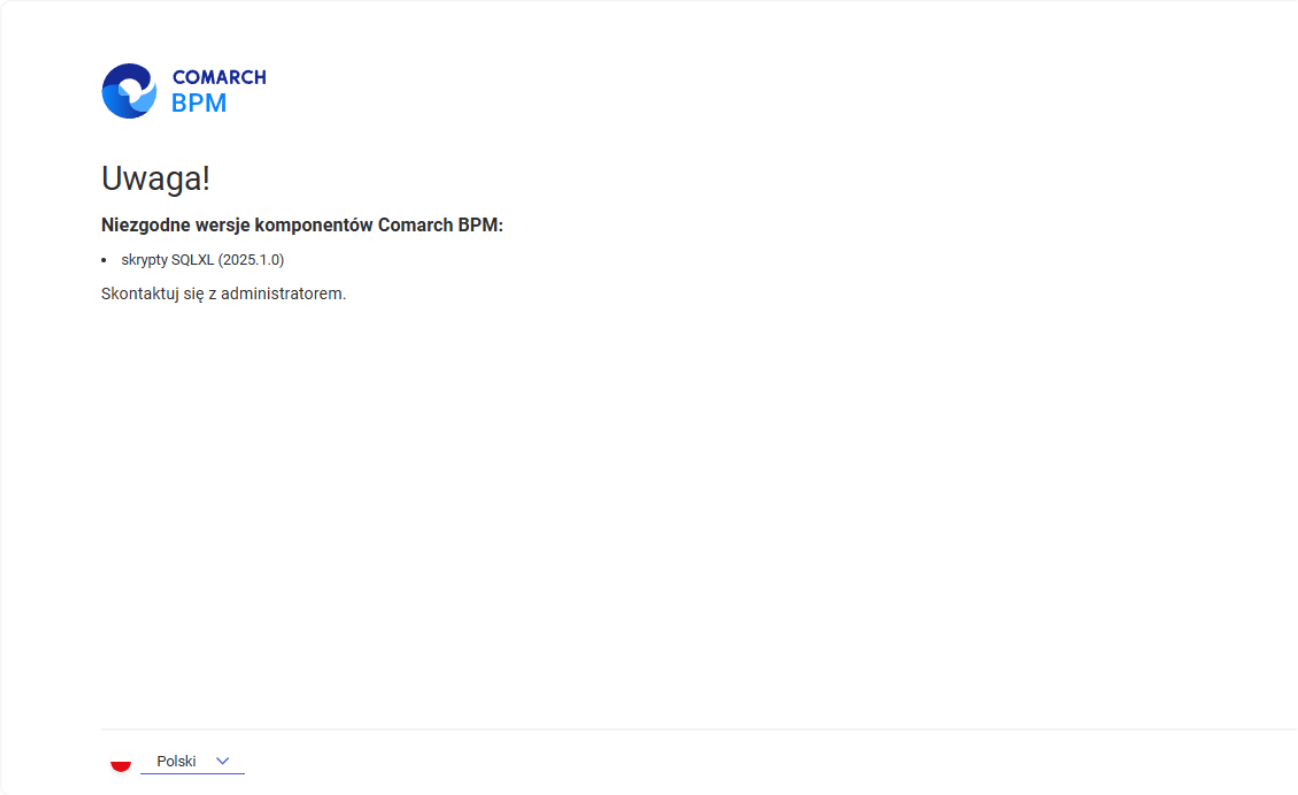
# Logowanie

W wersji 2025.0.0 dodano weryfikację skryptów na używanej bazie danych w przypadku próby przejścia do nowej aplikacji web Comarch BPM (dawniej DMS) – w przypadku wystąpienia niezgodności zostanie wyświetlony informujący o niej komunikat.

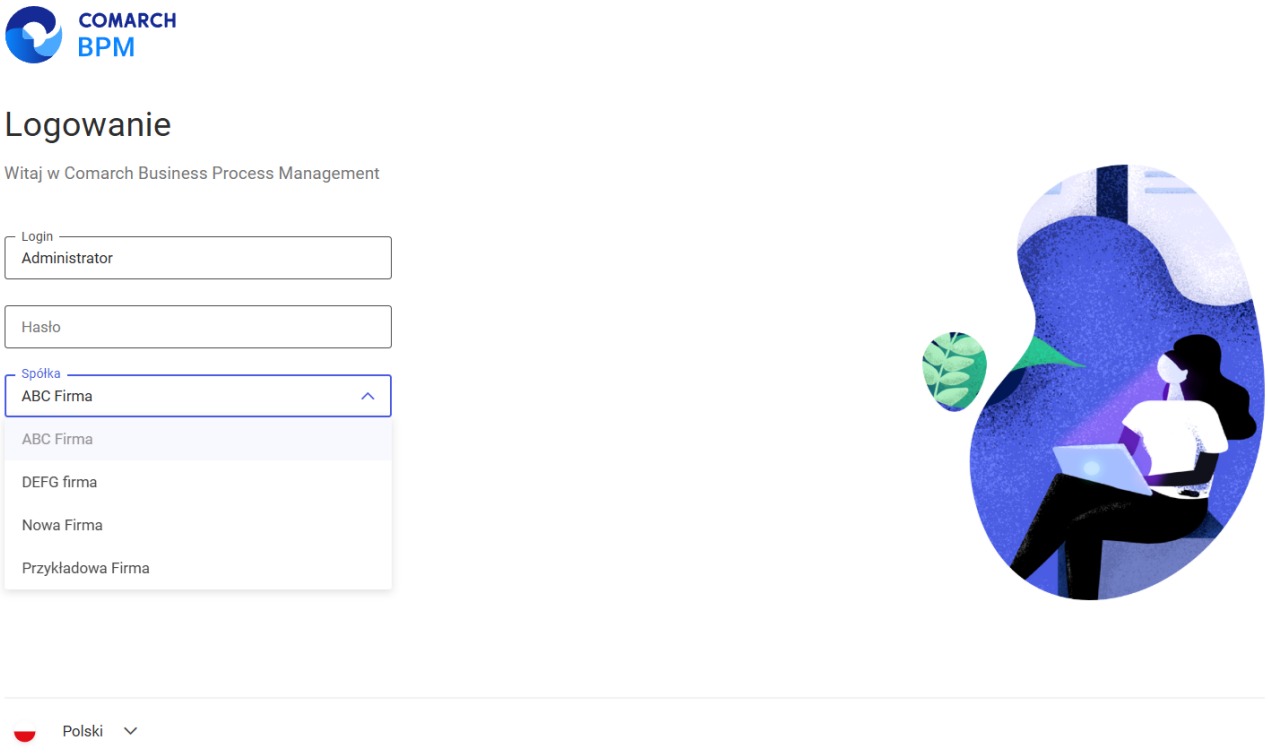



Przykładowy komunikat dotyczący niezgodności skryptów

Okno logowania zawiera **pola z nazwą operatora (login) oraz hasłem,** a także (od wersji 2024.1.1) **parametr „Zapamiętaj mnie”** oraz (od wersji 2025.0.0) **link „Nie pamiętasz hasła?”** (zob. Resetowanie hasła) . W przypadku trybu wielofirmowego prezentowane jest **dodatkowe pole z wyborem spółki**.

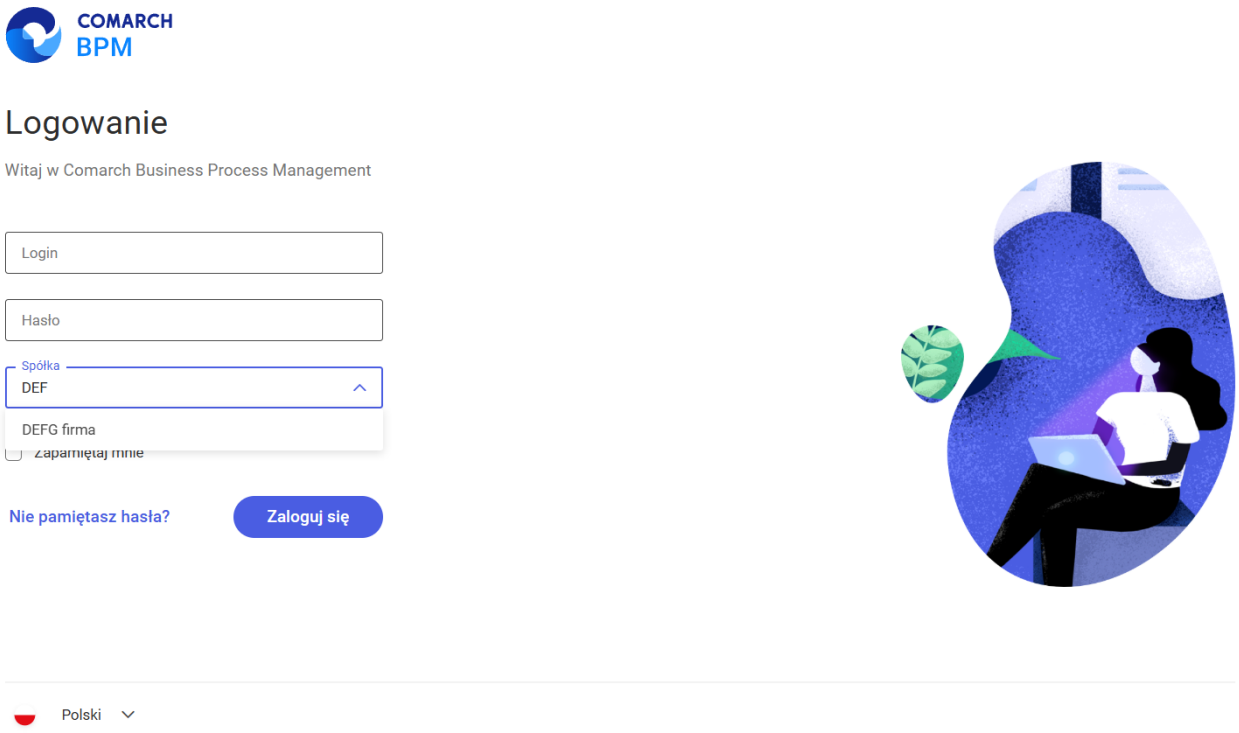
W wersji 2025.2.0 udostępniono opcję wymuszenia wprowadzenia ręcznie pełnej nazwy firmy w polu „Spółka” w oknie logowania. W tym celu w ramach pliku web.config w folderze z plikami aplikacji serwerowej Comarch BPM wprowadzono następujące zmiany:

- Usunięto parametr CompanyNameSearchModeEnabled;
- Wprowadzono parametr CompanySelectionMode, który może przyjąć następujące wartości:
  - List – wartość domyślna, ustawiana przez instalator podczas instalacji Comarch BPM – jeśli wprowadzono tę wartość, wówczas operator może wybrać spółkę z listy dostępnych spółek w oknie logowania;




Okno logowania, gdy w ramach parametru CompanySelectionMode wprowadzono wartość „List” (aplikacja web)

- Search – jeśli wprowadzono tę wartość, wówczas operator może wyszukać nazwę spółki wraz z sugerowaną nazwą spółki, która zawiera wpisaną frazę, na liście dostępnych spółek w oknie logowania. Jeśli lista nie zawiera danej frazy, wówczas nie zostanie wyświetlona (aplikacja desktop i aplikacja web) lub zostanie wyświetlona pusta lista (aplikacje mobilne);

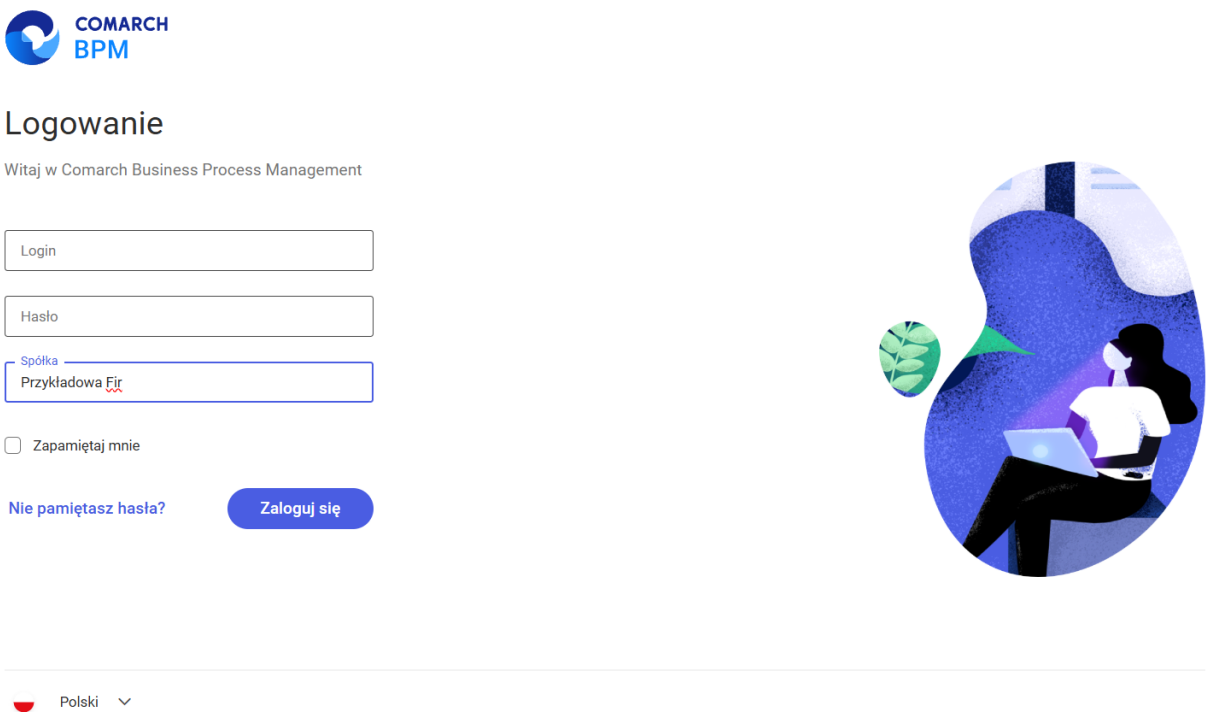



Okno logowania, gdy w ramach parametru CompanySelectionMode wprowadzono wartość „Search” (aplikacja web)

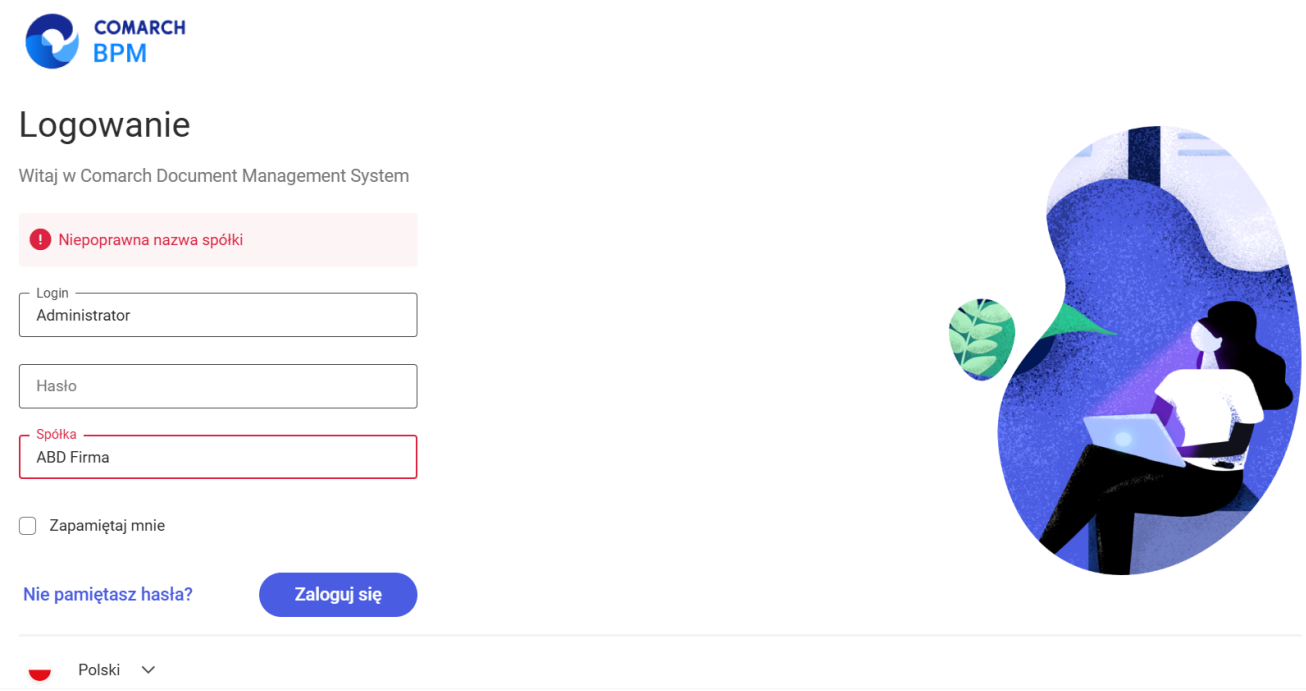
- Text – jeśli wprowadzono tę wartość, wówczas operator powinien wprowadzić nazwę spółki ręcznie w polu „Spółka” w oknie logowania. W przypadku, jeśli operator:
  - Wpisze poprawną nazwę spółki – zostanie zalogowany do aplikacji Comarch BPM. Jeśli

zostaną wprowadzone dodatkowe białe znaki (spacje) przed albo po nazwie spółki, wówczas zostanie uwzględniona nazwa bez spacji. W ramach pola można wprowadzić maksymalnie 100 dowolnych znaków;

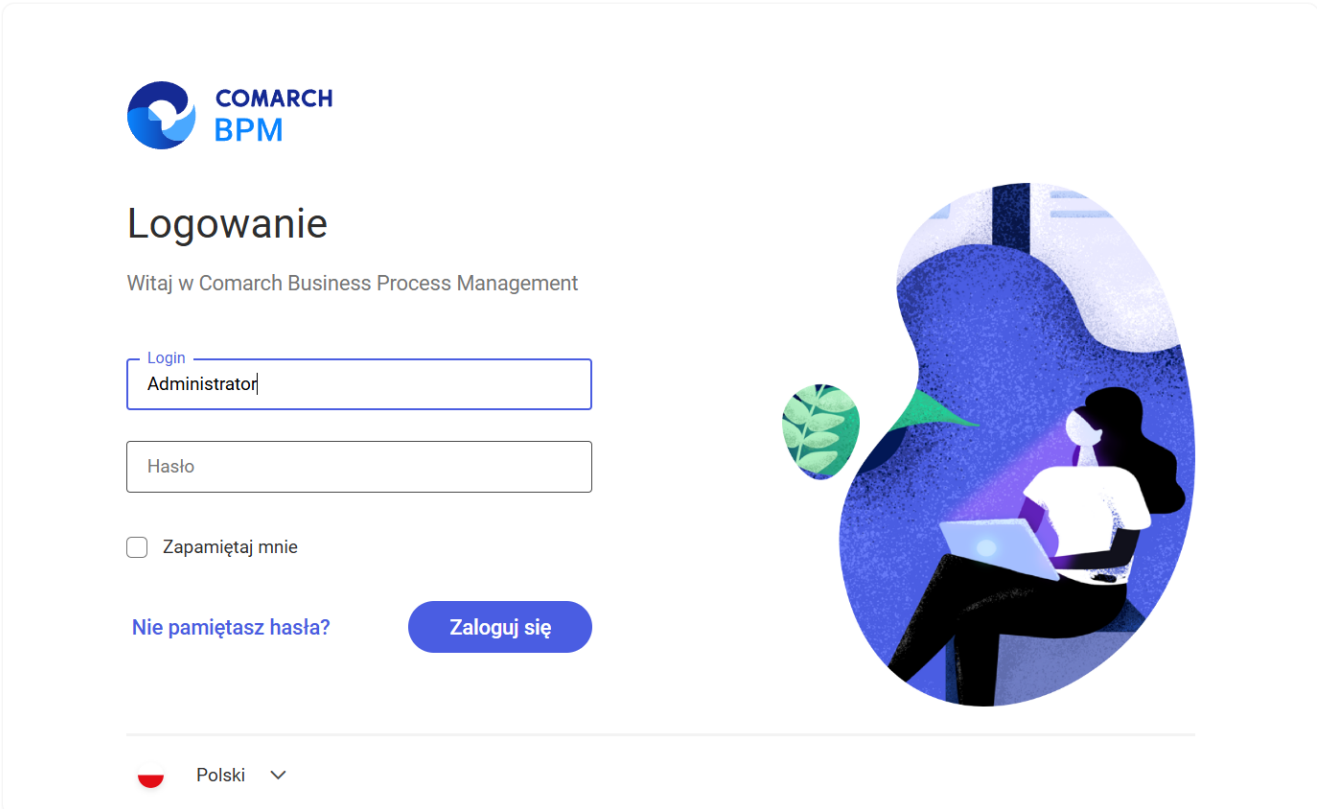
- Wpisze niepoprawną nazwę spółki lub nie uzupełni pola w aplikacji desktop – wówczas zostaną wyświetlone komunikaty – odpowiednio: „Pole spółka jest wymagane” i „Niepoprawna nazwa spółki”.
- Wpisze niepoprawną nazwę spółki w aplikacji web – w takim przypadku zostanie wyświetlony komunikat „Niepoprawna nazwa spółki”, a pole „Spółka” zostanie zaznaczone na czerwono
- Wpisze niepoprawną nazwę spółki w aplikacji mobilnej na system Android – w takim przypadku zostanie wyświetlony komunikat „Błąd logowania. Niepoprawna nazwa spółki”



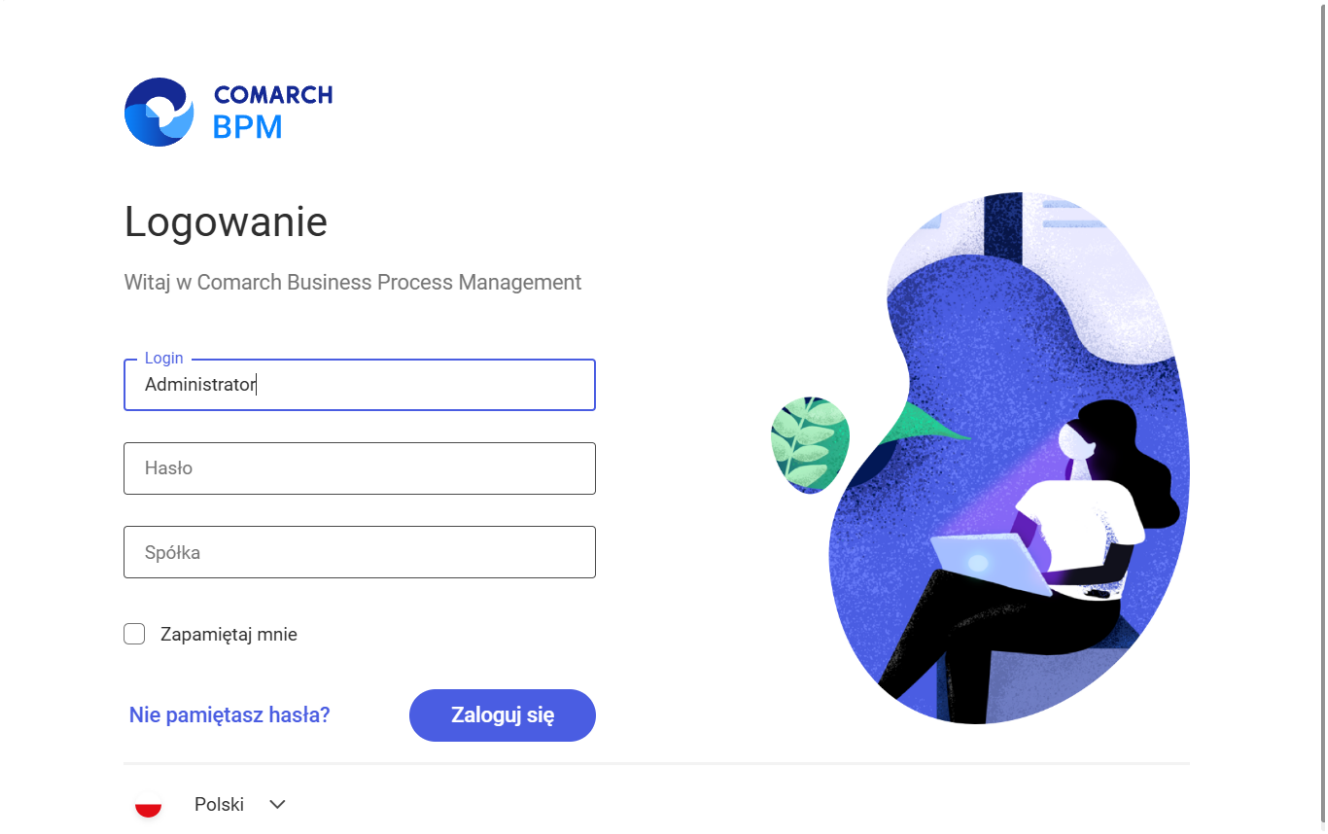

Okno logowania, gdy w ramach parametru CompanySelectionMode wprowadzono wartość „Text” (aplikacja web)




Komunikat wyświetlony, gdy parametr CompanySelectionMode ma wartość Text, a operator wpisał niepoprawną nazwę spółki w polu „Spółka” (aplikacja web)



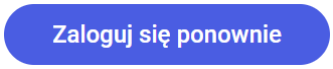

Okno logowania, tryb jednofirmowy w nowej aplikacji web Comarch BPM (dawniej DMS)




Okno logowania, tryb wielofirmowy w nowej aplikacji web Comarch BPM (dawniej DMS)

**W danym momencie operator może pracować tylko z jedną wersją (stacjonarną, WWW lub mobilną) aplikacji Comarch BPM (dawniej DMS).**

Podczas logowania, aplikacja weryfikuje czy operator nie jest już zalogowany do innej wersji aplikacji. Jeżeli weryfikacja wykaże, że **obecnie operator zalogowany jest do innej wersji**, wyświetlone zostanie okno z pytaniem dotyczącym automatycznego wylogowania.

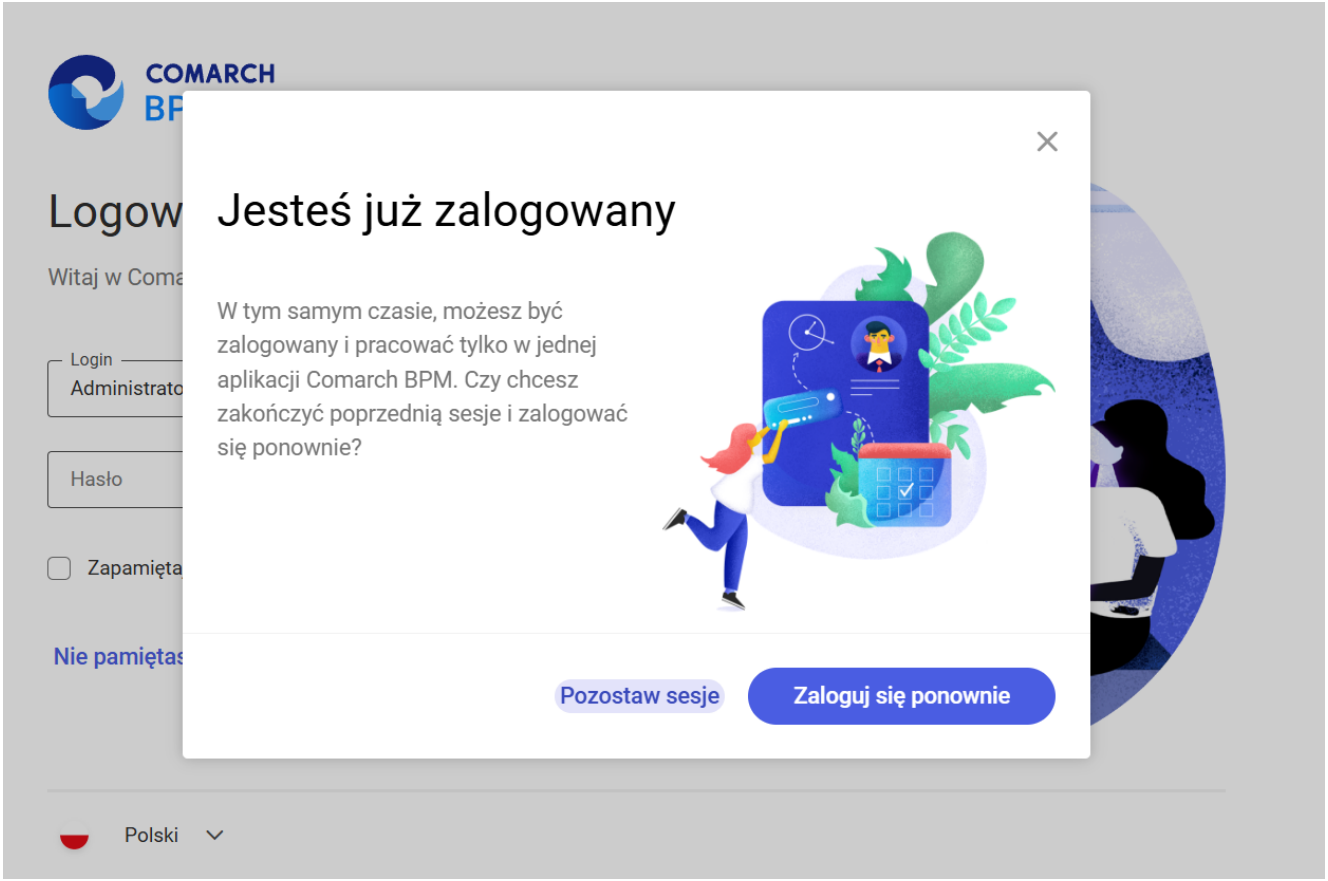
Wybór przycisku 

**[Zaloguj się ponownie]** spowoduje **wylogowanie operatora z dotychczasowej wersji aplikacji i umożliwi zalogowanie do nowej**.

Jeśli użytkownik wybierze przycisk

**[Pozostaw**

**sesje]**, wówczas **operator pozostanie zalogowany na dotychczasowej wersji aplikacji**.

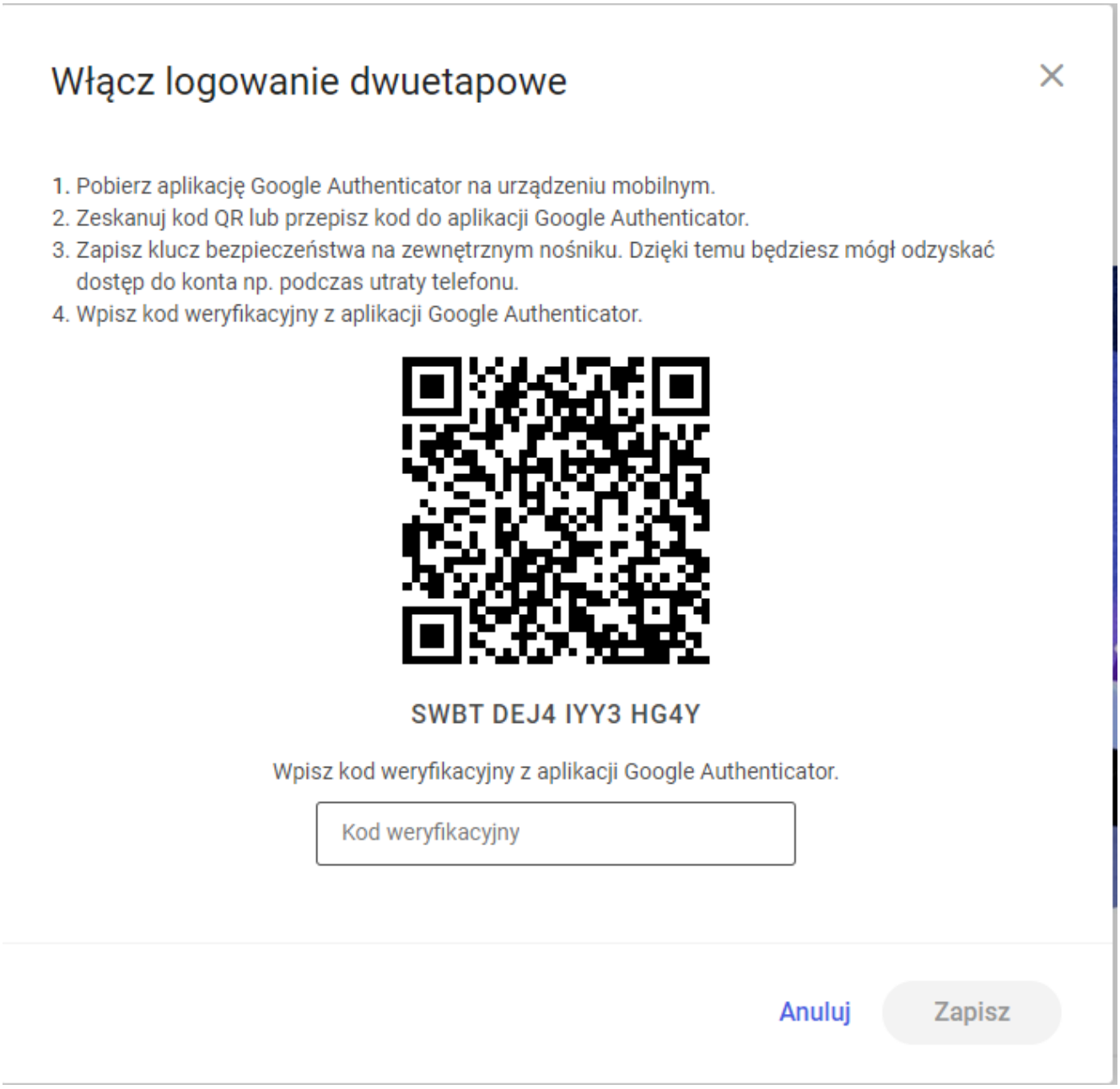



Okno podczas logowania do aplikacji webowej, jeśli dany operator jest już zalogowany do aplikacji

W wersji 2024.3.0 wprowadzono funkcjonalność uwierzytelnienia dwustopniowego. Uwierzytelnienie dwustopniowe może być:

- Obowiązkowe – jeśli zostało włączone przez administratora dla wszystkich użytkowników (zob. Narzędzia)
- Dobrowolne – jeśli zostało ustawione przez danego operatora z jego własnej woli (zob. Konfiguracja lub Preferencje)

Jeżeli administrator włączył obowiązkowe logowanie dwustopniowe dla wszystkich użytkowników, a dany operator nie ustawił wcześniej logowania dwustopniowego, wówczas musi je skonfigurować podczas kolejnego logowania – po wprowadzeniu loginu i hasła i kliknięciu „Zaloguj się” zostaje otwarte okno „Włącz logowanie dwuetapowe”.




Okno „Włącz logowanie dwuetapowe” wyświetlone przy logowaniu do nowej aplikacji web Comarch BPM (dawniej DMS) w przypadku,

jeśli administrator włączył wymuszenie logowania dwuetapowego, a dany operator nie miał go uruchomionego

Następnie operator musi kolejno wykonać następujące czynności:

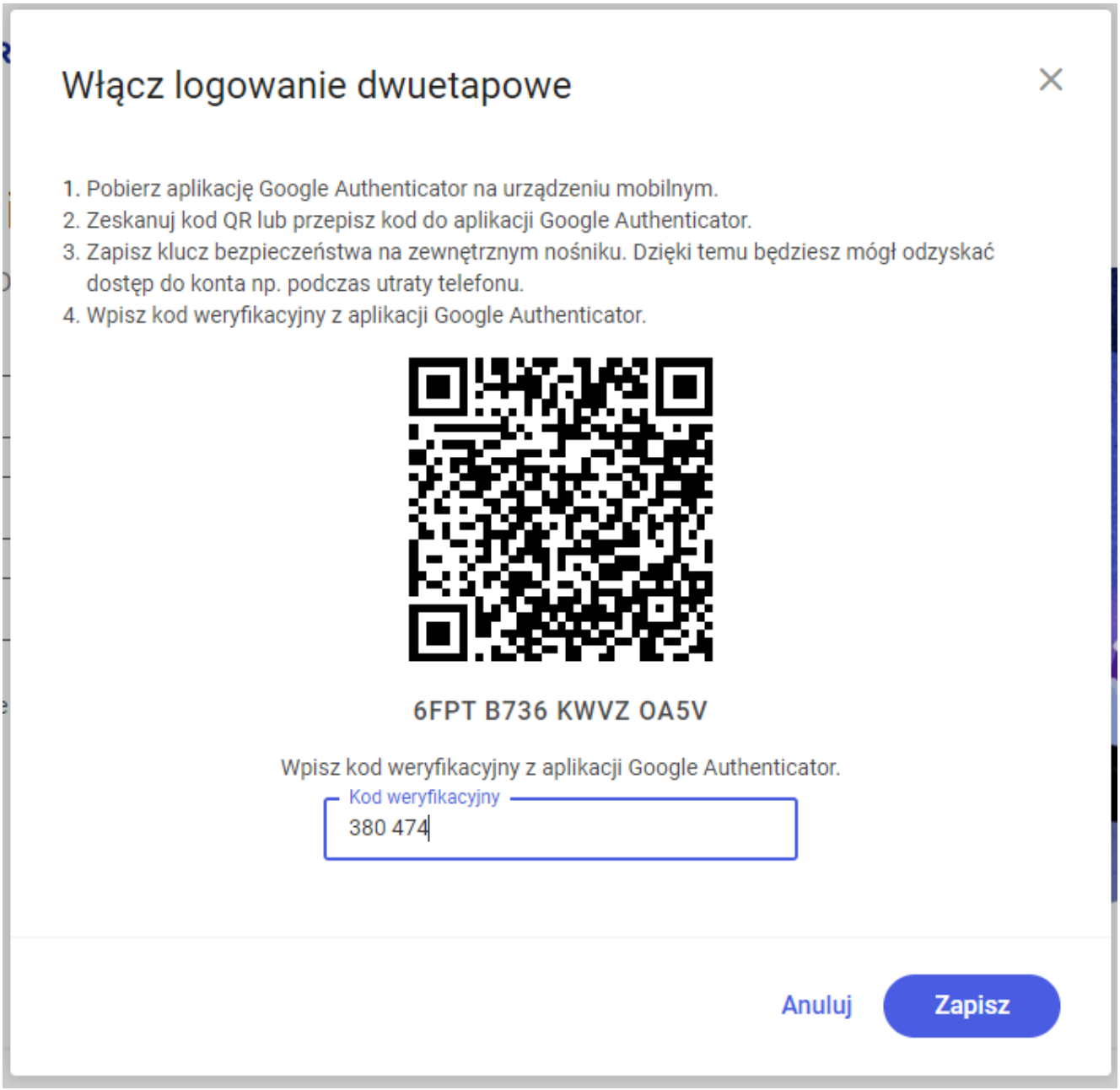
- Pobrać aplikację Google Authenticator na urządzeniu mobilnym
- Otworzyć aplikację Google Authenticator
- W aplikacji Google Authenticator kliknąć w przycisk „Dodaj kod”
- Wybrać jedną z następujących możliwych ścieżek postępowania:
    - kliknąć w opcję „Zeskanuj kod QR” w aplikacji Google Authenticator i zeskanować kod QR widoczny w oknie „Włącz logowanie dwuetapowe” w aplikacji Comarch BPM (dawniej DMS)

lub

    - kliknąć w opcję „Wpisz klucz konfiguracyjny” w aplikacji Google Authenticator, a następnie w polu „Nazwa konta” wprowadzić nazwę, pod jaką będzie widoczne konto w aplikacji Google Authenticator, a w polu „Twój klucz bezpieczeństwa” wpisać 16-cyfrowy kod dostępny w ramach pola „Klucz bezpieczeństwa” w oknie „Włącz logowanie dwuetapowe” w Comarch BPM (dawniej DMS) (widoczny poniżej kodu QR). Po wprowadzeniu wartości należy nacisnąć przycisk „Dodaj” w aplikacji Google Authenticator
- Zapisać kod z pola „Klucz bezpieczeństwa” na nośniku zewnętrznym – umożliwi to dostęp do konta w przypadku utraty lub usterki urządzenia mobilnego
- W polu „Wpisz kod weryfikacyjny z aplikacji Google Authenticator” dostępnym w oknie „Włącz logowanie dwuetapowe” w Comarch BPM (dawniej DMS) wpisać 6-cyfrowy

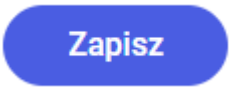
kod weryfikacyjny wyświetlany w aplikacji Google Authenticator, zanim upłynie jego ważność, oznaczona zanikającym niebieskim kołem (kod jest ważny 60 sekund) – jeśli dany kod wygasł, w Comarch BPM (dawniej DMS) należy wpisać kolejny wygenerowany kod

- Kliknąć przycisk Zapisz **[Zapisz]**.



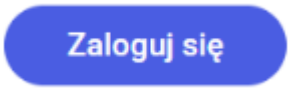

Okno „Włącz logowanie dwuetapowe” – wprowadzanie kodu w polu

„Wpisz kod weryfikacyjny z aplikacji Google Authenticator”

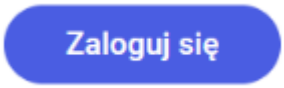



Po kliknięciu przycisku **[Zapisz]** operator zostanie zalogowany do nowej aplikacji web Comarch BPM (dawniej DMS) .

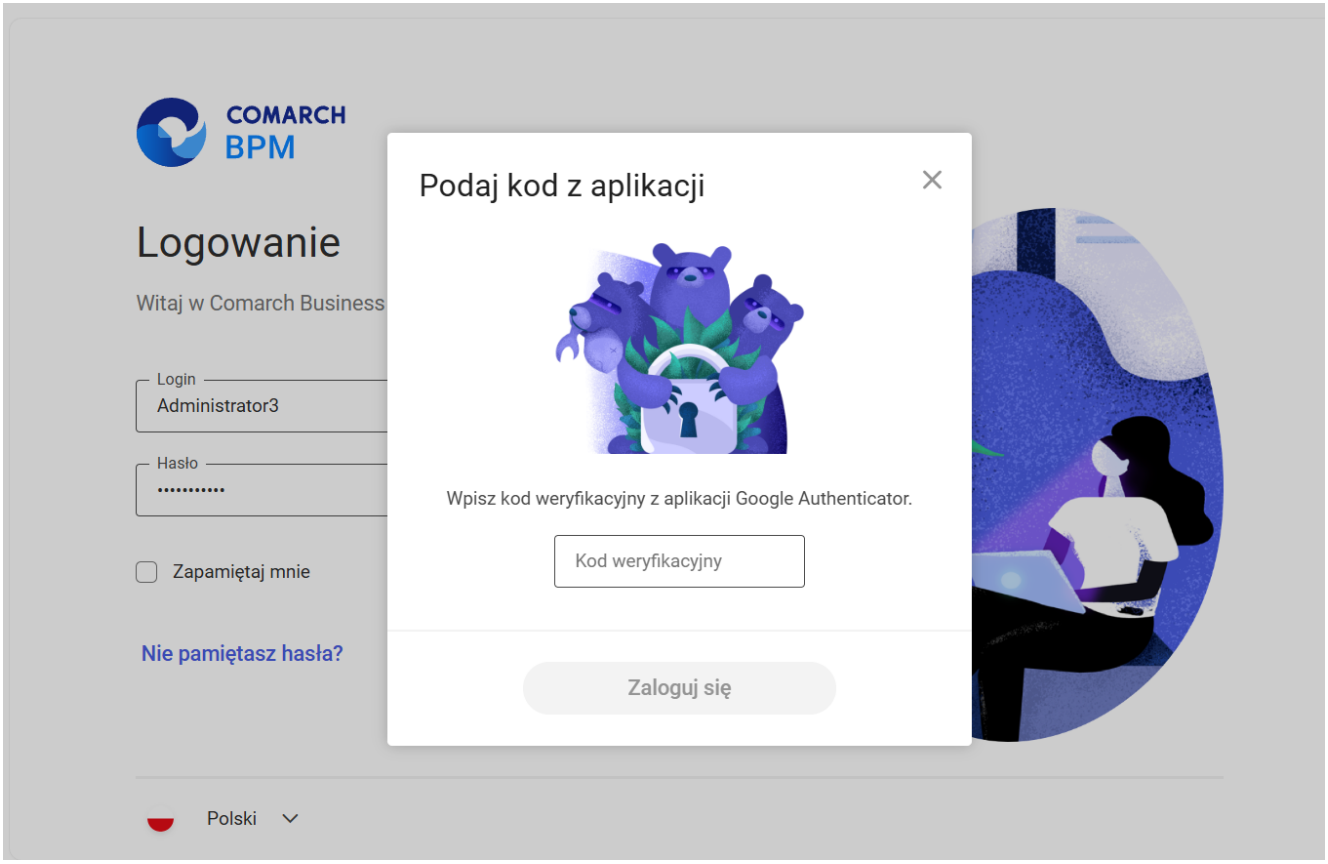
Jeżeli operator ma już włączoną weryfikację dwuetapową, wówczas przy kolejnym otwarciu okna logowania do aplikacji desktop i wprowadzeniu loginu i hasła, a następnie kliknięciu



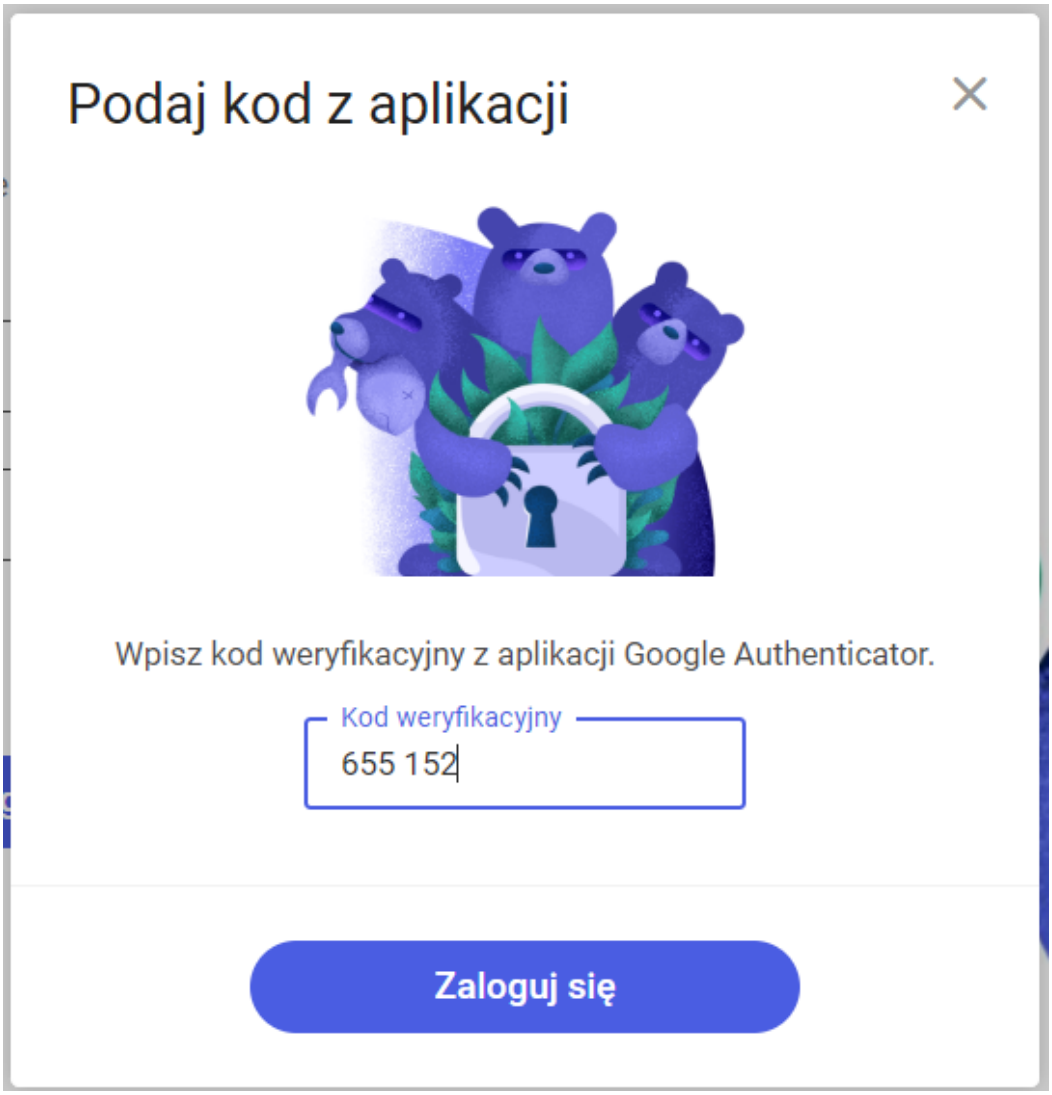

w przycisk **[Zaloguj się]** zostaje wyświetlone okno „Podaj kod z aplikacji”. W ramach tego okna należy wprowadzić 6-cyfrowy kod weryfikacyjny wyświetlany w aplikacji Google Authenticator (zanim upłynie jego ważność, oznaczona zanikającym niebieskim kołem (kod jest ważny 60 sekund) – jeśli dany kod wygasł, w oknie „Podaj kod z aplikacji” należy wpisać kolejny wygenerowany kod. Następnie operator powinien



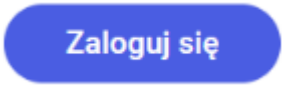

kliknąć w przycisk **[Zaloguj się]** dostępny w ramach okna „Podaj kod z aplikacji”.




Okno logowania do nowej aplikacji web Comarch BPM (dawniej DMS) z oknem „Podaj kod z aplikacji”




Okno „Podaj kod z aplikacji” w nowej aplikacji web Comarch BPM (dawniej DMS) – wprowadzanie kodu w polu „Wpisz kod weryfikacyjny z aplikacji Google Authenticator”

Po wprowadzeniu prawidłowego kodu weryfikacyjnego i naciśnięciu przycisku 

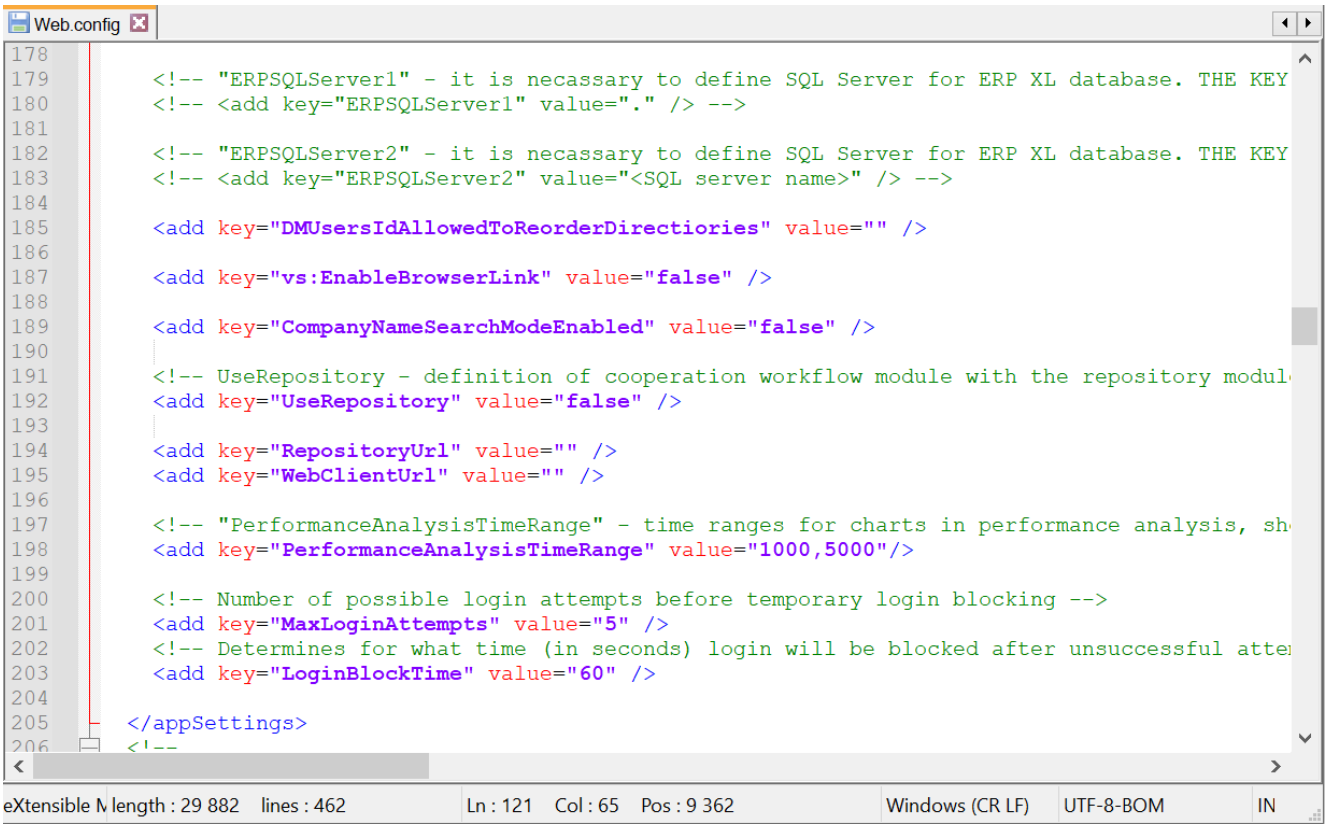
**[Zaloguj się]** okno logowania i okno „Podaj kod z aplikacji” zostają zamknięte, a otwiera się nowa aplikacja web Comarch BPM (dawniej DMS).

W wersji 2024.1.1 wprowadzono możliwość **zablokowania logowania** po określonej liczbie prób logowania na wybrany okres czasu.

W tym celu w pliku **Web.config** znajdującym się w katalogu z

plikami aplikacji serwerowej (dawna web) wprowadzono dwa nowe klucze:

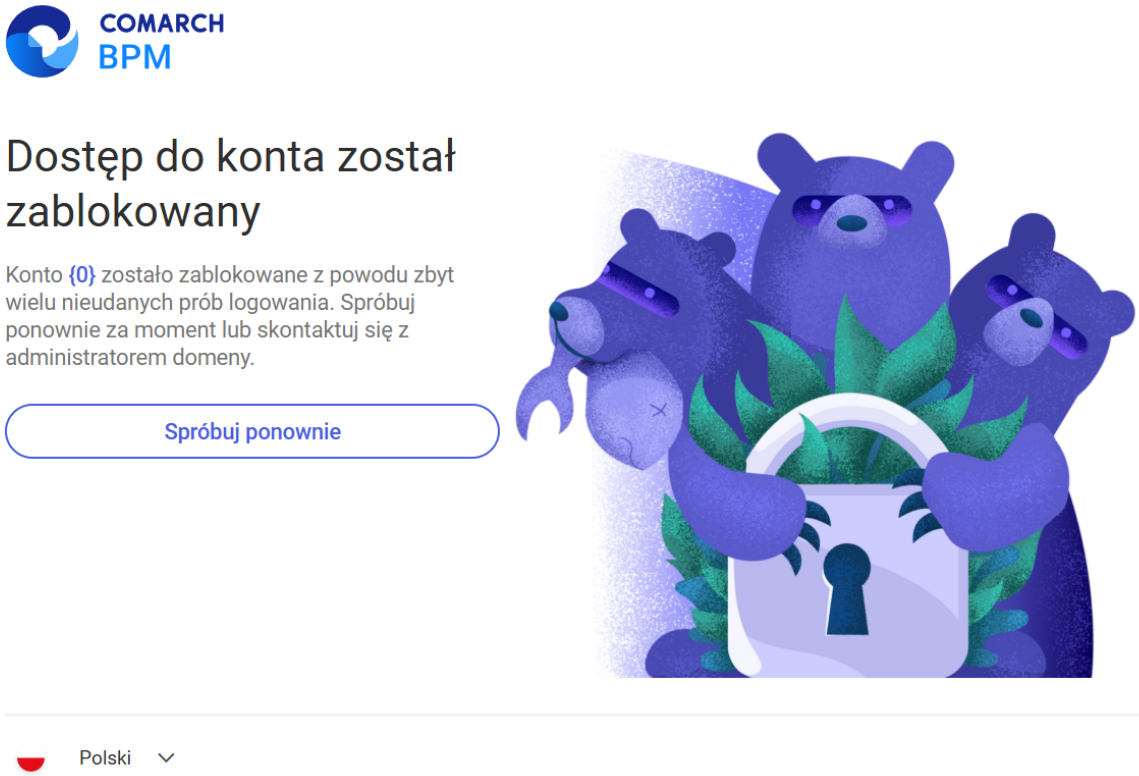
- **<add key='MaxLoginAttempts' value="5"/>** – w ramach tego klucza należy podać, jaka ma być maksymalna liczba prób logowania dla operatora zanim nastąpi zablokowanie logowania – domyślna wartość to 5
- **<add key='LoginBlockTime' value="60"/>** – w ramach tego klucza należy podać, po jakim czasie (liczonym w sekundach) operator będzie mógł podjąć kolejną próbę logowania, po tym, jak logowanie zostało zablokowane – domyślna wartość to 60.



Plik Web.config z nowymi kluczami MaxLoginAttempts i LoginBlockTime

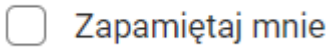
**Jeśli operator próbował zalogować się do nowej aplikacji web Comarch BPM (dawniej DMS) za pomocą błędnego loginu i/lub hasła, a liczba prób przekroczyła wartość wprowadzoną w ramach**

**klucza <add key='MaxLoginAttempts' value="5"/>**, wówczas powyżej pola „Login" zostanie wyświetlone okno z informacją *Konto zostało zablokowane z powodu zbyt wielu nieudanych prób logowania. Spróbuj ponownie za moment lub skontaktuj się z administratorem domeny.* Wówczas operator musi poczekać, aż upłynie czas określony w ramach klucza <add key='LoginBlockTime' value="60"/>, aby podjąć kolejną próbę **logowania**.




Okno logowania do nowej aplikacji web Comarch BPM (dawniej DMS)– jeśli operator próbował logować się za pomocą błędnych danych zbyt wiele razy

W wersji 2024.1.1 na stronie logowania do nowej aplikacji web Comarch BPM (dawniej DMS) dodano również **parametr**




**[Zapamiętaj mnie]**. Parametr znajduje się pod polem „Hasło” (w trybie jednofirmowym) lub pod polem „Spółka” (w trybie wielofirmowym).

**Po zaznaczeniu parametru operator jest zalogowany w Comarch BPM (dawniej DMS) aż do momentu, kiedy naciśnie**

**[Wyloguj się]**. Gdy zalogowany operator zamknie okno Comarch BPM (dawniej DMS) za pomocą przycisku lub

, wówczas przy ponownym uruchomieniu aplikacji **nie jest konieczne** wpisywanie loginu i hasła, logowanie przebiega automatycznie.

Rozpoczynasz pracę z Comarch BPM (dawniej DMS) i chcesz dowiedzieć się, jak korzystać z programu? A może masz już podstawową wiedzę o Comarch BPM (dawniej DMS) i chcesz dowiedzieć się więcej?

Sprawdź Szkolenia Comarch BPM!

Powrót do początku artykułu