Obowiązuje: dla umów zawieranych od 13 listopada 2024 r.

Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych

POSTANOWIENIA OGÓLNE

§1

1. Niniejszy Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych określa zasady i warunki udostępniania informacji o produktach Użytkownika oraz składania dyspozycji za pośrednictwem Kanałów Elektronicznych.
2. Regulamin jest załącznikiem do Umowy o świadczenie usług oferowanych przez Bank dla Osoby fizycznej i stanowi jej integralną część.
3. O ile w Regulaminie nie wskazano inaczej, to postanowienia Regulaminu nie mają zastosowania do umów zawartych z T-Mobile Usługi Bankowe i usług świadczonych poprzez T-Mobile Usługi Bankowe – obowiązuje do 28 listopada 2020.

§2

Użyte w dalszej części Regulaminu pojęcia oznaczają:

Aktywacja systemu Bankowości Mobilnej – szereg czynności wykonywanych przez Użytkownika w Bankowości Mobilnej po zainstalowaniu Aplikacji Mobilnej, mających na celu zdefiniowanie metody identyfikacji i autoryzacji w Aplikacji Mobilnej. Szczegółowa Instrukcja aktywacji została umieszczona na stronach internetowych Banku;

Alior Kids - aplikacja zainstalowana na Urządzeniu, dzięki której Użytkownik korzysta z Bankowości Mobilnej przeznaczona dla osób małoletnich w wieku od 7. do ukończenia 13. roku życia.

Aplikacja Mobilna - aplikacja zainstalowana na Urządzeniu, dzięki której Użytkownik korzysta z Bankowości Mobilnej. Aplikacją może być m.in.: Aplikacja Alior Mobile, Aplikacja Giełda, Aplikacja Kantor Walutowy, Aplikacja Alior Kids. Zakres funkcjonalny Aplikacji Mobilnej, w tym rodzaje dyspozycji, jakie mogą zostać złożone przy jej pomocy znajdują się na stronie internetowej Banku;

Bank – Alior Bank Spółka Akcyjna z siedzibą w Warszawie;

Bankowość Internetowa (Alior Online) – usługa zapewniająca dostęp do informacji o Produktach Użytkownika oraz możliwość składania dyspozycji z wykorzystaniem sieci Internet i urządzenia wyposażonego w przeglądarkę internetową. Zakres funkcjonalny Bankowości Internetowej, w tym rodzaje dyspozycji, jakie mogą zostać złożone przy jej pomocy, znajdują się na stronie internetowej Banku;

Bankowość Mobilna – usługa zapewniająca dostęp do informacji o Produktach Użytkownika oraz możliwość składania dyspozycji z wykorzystaniem urządzeń mobilnych takich jak palmtopy, tablety i telefony komórkowe z dostępem do Internetu, za pomocą przeglądarek internetowych lub Aplikacji Mobilnej; Zakres funkcjonalny Bankowości Mobilnej, w tym rodzaje dyspozycji, jakie mogą zostać złożone przy jej pomocy, znajdują się na stronie internetowej Banku.

Bankowość Telefoniczna – usługa zapewniająca dostęp do informacji o Produktach Użytkownika oraz możliwość składania dyspozycji przy użyciu telefonu z wybieraniem tonowym (może zostać naliczona opłata za połączenie zgodnie z taryfą operatora);

Biometria – metoda identyfikacji i uwierzytelnienia Użytkownika oraz autoryzacji Dyspozycji, polegająca na porównaniu indywidualnych cech fizycznych Klienta, ze wzorcem przechowywanym w systemie informatycznym producenta urządzenia, na którym zainstalowana jest Aplikacja Mobilna;

Biuro Maklerskie – wydzielona jednostka organizacyjna Banku odpowiedzialna za świadczenie przez Bank usług maklerskich;

Contact Center – jednostka Banku lub Biura Maklerskiego, świadcząca telefoniczną obsługę dla aktualnych oraz potencjalnych Użytkowników, w zakresie informacyjnym, sprzedażowym oraz transakcyjnym;

Dane identyfikujące – zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;

Dyspozycja – oświadczenie woli złożone przez Użytkownika za pośrednictwem Kanałów Elektronicznych i autoryzowane w sposób właściwy dla danego kanału;

Fraza Weryfikacyjna (hasło do zwrotnej weryfikacji Banku) – słowo, zwrot lub ciąg znaków ustalone przez Użytkownika, wykorzystywane do uwierzytelnienia pracownika Banku kontaktującego się telefonicznie z Użytkownikiem w sytuacji, gdy kontakt inicjowany jest przez Bank;

Hasło Dostępu – ciąg znaków, ustalany samodzielnie przez Użytkownika w Bankowości Internetowej, który użyty wraz z Identyfikatorem umożliwia dostęp do Bankowości Internetowej. W przypadku Użytkowników, których obowiązują umowy zawarte z T-Mobile Usługi Bankowe (od 29 listopada 2020 r.: T-Mobile Usługi Bankowe były Oddział Alior Bank S.A.), wykorzystywane może być hasło zdefiniowane w bankowości internetowej T-Mobile Usługi Bankowe (od 29 listopada 2020 r.: T-Mobile Usługi Bankowe były Oddział Alior Bank S.A.);

Hasło Startowe – ciąg cyfr przesyłany Użytkownikowi na Telefon do Kodów autoryzacyjnych w formie wiadomości tekstowej, służący do aktywacji Bankowości Internetowej;

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

Identyfikator biometryczny – zapis indywidualnych cech fizycznych Klienta (m.in. takich jak odcisk palca lub skan wizerunku jego twarzy), przechowywany i udostępniany na urządzeniu mobilnym przez jego producenta, umożliwiający logowanie do Aplikacji Mobilnej oraz autoryzację wybranych dyspozycji za pośrednictwem Aplikacji Mobilnej. Identyfikator biometryczny jest dostępny:

1. W Aplikacji Mobilnej, na urządzeniach z systemem operacyjnym iOS (od wersji numer 11.0), wspierającym rozwiązanie TouchID (czytnik linii papilarnych) lub FaceID (czytnik rozpoznawania twarzy) i umożliwia:

a. logowanie do Aplikacji Mobilnej,
b. autoryzację wybranych Dyspozycji zlecanych w Bankowości Mobilnej (od wersji numer 1.8.0).

2. W Aplikacji Mobilnej (od wersji numer 1.8.0) na urządzeniu z systemem operacyjnym Android (od wersji numer 6.0), wspierającym rozwiązanie Fingerprint Authentication (identyfikacja odcisku palca) i umożliwia:
   a. logowanie do Aplikacji Mobilnej,
   b. autoryzację wybranych Dyspozycji zlecanych w Bankowości Mobilnej.

IVR – usługa zapewniająca całodobowy, automatyczny dostęp do informacji o Produktach Użytkownika przy użyciu telefonu z wybieraniem tonowym;

Kanały Elektroniczne – Bankowość Internetowa (w tym traktowana odrębnie – funkcjonalność przeznaczona do inicjowania płatności przez podmioty trzecie oraz funkcjonalność przeznaczona do dostępu przez podmioty trzecie do informacji o rachunkach płatniczych, jak również przeznaczona dla usług dostawców wydających instrumenty oparte na karcie), Bankowość Telefoniczna, Bankowość Mobilna, IVR;

Kod autoryzacyjny – kod w formie wiadomości tekstowej przesyłany na Telefon zdefiniowany przez Użytkownika do autoryzacji zleceń, służący do autoryzacji Dyspozycji składanych przez Użytkownika w ramach Bankowości Internetowej, Bankowości Mobilnej lub Bankowości Telefonicznej;

Kod aktywacyjny - kod wyświetlany w Panelu rodzica, w aplikacji Alior Mobile, służący do aktywacji Aplikacji Alior Kids;

Limity kwotowe – to parametry określające wartość jednorazowej/dziennej/miesięcznej kwoty transakcji, przypisane według podziału dla bankowości internetowej (w tym dla dostawców świadczących usługi inicjowania płatności), dla bankowości mobilnej, dla kodów BLIK i dla poleceń przelewu na telefon BLIK

Kod BLIK – 6-cyfrowy kod generowany przez Aplikację Mobilną, który może być zastosowany w przypadku niektórych transakcji w Usłudze BLIK;

Komunikat PUSH – powiadomienia zdalnie wysyłane do Aplikacji Mobilnej przez Bank, dotyczące zdarzeń na Rachunkach, produktach, do których Klient ma dostęp lub zawierające inne 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);

MojeID – System pozwalający na autoryzację oświadczeń, w oparciu o bankowe mechanizmy uwierzytelnienia dostarczone przez Krajową Izbę Rozliczeniową S.A. (obowiązuje od momentu udostępnienia przez Bank, po uprzednim poinformowaniu Użytkownika nie później niż 7 dni przed datą udostępnienia usługi, poprzez Kanały Elektroniczne);

Panel rodzica - funkcjonalność aplikacji Alior Mobile, umożliwiająca przedstawicielom ustawowym zarządzanie dostępnymi funkcjonalnościami, ich limitami oraz produktami małoletniego Użytkownika, do czasu ukończenia 13 roku życia.

PIN autoryzacyjny – ciąg cyfr ustalany przez Użytkownika w sposób poufny podczas aktywacji Aplikacji Mobilnej, służący do logowania i autoryzacji Dyspozycji zlecanych przy pomocy Aplikacji Mobilnej;

Placówka Banku – jednostka organizacyjna Banku wykonująca czynności bankowe;

Powiadomienia finansowe – usługa umożliwiająca przesyłanie Użytkownikowi, informacji na temat Produktów użytkownika oraz usług świadczonych przez Bank lub Biuro Maklerskie; powiadomienia są przesyłane w postaci jawnej (nieszyfrowanej);

Polecenie przelewu na telefon BLIK – typ płatności krajowej w PLN umożliwiający zlecanie i otrzymywanie poleceń przelewu przez Użytkownika, którego tożsamość identyfikowana jest przez numer Telefonu do kodów Autoryzacyjnych. Zlecanie Polecenia przelewu na telefon BLIK jest dostępne bez dodatkowej aktywacji usługi w Aplikacji Mobilnej. Użytkownik wysyłając Polecenie przelewu na telefon BLIK wyraża zgodę na przekazanie przez Bank numeru rachunku bankowego innym uczestnikom transakcji. Odbieranie Polecenia przelewu na telefon BLIK jest dostępne po dodatkowej aktywacji usługi w Aplikacji Mobilnej. Aplikacja Mobilna posiada funkcję wyrejestrowania danego numeru telefonu z innego banku i powiązania go z rachunkiem w Alior Bank S.A.;

Profil behawioralny– profil Użytkownika tworzony w oparciu o charakterystyczne cechy behawioralne Użytkownika związane z użytkowaniem przez niego Bankowości Internetowej lub Bankowości Mobilnej – w tym np. charakterystyki użycia w tych Kanałach Elektronicznych urządzeń typu klawiatura, ekran dotykowy, płytka dotykowa, mysz lub sensorów urządzeń mobilnych. W oparciu o Profil behawioralny może być realizowane Silne uwierzytelnienie, jak również autoryzacja wybranych Dyspozycji;

Prośba o przelew BLIK – powiadomienie umożliwiające wysyłanie oraz odbieranie przez Użytkownika i dyspozycji na wykonanie Polecenia przelewu na telefon BLIK. Akceptacja Prośby o przelew BLIK przez jej adresata, automatycznie uruchamia wykonanie Polecenia przelewu na telefon BLIK, zgodnie z danymi zawartymi w dyspozycji. Ważność powiadomienia wynosi 72 godziny od momentu jego utworzenia. Prośba o przelew BLIK jest aktywowana automatycznie podczas aktywacji Polecenia przelewu na telefon BLIK. Aktywacja Prośby o przelew oznacza wyrażenie przez Użytkownika zgody na przekazanie przez Bank numeru rachunku bankowego innym uczestnikom transakcji (usługa obowiązuje od momentu udostępnienia przez Bank, po uprzednim poinformowaniu Użytkownika nie później niż 7 dni przed datą udostępnienia usługi, poprzez Kanały Elektroniczne);

Produkt – rachunek lub usługa oferowana przez Bank lub Biuro Maklerskie świadczona na podstawie zawarcia właściwej umowy i regulaminu;

Silne uwierzytelnienie – uwierzytelnienie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:
a) wiedza o czymś, o czym wie wyłącznie Użytkownik,
b) posiadanie czegoś, co posiada wyłącznie Użytkownik,
c) cechy charakterystyczne Użytkownika,
- będących integralną częścią tego uwierzytelnienia oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych;

Środek identyfikacji elektronicznej - niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usług online;

Telefon do Kodów autoryzacyjnych – podany przez Użytkownika numer telefonu komórkowego, na który przesyłane jest Hasło Startowe oraz Kody autoryzacyjne;

Tele PIN – ciąg cyfr ustalany przez Użytkownika w sposób poufny podczas aktywacji Bankowości Telefonicznej, służący do weryfikacji Użytkownika w ramach tej usługi;

T-Mobile Usługi Bankowe – oddział Alior Banku S.A. (obowiązuje do 28 listopada 2020 r.);

Trwały nośnik – nośnik umożliwiający udostępnienie Klientowi adresowanych do niego informacji w sposób umożliwiający dostęp do nich przez okres odpowiedni do celów sporządzenia tych informacji i pozwalający na odtworzenie przechowywanych informacji w niezmienionej postaci;

Umowa – Umowa ramowa o świadczenie usług oferowanych przez Bank dla Osoby Fizycznej, zawarta pomiędzy Bankiem i osobą fizyczną, na podstawie, której możliwe jest korzystanie z Kanałów Elektronicznych;

Urządzenie – urządzenie (w szczególności telefon komórkowy będący smartfonem), na którym

zainstalowana jest Aplikacja Mobilna (w tym z Usługą BLIK);
Urządzenie domyślne – urządzenie które Użytkownik używa w celu uwierzytelnienia Użytkownika i które jest uzgodnione pomiędzy Bankiem i Użytkownikiem (powiązane z Użytkownikiem) w tym celu. Urządzenie domyślne służy do przekazywania Komunikatów PUSH autoryzacyjnych;
Usługa/Usługa BLIK – usługa umożliwiająca składanie dyspozycji przy użyciu Aplikacji Mobilnej;
Uwierzytelnienie biometryczne – metoda logowania do Aplikacji Mobilnej umożliwiająca uwierzytelnienie użytkownika za pomocą Identyfikatora Biometrycznego;
Użytkownik – osoba fizyczna, która zawarła Umowę i jest uprawniona do składania Dyspozycji za pośrednictwem Kanałów Elektronicznych;
Wypłata gotówki BLIK – transakcja wypłaty w bankomacie z wykorzystaniem kodu BLIK.

WARUNKI UDOSTĘPNIANIA KANAŁÓW ELEKTRONICZNYCH

§3

Kanały Elektroniczne, są udostępniane po spełnieniu łącznie następujących warunków:

1. Zawarcia Umowy przez Użytkownika lub jego przedstawiciela ustawowego:
   a. osobiście, w Placówce Banku,
   b. korespondencyjnie,
   c. w inny wskazany przez Bank sposób zgodny z obowiązującymi przepisami prawa.
2. Dokonania przez Użytkownika aktywacji wybranego Kanału Elektronicznego poprzez podanie Identyfikatora lub wskazanie danej osobowej oraz:
   a. Hasła Startowego oraz wybrania sposobu logowania - w przypadku Bankowości Internetowej,
   b. ustanowienia kodu PIN do Aplikacji Mobilnej – w przypadku Bankowości Mobilnej. W przypadku Aplikacji Alior Kids, dodatkowo wymagany jest Kod aktywacyjny, wygenerowany przez przedstawiciela ustawowego,
   c. przeprowadzenia pozytywnej weryfikacji danych osobowych podczas rozmowy z konsultantem Contact Center - w przypadku Bankowości Telefonicznej.

3. Małoletni Użytkownik może posiadać tylko jedną aktywną Aplikację Alior Kids.
4. Wraz z ukończeniem przez małoletniego Użytkownika 13. roku życia, dostęp do Aplikacji Alior Kids jest dezaktywowany przez Bank. Użytkownik ma możliwość korzystania z Bankowości Internetowej (Alior Online) oraz możliwość aktywowania Aplikacji Alior Mobile.

§4

Bankowość Internetowa lub Bankowość Mobilna mogą być aktywowane niezależnie od siebie, w dowolnej kolejności.

§5

Po dokonaniu aktywacji Kanałów Elektronicznych, Użytkownik uzyskuje dostęp do wybranych Produktów, w tym otwartych w przyszłości.

ZAKRES USŁUG KANAŁÓW ELEKTRONICZNYCH

§6

Kanały Elektroniczne umożliwiają Użytkownikowi zarządzanie środkami finansowymi, uzyskiwanie informacji o posiadanych Produktach, zawieranie umów o wybrane Produkty oraz zarządzanie Danymi identyfikującymi (obowiązuje od momentu udostępnienia przez Bank, po uprzednim poinformowaniu Użytkownika nie później niż 7 dni przed datą udostępnienia usługi, poprzez Kanały Elektroniczne).

§7

Bank może zmienić zakres informacji i Dyspozycji dostępnych za pośrednictwem Kanałów Elektronicznych w przypadku wprowadzania nowych lub zmiany powszechnie obowiązujących przepisów prawa lub zmian w ofercie Banku.

§8

1. Bank udostępnia Użytkownikom usługę Powiadomień finansowych będących potwierdzeniem zdarzenia na rachunku Użytkownika.
2. Powiadomienia finansowe mogą być przesyłane:
   a. jako powiadamianie SMS,
   b. jako wiadomość email,
   c. poprzez Bankowość Internetową,
   d. jako Komunikaty PUSH.
3. Zakres powiadomień definiowany jest przez Użytkownika poprzez formularz dostępny w Bankowości Internetowej lub Mobilnej z zastrzeżeniem ust. 5
4. Powiadomienia finansowe wysyłane są niezwłocznie po wystąpieniu zdarzenia, z zastrzeżeniem, że w godzinach nocnych wysyłane są jedynie powiadomienia krytyczne (informacje o godzinach i zakresie powiadomień zostały podane w Bankowości Internetowej).
5. Bank ma prawo wysyłać dodatkowe powiadomienia z informacją o zdarzeniach na rachunku. Za powiadomienia takie nie jest pobierana opłata.

REALIZACJA DYSPOZYCJI I ZASADY KORZYSTANIA Z KANAŁÓW ELEKTRONICZNYCH

§9

Dyspozycje za pośrednictwem Kanałów Elektronicznych mogą być składane codziennie, w ciągu całej doby, za wyjątkiem ogłoszonych wcześniej przerw konserwacyjnych.

§10

Aktualne informacje o trybie i warunkach realizacji Dyspozycji są publikowane na stronie internetowej Banku i Biura Maklerskiego.

§11

1. Dyspozycje składane przez Bankowość Internetową mogą wymagać autoryzacji za pomocą Kodu autoryzacyjnego, Komunikatu PUSH lub na podstawie Profilu behawioralnego.
2. Dyspozycje składane za pośrednictwem Aplikacji Mobilnej mogą wymagać autoryzacji za pomocą PINu autoryzacyjnego, Identyfikatora biometrycznego, Komunikatu PUSH lub na podstawie Profilu behawioralnego.
3. Dyspozycje składane przez Bankowość Telefoniczną mogą wymagać autoryzacji za pomocą Kodu autoryzacyjnego lub Komunikatu PUSH (usługa obowiązuje od momentu udostępnienia przez Bank, po uprzednim poinformowaniu Użytkownika nie później niż 7 dni przed datą udostępnienia usługi, poprzez Kanały Elektroniczne).
4. Użytkownik nie może podważać autentyczności prawidłowo zautoryzowanej Dyspozycji.

§12

1. Dyspozycja z bieżącą datą realizacji, prawidłowo zautoryzowana, nie może być anulowana.
2. Zapisy ust. 1 nie wykluczają możliwości złożenia Dyspozycji anulowania zlecenia w ramach świadczonych usług maklerskich na zasadach określonych w regulaminie świadczenia danej usługi maklerskiej.

§13

1. Dane niezbędne do prawidłowej realizacji Dyspozycji powinny być podane zgodnie z opisem pól występujących w formularzu Dyspozycji.
2. Przed dokonaniem autoryzacji, Użytkownik powinien upewnić się, że Dyspozycje są jednoznaczne i zgodne z jego intencją, w tym w szczególności te, które są zlecane na podstawie zdjęć faktur lub rachunków wykonywanych przez urządzenie mobilne.

§14

1. Bank rejestruje i przechowuje na nośnikach elektronicznych wszystkie rozmowy telefoniczne prowadzone w ramach Contact Center.
2. Użytkownik wyraża zgodę na rejestrowanie tych rozmów.
3. W przypadku braku zgody Użytkownika lub awarii urządzenia nagrywającego, Bank ma prawo odmówić przyjęcia Dyspozycji drogą telefoniczną.
4. W razie wątpliwości co do treści złożonej Dyspozycji, nagrania rozmów są rozstrzygające i mogą być wykorzystane w postępowaniu reklamacyjnym oraz dla celów dowodowych.

§15

Dyspozycje dotyczące obsługi zleceń stałych wykonywanych z rachunków bankowych oraz odwoływania poleceń przelewu z odroczoną datą realizacji są przyjmowane najpóźniej na jeden dzień roboczy przed datą realizacji Dyspozycji.

§16

Jeśli zachodzi uzasadnione podejrzenie co do autentyczności złożonej Dyspozycji, Bank może wstrzymać jej realizację do momentu wyjaśnienia wątpliwości lub odmówić jej wykonania.

§17

1. Maksymalna kwota, na jaką można zlecić polecenie przelewu poprzez Bankowość Internetową i Bankowość Mobilną, publikowana jest na stronie internetowej Banku i Biura Maklerskiego, przy czym limity te mogą być różne dla Bankowości Internetowej i Aplikacji Mobilnej oraz dla różnych typów Dyspozycji i różnych segmentów Użytkowników. Polecenia przelewu przekraczające wskazaną kwotę nie są realizowane.
2. W przypadku poleceń przelewu wykonywanych w walutach obcych, maksymalna kwota wyznaczana jest poprzez przeliczanie na PLN kwoty, o której mowa w ust. 1. Przeliczenie realizowane jest według aktualnego kursu kupna/sprzedaży dewiz obowiązującego w Banku w chwili zlecania polecenia przelewu.
3. Ograniczenie, o którym mowa w ust. 1 i 2 nie ma zastosowania do poleceń przelewu zlecanych z wykorzystaniem szablonu płatności zdefiniowanego w Placówce Banku oraz do poleceń przelewu własnych. Polecenia przelewu realizowane poprzez Bankowość Telefoniczną podlegają odrębnym Limitom kwotowym. Informacje o maksymalnej kwocie polecenia przelewu realizowanego poprzez Contact Center zamieszczone są na stronach internetowych Banku oraz dostępne u konsultantów.
4. Użytkownik, po zalogowaniu się do Bankowości Internetowej jako pełnomocnik klienta, w tym za pośrednictwem podmiotów, o których mowa w § 37, może realizować jedynie te czynności, do których jest umocowany na podstawie pełnomocnictwa.

USŁUGA BLIK, USŁUGA POLECEŃ PRZELEWU NA TELEFON BLIK ORAZ PROŚBA O PRZELEW BLIK – ZASADY REJESTRACJI USŁUGI, ZLECENIA DYSPOZYCJI, LIMITY I ROZLICZENIA OPERACJI

§18

1. Z Usługi BLIK, Poleceń przelewu na telefon BLIK oraz Prośby o przelew BLIK mogą korzystać wszyscy Klienci, którzy zainstalowali Aplikację Mobilną. Status powyższych usług można zweryfikować w ustawieniach Aplikacji Mobilnej i tam też jest możliwe aktywowanie i dezaktywowanie danej usługi.
2. Aktywacji Kodów BLIK dokonuje Użytkownik po aktywacji Aplikacji Mobilnej lub w sposób automatyczny w trakcie aktywacji Aplikacji Mobilnej z zastrzeżeniem ust. 5.
3. W przypadku, gdy telefon do Kodów Autoryzacyjnych nie jest powiązany z rachunkiem w innym banku, aktywacja zlecenia Polecenia przelewu na telefon BLIK może nastąpić w sposób automatyczny w trakcie aktywacji Aplikacji Mobilnej. Aktywacja powoduje, że Przelewy BLIK kierowane na powyższy numer telefonu będą księgowane na rachunku w Alior Bank S.A. zdefiniowany w ust. 4 § 20.
4. Do rejestracji w Usłudze BLIK, usłudze Poleceń przelewu na telefon BLIK oraz w usłudze Prośby o przelew BLIK, uprawnieni są Klienci spełniający łącznie warunki:
   a. posiadają odpowiednie wyposażenie techniczne, w szczególności urządzenie mobilne powiązane z numerem telefonu komórkowego operatora sieci telefonii komórkowej działającego na terytorium Rzeczpospolitej Polskiej,
   b. posiadają zawartą Umowę o świadczenie usług przez Bank dla osoby fizycznej,
   c. posiadają aktywną Aplikację mobilną,
   d. posiadają rachunek oszczędnościowo-rozliczeniowy w złotych prowadzony w Banku.
5. W przypadku Użytkownika Aplikacji Alior Kids aktywacji Kodów Blik dokonuje przedstawiciel ustawowy, w Panelu rodzica.

§19

1. Operacje wykonywane za pośrednictwem Aplikacji Mobilnej z Usługą BLIK oraz usługą Poleceń przelewu na telefon BLIK mogą być wykonywane w ramach jednorazowych, dziennych i miesięcznych Limitów kwotowych dla tej Usługi.
2. Po aktywacji, wartości limitów, o których mowa w ust. 1, są zgodne z limitami określonymi przez Bank.
3. Użytkownik może skorzystać z funkcjonalności składania dyspozycji bez konieczności zalogowania się do Aplikacji Mobilnej.
4. Użytkownik może modyfikować Limity kwotowe dla Usługi BLIK w Bankowości Internetowej (Alior Online).
5. Bank przyjmuje dyspozycje złożone za pośrednictwem kanału mobilnego z wyłączeniem okresu przerw niezbędnych do konserwacji, napraw technicznych lub przywrócenia poprawności funkcjonowania kanału mobilnego, w tym Aplikacji Mobilnej z Usługą BLIK.

§20

1. W ramach usługi BLIK oraz usługi Poleceń przelewu na telefon BLIK Bank udostępnia dokonywanie:
   a. zapłaty za towary lub usługi nabyte za pośrednictwem serwisu internetowego lub aplikacji podmiotu oferującego te towary lub usługi poprzez autoryzację operacji przez Użytkownika w Aplikacji Mobilnej z Usługą BLIK,
   b. operacji wypłat gotówki w wybranych bankomatach oraz terminalach płatniczych POS,
   c. operacji płatności za towary i usługi w oznaczonych punktach wyposażonych w terminale POS lub inne

urządzenia umożliwiające wykonanie operacji zlecanych za pośrednictwem kanału mobilnego.

2. W ramach usługi Prośby o przelew BLIK Bank udostępnia dokonywanie:
   a. dyspozycji na wykonanie Polecenia przelewu na telefon BLIK;
   b. automatycznej blokady odbioru dyspozycji Polecenia przelewu na telefon BLIK wysyłanych przez innych uczestników transakcji;
   c. automatycznego odrzucenia otrzymanych dyspozycji Polecenia przelewu na telefon BLIK, wysyłanych przez innych uczestników transakcji.
3. Każdorazowo jako numer telefonu powiązany z rachunkiem zdefiniowanym w ust.4 ustawiany jest Telefon do Kodów Autoryzacyjnych (dalej Alias). Użytkownik – aktywując usługę BLIK – wyraża zgodę na przetwarzanie danych zawartych w książce adresowej tego telefonu w celu prezentacji odbiorców, których numery telefonów są zarejestrowane w bazie BLIK. Użytkownik – aktywując usługę – wyraża zgodę na przekazanie przez Bank numeru rachunku bankowego innym uczestnikom transakcji. Zlecenie Polecenia przelewu na telefon BLIK oraz Prośby o przelew BLIK wymaga od Użytkownika podania numeru telefonicznego odbiorcy, kwoty oraz tytułu polecenia przelewu. Zmiana Telefonu do Kodów autoryzacyjnych, w przypadku aktywnej usługi Poleceń przelewu na telefon BLIK oraz Prośby o przelew na telefon BLIK, automatycznie ją wyłącza. W przypadku chęci aktualizacji Aliasu w usłudze Poleceń przelewu na telefon BLIK należy ponownie ją aktywować. Aktualizacja Aliasu w usłudze Poleceń przelewu na telefon BLIK automatycznie aktualizuje numer Telefonu zdefiniowany w usłudze Prośby o przelew BLIK.
4. Rachunkiem obciążanym w ramach Usługi BLIK, do obsługi Poleceń przelewu na telefon BLIK oraz Prośby o przelew BLIK jest rejestrowany rachunek opłat, który jest rachunkiem oszczędnościowo–rozliczeniowym w PLN;
5. Polecenia przelewu na telefon BLIK wychodzące z Banku są możliwe wyłącznie w sytuacji, gdy numer telefonu odbiorcy jest zarejestrowany w bazie telefonów BLIK, wówczas są realizowane jako:
   a. polecenia przelewu wewnętrzne, w sytuacji, gdy rachunek odbiorcy jest rachunkiem prowadzonym w Banku,
   b. polecenia przelewu Express Elixir, w sytuacji, gdy rachunek odbiorcy jest rachunkiem nieprowadzonym w Banku.

MojeID

§21

1. Z systemu MojeID mogą korzystać wszyscy Użytkownicy, którzy posiadają wydany przez Bank Środek identyfikacji elektronicznej.
2. Środek identyfikacji elektronicznej zawiera Dane identyfikujące.
3. Środek identyfikacji elektronicznej może zostać wydany tylko Użytkownikom o zweryfikowanej przez Bank tożsamości.
4. Środek identyfikacji elektronicznej wydawany jest na określony czas.
5. Do Danych identyfikujących dla osób fizycznych zaliczają się:
   a. nazwisko;
   b. imię lub imiona;
   c. data urodzenia;
   d. PESEL.
6. Zmiana Danych identyfikujących przez Użytkownika powoduje wygaśniecie obecnego Środka identyfikacji elektronicznej i wydanie w to miejsce nowego.
7. W ramach systemu MojeID mogą zostać przekazane za zgodą Użytkownika dodatkowe dane. Dane te będą przekazywane jako atrybuty dodatkowe.

ZASADY BEZPIECZEŃSTWA

§22

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.

§23

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 powinien z należytą starannością chronić dane wykorzystywane do logowania w Kanałach Elektronicznych (Identyfikator, w tym również Identyfikator biometryczny, hasła, PINy) oraz telefon komórkowy, którego numer został podany w Banku jako Telefon do Kodów autoryzacyjnych oraz zobowiązany jest każdorazowo do dokładnego zapoznania się z treścią powiadomienia SMS zawierającego poszczególny Kod autoryzacyjny lub Komunikatu PUSH, w celu zweryfikowania jego zgodności ze złożoną przez siebie Dyspozycją. Użytkownik jest zobowiązany również z należytą starannością chronić urządzenie z zainstalowaną Aplikacją Mobilną.

§24

Użytkownik zobowiązany jest do niezwłocznego poinformowania Banku oraz niezwłocznego dokonania zmiany hasła PINu lub zablokowania Kanałów Elektronicznych w przypadku:

1. ujawnienia lub udostępnienia osobom trzecim danych logowania lub podejrzenia takiego zdarzenia,
2. nieautoryzowanego użycia Kanałów Elektronicznych,
3. wykrycia nieautoryzowanych transakcji i operacji na swoich rachunkach,
4. utraty lub kradzieży danych logowania,
5. zmiany, utraty lub udostępnieniu osobom trzecim numeru telefonu używanego do kontaktu z Bankiem, w szczególności używanego do autoryzacji transakcji,
6. utraty urządzenia mobilnego umożliwiającego korzystanie z bankowości mobilnej,
7. podejrzenia zainfekowania Urządzenia złośliwym oprogramowaniem.

§25

Bank zastrzega sobie prawo wprowadzenia dodatkowych ograniczeń i zabezpieczeń w stosunku do dyspozycji składanych w Kanałach Elektronicznych, w przypadku wystąpienia ważnych okoliczności uzasadniających wprowadzenie takich środków.

§26

1. Szczegółowe informacje dotyczące zasad bezpiecznego korzystania z Kanałów Elektronicznych oraz ryzyka związanego z korzystaniem z nich, wskazane zostały w §27 oraz zamieszczone są na stronach internetowych Banku, a także udzielane przez konsultantów Contact Center.
2. Użytkownik zobowiązany jest przestrzegać zasad bezpiecznego korzystania z Kanałów Elektronicznych, a w przypadku ich nieprzestrzegania działa na własne ryzyko i ponosi odpowiedzialność za skutki takiego zaniechania.

§27

Użytkownik przyjmuje do wiadomości, że elektroniczny dostęp do systemów Bankowości Internetowej, Mobilnej i Telefonicznej, wiąże się z ryzykiem – w szczególności w

przypadku nieprzestrzegania zasad bezpieczeństwa określonych przez Bank. Ryzyko to obejmuje:

1. Zagubienie lub kradzież przez osoby nieuprawnione danych lub urządzeń:
   a. służących do zalogowania do systemu (np. identyfikator, tym również Identyfikator biometryczny, PIN do Aplikacji Mobilnej),
   b. służących do zatwierdzania transakcji (np. urządzenia mobilnego z zainstalowaną aplikacją).
2. Wystąpienia ataków socjotechnicznych, w których osoby trzecie będą – podszywając się pod Bank – nakłaniały Użytkownika do zatwierdzania operacji (np. fałszywa informacja o konieczności wykupienia transakcji).
3. Nieświadome zatwierdzenie przez Użytkownika niezamierzonych zleceń (np. bez zapoznania się z operacją opisaną w Kodzie autoryzacyjnym lub w Komunikacie PUSH).
4. Wykorzystanie, w trakcie korzystania z Kanałów Elektronicznych, urządzeń nad którymi kontrolę w sposób zdalny lub fizyczny przejęły osoby trzecie (np. za pomocą złośliwego oprogramowania, takiego jak wirusy).
5. Konsekwencjami wystąpienia ww. zdarzeń mogą być:
   a. dostęp osób trzecich do danych Użytkownika dostępnych w Kanałach Elektronicznych,
   b. możliwość realizacji transakcji przez osoby trzecie w imieniu Użytkownika – w tym finansowych (np. wykonywanie poleceń przelewu),
   c. możliwość zatwierdzenia niechcianej transakcji przez Użytkownika.

§28

Podczas korzystania z Bankowości Internetowej oraz Bankowości Mobilnej, Bank zaleca używanie przeglądarek internetowych, urządzeń i systemów operacyjnych z listy referencyjnej umieszczonej na stronie internetowej Banku. Bank nie ponosi odpowiedzialności za ewentualne nieprawidłowości w funkcjonowaniu Bankowości Internetowej oraz Bankowości Mobilnej w przypadku używania przeglądarek spoza tej listy.

§29

Podstawowe zasady bezpieczeństwa w trakcie korzystania z Kanałów Elektronicznych:

1. Zawsze należy sprawdzać poprawność adresu logowania do Bankowości Internetowej. Przy logowaniu należy zwracać uwagę czy przeglądarka nie wyświetla ostrzeżeń związanych z certyfikatem bezpieczeństwa (należy sprawdzić i zweryfikować jego szczegóły) oraz na przedrostek HTTPS w adresie strony logowania, świadczący o szyfrowaniu połączenia ze stroną Systemu Bankowości Internetowej.
2. Należy uważnie czytać treść Kodów autoryzacyjnych i Komunikatów PUSH autoryzacyjnych. Przed potwierdzeniem operacji należy przeczytać dokładnie całą treść powiadomienia SMS lub Komunikatu PUSH autoryzacyjnego. Bank nigdy nie poprosi o potwierdzenie operacji, która nie została zlecona przez Użytkownika.
3. Bank zaleca regularne aktualizacje systemu operacyjnego oraz zainstalowanego na nim oprogramowania, w szczególności oprogramowania antywirusowego (wraz z bazą sygnatur wirusów) oraz wykorzystywanej przeglądarki internetowej.
4. Nie należy 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.
5. Nie należy korzystać z niezaufanych urządzeń do instalowania Aplikacji mobilnej i logowania do niej – do tego celu nie należy również używać publicznych sieci Wi-Fi.
6. Należy zwrócić szczególną uwagę na ataki mające na celu namówienie do wykonania jakiejś akcji (np. kliknięcie w link, pobranie oprogramowania, podanie swoich danych), zatwierdzenie Komunikatu PUSH autoryzacyjnego, które są przesyłane w e-mailach, wiadomościach SMS/MMS, sieciach społecznościowych, komunikatorach lub są przekazywane telefonicznie.
7. Bank zaleca, aby 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.
8. Istotne dane (adres, numery PESEL, hasła, loginy 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.
9. Należy zwracać uwagę na informacje o nowych zagrożeniach – na stronach Banku pojawiają się informacje w jaki sposób je rozpoznać i jak się przed nimi ustrzec (w sekcji Nowe zagrożenia oraz poprzez banery informacyjne na stronie logowania).
10. 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, użytkownik jest proszony o dokonanie dodatkowych czynności) należy niezwłocznie skontaktować się z Contact Center – może to świadczyć o tym, że komputer jest zarażony złośliwym oprogramowaniem.
11. Użytkownik ponosi pełną odpowiedzialność za operacje i czynności wykonane przez osoby, którym ujawnił poświadczenia logowania lub udostępnił urządzenie służące do uwierzytelnienia i/lub autoryzacji operacji w Kanale Elektronicznym oraz za czynności i operacje, do których doszło w wyniku naruszenia przez użytkownika postanowień niniejszego Regulaminu.
12. Użytkownik zobowiązuje się chronić dostęp do swojego urządzenia mobilnego i przyjmuje do wiadomości, że pozyskanie przez osoby trzecie jego zarejestrowanych Identyfikatorów biometrycznych może prowadzić do uzyskania przez te osoby nieuprawnionego dostępu do Aplikacji Mobilnej.
13. Użytkownik ponosi odpowiedzialność z tytułu umożliwienia osobom trzecim zarejestrowania przez nich swoich Identyfikatorów biometrycznych na urządzeniu mobilnym, na którym jest zainstalowana Aplikacja Mobilna z włączoną funkcją Logowania Odciskiem Palca.
14. Użytkownik jest zobowiązany poinformować Bank o zmianie numeru telefonu komórkowego, w formie pisemnej lub przez Kanały elektroniczne, niezwłocznie po zaistnieniu sytuacji. Użytkownik narażony jest i ponosi odpowiedzialność za negatywne konsekwencje w przypadku braku aktualizacji tego numeru.
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. Wszelkie informacje o incydentach bezpieczeństwa (nie dotyczy przypadków indywidualnych) są umieszczane na stronach internetowych Banku w sekcji Bezpieczeństwo.

ZABLOKOWANIE I REZYGNACJA Z KANAŁÓW ELEKTRONICZNYCH

§30

1. Przez zablokowanie należy rozumieć brak możliwości korzystania przez Użytkownika z danego Kanału Elektronicznego.
2. Zablokowanie Bankowości Internetowej oraz zablokowanie Bankowości Mobilnej mogą nastąpić zarówno łącznie, jak i niezależnie od siebie.

§31

1. Zablokowanie każdego z Kanałów Elektronicznych, może nastąpić w wyniku:
   a. dyspozycji złożonej konsultantowi Contact Center przez Użytkownika, lub w przypadku Użytkownika małoletniego przez przedstawiciela ustawowego,
   b. dyspozycji złożonej w Placówce Banku, przez Użytkownika, lub w przypadku Użytkownika małoletniego przez przedstawiciela ustawowego,
   c. przekroczenia ustalonego dla danego Kanału Elektronicznego limitu błędnych prób logowania.
2. Zablokowanie Bankowości Internetowej może nastąpić w wyniku:
   a. przekroczenia limitu 5 błędnych, następujących po sobie, prób logowania,
   b. przekroczenia limitu 5 błędnych, następujących po sobie, prób autoryzacji Dyspozycji.
3. Zablokowanie Aplikacji Mobilnej może nastąpić w wyniku:
   a. przekroczenia w limitu 5 błędnych, następujących po sobie, prób logowania,
   b. przekroczenia limitu 5 błędnych, następujących po sobie, prób autoryzacji Dyspozycji.
   c. dyspozycji złożonej w Panelu rodzica przez przedstawiciela ustawowego małoletniego Użytkownika w przypadku Aplikacji Alior Kids.
4. Zablokowanie każdego z Kanałów Elektronicznych może zostać dokonane przez Bank na podstawie analizy danych systemowych w przypadku:
   a. zagrożenia przechwycenia danych dostępowych Użytkownika przez złośliwe oprogramowanie,
   b. wykorzystywania danych dostępowych Użytkownika przez oprogramowanie automatycznie logujące się z dużą częstotliwością,
   c. wykorzystywania systemów lub rachunków w sposób niezgodny z obowiązującymi przepisami prawa,
   d. wykonywanie działań mogących zagrażać bezpieczeństwu systemu i danych w nim przetwarzanych,
   e. podejrzenia przez Bank, że osoba trzecia weszła w posiadanie dostępu do Kanałów Elektronicznych Użytkownika,
   f. braku aktywacji przez Użytkownika Kanału Elektronicznego w ciągu trzech miesięcy od podpisania Umowy,
   g. przeniesienia Użytkownika do innego systemu Bankowości Internetowej, gdy dostęp w pierwotnym systemie był zablokowany.
5. Niezwłocznie po zablokowaniu Bank uruchamia procedurę powiadamiania polegającą na podjęciu próby skontaktowania się z Użytkownikiem za pomocą dostępnych kanałów komunikacji celem wyjaśnienia sytuacji. Nie dotyczy to sytuacji opisanej w ust. 4 lit. f.

§32

Użytkownik może odblokować:

1. Bankowość Telefoniczną – w drodze Dyspozycji złożonej konsultantowi Contact Center, w Placówce Banku lub samodzielnie w Bankowości Internetowej, o ile kanał ten jest aktywny,
2. Bankowość Internetową i Mobilną:
   a. w Placówce Banku,
   b. w drodze Dyspozycji złożonej konsultantowi Contact Center,
   c. za pośrednictwem formularza dostępnego na stronie logowania Bankowości Internetowej (obowiązuje od momentu udostępnienia formularza przez Bank, po uprzednim poinformowaniu Użytkownika nie później niż 7 dni przed datą udostępnienia formularza, poprzez Kanały Elektroniczne).

§33

1. Zawarcie Umowy wymaga formy pisemnej lub innej formy zrównanej z pisemną.
2. Umowa zawarta jest na czas nieokreślony i może być rozwiązana przez każdą ze stron w formie pisemnej. Rozwiązanie umowy pozostaje bez wpływu na skuteczność zawartych na jej podstawie Umów Produktów oferowanych przez Bank dla osób fizycznych.
3. W momencie rozwiązania Umowy, Użytkownik traci możliwość korzystania z Kanałów Elektronicznych.
4. W przypadku, gdy Umowa została zawarta poza Placówką Banku, Użytkownik może odstąpić od niej w ciągu 14 dni od dnia jej zawarcia**,** bez podania przyczyn, składając Bankowi stosowne oświadczenie.

§34

Bank ma prawo do czasowego wyłączenia Kanałów Elektronicznych, po uprzednim umieszczeniu stosownego komunikatu na stronach internetowych Banku.

SILNE UWIERZYTELNIENIE UŻYTKOWNIKA

§35

1. Bank stosuje Silne uwierzytelnianie w przypadku, gdy:
   a. Użytkownik uzyskuje dostęp do swojego rachunku w trybie on-line za pośrednictwem Bankowości Internetowej lub Bankowości Mobilnej lub
   b. Użytkownik inicjuje transakcję płatniczą za pośrednictwem Bankowości Internetowej lub Bankowości Mobilnej lub
   c. Użytkownik za pośrednictwem Bankowości Internetowej lub Bankowości Mobilnej: inicjuje utworzenie lub zmianę szablonu płatności, zmianę danych dostępowych do Kanałów Elektronicznych, zmianę danych lub metod wykorzystywanych w ramach Silnego uwierzytelnienia, zmianę Limitów kwotowych w Kanałach Elektronicznych, zmianę limitów operacji dla karty płatniczej, aktywację karty płatniczej lub realizuje tokenizację karty płatniczej lub
   d. Użytkownik karty płatniczej będący jednocześnie Użytkownikiem Aplikacji Mobilnej inicjuje przy pomocy karty płatniczej transakcję typu e-commerce za pośrednictwem sieci Internet na zasadach określonych w Regulaminie kart płatniczych Alior Banku SA.
2. W celu zalogowania się do Bankowości Internetowej, Bank stosuje Silne uwierzytelnienie z zastosowaniem następujących metod:
   a. Użytkownik podaje Identyfikator oraz Hasło Dostępu a następnie:

i. w przypadku logowania przy użyciu Kodu autoryzacyjnego – Użytkownik wpisuje Kod autoryzacyjny w Bankowości Internetowej;
ii. w przypadku logowania przy użyciu Komunikatu PUSH – Użytkownik zatwierdza komunikat na Urządzeniu domyślnym. Zamiennie możliwe jest zeskanowanie przez Użytkownika wyświetlonego kodu QR przy pomocy Urządzenia domyślnego, a następnie wpisania w Bankowości Internetowej uzyskanego kodu jednorazowego.

b. Użytkownik może zdefiniować urządzenie, z którego następuje logowanie jako urządzenie dedykowane. W takim przypadku użytkownik zaznacza w Bankowości Internetowej dane urządzenie jako urządzenie dedykowane i zobowiązuje się zapewnić, że będzie jedynym użytkownikiem tego urządzenia dedykowanego. 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.
c. Logowanie przy użyciu urządzenia dedykowanego może następować przez określony przez Bank okres, przy czym Bank może wymagać uwierzytelnienia przy pomocy Kodu autoryzacyjnego lub Komunikatu PUSH także ze względów bezpieczeństwa.
d. Silne uwierzytelnienie Użytkownika może być również zrealizowane po podaniu Identyfikatora i Hasła, a następnie na podstawie jego Profilu behawioralnego.

3. Silne uwierzytelnienie w celu zalogowania się do Aplikacji Mobilnej, realizowane jest poprzez
a. zweryfikowanie przez Bank Urządzenia, z aktywną Aplikacją Mobilną, a następnie:
i. w przypadku logowania przy użyciu PINu autoryzacyjnego – podanie przez Użytkownika PINu autoryzacyjnego w Aplikacji Mobilnej;
ii. w przypadku logowania przy użyciu Uwierzytelnienia biometrycznego – uwierzytelnienie się Użytkownika za pomocą Identyfikatora biometrycznego.
iii. Zweryfikowanie przez Bank Użytkownika na podstawie jego Profilu behawioralnego.

§36

Użytkownik oświadcza, że jest jedynym posiadaczem urządzenia dedykowanego o którym mowa w §35 ust. 2b i ust. 3. oraz zobowiązuje się do nieudostępniania przedmiotowego urządzenia osobom trzecim.

§37

Bank udostępnia dostawcom świadczącym usługę dostępu do informacji o rachunku, dostawcom świadczącym usługę inicjowania płatności oraz dostawcom usług płatniczych wydającym instrumenty płatnicze oparte na karcie dedykowany interfejs dostępowy dla celu świadczenia tych usług.

REKLAMACJE

§38

1. Bank rozpatruje reklamacje niezwłocznie, nie później niż w terminie 15 dni roboczych (dotyczy świadczenia usług płatniczych) lub 30 dni kalendarzowych (dotyczy pozostałych przypadków) od dnia otrzymania reklamacji.
W przypadku usług płatniczych - w szczególnie skomplikowanych przypadkach uniemożliwiających rozpatrzenie reklamacji i udzielenie odpowiedzi w ww. terminie Bank:
1) wyjaśnia przyczynę opóźnienia;
2) wskazuje okoliczności, które muszą zostać ustalone dla rozpatrzenia sprawy;
3) określa przewidywany termin rozpatrzenia reklamacji i udzielenia odpowiedzi, który nie może przekroczyć 35 dni roboczych od dnia otrzymania reklamacji.

W pozostałych szczególnie skomplikowanych przypadkach (niedotyczących usług płatniczych) termin ten może zostać przedłużony, nie więcej jednak niż do 60 dni kalendarzowych od dnia otrzymania reklamacji. O przyczynach opóźnienia, okolicznościach wymagających ustalenia oraz przewidywanym terminie rozpatrzenia reklamacji i udzielenia odpowiedzi Użytkownik zostanie poinformowany.

2. Użytkownik zobowiązany jest dostarczyć Bankowi wszelkie informacje oraz dokumentację dot. reklamacji i współpracować z Bankiem do czasu zakończenia rozpatrywania reklamacji.
3. Reklamacja może być zgłoszona:
a. bezpośrednio w Placówce Banku,
b. telefonicznie w Contact Center,
c. poprzez System Bankowości Internetowej (dla Użytkownika zalogowanego),
d. poprzez Aplikację Mobilną (dla Użytkownika zalogowanego),
e. listownie – na adres korespondencyjny Banku.
f. na adres do doręczeń elektronicznych (e-Doręczenia): AE:PL-18375-10021-DTBRC-21
4. Odpowiedź na reklamację może zostać udzielona:
a. listownie,
b. poprzez System Bankowości Internetowej (dla użytkownika zalogowanego),
c. poprzez Aplikację Mobilną (dla Użytkownika zalogowanego),
d. poprzez powiadamianie SMS,
a także w uzasadnionych przypadkach, dodatkowo:
e. telefonicznie,
f. w placówce Banku.
5. Użytkownik niezadowolony ze sposobu rozpatrzenia reklamacji uprawniony jest do zwrócenia się w sprawie sporu dotyczącego relacji z Bankiem:
a. do Arbitra Bankowego – w trybie pozasądowego postępowania w celu rozwiązania sporu (szczegółowe informacje o Bankowym Arbitrażu Konsumenckim dostępne są na stronie internetowej Banku, w rejestrze podmiotów uprawnionych prowadzonym przez Prezesa UOKiK oraz na stronie internetowej www.zbp.pl);
b. do Rzecznika Finansowego – w trybie skargowym lub pozasądowego postępowania w celu rozwiązywania sporu (szczegółowe informacje dostępne na stronie internetowej www.rf.gov.pl).

POSTANOWIENIA KOŃCOWE

§39

1. Za czynności związane z udostępnieniem i obsługą Kanałów Elektronicznych Bank pobiera opłaty i prowizje zgodnie z obowiązującą Taryfą Opłat i Prowizji Alior Banku S.A. dla Klientów Indywidualnych lub Biura Maklerskiego., która określa:
1) wysokość i zasady pobierania opłat i prowizji za czynności związane z obsługą oraz zmianą umowy,
2) warunki, wysokość i zasady zmian opłat i prowizji,
3) zasady oraz sposób informowania o zmianach Taryfy Opłat i Prowizji.
2. Bank zastrzega sobie możliwość odstąpienia od pobierania opłat i prowizji.

3. Aktualna Taryfa Opłat i Prowizji dostępna jest na stronach internetowych Banku oraz w Placówkach Banku.

§40

1. Bank zastrzega sobie prawo do dokonania zmiany niniejszego Regulaminu, w przypadku wystąpienia przynajmniej jednej z poniższych przyczyn:
   a. zmiana w zakresie funkcjonowania oferowanych przez Bank produktów i usług; w tym wycofanie produktu lub usługi do którego/której mają zastosowanie postanowienia Regulaminu,
   b. wprowadzenie przez Bank nowych produktów lub usług, do których będą miały zastosowanie postanowienia Regulaminu;
   c. zmiana systemów informatycznych wykorzystywanych do obsługi oferowanych przez Bank produktów i usług, do których mają zastosowanie postanowienia Regulaminu;
   d. zmiana przepisów prawa:
      1) regulujących produkty lub usługi oferowane przez Bank; do których zastosowanie mają postanowienia Regulaminu;
      2) mających wpływ na wykonywanie Umowy lub Regulaminu;
   e. zmiana lub wydanie nowych orzeczeń sądowych, orzeczeń organów administracji, zaleceń lub rekomendacji uprawnionych organów, w tym Komisji Nadzoru Finansowego – w zakresie związanym z wykonywaniem umowy lub Regulaminu.

   W przypadku zmiany Regulaminu, Bank dostarczy Użytkownikowi tekst jednolity Regulaminu. Regulamin lub wykaz zmian do Regulaminu dostarczane będą wyłącznie drogą elektroniczną (w formie elektronicznej na adres mailowy podany przez Posiadacza lub poprzez stronę internetową w postaci udostępnionego na niej pliku elektronicznego zapisanego na Trwałym nośniku po uprzednim poinformowaniu, w szczególności listem, SMS, e-mailem, o dostępności informacji o zmianie niniejszego Regulaminu na tej stronie internetowej. Dodatkowo Bank może także udostępnić informację o zmianach niniejszego Regulaminu w Bankowości Internetowej) nie później niż 2 miesiące przed proponowaną datą ich wejścia w życie, z zastrzeżeniem ust. 5. Brak zgłoszenia sprzeciwu Użytkownika wobec proponowanych zmian jest równoznaczny z wyrażeniem na nie zgody.
2. Regulamin dostarczony w sposób opisany w ust. 1 uznaje się za doręczony.
3. Użytkownik ma prawo, przed datą proponowanego wejścia w życie zmian, wypowiedzieć Umowę ze skutkiem natychmiastowym bez ponoszenia opłat związanych z wypowiedzeniem Umowy lub opłat wynikających z proponowanych zmian.
4. W przypadku, gdy Użytkownik zgłosi sprzeciw zgodnie z ust. 1, ale nie dokona wypowiedzenia Umowy, Umowa wygasa z dniem poprzedzającym dzień wejścia w życie proponowanych zmian, bez ponoszenia opłat związanych z wypowiedzeniem umowy lub opłat wynikających z proponowanych zmian.
5. W przypadku zmiany Regulaminu z powodu rozszerzenia zakresu czynności, które będą możliwe do wykonania przez Użytkownika w Kanałach Elektronicznych, Bank informuje Użytkownika o zmianie Regulaminu w sposób ogólnodostępny w Placówce Banku, na stronach internetowych Banku lub poprzez Kanały Elektroniczne, a w przypadku braku możliwości wykorzystania Kanałów Elektronicznych – za pośrednictwem poczty lub na adres mailowy wskazany przez Użytkownika. Zmieniony Regulamin obowiązuje od momentu wprowadzenia.

§41

1. Bank zastrzega sobie prawo wykonywania niektórych usług w ramach Kanałów Elektronicznych za pośrednictwem podmiotów zewnętrznych, w szczególności podmiotów zależnych. Przekazywane do tych podmiotów dane objęte są tajemnicą bankową oraz postanowieniami przepisów dotyczących ochrony danych i podlegają ochronie w takim samym stopniu i zakresie jak w przypadku Banku. Bank ponosi pełną odpowiedzialność za transakcje wykonywane za pośrednictwem tych podmiotów.
2. Stosowanie Profilu behawioralnego ma na celu zapewnienie Użytkownikowi zasad bezpieczeństwa o których mowa w §22 niniejszego Regulaminu. Podstawą prawną przetwarzania danych na podstawie Profilu behawioralnego jest art. 9 ust. 2 lit g Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych), czyli „przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym na podstawie prawa Unii lub prawa państwa członkowskiego". Tym prawem są przepisy:
   a. art. 97 – 98 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (Dyrektywy PSD2),
   b. art. 2 i art. 18 Rozporządzenia Delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji,
   c. art. 10 ustawy z 19 sierpnia 2011 o usługach płatniczych.