

Polityka prywatności aplikacji mobilnych Biura maklerskiego mBanku

1. Niniejszy dokument opisuje politykę prywatności aplikacji mobilnych Biura maklerskiego mBanku S.A. z siedzibą w Warszawie (dalej: mBm).
2. Na urządzeniu mobilnym przechowywane są:
 - 2.1. zaszyfrowany unikalny Identyfikator urządzenia, wymagany do działania powiadomień PUSH.
3. W celu identyfikacji Klienta niezbędnym do zalogowania się w Aplikacji przez Klientów usługi eMakler jest posiadanie sparowanej aplikacji mBanku i aplikacji mBm.
4. Klienci mBm niebędący klientami mBanku S.A. w celu zalogowania się w Aplikacji otrzymują wygenerowany indywidualny identyfikator i hasło.
5. Identyfikator Aplikacji o którym mowa w punkcie 2.1. oraz informacje o marce, modelu i identyfikatorze sprzętowym urządzenia mobilnego są wysyłane do Banku w procesie logowania urządzenia w Aplikacji oraz są wykorzystywane w celu jednoznacznego zidentyfikowania Aplikacji i urządzenia mobilnego.
6. Komunikacja między aplikacją mobilną a mBm odbywa się z użyciem mechanizmów szyfrujących.
7. W zależności od platformy mobilnej, aplikacje mogą uzyskać dostęp do następujących uprawnień na urządzeniu mobilnym:
 - 7.1. informacji o połączeniu na potrzeby odbierania danych z internetu (dostęp do sieci),
8. Aplikacja dla wybranych modeli telefonów, pozwala na korzystanie z technologii identyfikacji odciskiem palca służącej do sprawdzania tożsamości użytkownika na podstawie jego linii papilarnych.
9. Aplikacja dla wybranych modeli telefonów, pozwala na korzystanie z technologii identyfikacji Face ID, służącej do sprawdzania tożsamości użytkownika na podstawie skanowania jego twarzy.
10. W zależności od aplikacji mobilnej, uprawnienia aplikacji można odwołać przez zmianę ustawień systemowych na urządzeniu lub odinstalowanie aplikacji.
11. Aplikacje mobilne nie przechowują żadnych danych osobowych, które mogłyby umożliwić osobie trzeciej identyfikację konkretnego użytkownika aplikacji
12. W przypadku braku zgody na niniejszą politykę prywatności nie instaluj Aplikacji lub ją odinstaluj.
13. mBm zwraca uwagę na konieczność przechowywania danych do logowania do Aplikacji w bezpiecznym miejscu i nie ujawniania ich osobom trzecim. W przypadku nieautoryzowanego użycia danych do logowania przez osobę trzecią lub jakimkolwiek innym naruszeniu bezpieczeństwa, prosimy o niezwłoczny kontakt.
14. mBm dokłada należytej staranności, aby zapewnić i utrzymać ciągłość działania Aplikacji. W sytuacji zakłócenia działania, do czasu przywrócenia dostępu do usług Aplikacji należy używać wersji webowej systemu transakcyjnego bądź skorzystać w formy telefonicznego składania zleceń.