Spółdzielcza Grupa Bankowa

Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu

§ 1

1. Niniejszy załącznik do „Regulaminu świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów instytucjonalnych” określa prawa i obowiązki użytkowników instrumentów płatniczych.
2. Przez określenia użyte w niniejszym załączniku do regulaminu należy rozumieć:
   1) adres elektroniczny – oznaczenie systemu teleinformatycznego umożliwiającego porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności adresu poczty elektronicznej e-mail w sieci Internet;
   2) elektroniczny kanał dostępu – sposób komunikacji posiadacza rachunku z Bankiem lub Banku z posiadaczem na odległość, za pośrednictwem sieci teleinformatycznej lub urządzeń elektronicznych, obejmujący w szczególności: usługi bankowości elektronicznej (serwis internetowy) Internet Banking/Internet Banking dla Firm, powiadamianie SMS (serwis SMS Banking), lub inny znajdujący się w ofercie Banku;
   3) instrukcja użytkownika – dokument, w tym dokument w postaci elektronicznej, zawierający opis poszczególnych elektronicznych kanałów dostępu i zasady dotyczące prawidłowego posługiwania się tymi kanałami przez klienta instytucjonalnego;
   4) klucz zabezpieczający U2F/klucz sprzętowy – Universal 2 Factor, urządzenie zewnętrzne służące do silnego uwierzytelnienia
   5) pay by link – system, który automatycznie generuje w bankowości elektronicznej gotową dyspozycje przelewu, która po zatwierdzeniu przez klienta jest realizowana przez Bank;
   6) przelew typu pay by link – przelew realizowany przez klienta dokonującego zapłaty z tytułu zakupów w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem Integratorów płatności internetowych, w taki sposób, że klient wybiera jako formę płatności z tytułu zakupu przelew ze swojego rachunku bankowego, a następnie po przekserowaniu do usług bankowości elektronicznej Banku i zalogowaniu się otrzymuje wypełniony (kwota, tytuł przelewu i danymi odbiorcy) formularz przelewu po czym po dokonaniu autoryzacji przelewu powraca na strony internetowe sklepu lub Integratora płatności internetowych;
   7) system – system teleinformatyczny, służący do przekazywania posiadaczowi rachunku informacji związanych z obsługą jego rachunków oraz tworzenia i wymiany elektronicznych komunikatów pozwalających posiadaczowi rachunku na przygotowanie dyspozycji oraz przesłanie ich do Banku;
   8) indywidualne dane uwierzytelniające – indywidualne dane zapewniane użytkownikowi przez dostawcę usług płatniczych do celów uwierzytelniania;
   9) uwierzytelnianie – procedurę umożliwiającą Bankowi weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających;
   10) użytkownik systemu – odpowiednio posiadacza rachunku lub pełnomocnika, który został przez posiadacza rachunku umocowany do dysponowania rachunkiem za pośrednictwem elektronicznych kanałów dostępu i który otrzymał oAd Banku środki identyfikacji elektronicznej, także osobę korzystającą z biometrii.

Rozdział 1. Udostępnienie i warunki korzystania z elektronicznych kanałów dostępu

§ 2

1. Bank może świadczyć usługi w zakresie obsługi produktów i usług za pośrednictwem następujących elektronicznych kanałów dostępu:

1) w ramach bankowości elektronicznej - bankowość internetowa (serwis internetowy)
- dostęp i dyspozycje składane na komputerze lub urządzeniu mobilnym przy użyciu przeglądarki internetowej;

2) powiadomienia SMS (serwis SMS) – uzyskiwanie informacji związanych z transakcjami na rachunku w formie SMS oraz aktualnym saldzie rachunku;

3) innego kanału oferowanego przez Bank, jeżeli umowa umożliwia korzystanie z innego kanału.

3.1 Bank udostępnia wszystkim użytkownikom bankowości elektronicznej możliwość stosowania klucza zabezpieczającego U2F/klucza sprzętowego jako formy zabezpieczeń bankowości elektronicznej chroniącej przed phishingiem i wyłudzeniami danych do logowania zgodnie z Regulaminem ***korzystania z funkcji dwuetapowego logowania kluczami U2F w Banku Spółdzielczym w Człuchowie***, Link do dokumentu, o którym mowa w niniejszym punkcie Bank udostępnia na stronie internetowej *www.bsczluchow.pl*.

3.2 Metoda zabezpieczeń o której mowa w ust. 3.1 nie jest obligatoryjna dla Użytkowników bankowości elektronicznej, ale zalecana do stosowania.

2. Bank umożliwia dostęp do informacji o produktach i usługach oraz kontakt z konsultantami Banku przez Call Center. Wszystkie rozmowy prowadzone przez Call Center są nagrywane.

3. Wykaz produktów i usług dostępnych za pośrednictwem elektronicznych kanałów dostępu oraz warunki korzystania z usług określa instrukcja użytkownika. Instrukcja użytkownika zawiera opis poszczególnych elektronicznych kanałów dostępu, wymagania techniczne każdego kanału i zasady prawidłowego posługiwania się tymi kanałami przez klienta.

4. Serwis internetowy, o którym mowa w ust. 1 pkt 1, jest dostępny w dwóch wariantach:

1) wariant I - z jednoosobową autoryzacją dyspozycji;

2) wariant II - z wieloosobową autoryzacją dyspozycji dla wszystkich rodzajów dyspozycji, z zastosowaniem wymaganych przez Bank metod uwierzytelniania.

§ 3

1. Usługi bankowości elektronicznej mogą być udostępniane wyłącznie w przypadku posiadania przez posiadacza rachunku bieżącego prowadzonego w złotych; Bank może udostępnić elektroniczne kanały dostępu dla posiadaczy innych rachunków bez wymogu posiadania wyżej wymienionych produktów, o czym poinformuje na stronie internetowej Banku.

2. Posiadacz rachunku może wnioskować o udostępnienie kolejnych produktów lub usług oraz zmianę warunków świadczenia tych produktów lub usług i zawierać umowy za pośrednictwem elektronicznych kanałów dostępu o ile taki sposób został udostępniony przez Bank.

§ 4

1. Użytkownik uzyskuje dostęp do bankowości elektronicznej za pomocą indywidualnych danych uwierzytelniających z zastrzeżeniem § 11.
2. Bank może umożliwić korzystanie z usługi przy użyciu tych samych indywidualnych danych uwierzytelniających, użytkownikowi będącemu równocześnie posiadaczem/pełnomocnikiem do innego rachunku, z uwzględnieniem limitów operacji, o których mowa w Rozdziale 8.

§ 5

1. W przypadku korzystania i dokonywania transakcji z wykorzystaniem bankowości elektronicznej:
   1) zaleca się korzystanie z zaufanych komputerów posiadających aktualne oprogramowanie antywirusowe;
   2) należy sprawdzić czy transmisja jest szyfrowana protokołem SSL (ang. SecureSocket Layer), który zapewnia poufność i integralność transmisji danych;
   3) nie należy korzystać z otwartych i niezabezpieczonych sieci.
2. Użytkownikiem niebędącym posiadaczem rachunku, może być wyłącznie osoba, której posiadacz rachunku udzielił pełnomocnictwa stałego, chyba że z treści umowy wynika inaczej.
3. Warunkiem korzystania z usługi jest obsługa plików *cookies* w przeglądarce internetowej, które są konieczne do utrzymania aktywnej sesji po zalogowaniu do bankowości elektronicznej; szczegółowe informacje dotyczące rodzaju stosowanych plików *cookies* oraz celu ich wykorzystywania dostępne są na stronie internetowej Banku.

§ 6

1. Użytkownik systemu ma obowiązek korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem i instrukcją użytkownika oraz zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób nieuprawnionych i zapewnienia poufności tych środków lub danych w nich zawartych.
2. Użytkownik uzyskuje dostęp do rachunku za pomocą udostępnionych mu indywidualnych danych uwierzytelniających.
3. Z chwilą otrzymania indywidualnych danych uwierzytelniających, użytkownik podejmuje niezbędne środki służące zapobieżeniu naruszenia indywidualnych danych uwierzytelniających, w szczególności, że przyjmuje do wiadomości, że ze względów bezpieczeństwa, poszczególnych indywidualnych danych uwierzytelniających nie wolno przechowywać razem ze sobą.
4. Bank zapewnia należytą ochronę indywidualnych danych uwierzytelniających. Indywidualne dane uwierzytelniające są dostępne wyłącznie dla użytkownika uprawnionego do korzystania z nich.

§ 7

Zmiana zakresu usługi przez Bank wymaga zachowania warunków i trybu przewidzianego dla zmiany regulaminu.

Rozdział 2. Dyspozycje składane za pośrednictwem elektronicznych kanałów dostępu

§ 8

1. Wszelkie oświadczenia woli składane wobec Banku przez użytkownika systemu w postaci elektronicznej będą ważne i wiążące pod względem prawnym dla posiadacza rachunku, jeżeli przy użyciu środków identyfikacji elektronicznej dokonana została poprawna identyfikacja użytkownika

systemu składającego oświadczenie woli, z zastosowaniem wymaganych przez Bank metod uwierzytelniania, przy uwzględnieniu wymogów silnego uwierzytelniania.

§ 9

Zakres operacji udostępnianych użytkownikowi systemu przez Bank w ramach usługi może obejmować:

1) dokonywanie operacji biernych, w tym w szczególności:
- **a)** uzyskiwanie ogólnie dostępnych informacji o usługach bankowych, zasadach bezpiecznego użytkowania karty, systemu itp.;
- **b)** uzyskiwanie informacji o rachunkach bankowych, w tym kredytowych; posiadanych w Banku oraz operacjach dostępnych dla tych rachunków;
- **c)** uzyskiwanie powiadomień SMS o operacjach przeprowadzonych na rachunku oraz o aktualnym saldzie rachunku, jak również uzyskiwanie kodów służących do autoryzacji dyspozycji złożonych za pośrednictwem elektronicznych kanałów dostępu;
- **d)** otrzymywanie zawiadomień o dokonanych przez Bank zmianach w treści umowy, regulaminu lub Taryfy, a także o zmianach wprowadzonych w systemie, mających wpływ na zmianę dotychczasowego trybu dokonywania operacji biernych lub aktywnych;

2) dokonywanie operacji aktywnych, w tym w szczególności:
- **a)** składanie, zmianę dyspozycji płatniczych z rachunków, o których mowa w pkt 1 lit. b, na inne rachunki bankowe w Banku lub w innych bankach w kraju i zagranicą, z wyłączeniem rachunków kredytowych;
- **b)** odwoływanie niewykonanych jeszcze przez Bank dyspozycji płatniczych z odroczonym terminem realizacji;
- **c)** tworzenie, zmianę listy zdefiniowanych odbiorców (baza kontrahentów);
- **d)** składanie, zmianę zleceń stałych;
- **e)** odwoływanie niewykonanych jeszcze przez Bank zleceń stałych;
- **f)** pobieranie wydruku potwierdzenia wykonania operacji;
- **g)** składanie oświadczeń woli o otwarciu lub zamknięciu rachunku lokaty w ramach umowy i w granicach dostępnych środków na rachunku;
- **h)** składanie, zmianę lub odwoływanie dyspozycji zablokowania dostępu do systemu;
- **i)** zastrzeganie kart;

3) dokonywanie innych czynności z Bankiem, w tym w szczególności:
- **a)** dokonywanie zmiany danych zawartych w odpowiednim środku identyfikacji elektronicznej (zmiana hasła stałego) – w odniesieniu do środków, w przypadku których taka zmiana jest możliwa;
- **b)** składanie zamówienia na nowe indywidualne dane uwierzytelniające;
- **c)** pobierania plików udostępnionych przez Bank;
- **d)** zmiana sposobu autoryzacji z mobilnej na hasła SMS w przypadku utraty dostępu do aplikacji mobilnej „Nasz Bank”, po udzieleniu odpowiedzi na dodatkowe pytania weryfikacyjne;
- **e)** składanie wniosków o zmianę limitu pojedynczej transakcji/sumy transakcji dziennych;
- **f)** składanie wniosków o instrument płatniczy;
- **g)** składanie wniosków o anulowanie przelewu.[1]

o ile czynności te mieszczą się w zakresie funkcjonalności aktywowanych elektronicznych kanałów dostępu; aktualny zakres funkcjonalności poszczególnych elektronicznych kanałów dostępu

[1] Nie dotyczy Internet Banking dla Firm.

określa instrukcja użytkownika.

§ 10

1. Do dysponowania rachunkami za pośrednictwem elektronicznych kanałów dostępu mają zastosowanie ogólne zasady dotyczące dysponowania rachunkami określone w Rozdziale 2 regulaminu, dotyczące poszczególnych rodzajów rachunków, z zastrzeżeniem postanowień §§ 11 - 15 niniejszego załącznika oraz sposobu posługiwania się danym elektronicznym kanałem dostępu opisanym w instrukcji użytkownika oraz umowie.
2. Bank świadczy usługę oferowania przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link, przy czym:
   1) integratorem płatności internetowych jest podmiot świadczący usługi sklepom internetowym lub innym podmiotom prowadzącym sprzedaż towarów lub usług, polegające na udostępnieniu im możliwości przyjmowania płatności od ich klientów za pomocą przelewów typu pay by link,
   2) przelew typu [ay by link jest realizowany przez klienta dokonującego zapłaty za zakupy w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem integratorów płatności internetowych.
3. Zgody na wykonanie transakcji płatniczej użytkownik systemu może udzielić również za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej.
4. W przypadku inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji lub przez odbiorcę lub za jego pośrednictwem, posiadacz rachunku nie może odwołać zlecenia płatniczego po udzieleniu dostawcy świadczącemu usługę inicjowania transakcji, zgody na zainicjowanie transakcji albo po udzieleniu odbiorcy zgody na wykonanie transakcji.
5. Bank umożliwia w serwisie internetowym:
   1) składanie wniosków udostępnionych przez Bank dotyczących produktów lub usług na zasadach określonych w § 9,
   2) składanie wniosków o zainstalowanie terminala POS.

   Bank może udostępnić w serwisie internetowym inne wnioski.

§ 11

1. Wszelkie dyspozycje i zlecenia płatnicze w bankowości elektronicznej, użytkownik systemu składa Bankowi w postaci elektronicznej, po jego uwierzytelnieniu, w sposób umożliwiający Bankowi jego identyfikację i zapoznanie się z treścią dyspozycji; wyżej wymienione dyspozycje spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi (zgodnie z art. 7 ustawy Prawo bankowe).
2. Po złożeniu dyspozycji lub zlecenia płatniczego w bankowości elektronicznej, użytkownik dokonuje ich autoryzacji przy użyciu indywidualnych danych uwierzytelniających, z zastosowaniem wymaganych przez Bank metod uwierzytelniania, z zastrzeżeniem ust. 3.
3. Bank stosuje silne uwierzytelnianie, w przypadku gdy użytkownik:
   1) uzyskuje dostęp do swojego rachunku w trybie on-line;
   2) inicjuje transakcję płatniczą;
   3) przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć,

   za wyjątkiem sytuacji nie wymagających silnego uwierzytelniania wskazanych w ust. 4.
4. Bank może nie stosować silnego uwierzytelniania w następujących przypadkach:
   1) dostępu użytkownika systemu do jednej z wymienionych niżej pozycji w trybie on-line lub do obu tych pozycji bez ujawniania szczególnie chronionych danych dotyczących płatności:
      a) salda rachunku;
      b) transakcji płatniczych przeprowadzonych w ciągu ostatnich 90 dni za pośrednictwem rachunku z zastrzeżeniem ust. 5;

2) inicjowania transakcji, której odbiorca znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez użytkownika;

3) inicjowania kolejnych transakcji należących do serii transakcji cyklicznych, opiewających na tę samą kwotę na rzecz tego samego odbiorcy pod warunkiem, że utworzenie, zmiana lub zainicjowanie pierwszej transakcji cyklicznej odbyło się przy zastosowaniu silnego uwierzytelnienia;;

4) jeżeli użytkownik inicjuje transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i oba rachunku płatnicze są prowadzone przez Bank;

5) inicjowania zdalnej transakcji, którą Bank uzna za charakteryzującą się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji.

5. Bank stosuje silne uwierzytelnianie użytkownika, jeżeli spełniony jest którykolwiek z następujących warunków:

1) użytkownik systemu uzyskuje dostęp do informacji określonych w ust. 4 pkt 1 lit.a, w trybie online po raz pierwszy;

2) minęło więcej niż 90 dni odkąd użytkownik systemu po raz ostatni uzyskał dostęp do informacji określonych w ust. 4 pkt 1 lit. b w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie użytkownika systemu.

6. Bank zastrzega sobie prawo skontaktowania się z użytkownikiem w celu realizacji zlecenia płatniczego.

7. Dostęp użytkownika do serwisu internetowego następuje poprzez podanie identyfikatora użytkownika oraz udostępnionych użytkownikowi/pasywnemu użytkownikowi indywidualnych danych uwierzytelniających, o których mowa w ust. 8.

8. Dostęp oraz autoryzacja dyspozycji składanych za pośrednictwem serwisu internetowego przez użytkownika, odbywa się poprzez użycie następujących indywidualnych danych uwierzytelniających:

1) dla wariantu I, o którym mowa w § 1 ust. 3 pkt 1, poprzez podanie:

a) kodu SMS oraz kodu uwierzytelniającego,

b) e-PIN-u przypisanego do aplikacji mobilnej,

2) dla wariantu II, o którym mowa w § 1 ust. 3 pkt 2 poprzez użycie:

a) kodu SMS oraz kodu uwierzytelniającego,

b) e-PIN-u przypisanego do aplikacji mobilnej,

c) aplikacji nPodpis wraz z kartą chipową oraz numerem PIN,

chyba że Bank udostępni inne indywidualne dane uwierzytelniające, które są opisane w instrukcji użytkownika.

9. Autoryzacja dyspozycji składanych za pośrednictwem elektronicznego kanału dostępu, o którym mowa w § 1 ust. 1 pkt. 3, odbywa się poprzez podanie, za pośrednictwem telefonu z funkcją wybierania tonowego, identyfikatora oraz hasła stałego.

10. Jeżeli użytkownik, podczas procesu logowania się do bankowości internetowej doda urzadzenie, z którego loguje się do bankowości internetowej jako urzadzenie zaufane, kolejne logowania z tego urządzenia do bankowości internetowej w przeglądarce nie będą wymagały dodatkowego uwierzytelnienia użytkownika za pomoca kodów SMS,. Urzadzeniem zaufanym może być np. prywatny komputer, smartfon lub tablet, z którego korzysta wyłacznie użytkownik. Bank podczas procesu logowania weryfikuje określone cechy tego urzadzenia.

11. Użytkownik w dowolnym momencie ma możliwość poprzez bankowość internetową usunięcia swojego urzadzenia zaufanego, a każde kolejne logowanie do bankowości internetowej bedzie wymagało dodatkowego potwierdzenia w postaci kodów otrzymywanych poprzez wiadomości SMS.

12. Autoryzacja dokonana przez użytkownika systemu jest równoznaczna z poleceniem, złożonym Bankowi dokonania określonej czynności i stanowi podstawę jej dokonania przez Bank.

13. Bank przesyła kody autoryzacyjne wykorzystywane przy stosowanych metodach uwierzytelniania na numer telefonu komórkowego, który użytkownik wskazał w umowie, we wniosku o otwarcie rachunku lub druku pełnomocnictwa.

14. Bank może wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających poprzez udostępnienie ich użytkownikowi oraz zawiadomienie go o dokonanej zmianie; informacja o rodzajach stosowanych indywidualnych danych uwierzytelniających jest zamieszczona w instrukcji użytkownika udostępnianej na podstronie do logowania.

15. Użytkownik może zmienić stosowaną metodę autoryzacji na inną metodę za pośrednictwem Call Center, jeśli wskazał w Banku numer telefonu komórkowego, o którym mowa w ust. 13.

§ 12

Jeżeli z postanowień umowy, regulaminu lub obowiązujących przepisów prawa nie wynika nic innego, chwilą złożenia przez użytkownika oświadczenia w postaci elektronicznej, w szczególności złożenia dyspozycji lub dokonania jakiejkolwiek czynności faktycznej, jest moment zarejestrowania odpowiednich danych w systemie bankowości elektronicznej i przyjęcia tego oświadczenia przez serwer Banku.

§ 13

1. Realizacja dyspozycji składanych za pośrednictwem bankowości elektronicznej odbywa się drogą elektroniczną, przy czym użytkownik zobowiązuje się do stosowania zasad autoryzacji obowiązujących dla tego elektronicznego kanału dostępu.

2. Autoryzowane zlecenie płatnicze nie może zostać odwołane, za wyjątkiem sytuacji, o których mowa w § 24 ust. 6-9 regulaminu.

§ 14

1. Przyjęcie do realizacji dyspozycji złożonej za pośrednictwem elektronicznych kanałów dostępu Bank potwierdza w formie informacji wysyłanej za pośrednictwem tego kanału.

2. W przypadku nieprzyjęcia przez Bank dyspozycji złożonej za pośrednictwem elektronicznych kanałów dostępu z powodu:
   1) jej niekompletności;
   2) złożenia dyspozycji sprzecznych ze sobą;
   3) podania nieprawidłowego numeru rachunku odbiorcy;
   4) braku środków pieniężnych dla realizacji dyspozycji;
   5) innych okoliczności uniemożliwiających jej przyjęcie przez Bank,

   użytkownik otrzyma informację o fakcie i przyczynie niezrealizowania dyspozycji w formie właściwej dla danego elektronicznego kanału dostępu lub od pracownika placówki Banku.

§ 15

1. Bank ma prawo odmowy wykonania dyspozycji złożonej i uwierzytelnionej w bankowości elektronicznej w przypadku:
   1) gdy zaistniałe okoliczności uzasadniają wątpliwości, co do:
      a) złożenia lub autoryzacji dyspozycji przez użytkownika,
      b) zgodności dyspozycji z obowiązującymi przepisami prawa,
   2) gdy kwota lub kwoty dyspozycji oraz należne bankowi prowizje i opłaty przekraczają dostępne środki.

2. Bank ma prawo odmowy wykonania lub wprowadzenia dodatkowych ograniczeń i zabezpieczeń w stosunku do dyspozycji składanych za pośrednictwem elektronicznych kanałów dostępu, w przypadku wystąpienia ważnych okoliczności uniemożliwiających wykonanie tych dyspozycji, tj. względów bezpieczeństwa lub sprzeczności treści dyspozycji z wiążącymi użytkownika systemu postanowieniami umów zawartych z Bankiem.

Rozdział 3. Korzystanie z usług bankowości elektronicznej

§ 16

Za pośrednictwem elektronicznych kanałów dostępu, użytkownik uzyskuje dostęp do wszystkich rachunków otwartych przed dniem aktywowania usługi oraz do rachunków otwartych w terminie późniejszym, chyba że posiadacz rachunku zawnioskował ograniczony dostęp do rachunków, za pośrednictwem elektronicznych kanałów dostępu.

Rozdział 4. Ograniczenia w korzystaniu z usług bankowości elektronicznej

§ 17

1. Bank jest zobowiązany zablokować dostęp do bankowości elektronicznej, uniemożliwiając tym samym wykonanie transakcji w jednym z następujących przypadków:
   1) złożenia przez użytkownika dyspozycji zablokowania dostępu do serwisu internetowego;
   2) zastrzeżenia indywidualnych danych uwierzytelniających;
   3) powzięcia podejrzenia, iż osoba trzecia mogła uzyskać dostęp do indywidualnych danych uwierzytelniających, logowaniem z adresów IP z czarnej listy lub realizacją przelewów na rachunki z czarnej listy, zgodnie z obowiązującymi w Banku procedurami;
   4) kolejnego trzykrotnego wpisania nieprawidłowego hasła stałego do systemu.

2. Bank ma prawo częściowo ograniczyć lub zablokować dostęp do bankowości elektronicznej i/lub czasowo zablokować wykonanie dyspozycji w następujących przypadkach:
   1) uzasadnionych przyczyn związanych z bezpieczeństwem dostępu do serwisu internetowego i indywidualnych danych uwierzytelniających, w tym w przypadku podejrzenia popełnienia przestępstwa na szkodę użytkownika;
   2) umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej przez użytkownika lub uzasadnionego podejrzenia, że użytkownik będzie posługiwał się dostępem w sposób niezgodny z regulaminem;
   3) korzystania przez użytkownika z bankowości internetowej niezgodnie z zasadami bezpieczeństwa określonymi w niniejszym załączniku lub w sposób zagrażający bezpieczeństwu korzystania z bankowości internetowej;
   4) w związku z wystąpieniem restrykcji geolokalizacyjnych lub realizacją przelewów na rachunki z szarej listy, zgodnie z obowiązującymi w Banku regulacjami;
   5) dokonywania czynności konserwacyjnych bankowości elektronicznej lub innych systemów teleinformatycznych związanych z wykonaniem umowy, o czym Bank z wyprzedzeniem poinformuje na stronie internetowej Banku;
   6) dokonywania czynności mających na celu usunięcie awarii, usterek lub nieprawidłowości działania bankowości elektronicznej lub innych systemów teleinformatycznych związanych z wykonywaniem umowy;
   7) wymiany stosowanych indywidualnych danych uwierzytelniających, o czym Bank z wyprzedzeniem poinformuje użytkowników w sposób określony w umowie oraz na stronie internetowej Banku.
   8) uzasadnionego podejrzenia, iż transakcje na rachunku klienta mają związek z popełnieniem przestępstwa związanego z praniem pieniędzy lub finansowaniem terroryzmu;
   9) gdy na rachunku klienta wystąpi zamrożenie wartości majątkowych;
   10) braku możliwości zastosowania środków bezpieczeństwa finansowego.

3. Bank może uchylić ograniczenie albo blokadę dostępu do bankowości elektronicznej w przypadku, o którym mowa w ust. 2 pkt 1) jeżeli na wniosek złożony przez posiadacza rachunku, w sposób określony w ust. 4. W takim przypadku Bank wydaje użytkownikowi nowe indywidualne dane uwierzytelniające lub dokona uchylenia ograniczenia lub blokady przy zachowaniu dotychczasowych danych uwierzytelniających. Bank wyda użytkownikowi nowe indywidualne dane uwierzytelniające, umożliwiające bezpieczne korzystanie z usługi.

4. W przypadku, o którym mowa w ust. 2 pkt 1) uchylenie:
   1) ograniczenia lub blokady dostępu do bankowości elektronicznej następuje na podstawie telefonicznej lub złożonej w siedzibie lub dowolnej placówce Banku dyspozycji klienta;
   2) czasowej blokady dyspozycji następuje po telefonicznym lub pisemnym kontakcie pracownika Banku z klientem i po potwierdzeniu przez klienta złożonej dyspozycji.

5. Z zastrzeżeniem ust. 6 Bank informuje użytkownika o zamiarze zablokowania indywidualnych danych uwierzytelniających w przypadkach okreslonych w ust. 2 pkt 1) 3), przed ich zablokowaniem, a jeżeli nie jest to możliwe – niezwłocznie po zablokowaniu telefonicznie.

6. Bank nie przekazuje informacji o zablokowaniu, jezeli przekazanie tej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.

7. W przypadkach, o których mowa w ust. 2 pkt 4-6) ograniczenie lub blokada dostepu do serwisu internetowego i/lub czasowa blokada dyspozycji nastepuje przez możliwie krótki okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.

Rozdział 5. Blokowanie i zastrzeganie dostępu do serwisu internetowego

§ 18

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowany przez:
   1) Bank - zgodnie z postanowieniami § 20;
   2) użytkownika.

2. Na wniosek posiadacza rachunku Bank może zablokować dostęp do usługi bankowości elektronicznej uniemożliwiając jednocześnie dokonywanie transakcji przez wszystkich użytkowników.

§ 19

1. W przypadku utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia indywidualnych danych uwierzytelniających lub nieuprawnionego dostępu do serwisu internetowego jego użytkownik powinien go niezwłocznie telefonicznie zastrzec, podając swoje dane personalne.

2. Zastrzeżenia, o którym mowa w ust. 1, można dokonywać osobiście w placówce Banku prowadzącej rachunek lub pod numerami telefonów wskazanymi przez Bank w komunikacie zamieszczonym w placówkach Banku lub na stronie internetowej Banku, a także za pośrednictwem udostępnionego przez Bank elektronicznego kanału dostępu.

3. Bank ma prawo do zmiany numerów, pod którymi dokonywane są zastrzeżenia; w razie skorzystania z tego uprawnienia, Bank powiadomi użytkownika o dokonanej zmianie drogą elektroniczną na adres poczty elektronicznej (e-mail) wskazany przez posiadacza rachunku lub w formie komunikatu przekazanego za pośrednictwem właściwego elektronicznego kanału dostępu oraz na wyciągach bankowych.

4. Zastrzeżenie, o którym mowa w ust. 1, nie może być odwołane i powoduje niemożność dalszego dostępu do serwisu internetowego.

5. W przypadku utraty indywidualnych danych uwierzytelniających oraz ich zastrzeżenia posiadacz rachunku może wystąpić z wnioskiem o wydanie nowych indywidualnych danych uwierzytelniających.

6. W przypadku utraty, kradzieży, przywłaszczenia lub stwierdzenia nieuprawnionego użycia telefonu komórkowego, który jest oznaczony, jako telefon do autoryzacji lub zmiany numeru telefonu do autoryzacji, użytkownik jest zobowiązany do dokonania zmiany danych zgodnie z zapisami ust. 7.

7. W przypadku, gdy użytkownik chce zmienić dotychczasowe dane niezbędne do otrzymywania kodów autoryzacyjnych SMS na nowe dane konieczne jest złożenie niezbędnej dyspozycji w Banku.

8. Do chwili otrzymania powiadomienia, o którym mowa w ust. 1, Bank nie ponosi odpowiedzialności za informacje uzyskane przez osoby trzecie lub operacje wykonane przez Bank na podstawie dyspozycji złożonych przez te osoby, jeżeli w wyniku nieuprawnionego użycia przez te osoby indywidualnych danych uwierzytelniających, system bankowy zidentyfikował podmiot składający oświadczenie woli, jako uprawniony do złożenia takiego oświadczenia woli zgodnie z umową.

9. Użytkownik ponosi odpowiedzialność za wszelkie skutki będące następstwem użycia przez osoby nieuprawnione indywidualnych danych uwierzytelniających lub niedopełnienia przez użytkownika obowiązków, o których mowa w niniejszym paragrafie.

§ 20

1. Bank ma prawo do zastrzeżenia indywidualnych danych uwierzytelniających:
   1) w przypadku wygaśnięcia lub rozwiązania umowy;
   2) z uzasadnionych przyczyn związanych z bezpieczeństwem indywidualnych danych uwierzytelniających, tzn. powzięcia informacji o wejściu w ich posiadanie osób nieuprawnionych;
   3) w związku z podejrzeniem nieuprawnionego użycia indywidualnych danych uwierzytelniających lub umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej.

2. Z zastrzeżeniem ust. 3, Bank informuje posiadacza rachunku o zamiarze zastrzeżenia indywidualnych danych uwierzytelniających w przypadkach określonych w ust. 1 pkt 2-3, przed ich zastrzeżeniem, a jeżeli nie jest to możliwe – niezwłocznie po jego zastrzeżeniu, telefonicznie lub faksem.

3. Bank nie przekazuje informacji o zastrzeżeniu, jeżeli przekazanie tej informacji byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.

Rozdział 6. Urządzenie zaufane

§ 21

1. Użytkownik system bankowości elektronicznej może zdefiniować urządzenie, z którego następuje logowanie do bankowości elektronicznej jako urządzenie zaufane.

2. Dodanie urządzenia przez użytkownika systemu wymaga:
   1) autoryzacji za pośrednictwem udostępnionej użytkownikowi autoryzacji, o której mowa w § 11 ust. 8,
   2) akceptacji oświadczenia, iż klient jest jedynym użytkownikiem urządzenia i wyraża zgodę na dodanie urządzenia jako zaufanego na potrzeby silnego uwierzytelnienia podczas logowania do system bankowości elektronicznej,
   3) akceptacji niniejszych zasad.

Rozdział 7. Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku. Potwierdzanie dostępności środków na rachunku

§ 22

1. Bank może udostępnić dostawcy świadczącemu usługi dostępu do informacji o rachunku, na podstawie wyrażonej przez użytkownika korzystającego z serwisu internetowego, zgody na dostęp do informacji o rachunku oraz transakcjach na tym rachunku.
2. Dostęp do informacji na rachunku, o którym mowa w ust. 1, jest również możliwy w przypadku dostawców inicjujących transakcję płatniczą dla użytkowników korzystających z serwisu internetowego.
3. Bank na wniosek dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej, niezwłocznie potwierdza dostępność na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej realizowanej w oparciu o tę kartę jeżeli:
   1) rachunek płatniczy użytkownika jest dostępny on-line w momencie występowania z wnioskiem oraz
   2) użytkownik udzielił Bankowi zgody na udzielanie odpowiedzi na wnioski dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej dotyczące potwierdzenia, że kwota odpowiadająca kwocie określonej w transakcji płatniczej realizowanej w oparciu o tę kartę jest dostępna na rachunku płatniczych użytkownika oraz
   3) zgoda, o której mowa w pkt 2, została udzielona przed wystąpieniem z pierwszym wnioskiem dotyczącym potwierdzenia.
4. Dostawca wydający instrumenty płatnicze oparte na karcie płatniczej może wystąpić z wnioskiem, o którym mowa w ust. 3 jeżeli:
   1) użytkownik udzielił temu dostawcy zgody na występowanie z wnioskiem, o którym mowa w ust. 3, oraz
   2) użytkownik bankowości elektronicznej zainicjował transakcję płatnicza realizowaną w oparciu o kartę płatniczą na daną kwotę przy użyciu instrumentu płatniczego opartego na tej karcie wydanego przez danego dostawcę, oraz
   3) dostawca uwierzytelnia siebie wobec Banku przed złożeniem wniosku, o którym mowa w ust. 3 oraz w sposób bezpieczny porozumiewa się z Bankiem.
5. Potwierdzenie, o którym mowa w ust. 3, polega na udzieleniu odpowiedzi „tak” albo „nie” i nie obejmuje podania salda rachunku. Odpowiedzi nie przechowuje się ani nie wykorzystuje do celów innych niż wykonanie transakcji płatniczej realizowanej w oparciu o kartę płatniczą.
6. Potwierdzenie, o którym mowa w ust. 3, nie umożliwia Bankowi dokonania blokady środków pieniężnych na rachunku płatniczym płatnika.
7. Użytkownik może zwrócić się do Banku o przekazanie mu danych identyfikujących dostawcę, o którym mowa w ust. 4, oraz udzielonej odpowiedzi, o której mowa w ust. 5.
8. 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 przez takiego dostawcę, w tym nieuprawnionym zainicjowaniem transakcji płatniczej. W takim przypadku Bank w uzgodniony sposób informuje płatnika o odmowie dostępu do rachunku i jej przyczynach. Informacja ta, o ile jest to możliwe, jest przekazywana płatnikowi 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 jej sprzeczne z odrębnymi przepisami. Bank umożliwia dostawcy świadczącemu usługę dostępu do informacji o rachunku oraz dostawcy świadczącemu usługę inicjowania transakcji płatniczej dostęp do rachunku płatniczego niezwłocznie po ustaniu przyczyn uzasadniających odmowę.

Rozdział 8. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia

§ 23

1. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem bankowości elektronicznej w walucie PLN.

Rodzaj podmiotu	Standardowy limit pojedynczej transakcji obowiązujący w Banku	Indywidualny limit pojedynczej transakcji ustalony na wniosek posiadacza rachunku[2]	Standardowy limit sumy transakcji dziennych obowiązujący w Banku	Indywidualny limit sumy transakcji dziennych ustalony na wniosek posiadacza rachunku[3]
Przedsiębiorstwa / spółki państwowe	**50 000,00 zł**	**do 150 000,00 zł**	**50 000,00 zł**	**do 150 000,00 zł**
Przedsiębiorstwa / spółki prywatne oraz spółdzielnie	**50 000,00 zł**	**do 150 000,00 zł**	**100 000,00 zł**	**do 150 000,00 zł**
Rolnicy indywidualni	**50 000,00 zł**	**do 100 000,00 zł**	**100 000,00 zł**	**do 150 000,00 zł**
Przedsiębiorcy indywidualni *(os. fizyczne prowadzące działalność gospodarczą)*	**30 000,00 zł**	**do 75 000,00 zł**	**75 000,00 zł**	**do 100 000,00 zł**
Pozostałe podmioty niefinansowe	**30 000,00 zł**	**do 50 000,00 zł**	**30 000,00 zł**	**do 50 000,00 zł**
Sektor instytucji rządowych i samorządowych	**-**	**Ustalany indywidualnie**	**-**	**Ustalany indywidualnie**

[2]Przelewy, których wartość przekracza limit indywidualny, można składać w placówkach Banku w tradycyjnej formie (papierowej)
[3]j.w

2. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem bankowości elektronicznej w walutach wymienialnych.

Rodzaj podmiotu	Standardowy limit pojedynczej transakcji obowiązujący w Banku			Indywidualny limit pojedynczej transakcji ustalony na wniosek posiadacza rachunku[4]			Standardowy limit sumy transakcji dziennych obowiązujący w Banku			Indywidualny limit sumy transakcji dziennych ustalony na wniosek posiadacza rachunku		
Przedsiebiorstwa/ Spółki prywatne oraz spółdzielnie	10 700 EUR	11 200 USD	9 200 GBP	do 32 100 EUR	do 33 500 USD	27 600 GBP	21 400 EUR	22 300 USD	18 400 GBP	do 32 100 EURO	do 33 500 USD	do 27 600 GBP
Rolnicy indywidualni	10 700 EUR	--	---	do 21 400 EUR	---	---	21 400 EUR	---	---	do 32 100 EURO	---	---
Przedsiebiorcy indywidualni *(os. fizyczne prowadzące działalność gospodarczą)*	6 400 EUR	6 700 USD	5 500 GBP	do 16 000 EUR	do 16 700 USD	do 13 800 GBP	16 000 EUR	16 700 USD	13 800 GPB	do 21 400 EUR	do 22 300 USD	do 18 400 GBP
Pozostałe podmioty niefinansowe	6 400 EUR	---	---	do 10 700 EUR	---	---	6 400 EUR	---	---	do 10 700 EUR	---	---

Limity na rachunkach bieżących walutowych przygotowano w oparciu o średni kurs z dnia 30.06.2022 roku: dla EURO 4,68 zł, USD – 4,48 zł oraz GBP – 5,44 zł.

3. Z zastrzeżeniem ust. 4 posiadacz rachunku może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1.

4. O wysokości limitów ostatecznie decyduje Bank.

[4] Przelewy, których wartość przekracza limit indywidualny, można składać w placówkach Banku w tradycyjnej formie (papierowej)

§ 24

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za zakupy w sklepach internetowych.

Rodzaj limitu	Standardowy limit obowiązujący w Banku
Limit pojedynczej transakcji	**3 000,00 zł**
Limit sum transakcji dziennych	**6 000,00 zł**

§ 25

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem aplikacji mobilnej Nasz Bank.

Rodzaj limitu	Standardowy limit obowiązujący w Banku
Limit pojedynczej transakcji	**300,00 zł**
Limit sum transakcji dziennych	**1 000,00 zł**

§ 26

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem interfejsu API (PSD2).

Rodzaj limitu	Standardowy limit obowiązujący w Banku
Limit pojedynczej transakcji	**300,00 zł**

Limit sum transakcji dziennych	**1 000,00 zł**

Rozdział 9. Usługa biometryczna

§ 27

1. Usługa biometryczna polega na identyfikacji użytkownika na podstawie danych biometrycznych tj. elektronicznego zapisu odwzorowania sieci naczyń krwionośnych dłoni.
2. Udostępnienie usługi biometrycznej następuje na podstawie wniosku użytkownika.
3. Usługa biometryczna jest aktywowana z chwilą wprowadzenia danych użytkownika do systemu informatycznego.
4. Dane, o których mowa w ust. 1, są przetwarzane przez Bank w systemie informatycznym wyłącznie w celu identyfikacji użytkownika oraz autoryzacji transakcji płatniczych użytkownika z wykorzystaniem czytnika biometrycznego.
5. Dane biometryczne są pobierane przez Bank za pośrednictwem urządzeń spełniających normy bezpieczeństwa oraz zapewniających wierność i dokładność zapisu.
6. Bank nie ponosi odpowiedzialności za niewykonanie identyfikacji lub autoryzacji biometrycznej spowodowane siłą wyższą lub następstwem wykonywania obowiązków wynikających z przepisów prawa.

Rozdział 10. Inne postanowienia

§ 28

Użytkownik zobowiązany jest do nieprzekazywania za pośrednictwem serwisu internetowego treści o charakterze bezprawnym (zakaz).