Regulamin Pilotażu nowej Bankowości Internetowej Alior Business i Aplikacji Mobilnej Alior Business Mobile

Obowiązuje od 15 października 2024 r. do dnia zakończenia Pilotażu

§ 1. Postanowienia ogólne

1. Organizatorem Pilotażu jest Alior Bank S.A. z siedzibą w Warszawie, ul. Łopuszańska 38D, 02-232 Warszawa, wpisany do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000305178, NIP: 1070010731, REGON: 141387142, o kapitale zakładowym w kwocie 1.305.539.910,00 zł wpłaconym w całości (dalej: „**Bank**").
2. Regulamin stanowi integralną część Umowy Pilotażowej zawieranej pomiędzy Klientem a Bankiem.
3. Regulamin:
   1) wraz z zawartą Umową Pilotażową określa zasady i warunki udziału Klienta w Pilotażu,
   2) określa warunki i zasady udostępnienia Bankowości Mobilnej oraz Bankowości Internetowej.
4. Celem Pilotażu jest:
   1) weryfikacja przez Klienta udostępnionej mu Bankowości Internetowej i Bankowości Mobilnej oraz zgłaszanie wszelkich uwag i sugestii związanych z ich korzystaniem. Pozyskane uwagi i sugestie Klientów pomocne będą w dalszym rozwoju Bankowości Internetowej oraz Bankowości Mobilnej oraz wprowadzaniu rozwiązań przyjaznych użytkownikom;
   2) zebranie najczęściej zadawanych pytań Klientów i określenie zapotrzebowania na materiały edukacyjne.
5. Czas trwania i zasady zakończenia Pilotażu określa Umowa Pilotażowa.
6. Zasady Remigracji (przywrócenia) Klienta do Systemu BusinessPro określa Umowa Pilotażowa.

§ 2. Definicje

Pojęcia zapisane w tym Regulaminie od wielkiej litery oznaczają:

Aktywacja Aplikacji – szereg czynności, wykonywanych przez Użytkownika po zainstalowaniu Aplikacji Mobilnej na pierwszym oraz kolejnych Urządzeniach, w tym służących zdefiniowaniu metody identyfikacji i autoryzacji w Aplikacji w celu udostępnienia Użytkownikowi Bankowości Mobilnej. Szczegółową Instrukcję Aktywacji Aplikacji Bank udostępnia w zakładce Wiadomości Systemu Alior Business oraz w aktualnościach w Systemie BusinessPro.

Aplikacja (Aplikacja Mobilna, Alior Business Mobile) – oprogramowanie pobrane z autoryzowanego sklepu Google Play lub App Store i zainstalowane na Urządzeniu, służące do obsługi Bankowości Mobilnej. Poprzez Aplikację Mobilną jest możliwa Autoryzacja Dyspozycji składanych w Bankowości Internetowej. Zakres funkcjonalny Aplikacji Mobilnej, w tym rodzaje Dyspozycji, jakie mogą zostać złożone przy jej pomocy znajdują się w Załączniku nr 1 do Regulaminu.

Autoryzacja - wyrażenie przez Użytkownika zgody na wykonanie Dyspozycji w sposób określony w Regulaminie.

Bankowość Internetowa (Alior Business) – usługa zapewniająca dostęp do informacji o Produktach oraz możliwość składania Dyspozycji z wykorzystaniem sieci Internet i komputera lub urządzenia mobilnego wyposażonego w przeglądarkę internetową. Zakres funkcjonalny Bankowości Internetowej, w tym rodzaje Dyspozycji, jakie mogą zostać złożone przy jej pomocy, znajdują się w Załączniku nr 1 do Regulaminu.

Bankowość Mobilna - usługa zapewniająca dostęp do informacji o Produktach oraz możliwość składania Dyspozycji z wykorzystaniem urządzeń mobilnych takich jak palmtopy, tablety i telefony komórkowe z dostępem do Internetu, za pomocą Aplikacji Mobilnej. Zakres funkcjonalny Bankowości Mobilnej, w tym rodzaje Dyspozycji, jakie mogą zostać złożone przy jej pomocy, znajdują się w Załączniku nr 1 do Regulaminu.

Dane Identyfikujące - zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej.

Dyspozycja – oświadczenie woli złożone przez uprawnionych Użytkowników wobec Banku za pośrednictwem Kanałów Elektronicznych i autoryzowane w sposób właściwy dla danego Kanału Elektronicznego. Wszelkie Dyspozycje (zwane także Wnioskami) złożone w postaci elektronicznej przez osobę, która została prawidłowo uwierzytelniona jako Użytkownik, są traktowane jako Dyspozycje Użytkownika, działającego w imieniu Klienta. Dyspozycje składane zgodnie z art. 7 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi.

Hasło Dostępu – ciąg znaków, ustalany samodzielnie przez Użytkownika w Bankowości Internetowej, który użyty wraz z Identyfikatorem oraz innymi wymaganymi danymi lub urządzeniami w ramach Silnego Uwierzytelnienia, umożliwia dostęp do Bankowości Internetowej. Hasło musi spełniać wymagania określone przez Bank w procesie logowania do Bankowości Internetowej.

Hasło Startowe – ciąg znaków przesyłany Użytkownikowi na Telefon Zaufany w formie wiadomości SMS służący do aktywacji Bankowości Internetowej.

Contact Center – usługa w ramach Pilotażu, polegająca na obsłudze Użytkowników w zakresie informacyjnym, operacyjnym i sprzedażowym. Obsługa może odbywać się następującymi kanałami:

1. Telefon
    1) obsługa przez dedykowanego konsultanta w ramach Pilotażu w dni robocze, w godzinach 8:00 - 17:00 pod numerem +48 877 391 413,
    2) Infolinia Banku pod numerem 12 370 70 70, czynna całą dobę.
2. Korespondencja elektroniczna – wiadomość w Bankowości Internetowej i Bankowości Mobilnej.

Identyfikator Biometryczny – zapis indywidualnych cech fizycznych Użytkownika (m.in. odcisku palca lub wizerunku jego twarzy), który jest przechowywany i udostępniany na Urządzeniu przez jego producenta. Identyfikator biometryczny służy do logowania do Aplikacji. Identyfikator biometryczny jest dostępny w Aplikacji:

1) na Urządzeniach z systemem iOS (od wersji 11.0) z czytnikiem linii papilarnych (TouchID) lub do rozpoznawania twarzy (FaceID),
2) na Urządzeniach z systemem Android (od wersji 6.0) z funkcją identyfikacji odcisku palca (Fingerprint Authentication).

Identyfikator (CIF) – unikalny numer nadany Użytkownikowi przez Bank, z którym jednoznacznie związane są dane osobowe i adresowe Użytkownika, służący m.in. do identyfikacji podczas korzystania z Kanałów Elektronicznych.

Instrument Płatniczy - zindywidualizowane urządzenie lub uzgodniony przez Użytkownika i dostawcę zindywidualizowany zbiór procedur, służących do inicjowania zlecenia płatniczego. Instrumentami Płatniczymi w rozumieniu Regulaminu są: Bankowość Internetowa, Bankowość Mobilna, Aplikacja Mobilna.

Kanały Elektroniczne – Bankowość Internetowa, Bankowość Mobilna. Kanały Elektroniczne dostępne są dla Klientów, którzy biorą udział w Pilotażu.

Karta Uprawnień Użytkownika – zdefiniowany poziom dostępu do określonych funkcjonalności w Systemie Alior Business, ustalony przez Klienta dla danego Użytkownika. Karta Uprawnień Użytkownika ma na celu zebranie informacji o uprawnieniach Użytkownika do funkcjonalności Systemu Alior Business oraz dostępach do rachunków.

Klient – przedsiębiorca lub inna osoba prawna lub jednostka organizacyjna utworzona zgodnie z przepisami prawa, które zawarły Umową Pilotażową.

Kod Autoryzacyjny (SMS) – jednorazowy kod w formie wiadomości tekstowej przesyłany na Telefon Zaufany do Autoryzacji Dyspozycji składanych przez Użytkownika w ramach Bankowości Internetowej, przesyłany Użytkownikowi w przypadku, gdy wybrał taką metodę autoryzacji.

Komunikat PUSH – powiadomienie, zdalnie wysyłane do Aplikacji Mobilnej przez Bank, służące:

1. informacji o zdarzeniach na rachunkach, Produktach, do których Użytkownik ma dostęp;
2. Autoryzacji Dyspozycji składanych w Bankowości Mobilnej i Bankowości Internetowej;
3. zawierające inne komunikaty lub informacje z Banku;

(przy czym określone funkcje Komunikatów PUSH będą udostępniane od momentu wdrożenia w Banku, po uprzednim poinformowaniu Użytkownika nie później niż 7 dni przed datą udostępnienia usługi, poprzez Kanały Elektroniczne).

Limity kwotowe – parametry określające wartość jednorazowej/dziennej/tygodniowej/miesięcznej kwoty transakcji, przypisane według podziału dla Bankowości Internetowej oraz Bankowości Mobilnej. Maksymalna

kwota, na jaką można zlecić polecenie przelewu poprzez Bankowość Internetową i Bankowość Mobilną, publikowana jest na stronie internetowej Banku. Bank nie realizuje Dyspozycji powyżej limitów.

Limity wynikające ze Schematów Akceptacji

– maksymalna wartość jednorazowej/dziennej/tygodniowej/miesięcznej kwoty transakcji, ustalone przez Klienta. Limity dla danego Użytkownika, które obowiązywały w Systemie BusinessPro zostaną przeniesione do Systemu Alior Business.

Metoda DFP - mechanizm pozwalający na weryfikację i identyfikację urządzenia Użytkownika służącego do logowania się i zlecenia transakcji płatniczych w Bankowości Internetowej i Bankowości Mobilnej. Polega na badaniu określonego zestawu cech urządzenia (PC, laptop, smartfon, tablet, itp.), które potwierdzają, że jest to urządzenie wykorzystywane przez Klienta. Parametry przekazywane do analizy mogą obejmować m.in.:

1) wersję systemu operacyjnego urządzenia,
2) wartości w rejestrze związane ze środowiskiem uruchomieniowym (profil w Windows, wersja językowa),
3) dane przeglądarki (m.in. wersja przeglądarki, ustawiony język),
4) zaszyfrowane ciasteczka ze specyficznymi wartościami przechowywanymi dla danego Klienta,
5) parametry karty graficznej, karty dźwiękowej,
6) parametry procesora oraz pamięci RAM,
7) ustawienia i rozdzielczość ekranu,
8) dane o środowisku uruchomieniowym przeglądarki,
9) dodatkowo istnieje możliwość zapisania określonej wartości (część przeglądarek umożliwia przechowywanie danych, które przyszły w sesji internetowej w WebStorage) unikatowej dla klienta, która jest z nim związana.

Urządzenie zidentyfikowane Metodą DFP jest elementem Silnego Uwierzytelnienia.

Obrazek Bezpieczeństwa – obrazek wybrany przez Użytkownika spośród prezentowanych grafik podczas pierwszego logowania lub logowania po resecie Hasła Dostępu w Bankowości Internetowej. Obrazek Bezpieczeństwa jest prezentowany Użytkownikowi podczas każdego logowania do Bankowości Internetowej w celu weryfikacji autentyczności strony Banku przed zalogowaniem przez Użytkownika. Obrazek Bezpieczeństwa Użytkownik może zmienić w Bankowości Internetowej. W przypadku migracji Klienta na System Alior Business Klientowi będzie prezentował się obrazek ustawiony przez Klient w Systemie BusinessPro.

Pakiet Abonamentowy – zestaw (pakiet) funkcjonalności dostępnych dla Użytkowników w Kanałach Elektronicznych. Opłata za Pakiet Abonamentowy w Systemie Alior Business jest w tej samej wysokości, jak w Systemie BusinessPro. Zakres funkcjonalności dostępnych w ramach Pakietu Abonamentowego określa Załącznik nr 1 do Regulaminu.

Pilotaż – działania Banku w ramach projektu uruchomienia nowego Systemu Alior Business i Alior Business Mobile dla przedsiębiorców i innych podmiotów, obejmujące udostępnienie wybranym Klientom, na czas określony, systemów nowej Bankowości Internetowej i Bankowości Mobilnej, na zasadach określonych w Regulaminie i Umowie Pilotażowej.

PIN (Master PIN) – ciąg cyfr ustalany przez Użytkownika w sposób poufny podczas pierwszej Aktywacji Aplikacji na pierwszym Urządzeniu. Służy do logowania do Aplikacji i Autoryzacji Dyspozycji. Jest taki sam na wszystkich Urządzeniach Użytkownika, z zainstalowaną Aplikacją.

Placówka (Punkt Sprzedaży) – jednostka organizacyjna Banku, która wykonuje czynności bankowe w imieniu i na rzecz Banku. Placówkami są oddziały Banku i placówki partnerskie – agencje, które świadczą w imieniu Banku usługi na podstawie umowy agencyjnej.

Produkt – rachunek lub usługa, którą oferuje Bank, świadczona na podstawie odpowiedniej umowy i regulaminu.

Przeglądarka Zaufana (Urządzenie Dedykowane) – przeglądarka, którą Użytkownik uznał za zaufaną w ramach Metody DFP.

Regulamin - niniejszy „Regulamin Pilotażu nowej Bankowości Internetowej Alior Business i Bankowości Mobilnej Alior Business Mobile".

Remigracja – zwrotne przeniesienie rachunków i kont Klienta do Systemu BusinessPro z Systemu Alior Business.

Silne Uwierzytelnienie – Uwierzytelnienie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:

1) wiedza o czymś, o czym wie wyłącznie Użytkownik – na przykład hasło do konta (Hasło dostępu),

2) posiadanie czegoś, co posiada wyłącznie Użytkownik – na przykład telefon (Urządzenie),
3) cechy charakterystyczne Użytkownika – na przykład odcisk palca (Identyfikator biometryczny),

będących integralną częścią tego uwierzytelnienia oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych.

System BusinessPro – system bankowości internetowej Banku, dedykowany dla klientów biznesowych, z którego rachunki i konta Klienta zostały przeniesione na System Alior Business.

Telefon Zaufany (Numer telefonu zaufanego) – podany przez Użytkownika numer telefonu komórkowego, na który Bank m.in. przesyła Hasło Startowe oraz Kody autoryzacyjne (SMS).

Umowa Pilotażowa – umowa zawarta pomiędzy Bankiem a Klientem pod nazwą: Umowa przystąpienia do Pilotażu „Family&Friends".

Umowa Ramowa – umowa zawarta pomiędzy Bankiem a Klientem dotycząca świadczenia przez Bank usług bankowych oraz prowadzenia rachunków i lokat dla przedsiębiorców i innych podmiotów,.

Urządzenie – urządzenie (np. smartfon), na którym jest zainstalowana Aplikacja Mobilna.

Urządzenie domyślne – Urządzenie, które Użytkownik używa w celu Uwierzytelnienia i które jest uzgodnione pomiędzy Bankiem i Użytkownikiem (powiązane z Użytkownikiem) w tym celu. Na Urządzenie domyślne Bank wysyła Użytkownikowi Komunikaty PUSH.

Uwierzytelnianie/Uwierzytelnienie – procedura umożliwiająca Bankowi weryfikację tożsamości Użytkownika lub ważności stosowania konkretnego Instrumentu Płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających.

Uwierzytelnienie biometryczne – metoda logowania do Aplikacji Mobilnej umożliwiająca Uwierzytelnienie użytkownika za pomocą Identyfikatora Biometrycznego.

Ustawa UUP (UUP) - ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych.

Użytkownik – Klient lub osoba fizyczna, posiadająca pełną zdolność do czynności prawnych, upoważniona do samodzielnego składania Dyspozycji za pośrednictwem Kanałów Elektronicznych, w ramach uprawnień wskazanych w Karcie Uprawnień Użytkownika, w imieniu i na rzecz Klienta, w zakresie czynności bankowych, o które Bank zawarł z Klientem Umowę Ramową oraz Umowę Pilotażową, spełniająca wymagania opisane w niniejszym Regulaminie. Użytkownikiem innym niż Klient może zostać wyłącznie osoba, która została dopuszczona do Kanałów Elektronicznych za wyraźną zgodą Banku.

§ 3. Warunki udostępniania Kanałów Elektronicznych

1. Bank udostępnia Klientowi Kanały Elektroniczne: Alior Business (Bankowość Internetowa) oraz Alior Business Mobile (Bankowość Mobilna) po spełnieniu łącznie przez Klienta następujących warunków:
   1) posiadanie zawartej Umowy Ramowej,
   2) zawarcie Umowy Pilotażowej,
   3) akceptacja Regulaminu oraz Polityki prywatności Banku,
   4) dokonanie aktywacji wybranego Kanału Elektronicznego.
2. Aktywacja Bankowości Internetowej przez Użytkownika następuje poprzez:
   1) podanie Identyfikatora oraz
   2) wprowadzenie otrzymanego z Banku Hasła Startowego oraz
   3) ustanowienie Hasła Dostępu i wybór Obrazka Bezpieczeństwa.
3. Aktywacja Bankowości Mobilnej (Aplikacji Mobilnej) przez Użytkownika następuje poprzez:
   1) akceptację Polityki prywatności Banku oraz
   2) podanie Identyfikatora oraz
   3) wprowadzenie żądanych danych osobowych, kodu aktywacyjnego otrzymanego telefonicznie z Banku oraz
   4) ustawienie PIN.
4. Proces aktywacji Bankowości Internetowej oraz Bankowości Mobilnej kończy się z chwilą pojawienia się ekranu pierwszego logowania odpowiednio do Bankowości Internetowej lub Bankowości Mobilnej.
5. Warunkiem udostępnienia Bankowości Mobilnej jest wcześniejsza aktywacja Bankowości Internetowej.
6. Użytkownicy nie będący Klientem mogą korzystać z Kanałów Elektronicznych wyłącznie za wyraźną zgodą Banku. Nadanie przez Klienta Użytkownikowi uprawnień do korzystania z Kanałów Elektronicznych jest równoznaczne z

udzieleniem mu pełnomocnictwa do dokonywania, w imieniu i na rzecz Klienta, czynności określonych w Karcie Uprawnień Użytkownika.

7. Po aktywacji danego Kanału Elektronicznego Użytkownik uzyskuje dostęp do Produktów w ramach dostępnych funkcjonalności oraz aktywowanego Kanału Elektronicznego.
8. Klient może w każdym czasie dezaktywować dany Kanał Elektroniczny i ponownie go aktywować.
9. Logowanie do Bankowości Internetowej następuje przy użyciu Identyfikatora oraz Hasła Dostępu oraz wybranej przez Użytkownika metody logowania: jednorazowego Kodu autoryzacyjnego (SMS) albo Komunikatu PUSH.
10. Logowanie do Aplikacji następuje poprzez podanie PIN albo Identyfikatora Biometrycznego według wyboru Użytkownika.
11. Bank może ograniczyć dostęp do Bankowości Internetowej lub Bankowości Mobilnej. Szczegółowe warunki ograniczania oraz blokowania Kanałów Elektronicznych przez Bank wskazane zostały w § 7 niniejszego Regulaminu.
12. Za zakres uprawnień przydzielonych danemu Użytkownikowi, zgodnie z Kartą Uprawnień Użytkownika, odpowiada wyłącznie Klient. Bank nie ponosi odpowiedzialności za jakiekolwiek ewentualne szkody, które mogą powstać na skutek działania lub zaniechania Użytkownika, działającego zgodnie z zakresem uprawnień określonym w Karcie Uprawnień Użytkownika.

§ 3. Zakres usług Kanałów Elektronicznych

1. Za pośrednictwem Kanałów Elektronicznych można:
   1) zarządzać środkami finansowymi,
   2) uzyskiwać informacje o posiadanych Produktach ,
   3) składać wnioski oraz zawierać umowy o wybrane Produkty.
2. Wykaz funkcjonalności dostępnych w ramach Bankowości Internetowej oraz Bankowości Mobilnej określa Załącznik nr 1 do Regulaminu.
3. Bank może zmienić zakres informacji i Dyspozycji dostępnych za pośrednictwem Kanałów Elektronicznych w przypadku wprowadzania nowych lub zmiany powszechnie obowiązujących przepisów prawa.

§ 4. Realizacja Dyspozycji i zasady korzystania z Kanałów Elektronicznych

1. Dyspozycje składane za pośrednictwem Kanałów Elektronicznych mogą być składane codziennie, w ciągu całej doby, z wyłączeniem czasu ogłoszonej wcześniej przez Bank przerwy technicznej oraz z z zastrzeżeniem, że nie każdy rodzaj Dyspozycji może być wykonywany w trybie natychmiastowym. Aktualne informacje o trybie i warunkach realizacji Dyspozycji są publikowane na stronie internetowej Banku.
2. Klient jest zobowiązany do bieżącego sprawdzania stanu swoich rachunków, poprawności wykonania transakcji płatniczych oraz pozostałych czynności zleconych za pośrednictwem Kanałów Elektronicznych i niezwłocznego zgłaszania wszelkich nieprawidłowości.
3. Dyspozycja z bieżącą datą realizacji, prawidłowo zautoryzowana, nie może być anulowana.
4. Dane niezbędne do prawidłowej realizacji Dyspozycji powinny być podane przez Użytkownika zgodnie z opisem pól występujących w formularzu Dyspozycji. Użytkownik powinien się upewnić, że wszystkie wymagane dane zostały przez niego podane prawidłowo i zgodnie z jego wolą.
5. Przed dokonaniem Autoryzacji Dyspozycji Użytkownik powinien działać ze świadomością wykonania Dyspozycji oraz upewnić się, że Dyspozycja jest jednoznaczna i zgodna z jego intencją. W przypadku realizowania Dyspozycji wymagających Autoryzacji za pomocą Kodu Autoryzacyjnego (SMS) lub Komunikatu PUSH, Użytkownik powinien zweryfikować czy treść otrzymanej wiadomości tekstowej z Kodem Autoryzacyjnym (SMS) lub treść Komunikatu PUSH jest zgodna z intencją Użytkownika, zwłaszcza w zakresie kwoty i waluty transakcji, numeru rachunku oraz rodzaju operacji.
6. Dyspozycje dotyczące obsługi zleceń stałych wykonywanych z Rachunków oraz odwoływania przelewów z odroczoną datą realizacji są przyjmowane najpóźniej na jeden dzień roboczy przed datą realizacji Dyspozycji.
7. Jeśli zachodzi uzasadnione podejrzenie co do autentyczności złożonej Dyspozycji, Bank może wstrzymać jej realizację do momentu wyjaśnienia wątpliwości lub odmówić jej wykonania.
8. Autoryzacja Dyspozycji wymagająca Silnego Uwierzytelnienia następuje:
   1) w Bankowości Internetowej – przy użyciu Kodu Autoryzacyjnego(SMS) lub Komunikatu PUSH,

2) w Bankowości Mobilnej – przy użyciu PIN.

9. Bank ma prawo odmówić realizacji Dyspozycji z przyczyn wyraźnie przewidzianych Regulaminem, Umową Ramową, Umową Pilotażową lub powszechnie obowiązującymi przepisami prawa, a także z przyczyn wskazanych w regulaminach Produktów Klienta.
10. Użytkownik może działać wyłącznie w granicach umocowania przez Klienta.

§6. Zasady bezpieczeństwa

1. Bank, świadcząc usługi na podstawie niniejszego Regulaminu, zobowiązuje się do zapewnienia Użytkownikowi bezpieczeństwa wykonywania Dyspozycji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych.
2. Użytkownik nie może dostarczać danych o charakterze bezprawnym i zobowiązany jest stosować się do zaleceń Banku w zakresie zasad bezpieczeństwa podczas korzystania z Kanałów Elektronicznych, w szczególności Użytkownik zobowiązany jest chronić:
   1) dane wykorzystywane do logowania w Kanałach Elektronicznych w szczególności: Identyfikator CIF, hasła, PINy, token mobilny,
   2) token sprzętowy, sprzęt z zaufanym urządzeniem zidentyfikowanym Metodą DFP,
   3) telefon komórkowy, którego numer został podany w Banku jako Telefon do Kodów autoryzacyjnych (telefon zaufany). Użytkownik zobowiązany jest do dokładnego zapoznania się z treścią Kodu autoryzacyjnego (SMS) w celu zweryfikowania jego zgodności ze złożoną przez Użytkownika Dyspozycją. Użytkownik ponosi pełną odpowiedzialność za udostępnianie Kodu autoryzacyjnego (SMS) osobom trzecim.
3. Użytkownik ma obowiązek zgłaszać niezwłocznie Bankowi utratę, kradzież, przywłaszczenie albo nieuprawnione użycie Urządzenia z zainstalowaną Aplikacją lub użycie urządzenia z Zaufaną przeglądarką.
4. Użytkownik ma obowiązek przestrzegać zasad bezpiecznego korzystania z Kanałów Elektronicznych umieszczonych na stronie internetowej Banku raz innych zaleceń dotyczących zasad bezpieczeństwa otrzymanych z Banku, w szczególności dotyczących instalacji na komputerze, aktualnego programu antywirusowego (wraz z aktualną bazą wirusów) oraz zapory sieciowej firewall.
5. Użytkownik ma obowiązek jak najszybciej zmienić PIN / Hasło Dostępu lub zablokować swoje Kanały Elektroniczne, a także niezwłocznie powiadomić Bank, jeśli:
   1) Użytkownik podejrzewa lub wie, że ktoś inny uzyskał dostęp do jego danych do logowania do Kanałów Elektronicznych,
   2) ktoś inny użył Kanałów Elektronicznych Użytkownika lub w przypadku 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,
   3) Użytkownik zidentyfikował transakcje lub inne operacje, których nie zlecał,
   4) Użytkownik utracił dane do logowania do Kanałów Elektronicznych lub ktoś mu je ukradł,
   5) Użytkownik utracił lub zmienił Telefon Zaufany do Kodów Autoryzacyjnych (SMS) lub numer telefonu Zaufanego podany do kontaktu z Bankiem – np. utracił telefon z kartą SIM lub kartę SIM lub Urządzenie z zainstalowaną Aplikacją,
   6) Użytkownik podejrzewa, że jego Urządzenie jest zainfekowane złośliwym oprogramowaniem.
6. W szczególnych sytuacjach Bank ma prawo wprowadzić dodatkowe ograniczenia i zabezpieczenia do Autoryzacji Dyspozycji składanych w Kanałach Elektronicznych.
7. Elektroniczny dostęp do Bankowości internetowej, Aplikacji Mobilnej wiąże się z ryzykiem – szczególnie, jeśli Użytkownik nie będzie przestrzegać zasad bezpieczeństwa określonych przez Bank. Ryzyko to obejmuje sytuacje, gdy Użytkownik przez pomyłkę potwierdzi niezamierzoną Dyspozycję lub gdy ktoś będzie próbował:
   1) ukraść dane (np. PIN, Identyfikator biometryczny) lub urządzenie (np. Telefon do Kodów autoryzacyjnych, telefon z Aplikacją) Użytkownika,
   2) podszyć się pod Bank i nakłonić Użytkownika do potwierdzenia fałszywych Dyspozycji,

3) przejąć za pomocą złośliwego oprogramowania kontrolę nad Urządzeniem.

8. Bank zaleca, aby Użytkownik używał przeglądarek internetowych, urządzeń i systemów operacyjnych z listy umieszczonej na stronie internetowej Banku. Jeśli Użytkownik wybierze inną przeglądarkę, urządzenie lub system operacyjny, Bank nie ponosi odpowiedzialności za ewentualne nieprawidłowości w funkcjonowaniu Bankowości internetowej i Aplikacji Mobilnej.
9. Dodatkowo Bank zaleca aby:
   1) zawsze sprawdzać poprawność adresu logowania do Bankowości internetowej,
   2) przed rozpoczęciem procesu logowania do Bankowości Internetowej, zwracać uwagę, czy przeglądarka nie wyświetla ostrzeżeń związanych z certyfikatem bezpieczeństwa (należy wejść w szczegóły i sprawdzić ważność certyfikatu) oraz na przedrostek HTTPS w adresie strony logowania, świadczący o szyfrowaniu połączenia ze stroną Bankowości Internetowej,
   3) przed potwierdzeniem operacji przeczytać dokładnie całą treść wiadomości z Kodem Autoryzacyjnym (SMS) lub Komunikatu PUSH. Bank nigdy nie poprosi o potwierdzenie operacji, która nie została zlecona przez Użytkownika,
   4) regularnie dokonywać aktualizacji systemu operacyjnego oraz zainstalowanego na nim oprogramowania, w szczególności oprogramowania antywirusowego (wraz z bazą sygnatur wirusów) oraz wykorzystywanej przeglądarki internetowej,
   5) nie korzystać z niezaufanych urządzeń do logowania do Bankowości Internetowej (np. w kafejce internetowej) lub na komputerze, na którym zalogowany jest inny użytkownik - do tego celu nie należy również używać publicznych sieci Wi-Fi,
   6) nie korzystać z niezaufanych urządzeń do instalowania Aplikacji Mobilnej i logowania do niej – do tego celu nie należy również używać publicznych sieci Wi-Fi,
   7) zwrócić szczególną uwagę na ataki mające na celu namówienie do wykonania jakiejś akcji (np. kliknięcie w link, pobranie oprogramowania, podanie swoich danych), które są przesyłane w e-mailach, wiadomościach SMS/MMS, Komunikatach PUSH, sieciach społecznościowych, komunikatorach lub są przekazywane telefonicznie,
   8) nie otwierać załączników ani nie używać odnośników z podejrzanych e-maili (np. z błędami, literówkami, nieskładną gramatyką; pochodzących z innego adresu niż oficjalny, które nie były oczekiwane itp.) oraz aby na te wiadomości nie odpowiadać. Fałszywe maile są najczęstszą przyczyną zarażenia komputerów niebezpiecznym, złośliwym oprogramowaniem.
10. Użytkownik ponosi odpowiedzialność z tytułu umożliwienia osobom trzecim zarejestrowania przez ich swoich Identyfikatorów biometrycznych na urządzeniu mobilnym, na którym jest zainstalowana Aplikacja Mobilna z włączoną funkcją Logowania poprzez Biometrię.
11. Bank nigdy nie będzie wymagał od Klienta podania hasła do konta lub innych wrażliwych danych za pomocą wiadomości e-mail lub wiadomości SMS. Każdy email lub wiadomość SMS z niewiadomego źródła z linkiem lub odesłaniem do bankowości elektronicznej należy traktować jako próbę phishingu lub innej metody socjotechnicznej. W przypadku otrzymania takiej wiadomości należy ją niezwłocznie usunąć. Dodatkowo wskazane jest również powiadomić Bank, iż taka sytuacja miała miejsce.
12. Istotne dane (adres, numery PESEL, hasła, Identyfikator CIF i inne wrażliwe dane) powinny być należycie chronione. Niedopuszczalnym jest udostępnianie przez Użytkownika swoich danych niezaufanym podmiotom lub osobom. Należy chronić swoje dokumenty, a w razie ich zagubienia bądź kradzieży natychmiast je zastrzec. Należy pamiętać, że przejęcie danych przez przestępców może zostać przez nich wykorzystane do kradzieży tożsamości, danych lub środków.
13. W szczególności należy zwracać uwagę na informacje o nowych zagrożeniach – na stronach internetowych Banku regularnie pojawiają się informacje w jaki sposób je rozpoznać i jak się przed nimi ustrzec (w sekcji Nowe zagrożenia oraz poprzez bannery informacyjne na stronie logowania).

14. Należy zwracać uwagę na treści znajdujące się na stronie logowania do Bankowości Internetowej. Jeśli proces logowania wygląda inaczej niż zwykle (np. trwa znacznie dłużej, pojawiają się nowe okienka) należy niezwłocznie zaniechać logowania i skontaktować się z Contact Center - może to świadczyć o tym, że komputer jest zarażony złośliwym oprogramowaniem.
15. W przypadku pytań/wątpliwości dotyczących bezpieczeństwa usług Banku lub zgłoszenia zdarzenia związanego z bezpieczeństwem prosimy o kontakt z Contact Center lub dowolnym oddziałem Alior Banku.
16. W przypadku wątpliwości dotyczących autentyczności komunikatów bezpieczeństwa otrzymywanych drogą mailową lub innym kanałem, należy porównać je z informacjami znajdującymi się na stronach Banku w sekcji Bezpieczeństwo.
17. Bank zastrzega sobie prawo wprowadzenia dodatkowych ograniczeń i zabezpieczeń w stosunku do Dyspozycji składanych w Kanałach Elektronicznych, w przypadku wystąpienia ważnych okoliczności podyktowanych zachowaniem bezpieczeństwa systemów informatycznych Banku, ochroną danych Użytkowników, zapobieganiu i przeciwdziałaniu oszustwom.

§ 7. Zablokowanie Kanałów Elektronicznych

1. Zablokowanie oznacza brak możliwości korzystania przez Użytkownika z danego Kanału Elektronicznego. Zablokowanie Bankowości Internetowej jest równoznaczne z zablokowaniem Bankowości Mobilnej; zablokowanie Bankowości Mobilnej jest równoznaczne z zablokowaniem Bankowości Internetowej.
2. Kanały Elektroniczne mogą zostać zablokowane niezależnie od siebie – pojedynczo lub wszystkie jednocześnie.
3. Użytkownik może zablokować Kanały Elektroniczne, jeśli złoży Dyspozycję blokady na Infolinii, w Placówce lub innymi kanałami udostępnionymi przez Bank.
4. Bank może zablokować Kanały Elektroniczne – jeśli:
   1) Użytkownik przekroczy dozwoloną liczbę błędnych logowań: dla Bankowości Internetowej i Mobilnej. Liczba błędnych logowań definiowana jest przez reguły bezpieczeństwa Banku i może być niezależna dla wszystkich kanałów kontaktu udostępnionych przez Bank,
   2) Użytkownik przekroczy dozwoloną liczbę błędnych autoryzacji: dla Bankowości Internetowej i Mobilnej Liczba błędnych autoryzacji definiowana jest przez reguły bezpieczeństwa Banku i może być niezależna dla wszystkich kanałów kontaktu udostępnionych przez Bank,
   3) wystąpi zagrożenie przechwycenia danych Użytkownika przez złośliwe oprogramowanie,
   4) Bank wychwyci częste logowanie się danymi Użytkownika w krótkim czasie,
   5) Bank podejrzewa, że nieuprawniona osoba trzecia ma dostęp do Kanałów Elektronicznych Użytkownika,
   6) ktoś będzie wykorzystywał systemy lub Kanały Elektroniczne w Banku niezgodnie z prawem,
   7) ktoś wykona działania, które mogą zagrozić bezpieczeństwu systemów i danych w Banku,
   8) Użytkownik nie aktywuje Kanału Elektronicznego w ciągu 90 dni od podpisania Umowy,
   9) Użytkownik nie korzysta z Kanałów Elektronicznych – w ciągu 90 dni oraz nie ma aktywnych Produktów i Usług ani pełnomocnictw/ uprawnień do zarządzania Produktami i Usługami innych Użytkowników.
5. Bank niezwłocznie poinformuje Klienta o zablokowaniu danego Kanału Elektronicznego, chyba że byłoby to nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów. Nie dotyczy to sytuacji opisanych w punkcie 4 podpunkt 1),2), 8),9) powyżej.
6. Bank odblokowuje Kanały Elektroniczne, jeżeli przestały istnieć podstawy do utrzymywania blokady.
7. Użytkownik może odblokować Bankowość Internetową i Aplikację Mobilną:
   1) w Placówce,
   2) Dyspozycją, którą złoży poprzez Infolinię

   – z wyłączeniem ust. 4 pkt 8) i 9) oraz blokad wynikających ze względów bezpieczeństwa.

§ 8. Silne Uwierzytelnienie Użytkownika

1. Stosujemy Silne Uwierzytelnienie w przypadku, gdy:
   1) Użytkownik uzyskuje dostęp do rachunku w trybie on-line za pośrednictwem Bankowości Internetowej lub Bankowości Mobilnej lub
   2) inicjuje transakcję płatniczą za pośrednictwem Bankowości Internetowej lub Bankowości Mobilnej lub
   3) poprzez Kanał Elektroniczny przeprowadza czynność, która może się wiązać z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć, w tym kiedy Użytkownik za pośrednictwem Bankowości Internetowej lub Bankowości Mobilnej inicjuje zmianę danych dostępowych do Kanałów Elektronicznych, zmianę danych lub metod wykorzystywanych w ramach Silnego uwierzytelnienia, zmianę limitów operacji dla karty płatniczej, aktywację karty płatniczej.
2. Przy logowaniu do Bankowości Internetowej, stosujemy Silne Uwierzytelnienie z zastosowaniem następujących metod:
   1) Użytkownik podaje Identyfikator oraz Hasło Dostępu a następnie:
      a) w przypadku logowania przy użyciu Kodu Autoryzacyjnego (SMS) – wpisuje Kod Autoryzacyjny (SMS) w Bankowości Internetowej,
      b) w przypadku logowania przy użyciu Komunikatu PUSH – Użytkownik zatwierdza Komunikat PUSH na Urządzeniu domyślnym.
   2) Użytkownik może zdefiniować urządzenie, z którego następuje logowanie jako Urządzenie Dedykowane. W takim przypadku Użytkownik potwierdza w Bankowości Internetowej dane urządzenie jako Urządzenie Dedykowane i zobowiązany jest zapewnić, że będzie jedynym Użytkownikiem tego urządzenia. Następnie przy każdorazowym logowaniu Bank weryfikuje, czy Użytkownik dokonuje logowania przy użyciu Urządzenia Dedykowanego. Logowanie następuje po podaniu Identyfikatora i Hasła przez Użytkownika, a następnie zweryfikowaniu Urządzenia Dedykowanego przez Bank.
   3) Logowanie przy użyciu Urządzenia Dedykowanego może następować przez określony przez Bank okres, przy czym Bank może wymagać Uwierzytelnienia przy pomocy Kodu autoryzacyjnego (SMS) także ze względów bezpieczeństwa.
3. Przy logowaniu do Bankowości Mobilnej, stosujemy Silne Uwierzytelnienie z zastosowaniem następujących metod:
   1) zweryfikowanie przez Bank Urządzenia, z aktywną Aplikacją Mobilną, a następnie:
      a) w przypadku logowania przy użyciu PIN – podanie przez Użytkownika PIN w Aplikacji Mobilnej,
      b) w przypadku logowania przy użyciu Uwierzytelnienia biometrycznego – Uwierzytelnienie Użytkownika za pomocą Identyfikatora biometrycznego.
4. Użytkownik, może wskazać przeglądarkę, z której korzysta jako Przeglądarkę Zaufaną. Może to zrobić podczas logowania do Bankowości Internetowej lub podczas korzystania z niej. Okres ważności przeglądarki jako Przeglądarki Zaufanej jest wskazany w Bankowości Internetowej.
5. Użytkownik jest zobowiązany do:
   1) posiadania Urządzenia domyślnego i Urządzenia Dedykowanego , jako jedyny Użytkownik,
   2) nieudostępniania Urządzenia domyślnego i Urządzenia Dedykowanego osobom trzecim.

§ 9. Reklamacje

1. Użytkownik zobowiązany jest na bieżąco sprawdzać prawidłowość wykonania Dyspozycji.
2. Użytkownik może zgłosić reklamację:
   1) bezpośrednio –w Placówce,
   2) telefonicznie – w Contact Center,
   3) elektronicznie – w Bankowości Internetowej lub Aplikacji (dla Użytkownika zalogowanego),
   4) listownie – na adres korespondencyjny Banku,
   5) elektronicznie – na adres do doręczeń elektronicznych (e-Doręczenia): AE:PL-18375-10021-DTBRC-21.

3. Odpowiedź na reklamację udzielana jest na piśmie w postaci papierowej. Na wniosek Klienta dodatkowo odpowiedź na reklamację może zostać dostarczona poprzez Bankowość Internetową lub poprzez SMS.
4. Bank rozpatruje reklamacje najszybciej, jak to możliwe:
   1) do 15 dni roboczych od otrzymania reklamacji, jeśli dotyczy ona praw i obowiązków wynikających z Ustawy UUP, w tym usług płatniczych,
   2) do 30 dni kalendarzowych od otrzymania reklamacji, jeśli dotyczy ona innych przypadków.
5. Jeśli reklamacja dotyczy szczególnie skomplikowanych przypadków, Bank może odpowiedzieć na nią później. W takim przypadku Bank ma obowiązek wskazać Użytkownikowi:
   1) przyczynę opóźnienia,
   2) okoliczności, które muszą zostać ustalone dla rozpatrzenia sprawy,
   3) przewidywany termin rozpatrzenia reklamacji i udzielenia odpowiedzi – nie może on jednak przekroczyć 35 dni roboczych od otrzymania reklamacji opisanych w ust. 4 pkt 1 lub 60 dni kalendarzowych w pozostałych przypadkach, opisanych w ust. 4 pkt 2.
6. Użytkownik i Bank mają obowiązek współpracować ze sobą podczas rozpatrywania reklamacji.
7. Użytkownik powinien dostarczyć Bankowi wszelkie informacje i dokumentację dotyczącą reklamacji, a także zachować potwierdzenie Dyspozycji do momentu jej rozliczenia, aby móc udokumentować ewentualne niezgodności.
8. Bank może warunkowo uznać reklamację Użytkownika i zwrócić mu lub odblokować kwotę objętą reklamacją, zanim rozpatrzy tę reklamację. Jeśli jednak rozpatrzy reklamację negatywnie, Bank obciąży rachunek Klienta tą kwotą – niezależnie od salda dostępnego na rachunku. Bankowi przysługuje wobec Klienta roszczenie o zwrot do Banku środków z tytułu uznania rachunku Bankowego reklamowaną kwotą.
9. Jeśli Bank warunkowo uzna reklamację i zwróci lub odblokuje na rachunku daną kwotę, Klient nie może zamknąć tego rachunku do czasu rozpatrzenia reklamacji lub ewentualnego zwrotu Bankowi danej kwoty.
10. Klient powinien niezwłocznie powiadomić Bank o stwierdzonych, nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych. Roszczenia Klienta z tytułu nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcji płatniczych wygasają w terminie 3 miesięcy od dnia obciążenia Rachunku płatniczego albo od dnia, w którym transakcja miała być wykonana.
11. Klient, który złożył reklamacje, ma obowiązek w terminie regulować zobowiązania, które wynikają z Umowy Ramowej lub Umowy Pilotażowej.
12. Użytkownik niezadowolony ze sposobu rozpatrzenia reklamacji uprawniony jest do zwrócenia się w sprawie sporu dotyczącego relacji z Bankiem z wnioskiem do Rzecznika Finansowego.

§ 10. Zmiana Regulaminu.

1. Bank zastrzega sobie prawo do dokonania zmiany niniejszego Regulaminu, wyłącznie w przypadku wystąpienia przynajmniej jednej z poniższych przyczyn:
   1) zmiana powszechnie obowiązujących przepisów prawa regulujących wykonywanie Regulaminu przez Bank. Zmiana nastąpi w zakresie, w jakim zmiany mają bezpośredni wpływ na postanowienia zmienianych postanowień Regulaminu,
   2) wydanie decyzji, zalecenia, rekomendacji lub interpretacji dotyczących wykonywania Regulaminu, przez organ administracji publicznej lub inny organ, który na mocy powszechnie obowiązujących przepisów prawa ma lub uzyska w przyszłości władcze uprawnienia w stosunku do Banku, w tym przez Narodowy Bank Polski, Komisję Nadzoru Finansowego, Europejski Urząd Nadzoru Bankowego (EBA), Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) – w zakresie w jakim te decyzje, zalecenia, rekomendacje lub interpretacje mają bezpośredni wpływ na postanowienia zmienianej części Regulaminu,
   3) udostępnienie nowych funkcjonalności w Kanałach Elektronicznych (dalej: „funkcjonalność"), z zastrzeżeniem, że zmiany dokonane przez Bank nie mogą być podstawą do wprowadzenia lub zwiększenia opłat i prowizji w zakresie obsługi funkcjonalności (jeżeli zmiany są dokonywane bez zgody Klienta),

4) wycofanie funkcjonalności, w przypadku, jeśli koszt ponoszony przez Bank wynikający z utrzymania funkcjonalności jest: 1) niewspółmierny do liczby Klientów wykorzystujących daną funkcjonalność lub 2) liczba Klientów korzystających z danej funkcjonalności jest nieznaczna w stosunku do ogółu Klientów korzystających z systemu, który oferuje daną funkcjonalność lub 3) funkcjonalność jest przestarzała technologicznie w porównaniu z rozwiązaniami oferowanymi na rynku bankowym. O wycofaniu funkcjonalności Bank zawiadomi Klienta z minimum trzymiesięcznym wyprzedzeniem,
5) zmiana formy wykonywania usługi poprzez jej digitalizację (przeniesienie do Kanałów Elektronicznych), o ile zmiana nie jest sprzeczna z powszechnie obowiązującymi przepisami prawa lub wyraźnym wyborem Klienta wyrażonym przy zawieraniu Umowy,
6) wycofanie poszczególnych usług świadczonych w ramach Regulaminu, jeśli koszt ponoszony przez Bank w związku z wykonywaniem usługi jest: 1) niewspółmierny do liczby Klientów korzystających z usługi lub 2) liczba Klientów korzystających z danej usługi jest nieznaczna w stosunku do ogółu Klientów do których ma zastosowanie Regulamin. Wycofywane usługi nie mogą stanowić istotnych elementów treści Regulaminu. O wycofywaniu usługi Bank poinformuje Klienta z minimum trzymiesięcznym wyprzedzeniem,
7) zmiana aktualnie wykorzystywanych metod uwierzytelnienia w Kanałach Elektronicznych Banku, jeżeli na rynku finansowym udostępnione zostaną rozwiązania bezpieczniejsze w porównaniu do aktualnie stosowanych metod uwierzytelniania,
8) udostępnienie Klientom nowych usług lub funkcjonalności o charakterze opcjonalnym,
9) w razie dokonania zmian nazw usług lub uproszczenia postanowień Regulaminu, z zastrzeżeniem, że zmiany będą miały charakter redakcyjny i nie wpłyną na wzajemne prawa i obowiązki Banku i Klienta,
10) wprowadzenie zmian porządkowych wynikających ze zmian wprowadzonych z przyczyn wskazanych w punktach 1-9 powyżej.

2. W przypadku zmiany postanowień Regulaminu w czasie trwania Umowy Pilotażowej, Bank zobowiązany jest doręczyć Klientowi wprowadzone zmiany do Regulaminu lub Regulamin uwzględniający wprowadzone zmiany wraz z określeniem terminu wejścia w życie zmian, nie krótszego niż 14 dni od momentu doręczenia. Bank może powiadomić o zmianach:
   1) poprzez zamieszczenie zmian w wyciągu bankowym z rachunku doręczanym Klientowi, w sposób ustalony w umowie rachunku lub
   2) poprzez przesłanie wiadomości w formie elektronicznej na adres e-mail - w przypadku oferowania usługi przez Bank oraz podania przez Klienta, posiadacza rachunku/pakietu adresu e-mail do komunikacji z Bankiem lub
   3) poprzez dostarczenie wiadomości Klientowi w formie elektronicznej, za pośrednictwem systemu Bankowości Internetowej.
3. Jeżeli w terminie 14 dni od otrzymania tekstu wprowadzonych zmian Klient nie dokona wypowiedzenia Umowy Pilotażowej lub Umowy Ramowej uznaje się, że zmiany zostały przyjęte i obowiązują strony.

§ 11. Postanowienia końcowe

1. Na podstawie art. 16 Ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (Dz. U. Nr 199, poz. 1175) Bank wyłącza stosowanie w całości przepisy Działu II ustawy o usługach płatniczych. Strony postanawiają także – zgodnie z art. 33 ustawy o usługach płatniczych - o nie stosowaniu art. 35-37, art. 45, art. 46 ust. 2-5, art. 47, oraz art. 144-146 tej ustawy, uznając za wystarczającą regulację poczynioną w niniejszym Regulaminie oraz w obowiązujących Klienta regulaminach produktowych, a w dalszym zakresie odsyłając do reguł ogólnych prawa cywilnego. Termin wygaśnięcia roszczeń, o którym mowa w art. 44 ust. 2 ustawy z 19 sierpnia 2011 r. o usługach płatniczych strony ustalają na trzy miesiące.
2. Bank zastrzega sobie prawo do przeprowadzania prac serwisowych, które wiązać się mogą z przerwami technicznymi w systemie. O planowanych pracach Bank będzie informował Klienta z wyprzedzeniem 72 godzin za pośrednictwem Kanałów Elektronicznych.

Załącznik numer 1

Wykaz funkcjonalności dostępnych w Alior Business i Alior Business Mobile

Moduł lub grupa funkcjonalności	Funkcjonalność lub rodzaje operacji	Pakiet Firma
Limit liczby Użytkowników	Limit liczby Użytkowników w ramach Pakietu Abonamentowego	**1**
Personalizacja ustawień	Personalizacja pulpitu, wersje językowe (polska)	
Moduł Komunikacja (Inbox)	Platforma komunikacyjna dla dwukierunkowej wymiany korespondencji pomiędzy Bankiem i Klientem	
Informacje finansowe	Lista Rachunków Bankowych, historia operacji, wyciągi z Rachunków Bankowych (z wyłączeniem lokat), karty płatnicze (z wyłączeniem kart kredytowych)	
Kontrahenci	Lista zdefiniowanych kontrahentów, możliwość dodawania zarządzania listą kontrahentów	
Przelewy zdefiniowane	Lista przelewów zdefiniowanych, możliwość dodawania zarządzania listą przelewów zdefiniowanych	
Polecenie przelewu	Przelew krajowy wychodzący, przelew wewnętrzny/ własny (transfer między rachunkami prowadzonymi w Banku), przelew na rzecz organów podatkowych	
Zlecenia	Zarządzanie zleceniami - koszyk zleceń (podpisywanie i wysyłanie zleceń), historia zleceń	
Lokaty	Tworzenie lokat, przegląd lokat	
Aplikacja Mobilna	Aplikacja pobrana z autoryzowanego sklepu Google Play lub App Store i zainstalowana na Urządzeniu, dzięki któremu Użytkownik korzysta z usługi zapewniającej dostęp do swoich Produktów oraz możliwość składania dyspozycji z wykorzystaniem urządzeń mobilnych takich jak telefony komórkowe. Aplikacja występuje pod nazwą Alior Business Mobile.	