

Załącznik nr 3 do Regulaminu kont dla klientów indywidualnych

(dawniej zwanego: Regulamin świadczenia usług w zakresie prowadzenia rachunków bankowych dla klientów indywidualnych)

Elektroniczne kanały dostępu

**(dalej: zasady;
dawniej: Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu)**

Rozdział 1. Udostępnienie elektronicznych kanałów dostępu i warunki korzystania z nich

§ 1

1. Udostępniamy produkty i świadczymy usługi użytkownikom przez elektroniczne kanały dostępu:
 - 1) w bankowości elektronicznej – zapewniamy dostęp do informacji o produktach i usługach, które oferujemy, oraz umożliwiamy Ci składanie dyspozycji:
 - a) bankowość internetowa (serwis internetowy) – masz dostęp do informacji oraz składasz dyspozycje na komputerze lub urządzeniu mobilnym przez przeglądarkę internetową,
 - b) bankowość mobilna – masz dostęp do informacji oraz składasz dyspozycje przez zaufane urządzenie mobilne, w aplikacji mobilnej SGB Mobile,
 - 2) powiadamianie SMS (serwis SMS) – otrzymujesz SMS-y z informacjami o transakcjach na rachunku.
2. Umożliwiamy dostęp do informacji o produktach i usługach oraz kontakt z naszymi konsultantami przez call center. Wszystkie rozmowy prowadzone przez call center są nagrywane.
3. Wykaz produktów i usług dostępnych w elektronicznych kanałach dostępu oraz warunki korzystania z usług określa Przewodnik dla klienta na naszej stronie internetowej. Przewodnik dla klienta to instrukcja użytkowania, która zawiera opis poszczególnych elektronicznych kanałów dostępu, ich wymagania techniczne i zasady prawidłowej obsługi.
4. Informacje o aktualnej ofercie usług dostępnych w aplikacji mobilnej SGB Mobile znajdują się w Regulaminie korzystania z aplikacji mobilnej SGB Mobile na naszej stronie internetowej.

§ 2

1. Aby korzystać z elektronicznych kanałów dostępu, musisz mieć rachunek oszczędnościowo-rozliczeniowy lub podstawowy rachunek płatniczy, chyba że Regulamin korzystania z aplikacji mobilnej SGB Mobile stanowi inaczej.
2. Aby korzystać z elektronicznych kanałów dostępu, musisz być posiadaczem, współposiadaczem rachunku lub pełnomocnikiem, który ma pełnomocnictwo stałe. Młodoltni korzysta z elektronicznych kanałów dostępu na podstawie zgody przedstawiciela ustawowego, w ramach zawartej z nami umowy.
3. Możesz wnioskować o udostępnienie kolejnych produktów lub usług, zmianę warunków świadczenia tych produktów lub usług i zawierać umowy przez elektroniczne kanały dostępu, jeśli udostępniliśmy taki sposób zawierania umów. §7 określa szczegółowe zasady, zgodnie z którymi możemy składać oświadczenia woli dotyczące zawarcia lub zmiany warunków umowy przez elektroniczne kanały dostępu. Informacje o ofercie oraz dostępnych sposobach zawierania umów znajdują się na naszej stronie internetowej oraz w Przewodniku dla klienta.
4. Udostępniamy Ci Kantor SGB. Zasady, na których świadczymy tę usługę w bankowości elektronicznej, są załącznikiem nr 4 do regulaminu.

§ 3

1. Dostęp do bankowości elektronicznej uzyskujesz za pomocą indywidualnych danych uwierzytelniających, z wyjątkiem § 9 zasad.
2. Możemy umożliwić Ci korzystanie z usługi przy użyciu tych samych indywidualnych danych uwierzytelniających, jeśli jesteś równocześnie posiadaczem lub pełnomocnikiem stałym do rachunku innego klienta. Uwzględniamy przy tym limity transakcji z § 19 zasad.

§ 4

1. Kiedy wykonujesz transakcje:
 - 1) korzystaj z zaufanych komputerów z aktualnym oprogramowaniem antywirusowym;
 - 2) sprawdź, czy transmisja jest szyfrowana protokołem SSL (ang. Secure Socket Layer), który zapewnia poufność i integralność transmisji danych;
 - 3) nie korzystaj z otwartych i niezabezpieczonych sieci.
2. W Przewodniku dla klienta oraz na naszej stronie internetowej znajduje się szczegółowy opis środków bezpieczeństwa, które powinien(-naś) przedsięwziąć, aby bezpiecznie korzystać z elektronicznych kanałów dostępu.
3. Żeby korzystać z usługi, musisz zaakceptować pliki cookies w przeglądarce internetowej. Są one konieczne, aby utrzymać aktywną sesję po zalogowaniu się do bankowości elektronicznej. Szczegółowe informacje o wszystkich rodzajach naszych plików cookies oraz celu ich wykorzystywania znajdują się na naszej stronie internetowej.

§ 5

1. Musisz korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem i Przewodnikiem dla klienta. Musisz zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób trzecich i zapewnić ich poufność.
2. Gdy otrzymasz indywidualne dane uwierzytelniające z ust. 1, chroń je przed naruszeniem. Ze względów bezpieczeństwa nie przechowuj poszczególnych danych razem ze sobą.
3. Zapewniamy Ci należyłą ochronę indywidualnych danych uwierzytelniających. Są one dostępne wyłącznie dla użytkownika uprawnionego do korzystania z nich.

§ 6

Zakres usług możemy zmienić tylko zgodnie z warunkami i trybem przewidzianymi dla zmiany regulaminu.

Rozdział 2. Dyspozycje składane przez elektroniczne kanały dostępu

§ 7

1. Wszelkie oświadczenia woli, w tym dotyczące zawarcia umowy i zmiany jej warunków, które składasz nam w postaci elektronicznej, będą ważne i prawnie wiążące, jeżeli poprawnie zidentyfikujesz się indywidualnymi danymi uwierzytelniającymi i zastosujesz metody uwierzytelnienia, których wymagamy.
2. Oświadczenie woli zawarcia umowy składasz w postaci elektronicznej, co jest zrównane z formą pisemną, zgodnie z art. 7 ustawy Prawo bankowe. Wykorzystujesz przy tym indywidualne dane uwierzytelniające.
3. Oświadczenie woli zawarcia umowy zawieramy w postaci elektronicznej, co jest zrównane z formą pisemną, zgodnie z art. 7 ustawy Prawo bankowe.
4. Możemy zawierać z Tobą umowy przez elektroniczne kanały dostępu, posługując się pełnomocnikiem. Pełnomocnik składa w naszym imieniu oświadczenie woli zawarcia umowy w postaci elektronicznej, zrównane z formą pisemną, zgodnie z art. 7 ustawy Prawo bankowe i zasadami z ust. 3.
5. Umowę podpisaną zgodnie z ust. 3 i 4 udostępniamy Ci w sposób, który określa umowa.
6. Możesz odstąpić od umowy zawartej przez elektroniczne kanały dostępu w terminie i na warunkach, które określa umowa. Nie musisz podawać przyczyny odstąpienia.

7. Warunki zawierania umów rachunku przez elektroniczne kanały dostępu określają ogólne zasady dotyczące zawierania umów wskazane w regulaminie.

§ 8

1. Warunki dysponowania rachunkami przez elektroniczne kanały dostępu określają ogólne zasady dotyczące dysponowania rachunkami z rozdziału 2 regulaminu.
2. Dotyczą rachunków z rozdziału 4 regulaminu i uwzględniają postanowienia § 9-12 tych zasad. Sposób posługiwania się danym elektronicznym kanałem dostępu opisuje Przewodnik dla klienta.
3. W elektronicznych kanałach dostępu możesz:
 - 1) składać wniosek o wypłatę świadczenia wychowawczego z programu Rodzina 800+ wraz z załącznikami oraz Dobry start; dostępność usługi zależy od współpracy z Ministerstwem Rodziny i Polityki Społecznej,
 - 2) składać inne wnioski, które udostępniamy, oraz zawierać umowy zgodnie z §7,
 - 3) składać inne wnioski, które udostępniamy, dotyczące produktów lub usług podmiotów trzecich współpracujących z nami,
 - 4) wymieniać waluty w Kantorze SGB, jeśli udostępniliśmy Ci tę usługę.
4. Świadczymy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link we współpracy z nami, przy czym:
 - 1) integratorem płatności internetowych jest podmiot, który świadczy usługi sklepom internetowym lub innym podmiotom prowadzącym sprzedaż towarów lub usług; usługi te polegają na umożliwieniu im przyjmowania płatności od ich klientów za pomocą przelewów typu pay by link,
 - 2) przelew typu pay by link realizuje klient, który płaci za zakupy w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem integratorów płatności internetowych.
5. Możesz zgodzić się na transakcję również za pośrednictwem dostawcy, który świadczy usługę inicjowania transakcji płatniczej.
6. Nie możesz odwołać zlecenia płatniczego, jeśli zgodzisz się, aby dostawca świadczący usługę inicjowania transakcji zainicjował transakcję albo ją wykonał. Zasada ta dotyczy inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji lub przez odbiorcę lub za jego pośrednictwem.

§ 9

1. Aby złożyć elektronicznie dyspozycję lub zlecenie płatnicze, musisz się uwierzytelnić w sposób, który pozwoli nam Cię zidentyfikować i zapoznać się z treścią dyspozycji. Dyspozycje te spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi. Wybrane dyspozycje, które składa małoletni poniżej 13 roku życia, realizujemy, gdy w bankowości mobilnej zatwierdzi je przedstawiciel ustawowy (gdy wdrożymy taką funkcjonalność).
2. Gdy złożysz dyspozycję lub zlecenie płatnicze w bankowości elektronicznej, musisz je autoryzować indywidualnymi danymi uwierzytelniającymi, stosując metody uwierzytelniania, których wymagamy. Wyjątek stanowią zapisy ust. 1 i 3.
3. Stosujemy silne uwierzytelnianie, gdy:
 - 1) uzyskujesz dostęp do swojego rachunku w trybie online,
 - 2) inicjujesz transakcję płatniczą,
 - 3) przeprowadzasz w kanale zdalnym czynność, która może wiązać się z ryzykiem oszustwa lub innych nadużyć,z wyjątkiem sytuacji niewymagających silnego uwierzytelnienia, które wskazuje ust. 4. zasad.
4. Możemy nie stosować silnego uwierzytelniania, gdy:
 - 1) korzystasz z jednej z wymienionych niżej pozycji w trybie online lub z 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 wyjątkiem ust. 5,

- 2) inicjujesz transakcję do odbiorcy z listy zaufanych odbiorców, którą utworzyłeś(-aś) wcześniej, stosując silne uwierzytelnienie,
 - 3) inicjujesz kolejną transakcję z serii transakcji cyklicznych, na tę samą kwotę, dla tego samego odbiorcy pod warunkiem, że pierwszą transakcję cykliczną utworzyłeś(-aś), zmieniłeś(-aś) lub zainicjowałeś(-eś), stosując silne uwierzytelnienie,
 - 4) inicjujesz transakcję płatniczą w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i prowadzimy oba rachunki płatnicze,
 - 5) inicjujesz transakcję płatniczą, której poziom ryzyka uznajemy za niską, zgodnie z mechanizmem monitorowania naszych transakcji.
5. Stosujemy silne uwierzytelnianie, jeżeli:
- 1) po raz pierwszy uzyskujesz dostęp do informacji z ust. 4 pkt 1 lit. a w trybie online;
 - 2) minęło więcej niż 90 dni, odkąd po raz ostatni uzyskałeś(-aś) dostęp do informacji z ust. 4 pkt 1 lit. b w trybie online oraz odkąd ostatni raz zastosowałeś(-aś) silne uwierzytelnianie.
6. Możemy skontaktować się z Tobą, aby zrealizować zlecenie płatnicze.
7. Aby uzyskać dostęp do serwisu internetowego, musisz podać swój identyfikator albo kod QR (gdy udostępnimy taką funkcjonalność, kod QR opisuje Przewodnik dla klienta) oraz udostępnione Ci indywidualne dane uwierzytelniające, opisane w ust. 8.
8. Aby uzyskać dostęp do dyspozycji składanych przez serwis internetowy i móc je autoryzować, musisz zalogować się do serwisu internetowego, używając indywidualnych danych uwierzytelniających:
- 1) aplikacji mobilnej Token SGB (Token SGB) i PIN-u do Tokena SGB; wymogi oraz zasady instalacji Tokena SGB na urządzeniu mobilnym oraz sposób jego aktywacji opisuje Przewodnik dla klienta, lub
 - 2) hasła stałego i kodu SMS, z wyjątkiem ust. 10,
 - 3) podpisu kwalifikowanego,
 - 4) aplikacji mobilnej SGB Mobile (gdy wdrożymy taką funkcjonalność) i PIN-u do SGB Mobile; wymogi oraz zasady instalacji SGB Mobile na urządzeniu mobilnym i sposób jego aktywacji opisuje Przewodnik dla klienta.
- Oprócz PIN-u do Tokena SGB i SGB Mobile umożliwiamy użycie biometrycznych danych uwierzytelniających, takich jak: Face ID oraz Touch ID.
9. Hasło stałe z ust. 8 pkt 2 nadajesz po tym, gdy prześlemy Ci hasło tymczasowe. Nastąpi to podczas pierwszego logowania lub odblokowywania dostępu do bankowości internetowej. Zasady tworzenia hasła stałego (jego składniki) określa Przewodnik dla klienta.
10. Podczas logowania się do bankowości internetowej możesz dodać urządzenie, z którego się logujesz, jako urządzenie zaufane. Wtedy kolejne logowania z tego urządzenia do bankowości internetowej w przeglądarce będziesz przeprowadzać już bez dodatkowego uwierzytelnienia za pomocą kodów SMS. Urządzeniem zaufanym może być np. prywatny komputer, smartfon lub tablet, z którego korzystasz wyłącznie Ty. Podczas logowania weryfikujemy określone cechy tego urządzenia.
11. W dowolnym momencie możesz przez bankowość internetową usunąć swoje urządzenie zaufane. Wtedy każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzenia za pomocą kodów SMS.
12. Autoryzacja, którą wykonujesz, oznacza, że polecasz nam wykonać określoną czynność i jest to podstawą jej wykonania.
13. Przesyłamy kody SMS do aktywacji Tokena SGB oraz stosowane do uwierzytelnienia na numer telefonu komórkowego, który wskazałeś(-aś) w umowie, karcie informacyjnej lub pełnomocnictwie.
14. Możemy wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających. W takim przypadku udostępniamy Ci je oraz zawiadamiamy Cię o zmianie. Informację o stosowanych rodzajach indywidualnych danych uwierzytelniających zamieszczamy w Przewodniku dla klienta oraz na naszej stronie internetowej.
15. Możesz zmienić stosowaną metodę autoryzacji na inną przez call center, jeśli wskazałeś(-aś) nam numer telefonu komórkowego z ust. 13.

§ 10

Moment zarejestrowania odpowiednich danych w bankowości elektronicznej i przyjęcia tego oświadczenia przez nasz serwer uznajemy za chwilę, w której składasz oświadczenie w postaci elektronicznej, w szczególności dyspozycję, lub wykonujesz jakąkolwiek czynność. Od tej zasady mogą obowiązywać wyjątki, które określa umowa, regulamin lub obowiązujące przepisy prawa.

§ 11

1. Dyspozycje, które składasz przez bankowość elektroniczną, realizujemy elektronicznie. Stosujesz zasady autoryzacji obowiązujące dla tego elektronicznego kanału dostępu.
2. Autoryzowanego zlecenia płatniczego nie możesz odwołać, z wyjątkiem sytuacji z § 27 ust. 5 regulaminu.

§ 12

1. To, że przyjęliśmy do realizacji dyspozycję, którą złożyłeś(-aś) przez elektroniczne kanały dostępu, potwierdzamy przez ten sam kanał.
2. Jeśli nie przyjęliśmy dyspozycji, którą złożyłeś(-aś) przez elektroniczny kanał dostępu, powiadomimy Cię o tym oraz o przyczynie odmowy przez ten sam kanał lub pracownika naszej placówki. Możliwe powody:
 - 1) niekompletność dyspozycji,
 - 2) złożenie dyspozycji sprzecznych ze sobą,
 - 3) nieprawidłowy numer rachunku odbiorcy,
 - 4) brak środków do realizacji dyspozycji lub
 - 5) inne okoliczności, które uniemożliwiają nam przyjęcie dyspozycji.

Rozdział 3. Korzystanie z elektronicznych kanałów dostępu

§ 13

1. Z elektronicznych kanałów dostępu możesz korzystać 7 dni w tygodniu, 24 godziny na dobę, z wyjątkiem ograniczeń z § 14.
2. Przez elektroniczne kanały dostępu uzyskujesz dostęp do wszystkich rachunków: zarówno otwartych przed dniem aktywowania usługi, jak i po nim. Możesz jednak zawnieioskować o ograniczony dostęp do rachunków w elektronicznych kanałach dostępu.

Rozdział 4. Ograniczenia w korzystaniu z elektronicznych kanałów dostępu

§ 14

1. Zablokujemy Ci dostęp do serwisu internetowego i uniemożliwimy wykonanie transakcji, jeśli:
 - 1) złożysz dyspozycję zablokowania dostępu do serwisu internetowego,
 - 2) złożysz dyspozycję dezaktywacji Tokena SGB,
 - 3) trzy razy wpiszesz nieprawidłowy PIN do Tokena SGB lub kod SMS, lub nieprawidłowe hasło stałe.
2. Możemy ograniczyć lub zablokować dostęp do serwisu internetowego lub czasowo zablokować wykonanie dyspozycji, jeśli:
 - 1) istnieją uzasadnione przyczyny, które wiążą się z bezpieczeństwem dostępu do serwisu internetowego i indywidualnych danych uwierzytelniających; również gdy podejrzewamy, że ktoś popełnił przestępstwo na Twoją szkodę,
 - 2) umyślnie doprowadziłeś(-aś) do nieautoryzowanej transakcji płatniczej lub mamy uzasadnione podejrzenie, że będziesz posługiwać się dostępem niezgodnie z regulaminem,
 - 3) korzystasz z serwisu internetowego niezgodnie z zasadami bezpieczeństwa określonymi w tym załączniku lub zagrażasz bezpieczeństwu korzystania z serwisu internetowego,
 - 4) konserwujemy serwis internetowy lub inne systemy teleinformatyczne związane z wykonywaniem umowy; poinformujemy Cię o tym z wyprzedzeniem na naszej stronie internetowej,

- 5) usuwamy awarie, usterki lub nieprawidłowości działania w serwisie internetowym lub innych systemach teleinformatycznych związanych z wykonywaniem umowy,
 - 6) wymieniamy stosowane indywidualne dane uwierzytelniające; poinformujemy Cię o tym pisemnie lub na naszej stronie internetowej,
 - 7) mamy uzasadnione podejrzenie, że transakcje na Twoim rachunku mają związek z przestępstwem związanym z praniem pieniędzy lub finansowaniem terroryzmu,
 - 8) gdy na Twoim rachunku są zamrożone wartości majątkowe lub gdy wobec Ciebie należy stosować sankcje międzynarodowe albo embarga,
 - 9) nie możemy zastosować środków bezpieczeństwa finansowego; do tych sytuacji zaliczamy brak aktualnego dokumentu tożsamości Twojego lub osób upoważnionych do działania w Twoim imieniu.
3. Możemy uchylić ograniczenie albo blokadę dostępu do serwisu internetowego w przypadku z ust. 2 pkt 1, jeśli odpowiedni wniosek złożysz Ty lub pełnomocnik stały, w sposób określony w ust. 4 zasad. W takim przypadku albo wydajemy Ci nowe indywidualne dane uwierzytelniające, albo uchylamy ograniczenia lub blokady i zachowujesz dotychczasowe dane uwierzytelniające.
4. W przypadku z ust. 2 pkt 1 uchylenie:
- 1) ograniczenia lub blokady dostępu do serwisu internetowego następuje na podstawie Twojej dyspozycji telefonicznej lub złożonej w naszej siedzibie lub dowolnej placówce,
 - 2) czasowej blokady dyspozycji następuje po tym, jak nasz pracownik skontaktuje się z Tobą telefonicznie lub pisemnie, a Ty potwierdzisz złożoną dyspozycję.
5. Z wyjątkiem ust. 6, informujemy Cię, że zamierzamy zablokować indywidualne dane uwierzytelniające w przypadkach z ust. 2 pkt 1 i 3, zanim je zablokujemy, a jeżeli nie jest to możliwe – telefonicznie, niezwłocznie po zablokowaniu.
6. Nie informujemy o zablokowaniu, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub zabronione zgodnie z odrębnymi przepisami.
7. W przypadkach z ust. 2 pkt 4 i 5, ograniczenie lub blokada dostępu do serwisu internetowego lub czasowa blokada dyspozycji trwa możliwie krótko, tyle ile trwa usunięcie przyczyny.

Rozdział 5. Blokowanie i zastrzeganie dostępu do serwisu internetowego

§ 15

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowana przez:
 - 1) nas – zgodnie z postanowieniami § 17,
 - 2) Ciebie,
 - 3) przedstawiciela ustawowego małoletniego.
2. Możesz złożyć wniosek o zablokowanie dostępu do serwisu internetowego i uniemożliwić jednocześnie wykonanie transakcji.

§ 16

1. Jeśli jesteś użytkownikiem serwisu internetowego lub przedstawicielem ustawowym małoletniego, niezwłocznie zastrzeż dostęp do serwisu internetowego, podając swoje dane personalne. Zrób to, jeżeli indywidualne dane uwierzytelniające zostały utracone, skradzione lub przywłaszczone albo ktoś użył ich bez uprawnień.
2. Zastrzeżenie z ust. 1 możesz wykonywać w naszej placówce, przez call center lub pod innymi numerami telefonów, które wskazujemy i aktualizujemy w komunikacie w naszych placówkach lub na naszej stronie internetowej.
3. Możemy zmieniać numery telefonów służące do zastrzegania i blokowania dostępu do serwisu internetowego. Powiadomimy Cię o tym elektronicznie na adres poczty elektronicznej (e-mail), który wskazałeś(-aś), lub komunikatem we właściwym elektronicznym kanale dostępu.
4. Nie możesz odwołać zastrzeżenia z ust. 1. Powoduje ono, że nie masz dalszego dostępu do serwisu internetowego.

5. Jeśli jesteś posiadaczem rachunku lub działającym w jego imieniu przedstawicielem ustawowym, możesz wystąpić z wnioskiem o nowe indywidualne dane uwierzytelniające, jeśli je wcześniej utracisz oraz zastrzeżesz.
6. Jeśli ktoś ukradnie lub przywłaszczy Twój telefon komórkowy albo stwierdzisz, że został on użyty w nieuprawniony sposób, zmień dane zgodnie z ust. 7 zasad. Dotyczy to telefonu oznaczonego jako telefon do autoryzacji lub zmiany numeru telefonu do autoryzacji.
7. Jeśli chcesz zmienić dane niezbędne do otrzymywania kodów SMS na nowe i:
 - 1) masz dotychczasowy numer telefonu do autoryzacji, możesz zmienić numer w serwisie internetowym, jeśli udostępniemy taką funkcjonalność; możemy skontaktować się z Tobą, aby zweryfikować zlecenie zmiany numeru tego telefonu i zmienić numer telefonu,
 - 2) nie masz dotychczasowego telefonu do autoryzacji, musisz złożyć odpowiednią dyspozycję w naszej placówce.

§ 17

1. Możemy zastrzec indywidualne dane uwierzytelniające, jeśli:
 - 1) umowa wygaśnie lub zostanie rozwiązana,
 - 2) istnieją uzasadnione przyczyny związane z bezpieczeństwem indywidualnych danych uwierzytelniających, tzn. wiemy, że osoby trzecie weszły w ich posiadanie,
 - 3) podejrzewamy, że indywidualne dane uwierzytelniające zostały użyte w sposób nieuprawniony lub że umyślnie doprowadziłeś(-aś) do nieautoryzowanej transakcji płatniczej.
2. Z wyjątkiem ust. 3 informujemy Cię, że zamierzamy zastrzec indywidualne dane uwierzytelniające w przypadkach z ust. 1 pkt 2 i 3, zanim je zastrzeżemy, a jeżeli nie jest to możliwe – telefonicznie, niezwłocznie po zastrzeżeniu.
3. Nie informujemy o zastrzeżeniu, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub zabronione zgodnie z odrębnymi przepisami.

Rozdział 6. Udostępnianie informacji na potrzeby inicjowania transakcji płatniczych i dostępu do informacji o rachunku. Potwierdzanie dostępności pieniędzy na rachunku

§ 18

1. Jeśli korzystasz z serwisu internetowego i zgodzisz się na udostępnienie informacji o rachunku i transakcjach w nim, możemy udostępnić te informacje dostawcy, który świadczy usługi dostępu do informacji o rachunku.
2. Dostęp do informacji na rachunku z ust. 1 mogą mieć także dostawcy, którzy inicjują transakcje płatnicze dla użytkowników korzystających z serwisu internetowego.
3. Niezwłocznie potwierdzamy dostępność na rachunku kwoty niezbędnej do wykonania transakcji realizowanej kartą, jeżeliawnioskuje o to dostawca wydający instrumenty płatnicze oparte na karcie płatniczej. Dostępność pieniędzy potwierdzamy, jeśli:
 - 1) Twój rachunek płatniczy jest dostępny online w momencie, w którym otrzymamy wniosek,
 - 2) zgodziłeś(-aś) się, abyśmy odpowiadali na tego rodzaju wnioski dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej,
 - 3) zgody z pkt b udzieliłeś(-aś), zanim wpłynął do nas pierwszy wniosek dotyczący potwierdzenia.
4. Dostawca wydający instrumenty płatnicze oparte na karcie płatniczej może wystąpić z wnioskiem z ust. 3, jeżeli:
 - 1) zgodziłeś(-aś) się, aby występował z wnioskiem z ust. 3,
 - 2) zainicjowałeś(-aś) transakcję płatniczą realizowaną kartą płatniczą przy użyciu opartego na tej karcie instrumentu płatniczego, który wydał dany dostawca,
 - 3) dostawca uwierzytlni siebie wobec nas, zanim złoży wniosek z ust. 3, oraz porozumiewa się z nami w sposób bezpieczny.
5. Potwierdzenie z ust. 3 polega na tym, że udzielasz tylko odpowiedzi „tak” albo „nie” i nie podajesz salda rachunku. Odpowiedzi nie przechowujemy i wykorzystujemy ją tylko do wykonania transakcji realizowanej kartą płatniczą.

6. Potwierdzenie z ust. 3 nie umożliwia nam blokady pieniędzy na Twoim rachunku płatniczym.
7. Możesz zwrócić się do nas o przekazanie danych identyfikujących dostawcę z ust. 4 oraz udzielonej odpowiedzi z ust. 5.
8. Możemy odmówić dostępu do rachunku dostawcy świadczącemu usługę dostępu do informacji o rachunku lub dostawcy świadczącemu usługę inicjowania transakcji płatniczej. Mamy do tego prawo z przyczyn, które są obiektywnie uzasadnione i należycie udokumentowane lub mają związek z nielegalnym dostępem do rachunku takiego dostawcy, w tym z nieuprawnionym zainicjowaniem transakcji płatniczej. W takim przypadku w uzgodniony sposób informujemy Cię o odmowie dostępu do rachunku i jej przyczynach. Informujemy Cię, o ile jest to możliwe, zanim odmówimy dostępu, a jeżeli nie jest to możliwe – bezzwłocznie po takiej odmowie, najpóźniej w dniu roboczym następującym po dniu takiej odmowy. Nie informujemy o odmowie, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub sprzeczne z odrębnymi przepisami. Dostawcy świadczącemu usługę dostępu do informacji o rachunku oraz dostawcy świadczącemu usługę inicjowania transakcji płatniczej umożliwiamy dostęp do rachunku niezwłocznie po tym, gdy ustanie przyczyna odmowy.

Rozdział 7. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia

§ 19

1. Standardowe limity pojedynczej transakcji oraz limity wszystkich transakcji w ciągu dnia w serwisie internetowym na rachunku prezentuje poniższa tabela. Kwoty podajemy w jednostkach waluty, w której prowadzony jest dany rachunek. Wysokość limitów w polskich złotych dotyczy klientów, którym udostępniliśmy usługę od 16 czerwca 2025 r.

Waluta rachunku	Limit pojedynczej operacji	Limit wszystkich operacji w ciągu dnia
złoty polski	10 000	50 000
funt brytyjski	1000	4000
dolar amerykański	1000	4000
euro	1000	4000
korona szwedzka	1000	4000
korona norweska	1000	4000

2. Jeśli wprowadzimy do oferty rachunek w walucie innej w ust. 1, limity obliczamy, dzieląc odpowiedni limit w złotych przez kurs średni NBP nowej waluty, z poprzedniego dnia roboczego, który poprzedza dzień otwarcia rachunku.
3. Z wyjątkiem ust. 4 możesz wnioskować o indywidualne ustalenie limitów z ust. 1. Nie dotyczy to wysokości limitu 5.000 zł, który zdefiniowaliśmy dla zaufanego odbiorcy.
4. Decydujemy o ostatecznej wysokości limitów.

Rozdział 8. Inne postanowienia

§ 20

1. Nie wolno Ci przekazywać przez serwis internetowy bezprawnych treści.
2. Nie możesz wykorzystywać serwisu internetowego do popełniania, pomagania w popełnianiu lub podlegania do popełniania czynów zabronionych. W szczególności dotyczy to wprowadzania do obrotu finansowego wartości majątkowych, które pochodzą z nielegalnych lub nieujawnionych źródeł.