eurobank

WYKAZ ZMIAN
w Regulaminie świadczenia Usług Bankowości Elektronicznej wchodzącym w życie 6 sierpnia 2016 roku

W wykazie zacytowane zostały całe paragrafy Regulaminu, w których zostały dokonane zmiany. Nowe wersje zmienionych zapisów oznaczone są pogrubioną czcionką.

Dotychczasowa wersja zapisu:	Nowa wersja zapisu:
§ 6 1) Korzystanie z Bankowości Internetowej jest możliwe za pośrednictwem serwisu eurobank online, dostępnego pod adresem internetowym wskazanym w Serwisie informacyjnym, oraz za pośrednictwem Aplikacji mobilnej. 2) W celu korzystania z Bankowości Internetowej za pośrednictwem serwisu eurobank online Bank generuje i przekazuje Klientowi Identyfikator wraz z hasłem tymczasowym do Bankowości Internetowej, które umożliwiają pierwsze Logowanie. Do pierwszego Logowania w serwisie eurobank online służy ponadto kod jednorazowy wygenerowany przez Token GSM, jeżeli został on wydany na wniosek Klienta. 3) Podczas pierwszego Logowania w serwisie eurobank online Klient samodzielnie ustanawia znane tylko sobie Hasło oraz określa konieczność podawania przy każdym kolejnym Logowaniu kodu jednorazowego wygenerowanego przez Token GSM, jeżeli został on wydany na wniosek Klienta. Klient ma również możliwość zdefiniowania Identyfikatora dodatkowego, który może być używany zamiennie z Identyfikatorem. 4) Aplikacja mobilna wymaga aktywacji z wykorzystaniem Identyfikatora lub Identyfikatora dodatkowego i kodu aktywacyjnego. Po aktywacji Klient nadaje PIN oraz – jeżeli Urządzenie mobilne Klienta ma możliwości techniczne – określa,, czy do Logowania powinien być używany Kod biometryczny. 5) Token GSM wymaga aktywacji z wykorzystaniem kodu aktywacyjnego. Po aktywacji Klient nadaje PIN. Wygenerowanie kodu jednorazowego przez Token GSM wymaga podania PIN.	**§ 6** 1) Korzystanie z Bankowości Internetowej jest możliwe za pośrednictwem serwisu eurobank online, dostępnego pod adresem internetowym wskazanym w Serwisie informacyjnym, oraz za pośrednictwem Aplikacji mobilnej. **2) W celu korzystania z Bankowości Internetowej za pośrednictwem serwisu eurobank online Bank generuje i przekazuje Klientowi Identyfikator wraz z hasłem tymczasowym do Bankowości Internetowej, które umożliwiają pierwsze Logowanie.** **3) Podczas pierwszego Logowania w serwisie eurobank online Klient samodzielnie ustanawia znane tylko sobie Hasło.** 4) Aplikacja mobilna wymaga aktywacji z wykorzystaniem Identyfikatora lub Identyfikatora dodatkowego, o którym mowa w § 7 ust. 2, i kodu aktywacyjnego. Po aktywacji Klient nadaje PIN oraz – jeżeli Urządzenie mobilne Klienta ma możliwości techniczne – określa, czy do Logowania powinien być używany Kod biometryczny. 5) Token GSM wymaga aktywacji z wykorzystaniem kodu aktywacyjnego. Po aktywacji Klient nadaje PIN. Wygenerowanie kodu jednorazowego przez Token GSM wymaga podania PIN.
§ 7 1) Podczas kolejnego Logowania w serwisie eurobank online Bank wymaga podania: Identyfikatora lub Identyfikatora dodatkowego, jeśli został zdefiniowany	**§ 7** **1) Podczas kolejnego Logowania w serwisie eurobank online Bank wymaga podania: Identyfikatora lub Identyfikatora dodatkowego, jeśli został zdefiniowany**

zgodnie z § 6 ust. 3, Hasła oraz kodu jednorazowego wygenerowanego przez Token GSM, jeśli został on wydany i Klient wskazał taką konieczność zgodnie z § 6 ust. 3. 2) Za pośrednictwem serwisu eurobank online Klient może zmienić sposób Logowania w zakresie konieczności podawania kodu jednorazowego wygenerowanego przez Token GSM, jeżeli został on wydany na wniosek Klienta, oraz zdefiniować Identyfikator dodatkowy, który może być używany zamiennie z Identyfikatorem. 3) Każda dyspozycja w serwisie eurobank online, w tym każda Transakcja płatnicza, wymaga Autoryzacji. 4) Jeżeli Klientowi został wydany Token GSM lub zostały aktywowane Hasła SMS, Bank wymaga dodatkowej Autoryzacji w serwisie eurobank online polegającej na podaniu kodu jednorazowego dla wybranych dyspozycji. 5) Klient nieposiadający Tokena GSM lub niekorzystający z Haseł SMS może składać wyłącznie Zlecenia płatnicze w serwisie eurobank online, które nie wymagają uwierzytelnienia za pomocą kodu jednorazowego. Powyższe ograniczenie nie dotyczy Zleceń płatniczych na rzecz zdefiniowanego zaufanego odbiorcy.	**zgodnie z § 7 ust. 2, Hasła oraz kodu jednorazowego wygenerowanego przez Token GSM lub Hasła SMS, jeśli Klient wskazał taką konieczność zgodnie z § 7 ust. 2.** **2) Za pośrednictwem serwisu eurobank online Klient może zmienić sposób Logowania w zakresie konieczności podawania kodu jednorazowego wygenerowanego przez Token GSM lub Hasła SMS oraz zdefiniować Identyfikator dodatkowy, który może być używany zamiennie z Identyfikatorem.** 3) Każda dyspozycja w serwisie eurobank online, w tym każda Transakcja płatnicza, wymaga Autoryzacji. 4) Jeżeli Klientowi został wydany Token GSM lub zostały aktywowane Hasła SMS, Bank wymaga dodatkowej Autoryzacji w serwisie eurobank online polegającej na podaniu kodu jednorazowego dla wybranych dyspozycji. 5) Klient nieposiadający Tokena GSM lub niekorzystający z Haseł SMS może składać wyłącznie Zlecenia płatnicze w serwisie eurobank online, które nie wymagają uwierzytelnienia za pomocą kodu jednorazowego. Powyższe ograniczenie nie dotyczy Zleceń płatniczych na rzecz zdefiniowanego zaufanego odbiorcy.
§ 14 1) Klient zobowiązany jest do zachowania wszelkich niezbędnych środków ostrożności mających zapobiec nieuprawnionemu uzyskaniu przez osobę trzecią danych służących do Logowania i Autoryzacji poprzez Kanały Bankowości Elektronicznej lub ich utracie. 2) Klient zobowiązany jest do: a) przechowywania Hasła, Hasła SMS, PINu, Telekodu, Tokena GSM, Identyfikatora i Identyfikatora dodatkowego, z zachowaniem należytej staranności, w tym do przechowywania ich oddzielnie, b) nieudostępniania Hasła, Hasła SMS, PINu, Telekodu, Tokena GSM, Identyfikatora i Identyfikatora dodatkowego osobom nieuprawnionym, c) okresowej zmiany Hasła, nie rzadziej niż co 180 dni. 3) Jeżeli Urządzenie mobilne Klienta pozwala na wykorzystywanie Kodu biometrycznego, korzystanie z funkcji Logowania za pomocą Kodu biometrycznego jest dozwolone tylko w przypadku, gdy na Urządzeniu mobilnym nie jest zarejestrowany odcisk palca osoby trzeciej. 4) W przypadku podejrzenia lub stwierdzenia przez Klienta, że Hasło, Hasło SMS, PIN,	**§ 14** 1) Klient zobowiązany jest do zachowania wszelkich niezbędnych środków ostrożności mających zapobiec nieuprawnionemu uzyskaniu przez osobę trzecią danych służących do Logowania i Autoryzacji poprzez Kanały Bankowości Elektronicznej lub ich utracie. 2) Klient zobowiązany jest do: a) przechowywania Hasła, Hasła SMS, PINu, Telekodu, Tokena GSM, Identyfikatora i Identyfikatora dodatkowego, z zachowaniem należytej staranności, w tym do przechowywania ich oddzielnie, b) nieudostępniania Hasła, Hasła SMS, PINu, Telekodu, Tokena GSM, Identyfikatora i Identyfikatora dodatkowego osobom nieuprawnionym, c) okresowej zmiany Hasła, nie rzadziej niż co 180 dni. 3) Jeżeli Urządzenie mobilne Klienta pozwala na wykorzystywanie Kodu biometrycznego, korzystanie z funkcji Logowania za pomocą Kodu biometrycznego jest dozwolone tylko w przypadku, gdy na Urządzeniu mobilnym nie jest zarejestrowany odcisk palca osoby trzeciej. 4) W przypadku podejrzenia lub stwierdzenia przez Klienta, że Hasło, Hasło SMS, PIN,

Telekod, Identyfikator lub Identyfikator dodatkowy zostały utracone lub Kod biometryczny został pozyskany przez osobę trzecią, a także w razie nieuprawnionego dostępu do nich lub nieuprawnionego użycia ich przez osoby trzecie, Klient zobowiązany jest do niezwłocznej zmiany powyższych danych identyfikacyjnych. 5) W przypadku, gdy Bank wydał Klientowi Token GSM służący do Logowania lub Autoryzacji, Klient zobowiązany jest do niezwłocznego poinformowania Banku o podejrzeniu lub stwierdzeniu utraty Tokena, jego kradzieży, przywłaszczenia lub nieuprawnionego użycia przez osobę trzecią. 6) Jeżeli Bank aktywował Klientowi Hasła SMS do Autoryzacji, Klient zobowiązany jest do niezwłocznego poinformowania Banku o podejrzeniu lub stwierdzeniu utraty, kradzieży, przywłaszczenia lub nieuprawnionego użycia przez osobę trzecią telefonu, którego numer został wskazanego do wysyłki Haseł SMS. 7) Zmiana lub zgłoszenie, o których mowa w ust. 4-6, może zostać zrealizowana: a) w Placówce, b) w Kanale Bankowości Internetowej – w przypadku zmiany Hasła lub Identyfikatora dodatkowego, c) w Kanale Bankowości Telefonicznej – w przypadku zmiany Telekodu i zgłoszenia określonego w ust. 5 i 6, d) za pośrednictwem formularza dostępnego w Serwisie informacyjnym dla Klienta posiadającego Token GSM – w przypadku zmiany Hasła, e) w ustawieniach Urządzenia mobilnego – w przypadku Kodu biometrycznego.	Telekod, Identyfikator lub Identyfikator dodatkowy zostały utracone lub Kod biometryczny został pozyskany przez osobę trzecią, a także w razie nieuprawnionego dostępu do nich lub nieuprawnionego użycia ich przez osoby trzecie, Klient zobowiązany jest do niezwłocznej zmiany powyższych danych identyfikacyjnych. 5) W przypadku, gdy Bank wydał Klientowi Token GSM służący do Logowania lub Autoryzacji, Klient zobowiązany jest do niezwłocznego poinformowania Banku o podejrzeniu lub stwierdzeniu utraty Tokena, jego kradzieży, przywłaszczenia lub nieuprawnionego użycia przez osobę trzecią. 6) **Jeżeli Bank aktywował Klientowi Hasła SMS do Logowania lub Autoryzacji, Klient zobowiązany jest do niezwłocznego poinformowania Banku o podejrzeniu lub stwierdzeniu utraty, kradzieży, przywłaszczenia lub nieuprawnionego użycia przez osobę trzecią telefonu, którego numer został wskazanego do wysyłki Haseł SMS.** 7) Zmiana lub zgłoszenie, o których mowa w ust. 4-6, może zostać zrealizowana: a) w Placówce, b) w Kanale Bankowości Internetowej – w przypadku zmiany Hasła lub Identyfikatora dodatkowego, c) w Kanale Bankowości Telefonicznej – w przypadku zmiany Telekodu i zgłoszenia określonego w ust. 5 i 6, d) za pośrednictwem formularza dostępnego w Serwisie informacyjnym dla Klienta posiadającego Token GSM – w przypadku zmiany Hasła, e) w ustawieniach Urządzenia mobilnego – w przypadku Kodu biometrycznego.