Polityką cookies). W Systemie bankowości internetowej pliki cookies i inne technologie wykorzystywane są w celu ustanowienia i utrzymania sesji użytkownika w tym Systemie, wsparcia ochrony integralności transakcji oraz identyfikacji cech technicznych i technologicznych urządzenia używanego podczas korzystania z usług Systemu, w związku z wymogami bezpieczeństwa Systemu i dokonywanych transakcji. W przypadku, gdy użytkownik korzysta ze strony internetowej Banku ale nie z Systemu bankowości internetowej, może, zgodnie z Polityką Banku dotyczącą plików cookies, ustawić własną przeglądarkę internetową tak, aby nie akceptować plików cookies innych niż używane w Systemie. Stosowana przez Bank Polityka cookies jest dostępna na stronie internetowej Banku.

14. Wymogi techniczne korzystania z systemu

§ 28

1. Użytkownik może korzystać z Systemu po spełnieniu następujących, niezbędnych do współpracy z Systemem, minimalnych wymagań technicznych: posiadania urządzenia elektronicznego, w szczególności takiego jak komputer, telefon, inne urządzenie mobilne, z dostępem do internetu wraz z zainstalowanym na tym urządzeniu system operacyjnym i przeglądarką internetową. W przypadku zamiaru korzystania z funkcji obsługiwanych

przez odrębne aplikacje np. aplikacji mobilnej, konieczne jest zainstalowanie danej aplikacji na urządzeniu mobilnym.

2. W trakcie obowiązywania Umowy, Użytkownik musi wskazać telefon do autoryzacji i dysponować ostatnio wskazanym telefonem. Brak wskazania telefonu do autoryzacji uniemożliwia korzystanie z Systemu lub z poszczególnych jego funkcji.
3. Wymogi techniczne związane z komunikowaniem się użytkownika z Systemem:

   1) dla bankowości internetowej - system operacyjny Apple OS X oraz Windows,

   2) dla aplikacji mobilnej - system operacyjny iOS oraz Android.

   Dodatkowe informacje związane z komunikowaniem się użytkownika z Systemem lub z określonymi aplikacjami, programami, typami plików lub dotyczące przeglądarek internetowych i ich wersji oraz wersji systemów operacyjnych wskazane są w Komunikacie oraz na stronie internetowej Banku.
4. W związku z rozwojem technicznym i technologicznym, poszczególne wersje Systemu, mogą być aktualizowane, udoskonalane, zmieniane lub zastępowane nowymi wersjami. O ile będzie to możliwe, z technicznego punktu widzenia, aktualizacje lub udoskonalenia mogą być dokonywane podczas pracy Systemu. W przypadku, gdy którakolwiek z powyższych operacji wymaga ponownego uruchomienia lub zainstalowania, przez użytkownika, nowej wersji Systemu, Bank poinformuje go o tym przy pomocy odpowiednich ekranów, zawiadomień lub wiadomości.
5. Bank może wycofać starszą wersję Systemu, zastępując ją nowszą wersją. W takim przypadku użytkownik jest informowany, z odpowiednim wyprzedzeniem, o przewidywanej dacie zastąpienia starszej wersji nowszą i ewentualnych koniecznych czynnościach, o ile ze względów technicznych wymagane byłoby podjęcie przez użytkownika jakiekolwiek czynności, w szczególności pobranie i instalacja nowej wersji lub wykonanie tych czynności na danym rodzaju urządzenia.

15. Rozwiązanie, wypowiedzenie i wygaśnięcie umowy

§ 29

1. Klient ma prawo rozwiązać Umowę ze skutkiem natychmiastowym, bez okresu wypowiedzenia. Dyspozycja rozwiązania Umowy może być złożona w formie pisemnej pod rygorem nieważności lub za pomocą Systemu bankowości internetowej, o ile System umożliwia taki sposób złożenia oświadczenia o rozwiązaniu Umowy.
2. Bank ma prawo rozwiązać Umowę zawartą z klientem za dwumiesięcznym okresem wypowiedzenia.
3. Bank ma prawo do rozwiązania Umowy zawartej z klientem z zachowaniem odpowiedniego i przewidzianego powyżej okresu wypowiedzenia, w przypadku (ważne przyczyny rozwiązania Umowy za wypowiedzeniem):
   1) stwierdzenia przez Bank, że użytkownik nie przestrzega zasad bezpiecznego korzystania z Systemu, opisanych w rozdziale 13. Regulaminu,
   2) powzięcia przez Bank informacji stanowiących uzasadnione podejrzenie popełnienia przez użytkownika przestępstwa z wykorzystaniem Systemu bankowości internetowej lub przestępstwa na szkodę Banku,
   3) nieudzielania przez użytkownika, opisanych w Regulaminie, informacji niezbędnych dla aktywacji danej usługi lub niezbędnych do dalszego świadczenia usługi Systemu bankowości internetowej,
   4) podania przez użytkownika danych lub informacji nieprawdziwych, lub niezgodnych ze stanem faktycznym, w tym posłużenia się przez użytkownika dokumentami nieaktualnymi (również dokumentami, których data ważności upłynęła), dokumentami nieprawdziwymi, przerobionymi lub podrobionymi,
   5) braku możliwości wykonania przez Bank obowiązków w ramach stosowania środków bezpieczeństwa finansowego, określonych w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.
4. Umowa ulega rozwiązaniu z dniem śmierci klienta. Fakt śmierci może być potwierdzony wiarygodnym dokumentem m.in.:
   1) pełnym lub skróconym odpisem aktu zgonu,
   2) świadectwem zgonu,
   3) pismem organu rentowego,

4) informacją z rejestru Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL),

5) pismem z policji, z sądu, od komornika,

6) innym wiarygodnym dokumentem potwierdzającym fakt śmierci klienta.

W przypadku gdy dany dokument nasuwa wątpliwości, w szczególności co do jego autentyczności lub potwierdzenia faktu lub daty śmierci użytkownika, lub też zachodzą inne istotne okoliczności skutkujące wątpliwościami co do faktu lub daty śmierci użytkownika, za dokument potwierdzający fakt śmierci Bank będzie uznawał pełny lub skrócony odpis aktu zgonu, chyba że co innego wynika z orzeczenia sąd, lub przepisów prawa.

16. Reklamacje. Rozwiązywanie sporów

§ 30

1. W sprawach reklamacji dotyczących zleceń płatniczych przewidzianych w tym Regulaminie, ale związanych z rachunkami uregulowanymi odpowiednio w Regulaminie rachunków dla klientów indywidualnych stosuje się postanowienia tego z regulaminów, który jest właściwy dla danego rachunku. Pełnomocnictwo do warunkowego uznania rachunku albo obciążenia go kwotą wynikającą z reklamacji, które jest udzielone przez użytkownika zgodnie z umową rachunku, obejmuje także transakcje wynikające ze zleceń płatniczych przewidzianych niniejszym Regulaminem. Informacja pomocnicza o rachunkach, które podlegają odpowiednio Regulaminowi rachunków dla klientów indywidualnych.

2. Złożenie reklamacji dotyczącej nieautoryzowanych, nieprawidłowo zainicjowanych lub nienależycie wykonanych lub niewykonanych dyspozycji, które zostały złożone przez System musi nastąpić niezwłocznie, jednak nie później niż w ciągu 13 miesięcy od daty kwestionowanej dyspozycji.

3. Z zastrzeżeniem postanowień § 22 i § 22a, w przypadku wystąpienia nieautoryzowanej, przez osobę uprawnioną do dysponowania rachunkiem, transakcji płatniczej na rachunku, Bank zwróci niezwłocznie - nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika lub po dniu otrzymania stosownego zgłoszenia, z wyjątkiem przypadku gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw - kwotę nieautoryzowanej transakcji płatniczej i przywróci obciążony rachunek do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

4. Użytkownik ma prawo składać reklamacje. Reklamację można złożyć:

1) w postaci elektronicznej:

a) przez System bankowości internetowej,

b) na adres doręczeń elektronicznych wpisany do bazy adresów elektronicznych AE:PL-69368-51081-ERVRU-12, o ile usługa rejestrowanego doręczenia elektronicznego jest aktywna zgodnie z odpowiednimi przepisami prawa oraz umowami zawartymi przez posiadacza rachunku lokaty i bank,

2) ustnie:

a) telefonicznie pod numerami wskazanymi na stronie internetowej Banku (koszt połączenia wg stawek operatora),

b) osobiście w placówce bankowej realizującej tę czynność,

3) w formie pisemnej:

a) przesyłką pocztową na adres Banku wskazany na stronie internetowej Banku,

b) osobiście w placówce bankowej realizującej tę czynność.

5. W uzasadnionych przypadkach reklamacje złożone przez System bankowości internetowej lub telefonicznie przez infolinię, a dotyczące nieautoryzowanych, nieprawidłowo zainicjowanych, niewykonanych lub nienależycie wykonanych transakcji płatniczych lub dyspozycji, użytkownik zobowiązany jest potwierdzić dodatkowo w formie pisemnej w placówce bankowej realizującej tę czynność, w terminie do 14 dni kalendarzowych liczonych od daty złożenia reklamacji.

6. Odpowiedź na reklamację Bank przekazuje:

1) w postaci elektronicznej:

a) poprzez System bankowości internetowej,

b) na adres doręczeń elektronicznych wskazany przez posiadacza, o ile Bank posiada możliwość odpowiedzi na ten adres,

albo w jeden z poniżej wybranych przez klienta sposobów:

2) w formie papierowej – w placówce bankowej realizującej tę czynność albo listem na adres korespondencyjny,

3) na innym trwałym nośniku informacji - o ile strony tak postanowią.

7. Bank udzieli odpowiedzi najszybciej jak to możliwe, jednak nie później niż do 15 dni roboczych (w przypadku reklamacji dotyczących usług płatniczych) i 30 dni (w przypadku reklamacji niedotyczących usług płatniczych), licząc od daty jej otrzymania. W trakcie rozpatrywania reklamacji Bank może poprosić o dodatkowe informacje lub dokumenty. W szczególnie skomplikowanych przypadkach, uniemożliwiających rozpatrzenie reklamacji i udzielenie odpowiedzi w tym terminie, może on zostać wydłużony, jednak nie może przekroczyć 35 dni roboczych (w przypadku reklamacji dotyczących usług płatniczych) i 60 dni (w przypadku reklamacji niedotyczących usług płatniczych), licząc od daty otrzymania reklamacji. Bank poinformuje użytkownika o przyczynach opóźnienia, wskaże okoliczności, które muszą zostać ustalone dla rozpatrzenia reklamacji, przewidywanym terminie zakończenia postępowania reklamacyjnego.

8. W trakcie postępowania reklamacyjnego Bank może zwrócić się do użytkownika o przedstawienie dodatkowych wyjaśnień lub dokumentów. W przypadku konieczności wyjaśnienia dodatkowych okoliczności w związku z prowadzonym postępowaniem reklamacyjnym, Bank zastrzega sobie prawo do kontaktu telefonicznego z użytkownikiem na numer telefonu wskazany przez użytkownika do kontaktu z Bankiem.

9. W przypadku nieuznania reklamacji przez Bank użytkownik ma prawo złożenia odwołania. O ile użytkownikowi są znane nowe, mające znaczenie dla sprawy fakty, okoliczności lub dowody, powinien Bankowi je ujawnić w żądaniu. Bank rozpoznaje powtórnie reklamację w terminach wskazanych dla rozpoznawania reklamacji. Jeśli w wyniku reklamacji powstanie spór pomiędzy klientem a Bankiem, to może on zostać rozwiązany polubownie w drodze zawarcia ugody.

10. Ewentualne spory, które wynikają z Umowy zawartej przez Bank i użytkownika mogą być rozstrzygane w trybie pozasądowym. Wnioski można składać do:

1) Rzecznika Finansowego, strona: www.rf.gov.pl. Rzecznik działa zgodnie z ustawą o rozpatrywaniu reklamacji przez podmioty rynku finansowego, Rzeczniku Finansowym i o Funduszu Edukacji Finansowej,

2) Arbitra bankowego działającego przy Związku Banków Polskich, strona: www.zbp.pl/dla-konsumentow/arbiter-bankowy/dzialalnosc. Arbiter rozstrzyga spór i wydaje swoje orzeczenie zgodnie z regulaminem bankowego arbitrażu konsumenckiego.

11. Nawet jeśli użytkownik skorzysta z Platformy ODR, nadal może złożyć wniosek do Arbitra bankowego lub Rzecznika Finansowego. Bank również może złożyć wniosek o wszczęcie pozasądowego rozstrzygania sporu przeciwko użytkownikowi za pośrednictwem Platformy ODR – jeśli obie strony wcześniej zgodzą się na takie rozwiązanie, a regulamin podmiotu ADR i prawo nie wyłączają takiej możliwości.

12. Użytkownik może również zwrócić się o pomoc do rzecznika konsumenta (miejskiego lub powiatowego).

13. Spory wynikające z Umowy mogą być również rozstrzygane na drodze sądowej. Sądem właściwym dla ewentualnych sporów jest sąd ustalony zgodnie z przepisami kodeksu postępowania cywilnego.

14. Użytkownik może wnieść do organu sprawującego nadzór nad Bankiem (Komisja Nadzoru Finansowego) skargę na działanie Banku, jeżeli zdaniem użytkownika, działanie to narusza przepisy prawa oraz w przypadku odmowy świadczenia na rzecz użytkownika usług płatniczych.

17. Zmiana regulaminu

§ 31

1. Bank zastrzega sobie prawo zmiany Regulaminu z ważnych przyczyn. Za ważne przyczyny uznaje się następujące przyczyny, których skutkiem jest konieczność zmiany Regulaminu w niezbędnym - wynikającym z danej przyczyny - zakresie:

1) wprowadzenie nowych lub zmiana przepisów prawa określających zasady świadczenia przez Bank usług lub określających zasady korzystania z tych usług przez użytkownika,

2) wydanie przez organ nadzorczy lub inny uprawniony podmiot, decyzji, rekomendacji, zalecenia, stanowiska, orzeczenia lub innego dokumentu określającego zasady świadczenia przez Bank usług, lub określającego zasady korzystania z tych usług przez użytkownika w ramach zawartej z nim umowy,

3) rozszerzenie, zmianę lub ograniczenie funkcjonalności usług, zmianę zasad korzystania z usług przez użytkownika, wprowadzenie nowych usług, rezygnację z wykonywania niektórych czynności będących przedmiotem usług świadczonych przez Bank w ramach zawartej z użytkownikiem umowy,

4) zmiany w systemie informatycznym Banku wynikające z:

a) udoskonalenia systemów informatycznych Banku spowodowanych rozwojem technologicznym,

b) obligatoryjnych zmian wprowadzonych w międzybankowych systemach rozliczeniowych w odniesieniu do uczestników tych systemów,

c) zmian dostawców oprogramowania skutkujących zmianą funkcjonalności systemu informatycznego Banku,

- wpływające na objęte niniejszym Regulaminem usługi świadczone przez Bank lub zasady korzystania z tych usług przez użytkownika w ramach zawartej z nim umowy.

2. O zmianach Regulaminu Bank zawiadamia użytkownika, w sposób z nim uzgodniony i określony w § 32 ust. 2 nie później niż dwa miesiące przed proponowaną datą wejścia w życie zmian Regulaminu.

3. Użytkownik ma prawo, przed dniem proponowanego wejścia w życie zmian:

1) wypowiedzieć Umowę bez ponoszenia opłat ze skutkiem od dnia poinformowania go o zmianie, nie później jednak niż do dnia w którym te zmiany zostałyby zastosowane,

2) zgłosić sprzeciw wobec proponowanych zmian.

Jeżeli przed proponowaną datą wejścia w życie zmian użytkownik nie złoży pisemnego sprzeciwu wobec tych zmian, uważa się że wyraził na nie zgodę. W przypadku, gdy użytkownik złoży sprzeciw, ale nie dokona wypowiedzenia Umowy, Umowa wygasa z dniem poprzedzającym dzień wejścia w życie proponowanych zmian, bez ponoszenia opłat.

4. Zmiana funkcjonalności występujących w ramach Systemu lub w ramach poszczególnych usług, która jest spowodowana rozwojem technicznym/ technologicznym nie powoduje konieczności zmiany Regulaminu, o ile nie zmieni to zasad świadczonych użytkownikowi usług w ramach zawartej z nim Umowy.

5. Przed proponowaną datą wejścia w życie zmian Regulaminu Bank może umożliwić użytkownikowi korzystanie ze zmian w istniejących usługach lub korzystanie z nowych usług, o ile użytkownik zaakceptuje zmianę Regulaminu dotyczącą danej usługi.

18. Postanowienia końcowe

§ 32

1. Regulamin jest dostępny w placówkach bankowych oraz na stronie internetowej Banku.

2. Bank zawiadamia klienta o każdej zmianie Regulaminu w formie powiadomienia na trwałym nośniku informacji wysyłanego:

1) przez System bankowości internetowej, albo

2) w inny sposób uzgodniony przez strony.

3. Tytuły rozdziałów mają wyłącznie znaczenie informacyjne, ułatwiające orientację w tekście Regulaminu.

4. Regulamin jest ważny od 15 marca 2025 roku.

Załącznik 1

TRYB REALIZACJI ZLECEŃ PŁATNICZYCH I INNYCH DYSPOZYCJI SKŁADANYCH PRZEZ SYSTEM BANKOWOŚCI INTERNETOWEJ

Godziny graniczne przyjmowania zleceń płatniczych poprzez System bankowości internetowej uzależnione są od godzin działania systemów Banku co odzwierciedla poniższa tabela. Zlecenie płatnicze złożone poprzez System bankowości internetowej po godzinie granicznej uznaje się za otrzymane w pierwszym dniu roboczym następującym po dniu złożenia tego zlecenia.

Tryb realizacji zleceń płatniczych dotyczących polecenia przelewu, stałego zlecenia płatniczego:

Godzina graniczna przyjmowania zleceń płatniczych	Rodzaj zlecenia płatniczego	
	Z bieżącą datą realizacji	Z odroczoną datą realizacji bez względu na godzinę złożenia zlecenia
brak zlecenie wykonywane w czasie rzeczywistym	Zlecenia, które nie wymagają przewalutowania	
	a) polecenie przelewu wewnętrznego w PLN albo przelew w ramach usługi „Płać z ING” b) polecenie przelewu wewnętrznego w walutach obcych c) przelew krajowy złożony jako przelew Express ELIXIR albo przelew BlueCash	a) polecenie przelewu wewnętrznego w PLN b) polecenie przelewu wewnętrznego w walutach obcych c) zlecenie stałe na rachunki w banku
brak zlecenie wykonywane zgodnie z harmonogramem sesji rozliczeniowych banku	Zlecenia, które nie wymagają przewalutowania	
	a) przelew krajowy, w tym złożony jako przelew w ramach usługi „Płać z ING”	a) przelew krajowy b) zlecenie stałe na rachunki w innych bankach
15:00 (od poniedziałku do piątku)	Zlecenia, które wymagają i nie wymagają przewalutowania	
	a) przelew TARGET	a) przelew TARGET
17:00 (od poniedziałku do piątku)	Zlecenia, które nie wymagają przewalutowania	
	a) przelew walutowy poza krajem b) polecenie przelewu SEPA c) polecenie przelewu w walucie obcej	a) przelew walutowy poza krajem b) polecenie przelewu SEPA c) polecenie przelewu w walucie obcej
	Zlecenia, które wymagają przewalutowania	
	a) przelew krajowy b) przelew walutowy poza krajem c) polecenie przelewu SEPA d) polecenie przelewu w walucie obcej	a) przelew krajowy b) przelew walutowy poza krajem c) polecenie przelewu SEPA d) polecenie przelewu w walucie obcej
19:00 (od poniedziałku do piątku)	Zlecenia, które wymagają przewalutowania	
	a) polecenie przelewu wewnętrznego w PLN b) polecenie przelewu wewnętrznego w walutach obcych	a) polecenie przelewu wewnętrznego w PLN b) polecenie przelewu wewnętrznego w walutach obcych

ODWOŁYWANIE PRZELEWÓW ZŁOŻONYCH PRZEZ SYSTEM BANKOWOŚCI INTERNETOWEJ

Rodzaj przelewu który można odwołać - z bieżącą datą realizacji	Kiedy można odwołać przelew
Użytkownik może odwołać w Systemie bankowości internetowej przelew z rachunków oszczędnościowo-rozliczeniowych złożony przez ten System, za wyjątkiem przelewów z bieżącą datą realizacji inicjowanych przez dostawcę świadczącego usługę inicjowania transakcji płatniczej	
• przelew krajowy, który nie wymaga przewalutowania i nie jest realizowany w czasie rzeczywistym oraz nie jest złożony jako przelew w ramach usługi „Płać z ING	• złożony **od godziny 00:01 do 8:15 od poniedziałku do piątku** można odwołać do godziny 9:00 w dniu złożenia przelewu • złożony **od godziny 8:16 do 11:35 od poniedziałku do piątku** można odwołać do godziny 13:00 w dniu złożenia przelewu • złożony **od godziny 11:36 do 14:45 od poniedziałku do piątku** można odwołać do godziny 15:30 w dniu złożenia przelewu • złożony **od godziny 14:46 do 24:00 od poniedziałku do piątku** można odwołać do godziny 9:00 najbliższego dnia roboczego • złożony **od godziny 00:01 do 24:00 w sobotę, niedzielę lub w dniu ustawowo wolnym od pracy Banku** można odwołać do godziny 9:00 najbliższego dnia roboczego
• przelew TARGET • przelew krajowy, który wymaga przewalutowania • przelew walutowy poza krajem • polecenie przelewu SEPA • polecenie przelewu w walucie obcej	• złożony **od godziny 17:01 do 24:00 od poniedziałku do piątku** można odwołać do początku najbliższego dnia roboczego (do godziny 00:00) • złożony **od godziny 00:01 w sobotę, niedzielę lub w dniu ustawowo wolnym od pracy Banku** można odwołać do początku najbliższego dnia roboczego (do godziny 00:00)
• polecenie przelewu wewnętrznego, które wymaga przewalutowania	• złożony **od godziny 19:01 do 24:00 od poniedziałku do piątku** można odwołać do początku najbliższego dnia roboczego (do godziny 00:00) • złożony **od godziny 00:01 w sobotę, niedzielę lub w dniu ustawowo wolnym od pracy Banku** można odwołać do początku najbliższego dnia roboczego (do godziny 00:00)

Środki pieniężne z tytułu odwołanego przelewu zwrócimy na rachunek najpóźniej w najbliższym dniu roboczym.