REGULAMIN KART ZWIRTUALIZOWANYCH

§ 1.

„Regulamin kart zwirtualizowanych" (dalej „Regulamin") określa zasady dotyczące korzystania przez posiadacza karty płatniczej wydanej przez Bank Millennium S.A. (dalej „Bank"), z funkcjonalności w postaci wirtualizowania, tj. cyfrowego odwzorowania tej karty płatniczej na Urządzeniach mobilnych.

§ 2.

Użyte w Regulaminie określenia oznaczają:

1) **Aktywacja Karty zwirtualizowanej** – aktywowanie przez Posiadacza Karty Tokena w Aplikacji mobilnej, skutkujące udostępnieniem mu Karty zwirtualizowanej w Aplikacji mobilnej na danym Urządzeniu mobilnym,
2) **Dane identyfikujące** – dane, które powinny zostać wprowadzone przez Posiadacza Karty lub Posiadacza Karty zwirtualizowanej w celu uzyskania dostępu do Kanałów Bankowości Elektronicznej. Dane te służą do identyfikacji Posiadacza Karty lub Posiadacza Karty zwirtualizowanej oraz podpisania oświadczenia złożonego w Kanałach Bankowości Elektronicznej,
3) **Karta** – Karta debetowa, kredytowa lub przedpłacona w formie fizycznego nośnika, wydana przez Bank, w tym duplikat Karty, Karta dodatkowa, Karta zastępcza lub MiniKarta Zbliżeniowa,
4) **Karta zwirtualizowana** – powiązana z daną Kartą i będąca jej elektronicznym odpowiednikiem, Karta debetowa, kredytowa lub przedpłacona międzynarodowej organizacji VISA lub Mastercard, umożliwiająca dokonywanie Transakcji zbliżeniowych,
5) **Kanały Bankowości Elektronicznej** - usługa zdalnego dostępu do produktów i usług oferowanych przez Bank, umożliwiająca składanie oświadczeń woli i wiedzy. Do Kanałów Bankowości Elektronicznej należą:
   a) Usługa bankowości elektronicznej – usługa polegająca na dostępie do rachunku płatniczego przez Internet, umożliwiająca sprawdzenie salda rachunku płatniczego lub złożenie innego rodzaju dyspozycji do rachunku. Usługę tę stanowią:
      a. Millenet - dostępny za pośrednictwem sieci Internet oraz komputera lub Urządzenia mobilnego wyposażonego w rekomendowaną przeglądarkę,
      b. Aplikacja mobilna – dostępna po zainstalowaniu przez Posiadacza Karty lub Posiadacza Karty zwirtualizowanej oprogramowania Banku na podłączonych do Internetu Urządzeniach mobilnych oraz połączonych z nimi urządzeniach dodatkowych (w szczególności zegarkach typu smart watch),
   b) Usługa bankowości telefonicznej – usługa polegająca na dostępie do rachunku płatniczego przez telefon za pośrednictwem infolinii Banku, umożliwiająca w szczególności sprawdzenie salda rachunku płatniczego lub złożenie innego rodzaju dyspozycji do rachunku,
   c) Kanał bankomatowy – dostępny za pośrednictwem bankomatu/ Wpłatomatu z wykorzystaniem instrumentów płatniczych,
6) **Posiadacz Karty** – Posiadacz lub współposiadacz rachunku w Banku lub osoba fizyczna upoważniona przez Posiadacza rachunku do dysponowania środkami na rachunku w Banku przy użyciu wydanej jej Karty w imieniu i na rzecz Posiadacza rachunku, w tym Posiadacz Karty dodatkowej,
7) **Posiadacz Karty zwirtualizowanej** – Posiadacz Karty, który dokonał Aktywacji Karty zwirtualizowanej; w przypadku kart przedpłaconych Posiadaczem Karty zwirtualizowanej może być jedynie użytkownik Karty, który jednocześnie ma dostęp do Millenetu,
8) **Silne uwierzytelnianie** - oznacza uwierzytelnienie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów uwierzytelniania należących do kategorii:
   a) wiedza (coś, co wie wyłącznie Posiadacz karty lub Posiadacz karty zwirtualizowanej),
   b) posiadanie (coś, co posiada wyłącznie Posiadacz karty lub Posiadacz karty zwirtualizowanej),
   c) cechy Posiadacza karty lub Posiadacza karty zwirtualizowanej (coś, co charakteryzuje Posiadacza karty lub Posiadacza karty zwirtualizowanej),

   będących integralną częścią tego uwierzytelnienia oraz niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych,
9) **Token** - klucz (numer transakcyjny) umożliwiający korzystanie z Karty zwirtualizowanej. Dany Token jest przypisany do konkretnego Urządzenia mobilnego, na którym dokonano Aktywacji Karty zwirtualizowanej,
10) **Transakcja zbliżeniowa** – transakcja dokonana bezstykowo Urządzeniem mobilnym z Kartą zwirtualizowaną,
11) **Urządzenie mobilne** – urządzenie elektroniczne pozwalające na odbieranie, przetwarzanie i wysyłanie danych za pośrednictwem sieci Internet, które może być przenoszone i używane w dowolnym miejscu, spełniające wymagania techniczne, określone na stronie internetowej Banku, niezbędne do instalacji Aplikacji mobilnej, przystosowane do obsługi transakcji w technologii NFC,
12) **Wpłata gotówki** – usługa polegająca na wpłacie gotówki na rachunek płatniczy konsumenta za pomocą urządzenia umożliwiającego taką wpłatę lub w placówce Dostawcy,
13) **Wypłata gotówki** – usługa polegająca na wypłacie gotówki z rachunku płatniczego konsumenta za pomocą urządzenia umożliwiającego taką wypłatę lub w placówce Dostawcy.

§ 3.

1. Karta zwirtualizowana jest udostępniana przez Bank Posiadaczowi Karty w Aplikacji mobilnej na danym Urządzeniu mobilnym, po dokonaniu przez niego Aktywacji Karty zwirtualizowanej. Z Karty zwirtualizowanej można korzystać od momentu jej aktywacji.
2. Odstąpienie od umowy Karty lub umowy ROR, wypowiedzenie lub rozwiązanie lub wygaśnięcie którejkolwiek z tych umów, skutkuje usunięciem przez Bank Tokena i uniemożliwieniem korzystania z Karty zwirtualizowanej z chwilą skutecznego odstąpienia od którejkolwiek z tych umów, upływu okresu wypowiedzenia, rozwiązania lub wygaśnięcia.
3. W celu korzystania przez Posiadacza Karty zwirtualizowanej z tej Karty na więcej niż jednym Urządzeniu mobilnym, powinien on dokonać Aktywacji Karty zwirtualizowanej na każdym z tych urządzeń odrębnie.
4. Numer Karty, PIN i limity transakcji, w przypadku Karty zwirtualizowanej są takie same jak w przypadku Karty. Zmiana PINu lub limitów w stosunku do Karty skutkuje taką samą zmianą w stosunku do Karty zwirtualizowanej. Karta zwirtualizowana nie posiada kodu CVV2/CVC2, ani nie jest na niej umieszczany podpis Posiadacza Karty zwirtualizowanej.
5. Cennik usług może określać limit Transakcji zbliżeniowych, których dokonanie jest możliwe bez podłączenia Urządzenia mobilnego do Internetu. W przypadku jego przekroczenia, Posiadacz Karty zwirtualizowanej musi uzyskać dostęp do Internetu w celu jego odnowienia.

§ 4.

1. Karta zwirtualizowana umożliwia dokonywanie Transakcji zbliżeniowych bezgotówkowych w punktach akceptujących, wyposażonych w urządzenia z czytnikami zbliżeniowymi, pozwalającymi na dokonanie takich transakcji, oznaczonych odpowiednio symbolem VISA, Mastercard lub Maestro, z wyłączeniem płatności w Internecie, telefonicznie, Wypłat gotówki w bankomatach, Wpłat gotówki we wpłatomatach oraz Wypłat gotówki typu Cash back.
2. Transakcje zbliżeniowe, o których mowa w ust. 1, mogą być dokonane poprzez zbliżenie Urządzenia mobilnego z Kartą zwirtualizowaną, włączoną komunikacją NFC i odblokowanym ekranem, na odległość pozwalającą na jej wykrycie przez urządzenie z czytnikiem zbliżeniowym.

3. Transakcje zbliżeniowe dokonane Kartą zwirtualizowaną obciążają ten sam rachunek bankowy, który jest obciążany w przypadku dokonania transakcji Kartą.
4. Limit kwotowy dla jednorazowej bezgotówkowej Transakcji zbliżeniowej przeprowadzonej na terenie Polski bez konieczności wprowadzania kodu PIN lub podpisu Posiadacza Karty ustalany jest przez organizacje płatnicze i opisany w Cenniku usług – karty debetowe, Cenniku usług – karty kredytowe, Cenniku kart przedpłaconych. Z zastrzeżeniem ust. 10, Transakcję zbliżeniową:
   1) w ramach limitu uważa się za autoryzowaną z chwilą przekazania danych Karty wymaganych do realizacji transakcji, poprzez zbliżenie Karty do urządzenia umożliwiającego odczyt tych danych lub jeżeli została ona potwierdzona kodem PIN.
   2) powyżej limitu uważa się za autoryzowaną, jeżeli została potwierdzona kodem PIN.
5. Maksymalna kwota jednorazowej Transakcji zbliżeniowej bez konieczności wprowadzenia kodu PIN realizowanej za granicą może być różna od wysokości limitu obowiązującego w Polsce.
6. Zbliżeniowe transakcje Wypłaty gotówki z bankomatu wyposażonego w czytnik zbliżeniowy uważa się za autoryzowaną poprzez zbliżenie Urządzenia mobilnego do urządzenia umożliwiającego odczyt danych zapisanych na Karcie zwirtualizowanej oraz wprowadzenie kodu PIN.
7. Jeżeli Posiadacz Karty zwirtualizowanej zlecił Transakcję zbliżeniową zgodnie z ust. 2 i 4, uznaje się, że autoryzował jej wykonanie.
8. Odmowa wykonania autoryzowanego Zlecenia płatniczego może nastąpić w przypadku:
   1) próby dokonania Transakcji zbliżeniowej Kartą zwirtualizowaną zablokowaną lub której termin ważności upłynął,
   2) braku wystarczających środków na ROR, wystarczającego limitu kredytowego, przekroczenia limitów transakcji lub blokady środków na rachunku,
   3) błędnego Zlecenia płatniczego,
   4) uzasadnionych przyczyn związanych z bezpieczeństwem Karty zwirtualizowanej lub Urządzenia mobilnego,
   5) podejrzenia nieuprawnionego użycia Karty zwirtualizowanej lub umyślnego doprowadzenia do nieautoryzowanej Transakcji zbliżeniowej.
9. W przypadku zainstalowania na Urządzeniu mobilnym więcej niż jednej Karty zwirtualizowanej, Posiadacz Karty, powinien wybrać w Aplikacji mobilnej Kartę zwirtualizowaną, którą zamierza dokonać tej transakcji. W przypadku niedokonania wyboru realizacja Transakcji zbliżeniowej nastąpi Kartą zwirtualizowaną ustawioną jako domyślna w Aplikacji mobilnej.
10. Silne uwierzytelnianie Posiadacza Karty lub Posiadacza karty zwirtualizowanej, może być wymagane w przypadku gdy: uzyskuje on dostęp do rachunku w trybie online, inicjuje elektroniczną transakcję płatniczą, przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć.
11. W przypadku, gdy Bank, pomimo istniejącego obowiązku określonego w obowiązujących przepisach prawa, nie wymaga Silnego uwierzytelniania, Posiadacz Karty lub Posiadacz Karty zwirtualizowanej nie ponosi odpowiedzialności za nieautoryzowane Transakcje zbliżeniowe, chyba że działał umyślnie.
12. Każdy element uwierzytelnienia musi zostać ustanowiony i powiązany z Posiadaczem Karty lub Posiadaczem Karty zwirtualizowanej.
13. Lista elementów uwierzytelniania, z których Posiadacz Karty lub Posiadacz Karty zwirtualizowanej może korzystać (w zależności od komunikatu podanego przez Bank):
    1) Autoryzacja mobilna
    2) Bezpieczna koperta
    3) Dane aktywowane z wykorzystaniem modułu biometrycznego
    4) H@sło1
    5) Hasło mobilne
    6) Karta
    7) PIN
    8) PIN Mobilny
    9) Zaufana przeglądarka
    10) Zaufane urządzenie
    11) Zdefiniowany numer telefonu

§ 5.

1. Posiadacz Karty zwirtualizowanej może w stosunku do swojej Karty Zwirtualizowanej:
   1) zablokować lub odblokować możliwość dokonywania Transakcji zbliżeniowych (wyłączyć lub włączyć Token, bez jego usunięcia), bez rezygnacji z korzystania z Aplikacji mobilnej, przy czym:
      a) w przypadku dokonania ww. czynności w Aplikacji mobilnej, zainstalowanej na danym Urządzeniu mobilnym, czynności powyższe dotyczą jedynie Karty zwirtualizowanej na tym Urządzeniu mobilnym,
      b) w przypadku dokonania ww. czynności w Millenecie, czynności powyższe dotyczą Karty zwirtualizowanej, znajdującej się na każdym Urządzeniu mobilnym wskazanym przez Posiadacza Karty zwirtualizowanej,
   2) usunąć Token dla danej Karty zwirtualizowanej na wybranym Urządzeniu mobilnym w placówce Banku lub poprzez COT, bez rezygnacji z korzystania z Aplikacji mobilnej, przy czym usunięcie Tokenów danej Karty zwirtualizowanej z wszystkich Urządzeń mobilnych jest równoznaczne z rezygnacją z korzystania z tej Karty zwirtualizowanej ze skutkiem natychmiastowym,
   3) zablokować w Millenecie Aplikację mobilną na każdym Urządzeniu mobilnym wskazanym przez Posiadacza Karty zwirtualizowanej,
   4) zablokować w placówce Banku lub poprzez COT Aplikację Mobilną jako Kanał Bankowości Elektronicznej – w takim przypadku do czasu jej odblokowania w placówce Banku nie będzie możliwe korzystanie z Aplikacji mobilnej na żadnym Urządzeniu mobilnym.
2. Bank ma prawo zablokować możliwość dokonywania Transakcji zbliżeniowych za pomocą Karty zwirtualizowanej ze względu na:
   1) uzasadnione przyczyny związane z bezpieczeństwem Karty zwirtualizowanej lub Urządzenia mobilnego z Kartą zwirtualizowaną,
   2) podejrzenie nieuprawnionego użycia Karty zwirtualizowanej lub umyślnego doprowadzenia do nieautoryzowanej Transakcji zbliżeniowej.
3. Zablokowanie Karty oraz Tymczasowe zablokowanie Karty skutkuje niemożnością dokonania Aktywacji Karty zwirtualizowanej, jak również brakiem możliwości korzystania z Karty zwirtualizowanej od momentu zablokowania Karty do momentu jej odblokowania. Zablokowanie Karty, Tymczasowe zablokowanie Karty lub Karty zwirtualizowanej nie skutkuje usunięciem Tokena.
4. Zastrzeżenie Karty skutkuje niemożnością dokonania Aktywacji Karty zwirtualizowanej, jak również usunięciem Tokenów z wszystkich Urządzeń mobilnych i brakiem możliwości korzystania z Karty zwirtualizowanej dotyczącej zastrzeganej Karty od momentu zastrzeżenia tej Karty. W celu korzystania z Karty zwirtualizowanej dotyczącej nowej Karty, Posiadacz Karty powinien dokonać Aktywacji Karty zwirtualizowanej dotyczącej nowej Karty.
5. W przypadku Karty, nie jest możliwe dokonywanie Transakcji zbliżeniowych kredytową Kartą zwirtualizowaną, od momentu zablokowania w Millenecie, Aplikacji mobilnej lub COT przez Posiadacza Karty możliwości dokonywania transakcji tą Kartą do momentu odblokowania tej możliwości.
6. W przypadku wyłączenia przez Posiadacza Karty w Millenecie funkcjonalności transakcji zbliżeniowych, w tym na Karcie wyposażonej w technologię zbliżeniową Mastercard lub Visa payWave, nie jest możliwe dokonywanie Transakcji zbliżeniowych Kartą zwirtualizowaną do czasu włączenia tej funkcjonalności.
7. W przypadku zablokowania przez Bank możliwości dokonywania Transakcji zbliżeniowych za pomocą Karty zwirtualizowanej, Bank podejmie niezwłoczną próbę skontaktowania się z

Posiadaczem Karty zwirtualizowanej za pośrednictwem dostępnych środków komunikacji, chyba że byłoby to nieuzasadnione ze względów bezpieczeństwa lub ze względu na odrębne przepisy.

8. Bank odblokuje możliwość dokonywania Transakcji zbliżeniowych Kartą zwirtualizowaną, jeżeli przestaną istnieć podstawy do utrzymywania blokady, wymienione w ust. 2.
9. W przypadku rachunku wspólnego, czynności związane z blokowaniem Karty zwirtualizowanej nie mają skutku względem Kart zwirtualizowanych innych współposiadaczy rachunku.
10. Posiadacz Karty zwirtualizowanej jest zobowiązany do:
    1) korzystania z niej zgodnie z zawartymi z Bankiem umowami i regulaminami,
    2) podejmowania niezbędnych środków bezpieczeństwa służących zapobieżeniu wystąpieniu nieautoryzowanych Transakcji zbliżeniowych, w tym odpowiedniego zabezpieczenia Urządzenia mobilnego poprzez:
        a) aktualizacje systemu operacyjnego,
        b) stosowania oprogramowania antywirusowego,
        c) stosowania zapór bezpieczeństwa, jeżeli jest to możliwe,
        d) aktualizowania Aplikacji mobilnej na Urządzeniu mobilnym, w którym znajduje się Karta zwirtualizowana, niezwłocznie po otrzymaniu informacji o opublikowaniu przez Bank najnowszej wersji,
        e) korzystania z przeglądarek internetowych rekomendowanych przez Bank,
    3) ochrony i przechowywania osobno Urządzenia mobilnego z Kartą zwirtualizowaną, kodu PIN oraz kodu PIN Mobilnego, z zachowaniem należytej staranności, w tym nieprzechowywania kodu PIN lub PINu Mobilnego w pamięci Urządzenia mobilnego,
    4) nieudostępniania Urządzenia mobilnego z Kartą zwirtualizowaną innym osobom lub nieujawniania takim osobom kodu PIN lub kodu PIN Mobilnego,
    5) nieudostępniania indywidualnych danych uwierzytelniających, w szczególności Danych identyfikujących, osobom nieupoważnionym,
    6) niezwłocznego zgłaszania Bankowi stwierdzenia nieuprawnionego dostępu do Karty zwirtualizowanej lub nieuprawnionego użycia Karty zwirtualizowanej, jak również utraty, kradzieży lub przywłaszczenia Urządzenia mobilnego z Kartą zwirtualizowaną,
    7) powiadomienia Banku o stwierdzonych nieautoryzowanych, niewykonanych lub nienależycie wykonanych Transakcjach zbliżeniowych, niezwłocznie, jednak nie później niż w terminie 13 miesięcy od dnia obciążenia ROR albo od dnia, w którym Transakcja zbliżeniowa miała być wykonana.
11. Posiadacz Karty zwirtualizowanej jest zobowiązany zgłosić Policji fakt nieuprawnionego użycia lub dostępu do Karty zwirtualizowanej lub utraty, kradzieży lub przywłaszczenia Urządzenia mobilnego z Kartą zwirtualizowaną. Zdarzenie, o którym mowa w zdaniu poprzedzającym powinno zostać niezwłocznie zgłoszone Bankowi, jak również niezwłocznie powinien zostać zablokowany przez Posiadacza Karty zwirtualizowanej dostęp do tej Karty, w szczególności z wykorzystaniem środków określonych w ust. 1.
12. Posiadacz Karty zwirtualizowanej odpowiada za transakcje zbliżeniowe dokonane:
    1) po zgłoszeniu zdarzenia, o którym mowa w ust. 10 pkt. 6), o ile doszło do nich z winy umyślnej Posiadacza Karty zwirtualizowanej,
    2) z winy Posiadacza Karty zwirtualizowanej, gdy nie dopełnił on obowiązków określonych w ust. 10 pkt. 1) – 6),
    3) w przypadku użycia Karty zwirtualizowanej niezgodnie z prawem, w szczególności do realizacji płatności za zabronione towary i usługi,
    4) do czasu zgłoszenia zdarzenia, o którym mowa w ust. 10 pkt. 6),Posiadacz Karty odpowiada za nieautoryzowane Transakcje Kartą do wysokości równowartości w walucie polskiej 50 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji, jeżeli nieautoryzowana transakcja jest skutkiem:
        a) posłużenia się utraconym lub skradzionym Urządzeniem mobilnym z Kartą zwirtualizowaną, lub
        b) przywłaszczenia Urządzenia mobilnego z Kartą zwirtualizowaną

    chyba, że Posiadacz Karty nie miał możliwości stwierdzenia utraty, kradzieży lub przywłaszczenia Urządzenia mobilnego z Kartą zwirtualizowana przed wykonaniem transakcji z wyjątkiem przypadku, gdy Posiadacz Karty działał umyślnie.
13. W przypadku podejrzenia użycia Karty zwirtualizowanej przez osobę nieuprawnioną, Bank ma prawo do telefonicznej weryfikacji Transakcji zbliżeniowej z Posiadaczem Karty zwirtualizowanej oraz odmowy realizacji takiej transakcji, w przypadku negatywnej weryfikacji.

§ 6.

1. Karta zwirtualizowana jest ważna do ostatniego dnia miesiąca widniejącego na Karcie jako data ważności i po upływie tego terminu nie może być używana, z zastrzeżeniem ust. 2.
2. Warunkiem przedłużenia terminu ważności Karty zwirtualizowanej jest wznowienie Karty. Karta zwirtualizowana jest automatycznie aktywowana w Aplikacji mobilnej z momentem aktywacji wznawianej Karty lub aktywacji duplikatu Karty.
3. Zmiana typu lub rodzaju Karty lub wymiana Karty na nową, skutkuje brakiem możliwości korzystania z Karty zwirtualizowanej dotyczącej zmienianej lub wymienianej Karty. W celu korzystania z Karty zwirtualizowanej dotyczącej nowej Karty, Posiadacz Karty powinien dokonać Aktywacji Karty zwirtualizowanej dotyczącej nowej Karty.
4. Bank może podjąć decyzję o niewznawianiu Karty zwirtualizowanej, informując o tym na piśmie Posiadacza Karty zwirtualizowanej, na co najmniej 2 miesiące przed upływem terminu jej ważności.
5. W przypadku wycofania Karty zwirtualizowanej z oferty, Bank może usunąć Kartę zwirtualizowaną z Aplikacji mobilnej, niezależnie od przyczyn i trybu wskazanego w regulaminach, o których mowa w § 7 ust. 1, za dwumiesięcznym uprzednim pisemnym powiadomieniem Posiadacza Karty zwirtualizowanej.

§ 7.

1. W sprawach nieuregulowanych w niniejszym Regulaminie, zastosowanie mają odpowiednio postanowienia:
    1) Regulaminu ogólnego świadczenia usług bankowych dla osób fizycznych w Banku Millennium S.A. - w przypadku debetowych Kart zwirtualizowanych,
    2) Regulaminu kart kredytowych wydawanych przez Bank Millennium S.A. - w przypadku kredytowych Kart zwirtualizowanych,
    3) Regulaminu kart debetowych wydawanych do konta walutowego w Banku Millennium S.A. - w przypadku debetowych Kart zwirtualizowanych wydanych do konta walutowego,
    4) Regulaminu kart przedpłaconych dla klientów indywidualnych w Banku Millennium S.A. - w przypadku przedpłaconych Kart zwirtualizowanych.
2. W przypadku rozbieżności lub sprzeczności postanowień Regulaminu z regulaminami, o których mowa w ust. 1, decyduje treść Regulaminu.