TREŚĆ DOKUMENTU:	Polityka prywatności aplikacji mobilnej
WŁAŚCICIEL:	Biuro Ochrony Danych
KLASYFIKACJA:	Dokument Banku Millennium S.A. | poniższa treść do publikacji w Aplikacji Mobilnej i na stronie internetowej Banku

Polityka prywatności aplikacji mobilnej

Poniższe informacje są przeznaczone dla użytkowników aplikacji mobilnej Banku Millennium S.A. („**Bank**” lub „**Bank Millennium**”). Aplikacja mobilna to specjalne oprogramowanie instalowane na podłączonym do Internetu urządzeniu mobilnym oraz połączonych z nim urządzeniach dodatkowych (w szczególności zegarkach typu smart watch), umożliwiające dostęp do rachunków bankowych i korzystanie z usług bankowych („**Aplikacja Mobilna**”). Użytkownikami aplikacji są osoby, które zainstalowały aplikację mobilną na urządzeniu mobilnym, w tym Klienci Banku lub osoby uprawnione przez Klientów.

Zasady ochrony prywatności

Bank Millennium zapewnia swoim Klientom, w tym użytkownikom Aplikacji Mobilnej, bezpieczeństwo danych. Wszelkie informacje przekazywane przez użytkowników chronione są przy użyciu nowoczesnych technologii, zgodnie z obowiązującymi normami prawnymi, wymaganiami bezpieczeństwa i zasadami poufności. Bank aktywnie rozwija swoje systemy ochrony prywatności oraz bezpieczeństwa użytkowników wdrażając nowe zabezpieczenia organizacyjne oraz techniczne. O zmianach w stosowanych zasadach ochrony poufności Bank informuje użytkowników przy pomocy strony internetowej lub innej, uzgodnionej z użytkownikiem, drogi komunikacji.

Informacje ogólne dotyczące korzystania z aplikacji mobilnej Banku Millennium

Korzystanie z Aplikacji Mobilnej jest możliwe pod warunkiem:

1. Zawarcia umowy dostępu do usług przez Kanały Bankowości Elektronicznej („**KBE**”);
2. Posiadania aktywnego dostępu do KBE;
3. Instalacji Aplikacji Mobilnej na spełniającym wymogi techniczne urządzeniu mobilnym;
4. Aktywowania Aplikacji Mobilnej i uwierzytelnienia użytkownika:
    1) uruchomienia Aplikacji Mobilnej i podania Millekodu oraz hasła (H@sła SMS otrzymanego SMS-em lub odebrania połączenia wykonanego na zdefiniowany numer telefonu i poprawnego wykonania czynności podanych przez Bank oraz podanie Hasła Tymczasowego);
    2) podania Hasła Mobilnego lub Hasła1 (jeśli zostało ustalone) lub identyfikatora (np. numer PESEL lub dowodu tożsamości);
    3) ustalenie PIN i Hasła1 (jeśli nie zostało ustalone).

Szczegóły dotyczące sposobu pobrania Aplikacji Mobilnej, aktualne wymogi techniczne, instrukcja aktywacji Aplikacji Mobilnej a także pytania i odpowiedzi znajdują się na stronie https://www.bankmillennium.pl/bankowosc-prywatna/bankowosc-elektroniczna/bankowosc-mobilna/aplikacja-mobilna

Czy Aplikacja Mobilna jest bezpieczna?

Komunikacja pomiędzy Aplikacją Mobilną a systemami transakcyjnymi Banku odbywa się z wykorzystaniem bezpiecznych mechanizmów szyfrujących.

Bank, w celu zwiększenia bezpieczeństwa Klientów korzystających z Aplikacji Mobilnej oraz zapobiegania nadużyciom, zbiera następujące informacje:

- czy podstawowe zabezpieczenia urządzenia mobilnego zostały przełamane (root / jailbreak) – tj. czy dane przetwarzane na nim posiadają co najmniej poziom zabezpieczeń oczekiwany przez Google / Huawei / Apple (pozyskiwana informacja to odpowiedź tak/nie);
- informacje o urządzeniu – m.in. język, strefę czasową, model, markę, nazwę telefonu;
- psedounikalne* identyfikatory telefonu, oparte o różne elementy związane z urządzeniem (typu rozdzielczość, etc.) **bez składowych tych identyfikatorów.**

*Takie identyfikatory są unikalne w odniesieniu do pewnej grupy Klientów, która ma podobne ustawienia telefonu / podobny model.

Bank nie zbiera listy aplikacji. Możliwe jest jednak przeprowadzanie na urządzeniu mobilnym analizy, czy nie znajdują się na nim podejrzane aplikacje, instalowane spoza oficjalnego sklepu Google, które mają wysokie uprawnienia i mogą być zagrożeniem dla działań Klienta w Aplikacji Mobilnej – w takich wypadkach zbierany jest identyfikator aplikacji, jej skrót (tj. suma kontrola naliczona na pliku instalacyjnym) oraz zakres uprawnień aplikacji.

Dostęp do uprawnień lub informacji na urządzeniu mobilnym

Aplikacja Mobilna - w zależności od systemu operacyjnego, na którym jest instalowana, może uzyskać dostęp do uprawnień lub funkcji na urządzeniu mobilnym, m.in. do:

- danych technicznych urządzenia (w celu umożliwienia weryfikacji tożsamości użytkownika),
- wyświetlania połączeń sieciowych, odbierania danych z Internetu (w celu sprawdzania dostępu do Internetu przez aplikację i w celach bezpieczeństwa),
- korzystania z informacji dotyczących połączenia Wi-Fi – na potrzeby generowania unikalnych identyfikatorów aplikacji służącym szyfrowaniu danych i komunikacji Aplikacji Mobilnej z serwerem;
- żyroskopu, akcelerometru, sposobu korzystania z ekranu dotykowego (w celach bezpieczeństwa);
- pamięci urządzenia (podczas korzystania z funkcji przelewu QR);
- kontaktów (w celu pobrania adresu e-mail/numeru telefonu z listy kontaktów do przelewu na e-mail/telefon lub też do wysyłania potwierdzeń wykonania transakcji);
- dodawanie telefonu alarmowego do kontaktów (np. przy zakupie ubezpieczenia OC/AC);
- lokalizacji (w celu wyszukania najbliżej położonych bankomatów lub placówek Banku lub w celu zapisania lokalizacji na mapie w historii transakcji);
- zdjęć (np. w celu skorzystania z możliwości wybrania tapety z galerii zdjęć);
- aparatu fotograficznego (np. w celu skanowania kodu QR w opcji „Skanuj i Płać”);
- czytnika linii papilarnych (w celu logowania i zatwierdzania niektórych operacji za pomocą odcisku palca).

Szczegółowy katalog dostępów dla systemów iOS i Android wraz z wyjaśnieniem, do czego służy dany dostęp, znajduje się na stronie https://www.bankmillennium.pl/bankowosc-prywatna/bankowosc-elektroniczna/bankowosc-mobilna/aplikacja-mobilna w zakładce „Bezpieczeństwo i uprawnienia aplikacji".

Zarządzanie uprawnieniami dostępu

W zależności od wersji urządzenia i wersji systemu operacyjnego urządzenia mobilnego, uprawnienia akceptuje się przed instalacją Aplikacji Mobilnej lub przed użyciem danej funkcjonalności. Uprawnienia mogą być też nadane domyślnie. Uprawnienia (funkcje i informacje urządzenia mobilnego), które użytkownik nadaje Aplikacji Mobilnej, widoczne są w **panelu ustawień** urządzenia mobilnego, gdzie można zarządzać uprawnieniami dostępów (zmienić je lub odwołać). Należy pamiętać, że zmiana lub odwołanie może wiązać się z utratą funkcji Aplikacji Mobilnej połączonej z danym uprawnieniem. Uprawnienia Aplikacji Mobilnej można odwołać też poprzez odinstalowanie Aplikacji Mobilnej.

Szczegóły znajdują się na stronie https://www.bankmillennium.pl/bankowosc-prywatna/bankowosc-elektroniczna/bankowosc-mobilna/aplikacja-mobilna w podsekcji „Uprawnienia aplikacji" oraz w instrukcjach obsługi producentów: Android, Apple.

Informacje przechowywane na urządzeniu mobilnym

Identyfikatory urządzenia mobilnego

W aplikacjach mobilnych używa się **identyfikatorów urządzeń mobilnych**. Identyfikator urządzenia (ang. ***Device ID***) to seria cyfr i liter, która pozwala na identyfikację każdego urządzenia mobilnego (np. tabletu, smartfonu) i jest przechowywana w takim urządzeniu. Dostęp do identyfikatora może być uzyskany przez każdą pobieraną i instalowaną aplikację. Identyfikatory urządzenia mobilnego są wykorzystywane w Aplikacji Mobilnej do funkcjonowania wielu procesów. Aplikacje najczęściej wykorzystują identyfikator do komunikacji z serwerem.

Device ID jest niezbędne do procesów związanych w szczególności z:

- aktywacją Aplikacji Mobilnej,
- autoryzacją transakcji płatniczych,
- wirtualizacją karty płatniczej oraz płatnością z wykorzystaniem urządzenia mobilnego,
- transakcji BLIK,
- zakupem biletów komunikacji miejskiej,
- dodawaniem i wyświetlanie kart lojalnościowych w aplikacji mobilnej,
- konfiguracją i wyświetlaniem dodatków przed zalogowaniem.

Do identyfikacji urządzenia służy także ***Instance ID*** – jest to identyfikator generowany w procesie rejestracji/aktywacji Aplikacji Mobilnej; *Instance ID* aplikacji mobilnej ważny jest do czasu kolejnej aktywacji aplikacji. Bank wykorzystuje również identyfikatory umożliwiające zalogowanie, a także komunikację z urządzeniem po zalogowaniu.

Pliki *cookie*

W aplikacjach mobilnych wykorzystywane są pliki cookie, które nie służą do marketingu, ale są niezbędne do prawidłowego działania niektórych funkcjonalności Aplikacji Mobilnej. Pliki *cookie* (tzw. ciasteczka) to dane informatyczne, w szczególności pliki tekstowe, zapisywane w pamięci urządzenia końcowego (np. komputer, tablet, telefon), z którego użytkownik

korzysta. Pliki cookie w Aplikacji Mobilnej służą do funkcji wykorzystujących technologię Webview w aplikacji mobilnej, czyli technologię pozwalającą na wyświetlenie wybranych ekranów ze stron www wewnątrz aplikacji mobilnej z zastosowaniem interfejsu aplikacji mobilnej. Pliki *cookie* do procesów hybrydowych są tworzone przez aplikację mobilną i służą do utrzymania informacji o identyfikacji / autoryzacji klienta, aby można było otworzyć określoną stronę, z określoną funkcjonalnością, bez konieczności dodatkowego logowania przez użytkownika. Te pliki cookie **nie są zapisywane** w telefonie po wyłączeniu Aplikacji Mobilnej.

Więcej na temat wykorzystania plików *cookie* w kontekście stron internetowych Banku można znaleźć na stronie Polityka plików cookie - Bank Millennium.

Inne informacje

W procesie rejestracji Aplikacji Mobilnej Bank uzyskuje informacje dotyczące rodzaju urządzenia mobilnego (np. marka, model), które są **przekazywane** do Banku i wykorzystywane w celu zidentyfikowania Aplikacji Mobilnej i urządzenia mobilnego.

W momencie połączenia się przez użytkownika z Aplikacją Mobilną Bank może ponadto uzyskać dostęp do informacji o numerze IP, czasie połączenia użytkownika z Aplikacją Mobilną oraz korzystać z identyfikatora pozwalającego na śledzenie zdarzeń w Aplikacji Mobilnej.

Czy informacje przechowywane na urządzeniu mobilnym są niezbędne?

Informacje, które Bank przechowuje na urządzeniu mobilnym użytkownika, są niezbędne do prawidłowego funkcjonowania Aplikacji Mobilnej i świadczenia usług za jej pośrednictwem.

W aplikacjach mobilnych do celów marketingowych używa się niekiedy także identyfikatorów urządzeń mobilnych, które są dostarczane przez system operacyjny urządzenia mobilnego i mogą zostać zresetowane przez użytkownika. **Bank nie wykorzystuje w Aplikacji Mobilnej takich identyfikatorów.** Zasady wyświetlania reklam w Aplikacji Mobilnej opisane są w podrozdziale „Informacje szczegółowe".

Czy można usunąć informacje przechowywane na urządzeniu mobilnym?

DeviceID jest unikatową serią cyfr i liter przypisaną do urządzenia mobilnego i użytkownik nie może samodzielnie go zmienić ani zresetować. Dostęp do tego identyfikatora może być uzyskany przez każdą pobieraną i instalowaną aplikację.

Czynności związane z przechowywaniem i wysyłaniem *cookies* oraz wykorzystanie identyfikatorów wykonywane przez urządzenie mobilne nie są widoczne dla użytkownika. Nie ma możliwości ich wyłączenia za pomocą ustawień. Użytkownik, który nie akceptuje wykorzystywania identyfikatorów lub plików *cookie* nie powinien instalować Aplikacji Mobilnej lub logować się do niej. W przypadku sprzeciwu wobec korzystania z *cookies* lub identyfikatorów w trakcie korzystania z Aplikacji Mobilnej, użytkownik powinien ją odinstalować.

Lista identyfikatorów i informacji wykorzystywanych przez Bank

Do komunikacji pomiędzy serwerami Banku a urządzeniem mobilnym po zalogowaniu są wykorzystywane lub technicznie przekazywane następujące informacje:

- identyfikator instalacji/aktywacji Aplikacji Mobilnej (wspomniany wyżej Instance ID)
- unikalny identyfikator urządzenia mobilnego (wspomniany wyżej Device ID),
- informacja o języku urządzenia mobilnego (*Accept-Language*)

- informacja o wykorzystywanej platformie (iOS/ANDROID)
- informacja, czy urządzenie mobilne korzysta z serwisów Google czy Huawei (GMS lub HMS, *Mobile Services*)
- informacja o numerze wersji Aplikacji Mobilnej,
- typ/rodzaj urządzenia mobilnego użytkownika (*User-Agent*),
- „token", który weryfikuje sesję użytkownika na urządzeniu mobilnym, w tym sprawdza, czy sesja wciąż trwa i jest ważna (*Authorization token*)

Do komunikacji pomiędzy serwerami Banku a urządzeniem mobilnym przed zalogowaniem jest wykorzystywane rozwiązanie podobne do cookie/tokena na bazie Device ID, niezbędne do utrzymania konfiguracji widgetów przed zalogowaniem.

Przetwarzanie danych osobowych

Administrator danych

Administratorem danych osobowych użytkowników Aplikacji Mobilnej jest Bank Millennium S.A. z siedzibą w Warszawie:

- adres: ul. Stanisława Żaryna 2A, 02-593 Warszawa,
- telefon: (+48) 801 331 331 lub (+48) 22 598 40 40 – dla osób dzwoniących z telefonów komórkowych oraz z zagranicy (koszt połączenia według taryfy operatora),
- e-mail: kontakt@bankmillennium.pl.

Nadzór nad prawidłowym przetwarzaniem danych osobowych w Banku sprawuje Inspektor Ochrony Danych:

- adres: Inspektor Ochrony Danych, Bank Millennium S.A., ul. Stanisława Żaryna 2A, 02-593 Warszawa,
- e-mail: iod@bankmillennium.pl.

Można kontaktować się z Inspektorem we wszystkich sprawach związanych z przetwarzaniem danych osobowych, także w razie wątpliwości co do przysługujących użytkownikowi praw.

Cele przetwarzania danych osobowych użytkowników

Dane osobowe użytkowników Aplikacji Mobilnej, w zależności od łączących użytkownika z Bankiem relacji, przetwarzane są w następujących celach:

1. zawarcie i wykonanie umowy z Bankiem;
2. wypełnienia obowiązków wynikających z przepisów prawa;
3. cele realizowane w ramach tzw. prawnie uzasadnionego interesu Banku, tj.:
    1) zapewnianie bezpieczeństwa transakcji, w szczególności zapobieganie nadużyciom,
    2) dostosowywanie ofert marketingowych, produktów i usług Banku, jak również firm współpracujących z Bankiem, w oparciu o informacje uwzględniające cechy, zachowania lub preferencje użytkownika (profilowanie),
    3) wewnętrzne cele administracyjne, analityczne i statystyczne, w tym analizy portfela kredytowego, statystyki i raportowania wewnętrznego Banku oraz w ramach Grupy Kapitałowej Banku,
    4) marketing produktów i usług Banku, w szczególności realizowany poprzez przekazywanie informacji handlowych za pomocą tradycyjnej poczty lub w przypadku uzyskania stosownej zgody, również elektronicznie lub telefonicznie,

5) dostosowywanie treści marketingowych, w zależności od zachowań użytkownika,
6) realizacja komunikacji za pośrednictwem aplikacji mobilnej,
7) udzielanie odpowiedzi na zgłoszenia użytkownika,
8) w przypadku jeśli znajdzie to zastosowanie, w celach powiązanych z prowadzeniem postępowań spornych, a także postępowań przed organami władzy publicznej oraz innych postepowań, w tym w celu dochodzenia oraz obrony przed roszczeniami.

4. Realizacja działań prowadzonych na podstawie udzielonych zgód, w szczególności marketing usług i produktów podmiotów współpracujących z Bankiem.

Prawa użytkowników

Użytkownikowi w stosunku do danych osobowych przysługuje prawo:

1. dostępu,
2. sprostowania lub uzupełnienia,
3. usunięcia,
4. ograniczenia przetwarzania
5. wniesienia sprzeciwu wobec ich przetwarzania,
6. otrzymania od Banku danych osobowych w ustrukturyzowanym formacie oraz przenoszenia danych osobowych do innego administratora,
7. niepodlegania decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywołuje skutki prawne lub w inny sposób wpływa na użytkownika, chyba, że decyzja ta jest niezbędna do realizacji umowy, jest dozwolona prawem lub użytkownik wyraził wcześniej na to wyraźną zgodę;
8. w przypadkach, w których przetwarzanie danych odbywa się na podstawie udzielonej zgody - cofnięcia udzielonych zgód na poszczególne cele przetwarzania, w dowolnym momencie.

Informacje szczegółowe

Pozostałe informacje dotyczące zasad przetwarzania danych osobowych, w tym o przysługujących użytkownikowi prawach, dostępne są w polityce prywatności, oraz w dostępnym na tej stronie dokumencie „Informacje dotyczące przetwarzania danych osobowych w Banku Millennium S.A.”.

Podanie danych osobowych jest dobrowolne, ale niezbędne do korzystania z Aplikacji Mobilnej.

Reklamy w Aplikacji Mobilnej

Bank nie wykorzystuje w Aplikacji Mobilnej marketingowych plików *cookie* ani mobilnych identyfikatorów wyświetlania reklam, jednak w Aplikacji Mobilnej użytkownika mogą zostać wyświetlone reklamy.

Kampanie reklamowe są kierowane do użytkownika z uwzględnieniem wyrażonych przez niego oświadczeń w relacji z Bankiem, w tym udzielonych zgód. Aplikacja Mobilna jest w tym zakresie jedynie jednym z kanałów komunikacji Banku.

Brak zgody na Politykę prywatności aplikacji mobilnej

W przypadku braku zgody na niniejszą politykę prywatności użytkownik nie powinien instalować Aplikacji Mobilnej lub, jeśli została zainstalowana, odinstalować ją.

Przydatne linki

Szczegóły na temat Aplikacji Mobilnej https://www.bankmillennium.pl/bankowosc-prywatna/bankowosc-elektroniczna/bankowosc-mobilna/aplikacja-mobilna

Polityka Prywatności Banku oraz klauzule informacyjne Ochrona danych - Bank Millennium