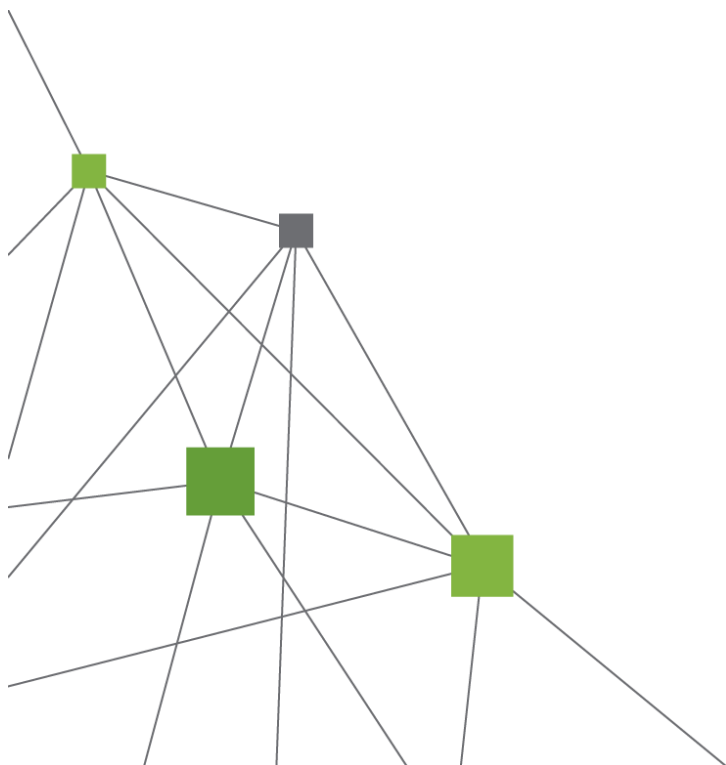


# PODRĘCZNIK UŻYTKOWNIKA

## PLATFORMA INTERNETOWA SGB



## Spis treści

1. Kilka zasad świadomego użytkownika systemu internetowego .....	3
2. Wymagania techniczne.....	6
3. Pierwsze logowanie.....	7
4. Ekran Główny .....	8
5. Kursy Walut .....	9
6. Transakcje walutowe.....	10
7. Transakcje z zaplanowanym późniejszym terminem realizacji .....	14
8. Zlecenia.....	16
9. Dane klienta.....	17
10. Zmiana hasła, wylogowanie .....	18
11. Pozostałe informacje .....	19

## 1. Kilka zasad świadomego użytkownika systemu internetowego

Internet ułatwia życie i pozwala oszczędzać czas i pieniądze. Korzystanie z Internetu niesie jednak za sobą wiele zagrożeń. Tak jak w życiu codziennym zmuszeni jesteśmy dbać o bezpieczeństwo własne i swojego majątku, tak korzystając z Internetu musimy przestrzegać pewnych zasad i dobrych praktyk aby uchronić się przed atakami hakerskimi, kradzieżą danych czy złośliwym wirusem.

Obsługa swoich finansów przez Internet powinna podlegać szczególnej ochronie ze względu na istniejące ryzyko poniesienia wymiernych strat. Używanie niezabezpieczonego urządzenia z dostępem do Internetu (np. komputera / telefonu) podczas korzystania z konta porównać można do pozostawiania otwartego mieszkania lub samochodu.

Poniżej przedstawiamy kilka istotnych reguł świadomego Użytkownika internetowych systemów bankowych. Przestrzeganie ich pozwoli istotnie ograniczyć ryzyko niepożądanych skutków włamań do systemów a jednocześnie nie musi wiązać się z żadnymi kosztami.

### 1. Używaj osobistego firewalla

Firewall (zapora przeciwogniowa) pełni funkcję strażnika chroniącego dostęp do komputera. Najczęściej jest to program instalowany w komputerze, umożliwiający blokowanie niechcianych i podejrzanych połączeń, wykrywanie programów szpiegujących albo przesyłających poufne informacje. Dostępne na rynku oprogramowanie tego typu jest często bezpłatne i zawiera wszystkie niezbędne funkcje. Firewall dostępny jest także w większości wersji systemu Windows w postaci Zapory systemu Windows. Jest obecny także w innych systemach operacyjnych.

Zmiana konfiguracji zapory wymaga od użytkownika świadomego działania. Jeżeli nie jesteś pewien efektów wprowadzanych zmian, nie wykonuj ich.

### 2. Zainstaluj i aktualizuj oprogramowanie antywirusowe - „antywirus”

Najczęstsze działania wirusów (złośliwego oprogramowania) to: kasowanie i niszczenie danych, rozsyłanie niechcianej poczty, kradzież danych (loginy, hasła, numery kart płatniczych), umożliwienie przejęcia kontroli nad komputerem, czy przekierowywanie połączeń na serwery należące do przestępców.

Dobrze jest zaopatrzyć się w program, który chroni nie tylko przed klasycznymi wirusami komputerowymi (w tym m.in. końmi trojańskimi oraz zagrożeniami ze strony adware/spyware) ale również wykorzystuje zaawansowane metody np. heurystyczne do wykrywania na bieżąco anomalii podczas pracy z komputerem, a także posiada filtry antyspamowe, mechanizmy antyphishingowe oraz ochronę przez złożonymi atakami bezpieczeństwa. Program antywirusowy pozwala zwalczać, usuwać oraz zabezpieczać nasze urządzenie z dostępem do Internetu przed większością zagrożeń. Codziennie pojawia się nawet kilkadziesiąt nowych zagrożeń, a producenci zazwyczaj co kilka godzin udostępniają na swoich serwerach aktualizacje.

Pamiętaj, by konfiguracja programu antywirusowego wykorzystywała w pełni jego możliwości (np. poprzez włączenie wszystkich zalecanych funkcji ochrony). Należy zwrócić uwagę na to, aby antywirus posiadał włączoną opcję skanowania ruchu internetowego z/do komputera (łącznie ze skanowaniem poczty przychodzącej i wychodzącej). Dobrym sposobem na zapewnienie ciągłej ochrony przed najnowszymi wirusami (w tym tzw. malware) jest również włączenie w programie antywirusowym aktualizacji automatycznych, co umożliwi ściągnięcie ich zaraz po opublikowaniu oraz uruchomienie wszystkich funkcji ochronnych.

Pamiętaj również o cyklicznym wykonywaniu (np. raz w tygodniu) pełnego skanowania komputera w poszukiwaniu zagrożeń (większość dostępnego oprogramowania antywirusowego umożliwia zaplanowanie takiego działania).

### **3. Instaluj „łatki” (*ang. patch*) na system operacyjny oraz aktualizuj na bieżąco jego istotne elementy (np. przeglądarkę internetową i jej dodatki/wtyczki)**

Żaden system operacyjny nie jest doskonały. Ciągłe wykrywane są luki, które mogą umożliwić skuteczny atak i spowodować straty użytkownika. Producenci oprogramowania bardzo często tworzą ‘łatki’ na system, które po zainstalowaniu pozwalają pozbyć się luki. Dlatego bardzo ważnym staje się fakt częstego wgrzywania poprawek do systemu.

Zalecane jest takie skonfigurowanie systemu (W przypadku Windows - moduł ‘Aktualizacje automatyczne’) aby on sam dbał o pobieranie aktualizacji ze strony producenta, zaraz po ich publikacji.

Aby zoptymalizować bezpieczeństwo związane z użytkowaniem systemu operacyjnego należy jak najrzadziej korzystać z trybu logowania na konto Administratora Systemu. Standardowe czynności w systemie, takie jak kopiowanie plików, korzystanie z Internetu, poczty elektronicznej, czy edytora tekstu można wykonywać na dodatkowo założonym koncie Użytkownika. Dodatkowo założonym – bo domyślnie założony przez system Windows użytkownik ma prawa administratora. Konto Użytkownika bez praw administratora dzięki swym ograniczeniom może uniemożliwić lub znacznie utrudnić próby włamania, instalowania złośliwego oprogramowania czy przejęcia kontroli. Unikaj również niezalecanych ustawień systemu operacyjnego. W niektórych przypadkach system operacyjny sam podpowie, że wykonywana zmiana ustawień obniża poziom bezpieczeństwa.

### **4. Chroń swoje dane**

**Pamiętaj, że dane do logowania do systemu którymi dysponujesz tj. Identyfikator i Hasło, umożliwiają przeprowadzenie transakcji na Twoim koncie. Jeżeli je ujawnisz ktoś może to wykorzystać.**

- nie zapisuj nigdzie w formie jawnej hasła do logowania. Najlepiej, jak zapamiętasz swoje hasło lub skorzystasz z profesjonalnych i sprawdzonych programów – menadżerów haseł.

- korzystaj tylko ze sprawdzonych i pewnych komputerów – nie loguj się na konto w kawiarence internetowej czy ogólnodostępnych komputerach w firmie,
- nie instaluj oprogramowania pochodzącego z niezauważanych, nieznanych Tobie źródeł.
- ignoruj wszelkie prośby (np. zawarte w sms, wiadomościach e-mail oraz kierowane w rozmowach telefonicznych), w których nadawca podszywając się pod bank lub inną zaufaną instytucję informuje o konieczności podania (np. w celach weryfikacyjnych) poufnych danych np. na stronie, do której podany jest link. W rzeczywistości strona ta jest często fałszywa, zaś oszuści wchodzą w posiadanie danych, dzięki którym realizują transakcje – **Nie podawaj nigdy nikomu swoich danych do logowania oraz innych danych autoryzacyjnych, np. kodów SMS!**
- nigdy nie loguj się do systemu za pośrednictwem otrzymanego w wiadomości e-mail lub sms linku,
- bądź ostrożny podczas podłączania zewnętrznych nośników danych (np. pendrive) oraz wszelkich urządzeń korzystających z portów USB. Nawet niewinnie wyglądający otrzymany w prezencie gadżet może okazać się urządzeniem wykradającym Twoje dane z komputera!
- unikaj stron www zachęcających do obejrzenia potencjalnie ciekawych treści lub zawierających atrakcyjne okazje cenowe,
- nie używaj wyszukiwarki internetowej do znalezienia strony www logowania do systemu. Bezpiecznym działaniem będzie wpisanie ręczne w pasku przeglądarki pełnego adresu (url) strony systemu,
- ostrożnie otwieraj załączniki lub linki (url) zawarte w komunikatorach, wiadomościach sms lub poczcie elektronicznej. Pamiętaj, że przestępcy wykorzystują bardzo sprawnie socjotechniki, aby np. wzbudzić Twoje zaufanie (tym samym usypiając czujność). Jeżeli masz wątpliwości co do autentyczności danej korespondencji elektronicznej, zawsze staraj się ją potwierdzić innym kanałem komunikacji (np. wykonując rozmowę telefoniczną z nadawcą na znany Tobie wcześniej numer telefonu),
- w przypadku dokumentów elektronicznych nieznanego pochodzenia, staraj się nie uruchamiać zawartych w nich zaawansowanych funkcji, np. makr,
- po zakończonej pracy z systemem zawsze pamiętaj, aby się z niego wylogować.

**Pamiętaj, że pracownik banku nigdy nie poprosi Ciebie w jakikolwiek sposób o Twoje indywidualne dane do logowania (oraz dane autoryzacyjne, np. kod SMS). Bank również nie zadzwoni do Ciebie i nie poprosi o dostęp do Twojego komputera, zwłaszcza dostęp zdalny!**

## **5. Zawsze sprawdzaj czy jesteś na właściwej stronie www**

Przed każdym zalogowaniem do serwisu internetowego sprawdź czy strona, na którą wchodzisz jest w rzeczywistości stroną Banku. Zdarzają się sytuacje, gdy hakerzy wykorzystując luki w oprogramowaniu lub niedostateczne zabezpieczenie komputera podstawiają fałszywą stronę imitującą stronę banku co pozwala przejść poufne dane.

- Sprawdź czy połączenie z bankiem jest szyfrowane – adres strony powinien rozpoczynać się od **https://** a nie **http://**, dodatkowo obok paska adresu lub w prawym dolnym rogu okna

przeglądarki powinien pojawić się żółty symbol kłódki, w niektórych przeglądarkach pasek z adresem lub część paska jest podświetlana na zielono,

- Upewnij się, że w pasku adresu (url) przeglądarki widnieje właściwy adres strony www banku. Zwracaj szczególną uwagę na literówki w nazwie adresu. Jeżeli masz wątpliwości adres strony banku otrzymasz na naszej Infolinii,
- sprawdź dane certyfikatu bezpieczeństwa serwisu (jeżeli nie wiesz jak, dowiedz się w Pomocy dla swojej przeglądarki jak sprawdzić certyfikat strony),
- czytaj informacje o alertach bezpieczeństwa, nie ignoruj komunikatów o błędnym certyfikacie,
- nie ignoruj zaobserwowanych różnic w wyglądzie strony lub w żądanych przez system danych.

## 6. Bądź czujny!

Podczas każdej pracy z urządzeniem posiadającym dostęp do Internetu (np. komputerem / telefonem) zawsze reaguj na wszelkiego rodzaju anomalie, np. nietypowy wygląd stron internetowych, powolną pracę urządzenia, zwłaszcza, jeżeli niepokojące symptomy pojawiły się nagle.

**Pamiętaj, że zawsze niezwłocznie możesz podzielić się z nami swoimi wątpliwościami, korzystając z naszej Infolinii.**

## 2. Wymagania techniczne

Do prawidłowego działania **Platformy internetowej SGB** potrzebna jest aktualna przeglądarka internetowa w najnowszej wersji:

### **Urządzenia stacjonarne (desktop/laptop):**

Chrome: wersja 77.x i wyższe

Mozilla: wersja 69.x i wyższe

MS Edge: wersja 43.x i wyższe

MS Internet Explorer: wersja 11.x i wyższe

Safari: wersja 11.x i wyższe

### **Urządzenia mobilne:**

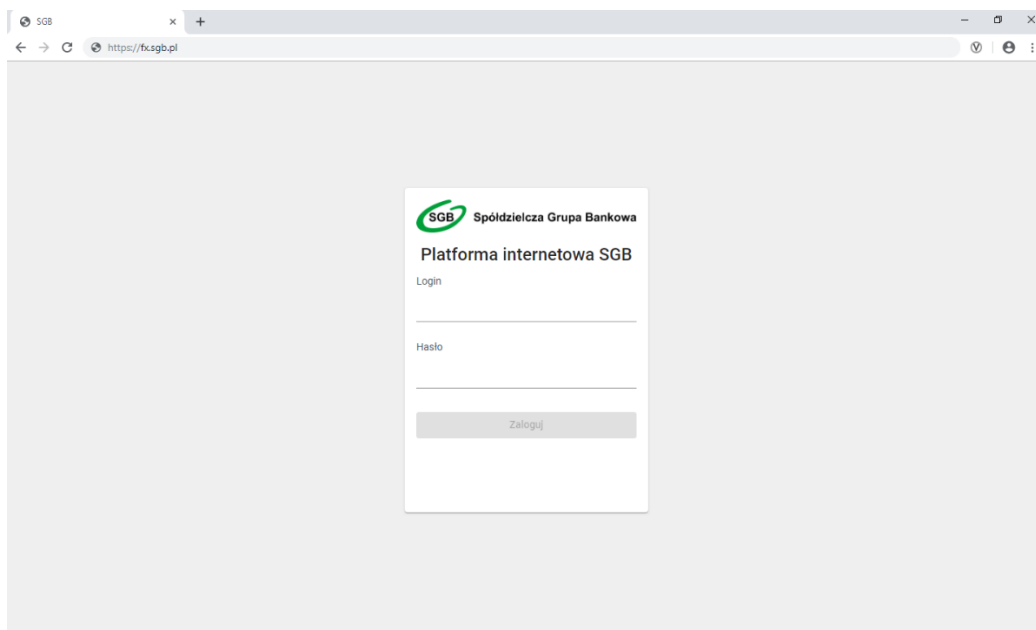
Przeglądarka wbudowana w system operacyjny Android: wersja Android 6.0 i wyższe

Przeglądarka wbudowana w system operacyjny iOS: wersja iOS 11.x i wyższe

Powyższa lista wersji przeglądarek jest listą właściwą na chwilę sporządzenia niniejszego dokumentu. Jak wyżej wskazano, obowiązuje zasada, że zawsze właściwa będzie najnowsza wersja danej przeglądarki.

### 3. Pierwsze logowanie

W celu zalogowania się do platformy, w przeglądarce należy wpisać adres: <https://fx.sgb.pl>



W oknie logowania należy wpisać nazwę użytkownika podaną w przesłanej do Klienta wiadomości e-mail oraz oddzielnie dostarczone przez SMS hasło. Należy zwrócić uwagę na małe/wielkie litery. Nazwa użytkownika jest nadawana wielkimi literami.

Nazwa użytkownika znajduje się również w załączniku nr 2 do *umowy zawierania transakcji wymiany walutowej z natychmiastową dostawą walut przez platformę internetową SGB dla klientów instytucjonalnych*.

Po wpisaniu loginu i hasła oraz wciśnięciu **Zaloguj**, przez SMS przesłany zostanie kod autoryzacyjny, który służy do potwierdzenia logowania.

Hasło oraz kod autoryzacyjny są wysyłane przez SMS na numer telefonu komórkowego pełnomocnika wskazanego w Umowie.

#### **Uwaga!**

Dostarczone hasło jest jednorazowe, platforma po pierwszym udanym logowaniu wymusi jego zmianę. Nowe hasło powinno zawierać minimum 8 znaków, w tym przynajmniej 1 wielką literę, 1 małą literę i 1 cyfrę.

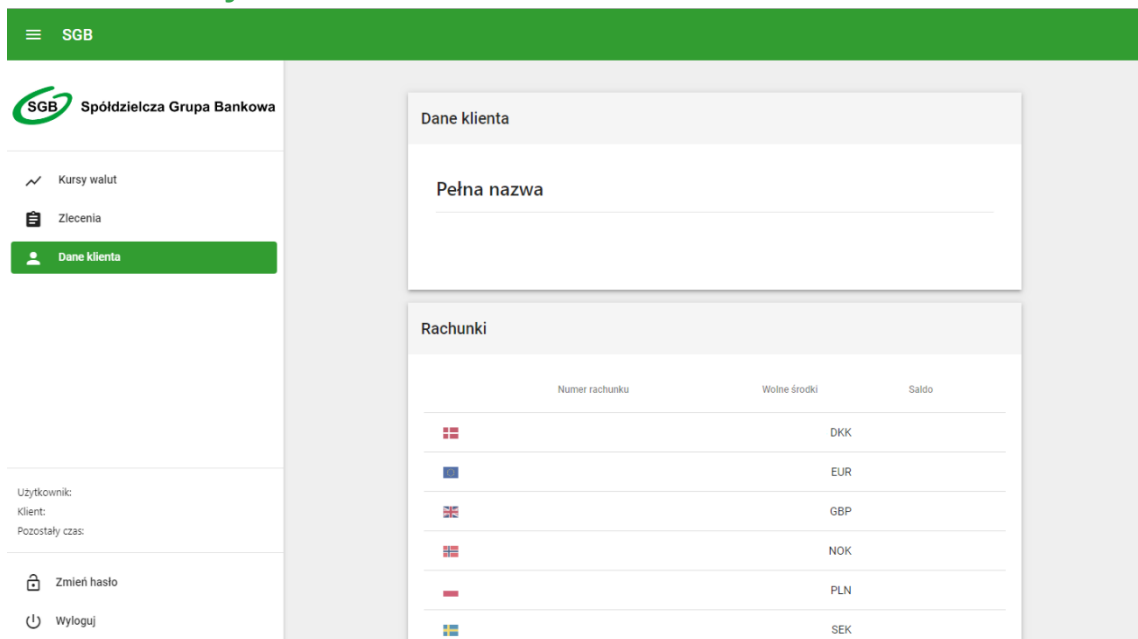
Klient ma 5 prób na zalogowanie się, przy 6-tej nieudanej próbie dostęp z przyczyn bezpieczeństwa zostanie zablokowany. W przypadku niepowodzenia zmiany hasła lub zablokowania platformy skontaktuj się z Infolinią SGB-Bank S.A. pod numerem telefonu:

**800 888 888** (dla połączeń krajowych, bezpłatne połączenie)

**(+48) 61 647 28 46** dla połączeń komórkowych oraz z zagranicy (opłata za połączenie zgodna z taryfą danego operatora),

Telefony dostępne przez całą dobę.


## 4. Ekran Główny



Ekran aplikacji podzielony jest na 3 części:

**1. Menu Nawigacji** w lewej części ekranu umożliwiające przechodzenie pomiędzy funkcjami:

- Kursy walut – opisana w Rozdziale 5
- Zlecenia – opisana w Rozdziale 8
- Dane klienta – opisana w Rozdziale 9

**2. Nagłówek** u góry ekranu umożliwiający ukrywanie bądź pokazywanie **Menu Nawigacji** za pomocą przycisku z trzema białymi belkami  znajdującego się po lewej stronie Nagłówka.

**3. Treść Właściwa** aplikacji znajdująca się w centralnej części ekranu. Jej zawartość jest zależna od funkcji, którą wybrano wcześniej za pośrednictwem **Menu Nawigacji**.



## 5. Kursy Walut

W funkcji **Kursy Walut** na ekranie przedstawione są aktualne kursy kupna/sprzedaży oraz wykresy zmian kursów dla wszystkich walut dostępnych w platformie internetowej SGB.

Pola w górnej części ekranu przedstawiają kursy walut uwzględniające maksymalną marżę ustaloną w ramach zaoferowanej Klientowi grupie marżowej.

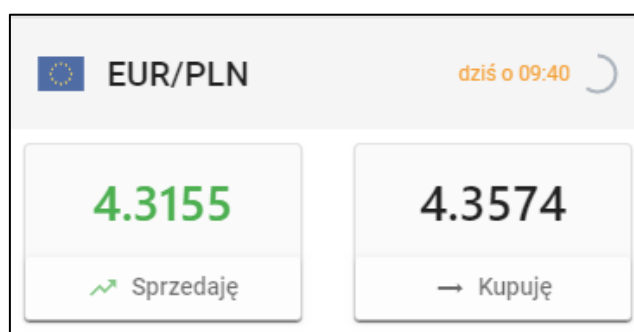
Po kliknięciu na daną parę walutową, w dolnej części ekranu aktualizuje się poglądowy wykres. Ma on charakter informacyjny i nie uwzględnia marży dla Klienta.



Na wykresie przedstawione są wartości opisujące oś pionową (kurs) oraz poziomą (czas). W prawym górnym rogu wykresu przedstawione jest rozwijane menu umożliwiające wybór zakresu czasu z jakiego brane są dane dla wykresu. Możliwymi do wyboru zakresami są:

- Bieżący dzień,
- Ostatnie 3 dni,
- Ostatni tydzień,
- Ostatni miesiąc.

W polu przedstawiającym parę walutową po prawej stronie przedstawiona jest godzina, z której pochodzi kurs oraz okrągły symbol aktywnie przedstawiający czas do cyklicznego odświeżenia kursu.

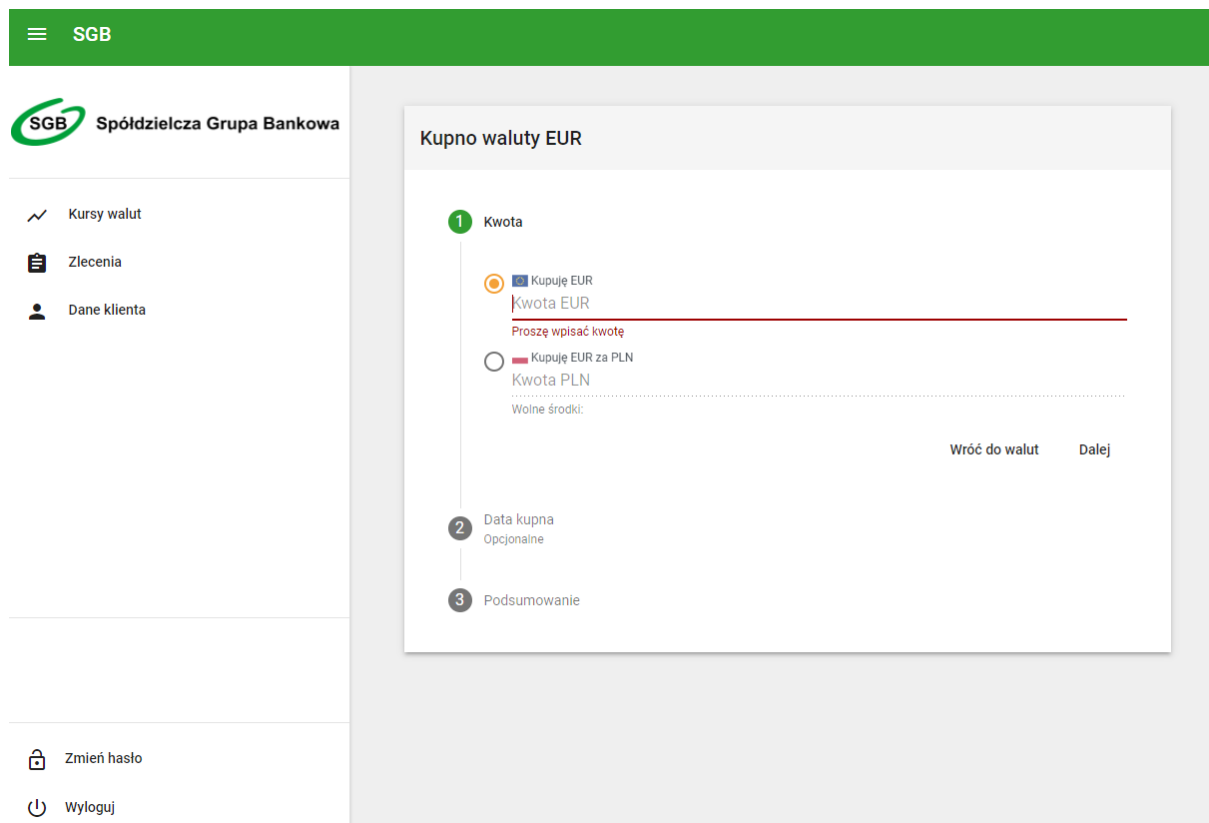


W polu widnieją przyciski umożliwiające odpowiednio **Sprzedaż** bądź **Kupno** danej waluty. Przyciski są aktywne jedynie dla walut, dla których Klient posiada rachunki walutowe przypisane w umowie do platformy, widoczne w **Menu Nawigacji** w zakładce **Dane Klienta**.

Przyknięcie jednego z nich spowoduje przejście do kolejnego procesu opisanego w rozdziale 6 – *Transakcje walutowe*.

## 6. Transakcje walutowe

Po wciśnięciu przycisku **Sprzedaję** lub **Kupuję** w opcji Kursy Walut następuje przejście do szczegółów transakcji walutowej.



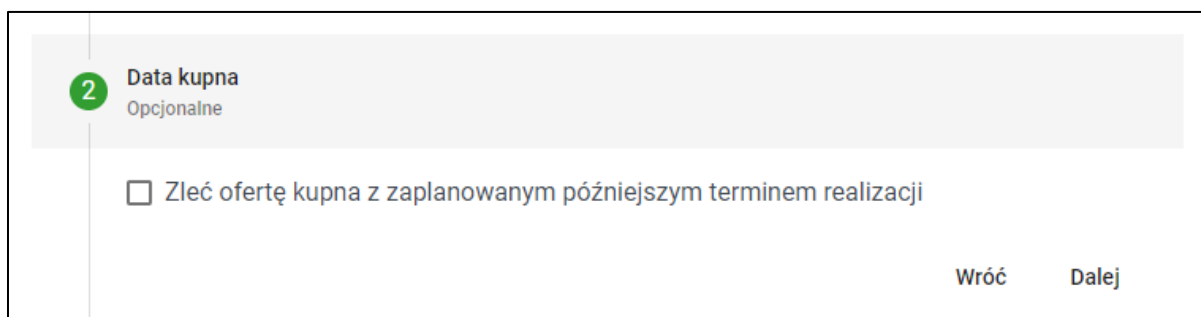
Transakcja przeprowadzana jest w kilku etapach.

**1. Pierwszym etapem** jest wpisanie kwoty transakcji w jeden z dwóch sposobów:

- a) Kwoty waluty, którą Klient zamierza kupić/sprzedać, lub
- b) Kwoty w PLN, którą Klient zamierza przeznaczyć na kupno lub uzyskać ze sprzedaży waluty.

Po wpisaniu kwoty należy zatwierdzić dane przyciskiem **Dalej**, co spowoduje przejście do kolejnego, opcjonalnego pola daty kupna lub sprzedaży.

**2. Drugim etapem** jest wybranie opcji, czy transakcja ma zostać zrealizowana w późniejszym terminie.



W przypadku chęci skorzystania z tej funkcji, należy zaznaczyć opcję „Zleć ofertę kupna/sprzedaży z zaplanowanym późniejszym terminem realizacji”. Szczegóły tego rozwiązania opisane są w Rozdziale 7 – *Transakcje z zaplanowanym późniejszym terminem realizacji*.

W przypadku zamiaru kupna/sprzedaży waluty w dniu zlecenia, należy przejść do kolejnego kroku przez użycie przycisku **Dalej**.

Przycisk **Wróć** służy po powrocie do pierwszego etapu.

**3. Trzecim etapem** jest potwierdzenie wcześniej wprowadzonych parametrów transakcji


Kupno	10 000,00 EUR
Kurs	 4.3483
Kwota w PLN	43 483,00 PLN
	<a href="#">Wróć</a> <input type="button" value="Kup"/>

Platforma prezentuje kwotę waluty, aktualny kurs rynkowy oraz kwotę w PLN.

W przypadku chęci zmiany parametrów, należy użyć przycisku **Wróć**, w przypadku akceptacji należy użyć przycisku **Kup** bądź **Sprzedaj**.

**4. Ostatnim etapem** jest zaakceptowanie aktualnego kursu zaproponowanego Klientowi.

Po kliknięciu **Kup** lub **Sprzedaj** platforma aktualizuje kurs, a Klient otrzymuje 20 sekund na ostateczne zatwierdzenie transakcji przyciskiem **Zatwierdź**

		13s
Kupno	2 300,44 EUR	
Kurs	4.3470	
Kwota w PLN	10 000,00 PLN	
	<a href="#">Anuluj</a> <input type="button" value="Zatwierdź"/>	

Brak użycia przycisku **Zatwierdź** lub użycie przycisku **Anuluj** powoduje powrót do poprzedniego etapu.

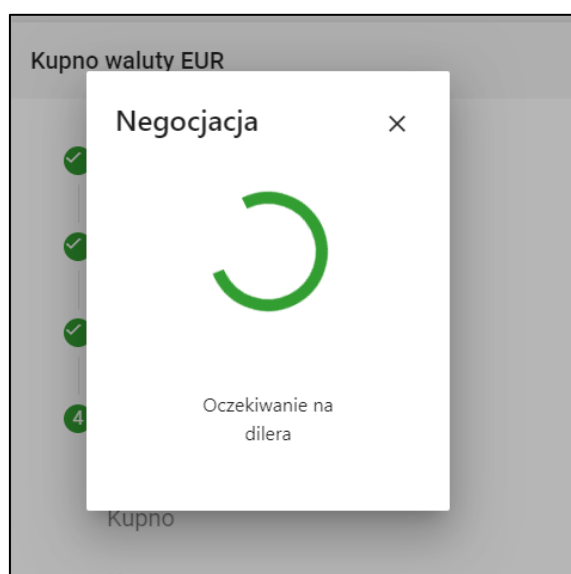
Po naciśnięciu przycisku **Zatwierdź** transakcja jest zawarta i automatycznie rozliczana poprzez ustanowione rachunki bankowe. **Transakcja jest zawarta nieodwołalnie**. Po zatwierdzeniu transakcji pojawi się informacja z podsumowaniem i możliwością wygenerowania potwierdzenia w formacie PDF.

W przypadku braku środków na pokrycie transakcji, nie zostanie ona zawarta.

**Uwaga!**

W przypadku transakcji opiewających na kwoty wyższe niż 2 000 000 PLN platforma przechodzi w tryb indywidualnego zapytania (w zależności od sytuacji na rynkach finansowych wysokość kwoty zapytania indywidualnego może ulec zmianie w komunikacie Banku).

W przypadku wystąpienia takiej sytuacji, w platformie pojawia się okno „Oczekiwanie na dilerą”



Po zaproponowaniu Klientowi kursu rynkowego przez pracownika Departamentu Skarbu, Klient otrzymuje 20 sekund na jego zaakceptowanie.



Brak użycia przycisku **Zatwierdź** powoduje ponowne przekazanie zapytania do dilerą, natomiast użycie przycisku **Anuluj** powoduje powrót do poprzedniego etapu.

Po naciśnięciu przycisku **Zatwierdź** transakcja jest zawarta i automatycznie rozliczana poprzez ustanowione rachunki bankowe. **Transakcja jest zawarta nieodwołalnie.** Po zatwierdzeniu transakcji pojawi się informacja z podsumowaniem i możliwością wygenerowania potwierdzenia w formacie PDF.

## 7. Transakcje z zaplanowanym późniejszym terminem realizacji

Platforma internetowa SGB umożliwia, oprócz transakcji natychmiastowych, składanie ofert zawarcia transakcji w zaplanowanym późniejszym terminie, których realizacja uzależniona jest od wskazanych przez Klienta parametrów. Funkcjonalność ta uruchamiana jest w drugim kroku opisanym w Rozdziale 6 *Transakcje walutowe*.

2
Data kupna

Zleć ofertę kupna z zaplanowanym późniejszym terminem realizacji  
 gdy kurs spadnie poniżej

Proszę wpisać kurs

Ważna do \*
📅 Godzina
🕒

Zlecenie musi być zaplanowane z co najmniej 10 minutowym wyprzedzeniem.

Wróć
Dalej

Zaznaczenie opcji „**Zleć ofertę kupna/sprzedaży w zaplanowanym późniejszym terminem realizacji**” pozwoli wypełnić formularz planowania oferty.

Planowanie oferty polega na ustaleniu kursu pozwalającego zrealizować transakcję w przyszłym terminie lecz nie później niż jeden miesiąc od bieżącej daty. Gdy kurs spadnie poniżej określonej wartości (dla kupna waluty) lub wzrośnie powyżej (dla sprzedaży waluty), w wybranym przez Klienta terminie, do którego zlecenie obowiązuje, Bank automatycznie przyjmie ofertę, co skutkuje zawarciem i realizacją transakcji zgodnie ze wszystkimi wcześniej wybranymi wartościami.

Istotne jest także określenie terminu (daty i godziny) ważności oferty. W przypadku, gdy wskazana oferta nie zostanie przyjęta przez Bank w określonym terminie jej ważności, zostanie ona automatycznie anulowana.

Przejdzie dalej wyświetli **Podsumowanie** danej transakcji. Przedstawione tu będą wszystkie dane, które wprowadzono w formularzu oraz opcje **Wróć** i **Zaplanuj**.

**3** Podsumowanie

Kupno	10 000,00 EUR
gdy kurs spadnie poniżej	4.0000
Oferta ważna do	31.12.2020 15:10

Automatyczne przyjęcie oferty z zaplanowanym późniejszym terminem realizacji i jej realizacja następuje tylko w dni robocze w godzinach działania platformy.

W pozostałym czasie automat nie monitoruje kursu i nie przyjmuje oferty oraz nie wykonuje zleceń.

[Wróć](#)[Zaplanuj](#)

W przypadku potwierdzenia oferty transakcji przez użycie przycisku **Zaplanuj**, platforma będzie monitorowała zmiany kursu rynkowego (uwzględniającego marżę dla Klienta odpowiednią dla danej kwoty transakcji).

W momencie, gdy warunki oferty zostaną spełnione:

- a) a na koncie będą odpowiednie środki do realizacji, Bank przyjmuje ofertę i transakcja jest zawarta oraz automatycznie rozliczana poprzez ustanowione rachunki bankowe. **Transakcja jest zawarta nieodwołalnie.**
- b) a na koncie nie będzie dostatecznych środków do przeprowadzenia transakcji, Bank nie przyjmuje oferty, a zlecenie oferty zostaje automatycznie anulowane.

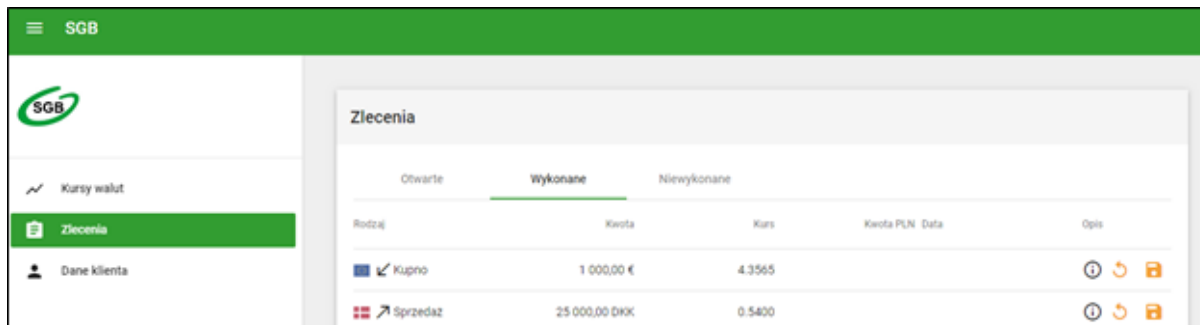
**Ważne!**

Transakcje zaplanowane w późniejszym terminie realizowane są tylko w dni robocze w godzinach działania platformy. Wyjątkiem jest sytuacja, gdy ze względu na warunki nadzwyczajne (np. awarie, wstrzymanie sesji związane z wyjątkowymi okolicznościami na rynkach finansowych) zawieranie wszystkich transakcji za pośrednictwem platformy internetowej SGB jest wstrzymane.

Do przeglądu złożonych ofert i ich ewentualnego wycofania z platformy służy funkcja **Zlecenia** opisana w Rozdziale 8.

## 8. Zlecenia

Platforma internetowa SGB w funkcji Zlecenia umożliwia sprawdzenie historii transakcji oraz przegląd aktualnie złożonych oraz niezrealizowanych ofert



Zlecenia						
Otwarte		Wykonane	Niewykonane			
Rodzaj	Kwota	Kurs	Kwota PLN	Data	Opis	
Kupno	1 000,00 €	4.3565				
Sprzedaż	25 000,00 DKK	0.5400				

Na ekranie znajdują się trzy grupy, pomiędzy którymi można przechodzić za pomocą zakładek u góry:

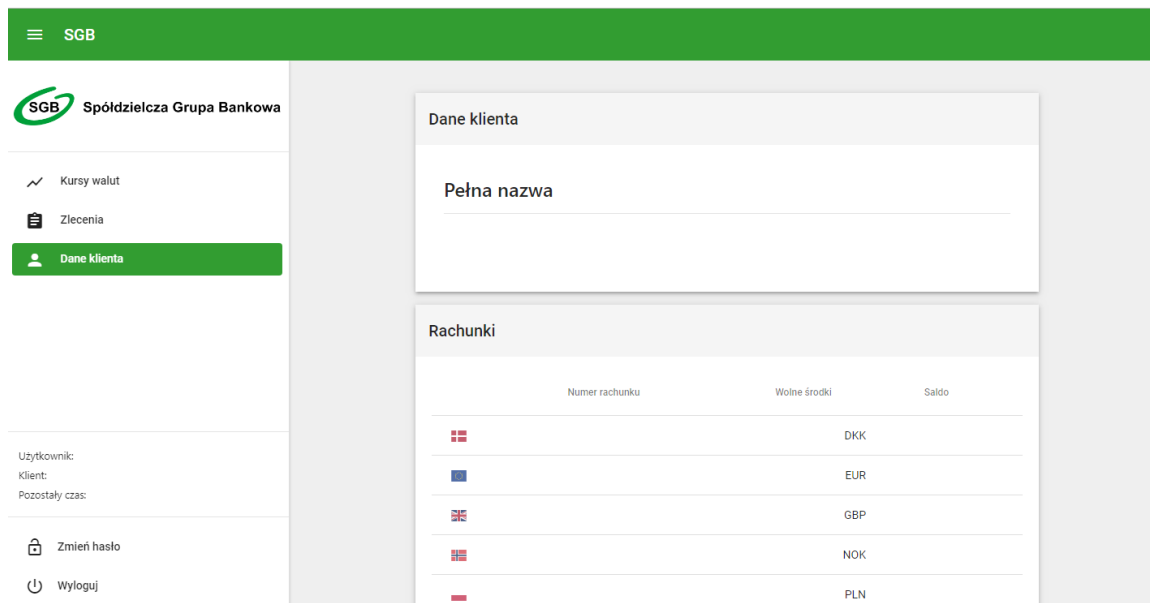
- **Otwarte** – niezrealizowane transakcje zaplanowane na późniejszy termin.
  - - najechnanie na ikonę powoduje wyświetlenie opisu oferty,
  - - kliknięcie powoduje usunięcie oferty (platforma prosi o potwierdzenie anulowania )
  - - kliknięcie umożliwi pobranie potwierdzenia złożenia oferty w formacie PDF
- **Wykonane** – wszystkie transakcje, które zostały wykonane w przeszłości:
  - - najechnanie na ikonę powoduje wyświetlenie opisu transakcji,
  - - kliknięcie umożliwi ponowne rozpoczęcie procesu zawarcia transakcji z taką samą stroną (kupno/sprzedaż) i liczbą jednostek waluty - nastąpi przejście do ekranu nowej transakcji walutowej z wypełnionymi danymi transakcji.
  - - kliknięcie umożliwi pobranie potwierdzenia transakcji w formacie PDF
- **Niewykonane** – niezrealizowane oferty, które zostały anulowane przez Klienta, lub które wygasły, czyli po osiągnięciu daty i godziny granicznej nie osiągnęły wprowadzonego kursu lub w momencie aktywacji Klient nie posiadał pokrycia w środkach na odpowiednim rachunku bankowym.

Wszystkie transakcje i oferty wyświetlane są chronologicznie.








## 9. Dane klienta

W funkcji Dane klienta na ekranie przedstawione są numery rachunków, na których rozliczane są transakcje walutowe zawarte za pośrednictwem platformy internetowej SGB.



The screenshot shows the SGB internet banking interface. At the top, there is a green header with the SGB logo and the text 'Spółdzielcza Grupa Bankowa'. Below the header, there is a navigation menu with options: 'Kursy walut', 'Zlecenia', and 'Dane klienta' (which is highlighted in green). On the left side, there is a user profile section with the text 'Użytkownik:', 'Klient:', and 'Pozostały czas:'. Below this, there are two options: 'Zmień hasło' and 'Wyloguj'. The main content area is divided into two sections: 'Dane klienta' and 'Rachunki'. The 'Dane klienta' section has a label 'Pełna nazwa' and a text input field. The 'Rachunki' section is a table with three columns: 'Numer rachunku', 'Wolne środki', and 'Saldo'. The table contains five rows, each representing a different currency: DKK, EUR, GBP, NOK, and PLN. Each row has a small flag icon next to the currency code.

Numer rachunku	Wolne środki	Saldo
		DKK
		EUR
		GBP
		NOK
		PLN

## 10. Zmiana hasła, wylogowanie

Platforma internetowa SGB wymaga zmiany hasła przy pierwszym logowaniu. W przypadku chęci późniejszej zmiany hasła, należy użyć przycisku „Zmień hasło” w dolnym lewym rogu ekranu. Po wciśnięciu pojawi się nowe okienko, gdzie należy wpisać obecne hasło oraz dwukrotnie nowe hasło. Nowe hasło powinno zawierać minimum 8 znaków, w tym przynajmniej 1 wielką literę, 1 małą literę i 1 cyfrę.

**Zmiana hasła**

Obecne hasło  

---

Proszę wpisać hasło

Nowe hasło  

---

Powtórz nowe hasło  

---

Po zakończeniu pracy należy się wylogować, korzystając z przycisku **Wyloguj** w dolnym lewym rogu ekranu.

## 11. Pozostałe informacje

Platforma internetowa SGB jest dostępna w dni robocze w godzinach 8:30-16:00 z zastrzeżeniem, że godziny funkcjonowania są dopasowane do możliwości rozliczeniowych Banku i mogą się zmienić w ramach komunikatu Banku.

W przypadku niemożności przeprowadzenia transakcji wymiany walut z przyczyn technicznych należy skontaktować się z Departamentem Skarbu SGB-Banku.

Kontakt do Departamentu Skarbu:

**(+48) 61 64 72 854**

W przypadku zapomnienia hasła, niepowodzenia zmiany hasła lub zablokowania dostępu należy skontaktować się z Infolinią pod numerem telefonu:

**800 888 888** (dla połączeń krajowych, bezpłatne połączenie)

**(+48) 61 647 28 46** dla połączeń komórkowych oraz z zagranicy (opłata za połączenie zgodna z taryfą danego operatora),

Telefony dostępne są przez całą dobę.