Warunki korzystania i bezpieczeństwo Aplikacji bossaMobile

Dom Maklerski Banku Ochrony Środowiska S.A. (dalej DM BOŚ) z siedzibą w Warszawie, ul. Marszałkowska 78/80 Warszawa (adres e-mail: makler@bossa.pl), świadczy usługi maklerskie za pośrednictwem Aplikacji bossaMobile w zakresie wykonywania zleceń nabycia lub zbycia instrumentów finansowych na rachunek dającego zlecenie składanych przez Klienta na podstawie następujących umów:

a. Umowy o wykonywanie zleceń nabycia lub zbycia instrumentów finansowych na rynku kasowym oraz przyjmowania i przekazywania zleceń,

b. Umowy o wykonywanie zleceń nabycia lub zbycia derywatów w obrocie zorganizowanym,

c. Umowy o wykonywanie zleceń nabycia lub zbycia derywatów w obrocie zorganizowanym na rachunku derywatów intraday,

d. Umowy o wykonywanie zleceń nabycia lub zbycia instrumentów finansowych na rynku kasowym zawierana w celu zawarcia Umowy IKE (Umowa maklerska IKE),

e. Umowy o wykonywanie zleceń nabycia lub zbycia instrumentów finansowych na rynku kasowym zawierana w celu zawarcia Umowy IKZE (Umowa maklerska IKZE).

DM BOŚ za pośrednictwem Aplikacji bossaMobile udostępnia Klientom, na podstawie Umowy o dystrybucję serwisów informacyjnych, notowania przekazywane na bieżąco przez Giełdę Papierów Wartościowych w Warszawie S.A., a za pośrednictwem Aplikacji bossaMobile DEMO - dla potencjalnych Klientów udostępnia notowania przekazywane na bieżąco, na okres próbny nieprzekraczający 30 dni, wyłącznie w celach demonstracyjnych. Aplikacja bossaMobile DEMO jest udostępniana wyłącznie w celach demonstracyjnych, bez możliwości zawierania rzeczywistych transakcji. Zakres instrumentów finansowych, których notowania będą dostępne w wersji DEMO bossaMobile może zostać ograniczony przez DM BOŚ. Klient i potencjalny Klient dalej zwani są łącznie Użytkownikiem.

DM BOŚ prowadzi działalność na podstawie zezwolenia Komisji Papierów Wartościowych i Giełd. DM BOŚ podlega nadzorowi Komisji Nadzoru Finansowego.

Aplikacja bossaMobile przechowuje na urządzeniu mobilnym Użytkownika przez okres zainstalowania Aplikacji, następujące dane:

1. ustawienia zdefiniowane przez Użytkownika,
2. zaszyfrowany unikalny identyfikator Aplikacji (parametr tworzony jest w procesie instalacji Aplikacji).

Dane, o których mowa powyżej są przechowywane na urządzeniu Użytkownika tak długo, jak długo jest zainstalowana Aplikacja.

Dane, o których mowa powyżej oraz informacje o marce, modelu i identyfikatorze sprzętowym urządzenia mobilnego są wysyłane do DM BOŚ w procesie logowania Użytkownika oraz są wykorzystane w celu jednoznacznego zidentyfikowania Aplikacji i urządzenia mobilnego. Komunikacja między aplikacją mobilną a systemami informatycznymi DM BOŚ odbywa się z użyciem protokołu SSL (Secure Socket Layer).

Aplikacja umożliwia przechowywanie Identyfikatora służącego do logowania przez Użytkownika do rachunku maklerskiego. Użytkownik może zrezygnować z funkcji przechowywania Identyfikatora.

Telefony i tablety działające pod kontrolą systemu iOS posiadające TouchID* lub FaceID* oraz urządzenia z systemem Android z możliwością autoryzacji poprzez odcisk palca, pozwalają na korzystanie z wymienionych technologii do sprawdzania tożsamości Użytkownika. Użytkownik przed pierwszym logowaniem za pośrednictwem wymienionych technologii określa dane biometryczne (odcisk palca, odwzorowanie twarzy), które będzie przypisane do jego identyfikatora i hasła do Aplikacji. W przypadku pozytywnej weryfikacji tożsamości przy pomocy tych danych biometrycznych identyfikator i hasło do Aplikacji zostaną wysłane do DM BOŚ w procesie logowania do Aplikacji. Wszystkie dane biometryczne znajdują się po stronie użytkownika (urządzenia) lub dostawcy urządzenia. DM BOŚ nie przechowuje żadnych danych biometrycznych.

Aplikacja w trakcie procesu instalacji może uzyskać dostęp do uprawnień umożliwiających komunikację sieciową i dostęp do Internetu, a także adresu e-mail Użytkownika.

W zależności od urządzenia mobilnego uprawnienia Aplikacji można odwołać przez zmianę ustawień systemowych na urządzeniu mobilnym lub poprzez odinstalowanie Aplikacji.

Użytkownik może korzystać z notowań przekazywanych na bieżąco przez Giełdę Papierów Wartościowych w Warszawie S.A. wyłącznie dla własnych wewnętrznych potrzeb informacyjnych niezwiązanych bezpośrednio z prowadzoną działalnością gospodarczą lub zawodową, bez prawa ich rozpowszechniania w jakiejkolwiek formie w całości lub w części. Użytkownik zobowiązuję się do niekorzystania z notowań przekazywanych na bieżąco przez Giełdę Papierów Wartościowych w Warszawie S.A. na więcej niż jednym urządzeniu w tym samym czasie. Użytkownik nie może dostarczać danych o charakterze bezprawnym ani składać zleceń lub dyspozycji sprzecznych z obowiązującymi przepisami prawa.

Tryb postępowania reklamacyjnego określa szczegółowo właściwy dla danej umowy świadczenia usług maklerskich regulamin. Regulaminy dostępne są na stronie Dokumenty.

Zakończenie korzystania z Aplikacji bossaMobile nie oznacza rozwiązania właściwej umowy świadczenia usług maklerskich, chyba że niezależnie od zakończenia korzystania z Aplikacji bossaMobile Klient wypowie umowę świadczenia usług maklerskich.

Bezpieczeństwo Aplikacji bossaMobile

Usługa bossaMobile pozwala na korzystanie z wielu funkcjonalności rachunku maklerskiego poprzez dedykowaną aplikację instalowaną na telefonie lub tablecie Użytkownika. Dom Maklerski Banku Ochrony Środowiska S.A. dokłada wszelkich starań, by korzystanie z rachunku maklerskiego drogą mobilną było równie bezpieczne, jak przy tradycyjnym dostępie z komputera stacjonarnego.

W jaki sposób zapewniamy bezpieczeństwo?

Usługa bossaMobile korzysta z dotychczasowych i rozszerzonych standardów bezpieczeństwa DM BOŚ:

- Logowanie identyfikatorem i dedykowanym hasłem – Użytkownik może zdefiniować oddzielne hasło do usługi bossaMobile, niż to wykorzystywane w dostępie z komputera stacjonarnego.
- Logowanie biometryczne – Użytkownik ma możliwość zalogowania się do aplikacji bossaMobile za pomocą danych biometrycznych – Odcisk palca (system Android), TouchID/FaceID (system iOS).
- Zarządzanie dostępem z poziomu rachunku maklerskiego – Użytkownik może w dowolnej chwili zmienić hasło do usługi lub zablokować dostęp.
- Systemy komputerowe DM BOŚ są chronione Firewallem – chronimy nasze systemy przed nieautoryzowanym dostępem.
- Szyfrowanie – w celu ochrony transmisji poufnych danych oraz integralności informacji wszystkie połączenia aplikacji bossaMobile są szyfrowane protokołem SSL.

Praca z Aplikacją bossaMobile

Każda sesja Użytkownika rozpoczyna się od pozytywnej weryfikacji identyfikatora i hasła bossaMobile wpisanego przez Użytkownika lub wysłanego do DM BOŚ na skutek pozytywnej identyfikacji Klienta przy pomocy danych biometrycznych oraz weryfikacji stanu usługi. Użytkownik kończy sesję wybierając opcję „Wyloguj” z menu aplikacji bossaMobile.

W jaki sposób Użytkownik powinien dbać o bezpieczeństwo korzystania z bossaMobile?

- Pobierać i instalować aplikację tylko z autoryzowanych źródeł – sklepy iTunes®App Store czy Google Play.
- Chronić swoje hasło bossaMobile – nie przekazywać danych logowania osobom trzecim,
- Zapamiętać swoje hasło bossaMobile – nie przechowywać zapisanego hasła w telefonie lub w innych miejscach,
- Zadbać o złożoność hasła bossaMobile – hasło powinno być trudne do odgadnięcia dla osób trzecich,
- Nigdy nie zostawiać urządzenia mobilnego bez nadzoru i odpowiedniego zabezpieczenia – osoba trzecia może wykorzystać sytuację, w której Użytkownik nie wylogował się z aplikacji, lub zalogować się przy pomocy danych biometrycznych Użytkownika w czasie jego snu,
- Wylogować się z aplikacji bossaMobile po zakończeniu korzystania,
- Wykorzystać wbudowane funkcje zabezpieczeń telefonu –Użytkownik może wykorzystać mechanizmy zabezpieczeń dostarczone przez producenta telefonu, tj. hasło dostępowe przy odblokowaniu urządzenia.

Szczególne zagrożenia związane z korzystaniem z Aplikacji bossaMobile

Podstawowym zagrożeniem każdego Użytkownika Internetu, w tym osób korzystających z usług świadczonych drogą elektroniczną, jest możliwość „zainfekowania” urządzenia Użytkownika przez niepożądane oprogramowanie tworzone głównie w celu wyrządzania szkód, np. wirusy, czy „konie trojańskie”.

W szczególności:

- obecność i działanie oprogramowania typu malware po uruchomieniu może zarazić pliki w sposób samopowielający, zazwyczaj nie będąc zauważonym przez Użytkownika; wirusy mogą być mniej lub bardziej szkodliwe dla systemu operacyjnego, w którym się znajdują, ale nawet w najmniej poważnym przypadku są marnotrawstwem pamięci RAM, CPU i miejsca na twardym dysku (więcej: http://pl.wikipedia.org/wiki/Malware);

- obecność i działanie robaków internetowych (worm), czyli szkodliwego oprogramowania zdolnego do samopowielania; e-mail worm jest niszczącym atakiem przeciwko sieci, polegającym na zebraniu wszystkich adresów e-mail znajdujących się w lokalnym programie (na przykład w MS Outlook) i wysłaniu na nie setek e-maili zawierających robaka w niewidocznym załączniku;
- możliwość zadziałania oprogramowania typu spyware, to jest oprogramowania szpiegującego działania Użytkownika w Internecie, instalującego się bez jego wiedzy, zgody i kontroli;
- możliwość bycia narażonym na cracking lub phishing (łowienie haseł) - w kontekście informatycznym phishing oznacza technikę łamania zabezpieczeń (cracking), używaną do pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne.

By uniknąć zagrożeń tego typu Użytkownik nie powinien instalować niepotrzebnego oprogramowania w swoim telefonie lub tablecie, używać tylko autoryzowanych przez producenta telefonu źródeł oprogramowania. DM BOŚ zaleca również rozważenie przez Użytkownika instalacji oprogramowania antywirusowego na urządzeniu przenośnym.

Wymagania techniczne niezbędne do współpracy:

Telefony		
	Android	**iOS**
Wymagania minimalne:	Android 5.0 Lollipop Rozdzielczość: HD Pamięć: 2 GB RAM	iOS10 Rozdzielczość: 1334x750px Pamięć: 2 GB RAM
Wymagania zalecane:	Android 7.0 Nougat lub nowszy Rozdzielczość: FHD lub większa Pamięć: 4 GB RAM lub więcej	iOS12 lub nowszy Rozdzielczość: 1334x750px lub większa Pamięć: 3 GB RAM lub więcej
Tablety		
	Android	**iOS**
Wymagania minimalne:	Android 5.0 Lollipop Rozdzielczość: HD Pamięć: 2 GB RAM	iOS10 Rozdzielczość: 1536x2048px Pamięć: 2 GB RAM
Wymagania zalecane:	Android 7.0 Nougat lub nowszy Rozdzielczość: FHD lub większa Pamięć: 4 GB RAM lub więcej	iOS12 lub nowszy Rozdzielczość: 1536x2048px lub większa Pamięć: 3 GB RAM lub więcej

Wymagania minimalne jak i zalecane mają charakter informacyjny, gdyż aplikacja bossaMobile pozwala na otwieranie dowolnej liczby wykresów o potencjalnie dużych zakresach prezentowanych danych, co wiąże się bezpośrednio z wykorzystywaniem coraz większych zasobów systemowych wybranego urządzenia. W związku z powyższym, przedstawione i ww. wymagania techniczne mogą nie spełniać potrzeb Użytkownika, w zależności od sposobu wykorzystywania aplikacji bossaMobile.

Zmiana powyższych Wymagań Technicznych będzie podawana do wiadomości Klienta za pośrednictwem strony internetowej Warunki Korzystania bossaMobile poprzez opublikowanie jej nowej wersji.

W przypadku braku zgody na powyższe warunki, korzystanie z Aplikacji nie jest dopuszczalne.

* TouchID i FaceID są znakami towarowymi Apple Inc. zarejestrowanymi w Stanach Zjednoczonych i innych krajach.