**Instrukcja użytkownika CST2021**

**Aplikacja System Zarządzania Tożsamością (SZT2021)**

****Spis treści****

[1. Wstęp 4](#_Toc209702737)

[2. Zmiana języka aplikacji przez niezalogowanego użytkownika 6](#_Toc209702738)

[3. Rejestracja konta 7](#_Toc209702739)

[3.1 Rejestracja konta przez niezalogowanego użytkownika 7](#_Toc209702740)

[3.2 Określenie hasła 11](#_Toc209702741)

[4. Logowanie 12](#_Toc209702742)

[4.1 Logowanie przy włączonym uwierzytelnianiu dwuetapowym – wprowadzenie 18](#_Toc209702743)

[4.2 Logowanie za pomocą kodu 19](#_Toc209702744)

[4.3 Logowanie za pomocą powiadomienia 22](#_Toc209702745)

[5. Akceptacja Regulaminu 25](#_Toc209702746)

[6. Przedłużanie sesji 26](#_Toc209702747)

[7. Wylogowanie z aplikacji 27](#_Toc209702748)

[8. Przypomnienie hasła 30](#_Toc209702749)

[9. Edycja własnych danych oraz zmiana hasła 33](#_Toc209702750)

[10. Zarządzanie ustawieniami uwierzytelniania dwuetapowego (2FA) 37](#_Toc209702751)

[10.1 Konfiguracja kodu 41](#_Toc209702752)

[10.2 Konfiguracja powiadomienia 46](#_Toc209702753)

[10.3 Kod zapasowy 51](#_Toc209702754)

[10.4 Zmiana nazwy konta w aplikacji uwierzytelniającej 53](#_Toc209702755)

[10.5 Wyłączanie i resetowanie uwierzytelniania dwuetapowego (2FA) 54](#_Toc209702756)

[11. Wybór kontekstu pracy 55](#_Toc209702757)

[12. Komunikaty informacyjne 58](#_Toc209702758)

[13. Responsywność i dostępność 59](#_Toc209702759)

# Wstęp

W tej instrukcji przeczytasz o pierwszych stronach systemu CST2021, na których możesz między innymi:

- zarejestrować się,

- zalogować i wylogować,

- odzyskać zapomniane hasło,

- zapoznać się z regulaminem systemu,

- oglądać i edytować dane swojego konta,

- przechodzić pomiędzy poszczególnymi aplikacjami bez konieczności ponownego potwierdzania tożsamości,

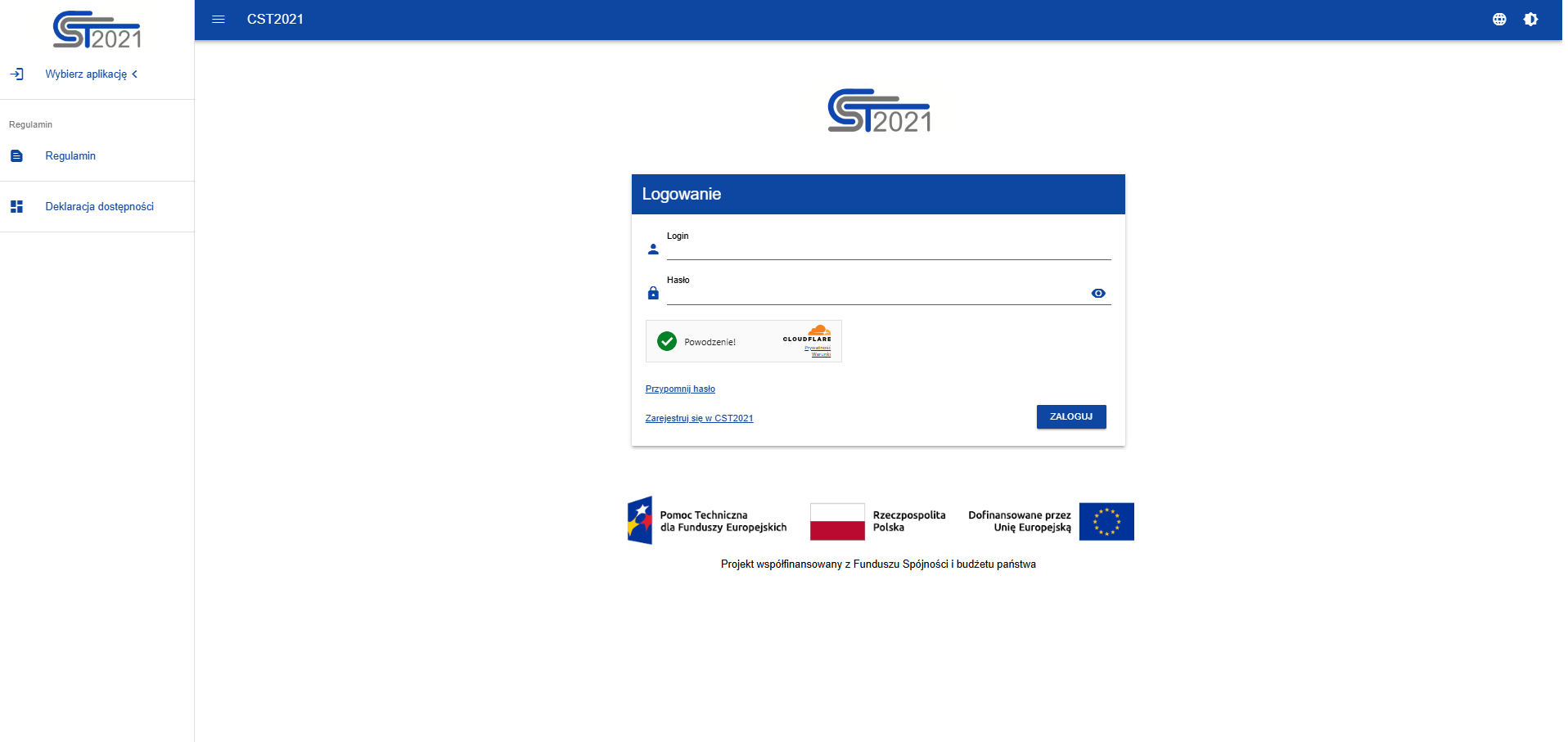
- zmieniać kontekst pracy, czyli organizację, w ramach której będziesz pracować na tym samym koncie użytkownika.

Te pierwsze strony systemu CST2021 to aplikacja SZT2021. Aby móc w pełni korzystać ze wszystkich funkcjonalności systemu, powinieneś pracować w aktualnej wersji jednej z przeglądarek: Mozilla Firefox, Google Chrome, Microsoft Edge.

Na stronie startowej **cst2021.gov.pl** znajduje się przede wszystkim formularz logowania wraz z linkami do rejestracji nowego konta oraz przypomnienia hasła. Zastosowaliśmy zabezpieczenie Cloudflare Turnstile, które ma na celu ochronę systemu przed nadużyciami ze strony botów. Rozwiązanie to przeprowadza test, czy wchodzący na stronę nie jest botem. Na formularzu widać widżet prezentujący status testu.



Test zwykle kończy się automatycznym sukcesem, jednak czasem możesz zostać poproszony o potwierdzenie poprzez zaznaczenie jednego dodatkowego pola. Kiedy zobaczysz komunikat „Powodzenie”, możesz dokonać logowania, rejestracji konta lub przypomnienia hasła.



W menu bocznym możesz wybrać linki *Regulamin* oraz *Deklaracja dostępności*. Znajdziesz tam informacje o systemie dostępne dla każdego użytkownika. W prawym górnym rogu ekranu masz możliwość zmiany języka oraz ustawienia odpowiedniego kontrastu.

# Zmiana języka aplikacji przez niezalogowanego użytkownika

Treści na stronach aplikacji SZT dostępne dla niezalogowanego użytkownika domyślnie wyświetlane są w języku wskazanym w ustawieniach przeglądarki użytkownika. Masz jednak możliwość zmiany wersji językowej aplikacji na jedną z dostępnych (polska, angielska, niemiecka, słowacka). W tym celu kliknij ikonę *Język* w prawym górnym rogu ekranu oraz wybierz pożądany język.



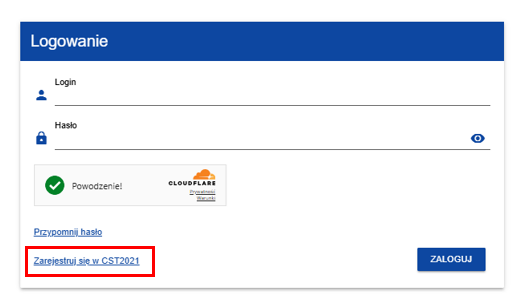
Bezpośrednio po wskazaniu języka wyświetlane treści zostają dostosowane do wybranej wersji językowej.

# Rejestracja konta

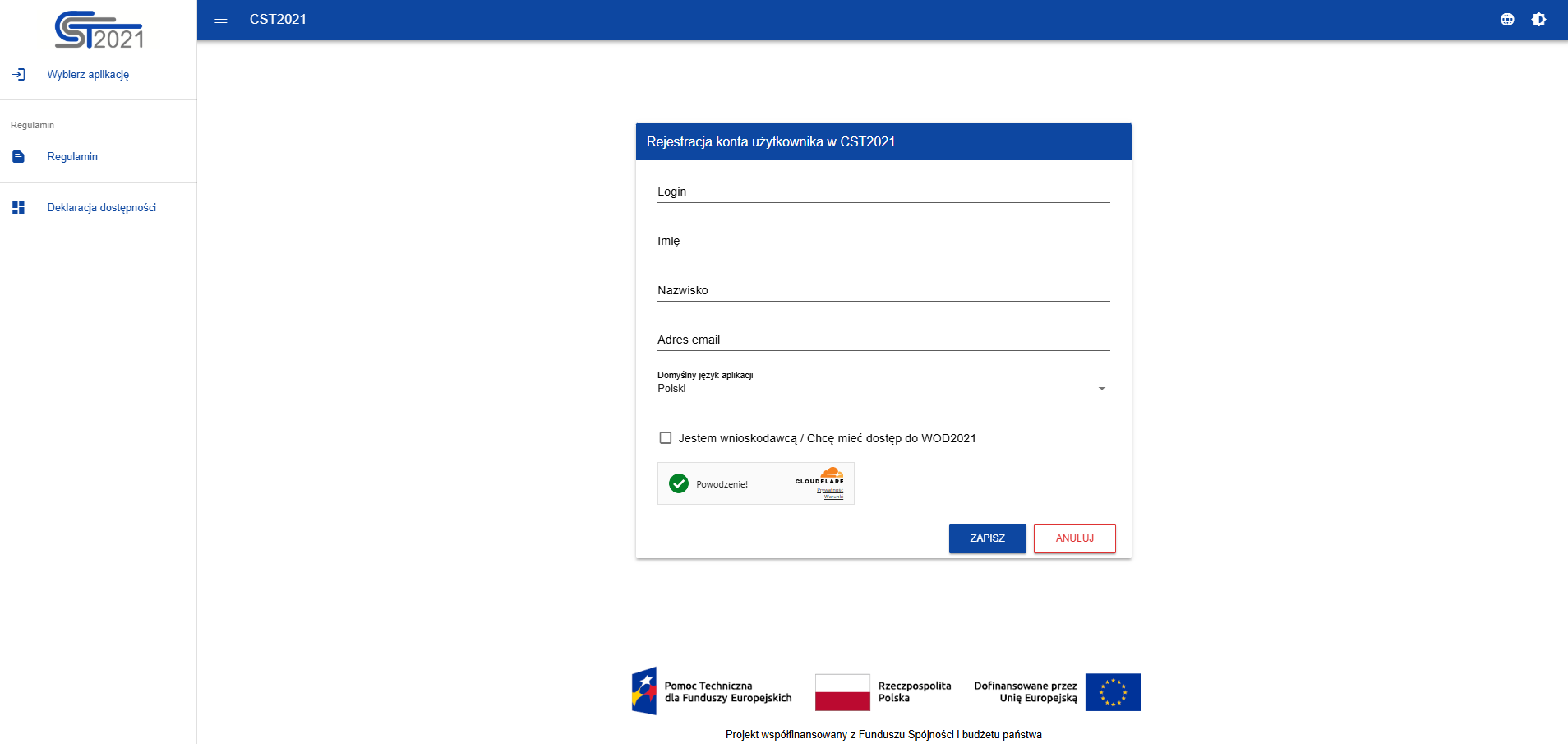
W aplikacji Administracja mogą pracować tylko zarejestrowani i zalogowani użytkownicy. Możesz sam zarejestrować swoje konto lub może zrobić to za Ciebie uprawniony Administrator.

### Rejestracja konta przez niezalogowanego użytkownika

Wybierz na stronie startowej SZT link *Zarejestruj się,* aby utworzyć konto



Aplikacja wyświetli okno rejestracji użytkownika.



Okno *Rejestracja konta użytkownika* składa się z sześciu pól:

* login,
* imię – pole może zawierać jedynie litery z alfabetu łacińskiego, w tym diakrytyczne oraz inne litery charakterystyczne dla różnych języków. Dozwolone są również znaki specjalne takie jak spacja ( ), apostrof (‘), myślnik (–) oraz kropka (.). Imię musi składać się co najmniej z 2 znaków i może zawierać maksymalnie 30 znaków.
* nazwisko – pole może zawierać jedynie litery z alfabetu łacińskiego, w tym te z diaktrykami oraz inne litery charakterystyczne dla różnych języków. Dozwolone są również znaki specjalne takie jak spacja ( ), apostrof (‘), myślnik (–) oraz kropka (.). Nazwisko musi składać się co najmniej z 2 znaków i może zawierać maksymalnie 30 znaków.
* adres email, na który system będzie wysyłał wiadomości pozwalające np. na ustawienie hasła. Każdy użytkownik musi posiadać inny adres email;
* domyślny język aplikacji – pole typu lista, w którym możesz wskazać język, w jakim domyślnie wyświetlane będą Tobie elementy interfejsu użytkownika (komunikaty, walidacje, etykiety pól, nazwy przycisków) w aplikacjach SZT oraz WOD2021 (po zalogowaniu do aplikacji). W tym języku wysyłane będą również wszelkie wiadomości mailowe z aplikacji. Domyślny język będziesz mógł zmienić w dowolnym momencie po utworzeniu konta edytując dane swojego konta w aplikacji SZT. Domyślnie wybranym językiem w tym polu jest polski;
* checkbox „Jestem wnioskodawcą / Chcę mieć dostęp do WOD2021.” - zaznaczenie spowoduje, że konto użytkownika zostanie zarejestrowane zarówno w WOD2021 jak i SZT – analogicznie jak po skorzystaniu z funkcji *Utwórz konto w WOD2021* dostępnej w menu użytkownika na stronie <https://wod.cst2021.gov.pl/>. Natomiast niezaznaczenie checkboxa spowoduje, że konto użytkownika zostanie zarejestrowane tylko w SZT. To konto nie zostanie utworzone w WOD2021.

Na dole okna widoczny jest widżet usługi zabezpieczającej Cloudflare Turnstile:



Wskazuje on status przeprowadzonego testu. Jeśli prezentowana jest informacja „Powodzenie!”, możesz zarejestrować swoje konto.

masz do wyboru dwa przyciski – *Anuluj* oraz

Wybierając przycisk *Anuluj* powodujesz powrót do strony startowej (strony logowania) SZT.

Wybierając przycisk *Zapisz* powodujesz uruchomienie walidacji sprawdzających czy wszystkie pola zostały wypełnione oraz czy login i email nie zostały już zarejestrowane. Jeśli nie wypełniłeś pola, które jest wymagalne, aplikacja wyróżni to pole kolorem czerwonym oraz wyświetli pod nim komunikat o wymagalności pola.

Jeśli wprowadzisz błędne dane, system wyświetli komunikat informujący, na czym polega błąd.

Jeśli wprowadzisz i zapiszesz prawidłowe dane, system wyświetli komunikat o utworzeniu konta.

Jeśli posiadasz już konto na jednym środowisku aplikacji (np. szkoleniowym) i będziesz chciał utworzyć konto na drugim środowisku (np. produkcyjnym) to aplikacja pozwoli na takie działanie i powiąże oba konta, o ile login i adres email będą takie same na obu środowiskach. W takim przypadku system wyświetli komunikat o utworzeniu konta wraz z informacją, że takie samo konto jest już w ekosystemie CST2021, dlatego do logowania powinieneś użyć dotychczasowego hasła. Jeśli tylko login lub e-mail będzie taki sam to aplikacja zwróci komunikat odpowiednio o braku możliwości zarejestrowania konta z takim loginem lub adresem emailem.

**Uwaga:** utworzenie konta umożliwi zalogowanie się do systemu oraz podgląd własnych danych, ale nie wystarczy do rozpoczęcia pracy. Aby faktycznie działać w aplikacji, Administrator – zwykle Administrator w Twojej organizacji – musi nadać użytkownikowi rolę z odpowiednimi uprawnieniami.

Na adres email wskazany podczas rejestracji otrzymasz wiadomości:

* wiadomość powitalną z CST2021,
* wiadomość z linkiem do nadania hasła do konta.

Wiadomości generowane są w języku, który wskazałeś jako domyślny dla swojego konta na etapie rejestracji.

Wiadomość z linkiem do nadania hasła zawiera przycisk *UTWÓRZ HASŁO*. Kiedy go klikniesz, otworzy się nowe okno przeglądarki, w którym możesz określić swoje hasło.

### Określenie hasła

Hasło musi zawierać:

* wielkie litery,
* małe litery,
* znaki specjalne,
* liczby,
* musi składać się z minimum 10 znaków,
* nie może składać się z więcej niż 32 znaków,
* nie może składać się z kolejnych znaków loginu,
* jeśli zmieniasz hasło – musi się ono różnić od wszystkich Twoich poprzednich haseł.

Okno *Zmiana hasła* zawiera graficzny wskaźnik siły hasła, który w zależności od wprowadzonego hasła przyjmuje jeden z trzech kolorów:

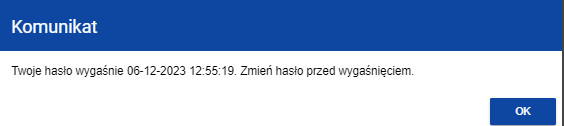
* czerwony – hasło słabe, zapewniające niski poziom zabezpieczenia, hasła o długości od 0 do 13 znaków;
* żółty – hasło o średniej sile, zapewniające umiarkowany poziom zabezpieczenia, hasła o długości od 14 do 19 znaków;
* zielony – hasło mocne, zapewniające wysoki poziom zabezpieczenia, hasła o długości od 20 znaków.

Po uzupełnieniu pól *Nowe* hasło oraz *Powtórz nowe hasło* zatwierdź zmianę hasła przyciskiem *Zmień hasło.*

Aby zobaczyć hasło, które zostało wprowadzone należy kliknąć przycisk , natomiast w celu ukrycia hasła, należy kliknąć przycisk .

Utworzenie nowego hasła system potwierdza komunikatem *Utworzyłeś hasło.*

Hasło użytkownika wygasa po 180 dniach. Jeżeli do jego wygaśnięcia zostało 30 dni lub mniej, po zalogowaniu do systemu wyświetli się komunikat:

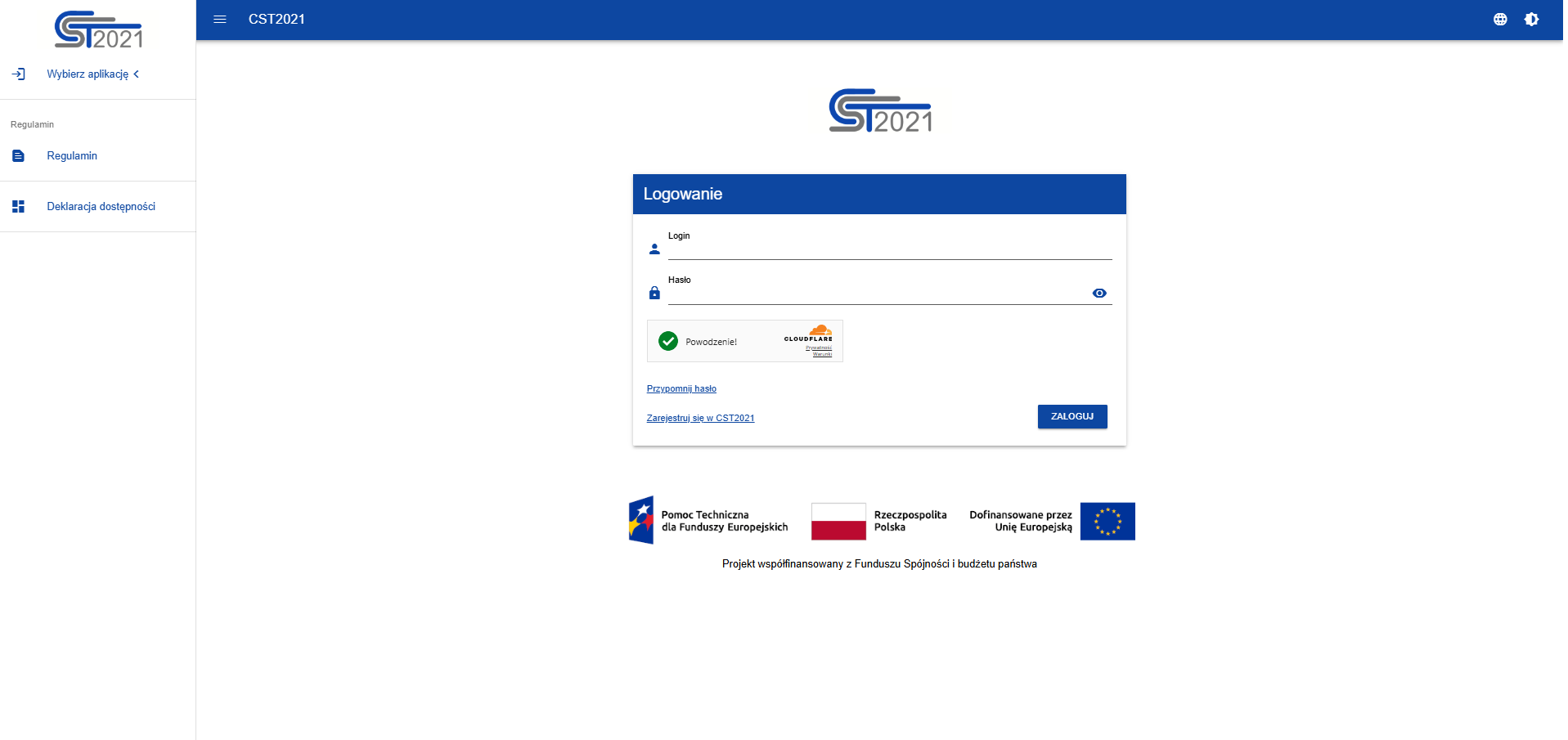


Po zamknięciu komunikatu przez użytkownika, system wyświetli okno *Zmiana hasła*.

# Logowanie

Wpisz w przeglądarce adres **cst2021.gov.pl**. Uzupełnij pola *Login* i *Hasło*, a następnie wybierz przycisk *Zaloguj*.

Uwaga! Dopóki ktoś nie nada Ci uprawnień, możesz się wprawdzie zalogować, ale nie będziesz mógł pracować w CST2021. Uprawnienia umożliwiające wykonywanie działań w systemie CST2021 (w aplikacjach Administracja, Projekty, e-Kontrole, Raporty) w imieniu jakiejś organizacji nazywamy kontekstem pracy w tej organizacji. Pomiędzy różnymi organizacjami, które reprezentujesz, przełączasz się poprzez zmienianie kontekstu pracy. Opisuje to rozdział 11 tej instrukcji.



Pod polem *Hasło* widzisz widżet usługi zabezpieczającej Cloudflare Turnstile:



Wskazuje on status przeprowadzonego testu. Jeśli prezentowana jest informacja „Powodzenie!”, możesz zalogować się do systemu.

Aby zobaczyć hasło, które zostało wprowadzone należy kliknąć przycisk , natomiast w celu ukrycia hasła, należy kliknąć przycisk .

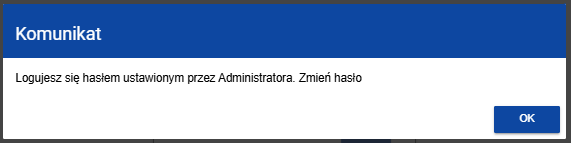
W przypadku wprowadzenia błędnego loginu lub hasła aplikacja wyświetli komunikat o błędzie.

Jeśli próbę logowania (z użyciem poprawnego loginu i hasła) podejmiesz w sytuacji, kiedy Twoje konto jest zablokowane, aplikacja uniemożliwi zalogowanie oraz wyświetli komunikat *Twoje konto nie jest aktywne – skontaktuj się z administratorem*

Po prawidłowym zalogowaniu zostaniesz automatycznie przeniesiony do wybranej uprzednio aplikacji.

Z kolei, aby zalogować się do aplikacji SZT wpisz w przeglądarce jej adres, uzupełnij pola *Login* i *Hasło*, a następnie wybierz przycisk *Zaloguj*.

Jeśli Twoje hasło zostało nadane przez Administratora, system wyświetla komunikat *Logujesz się hasłem ustawionym przez Administratora. Zmień hasło.*

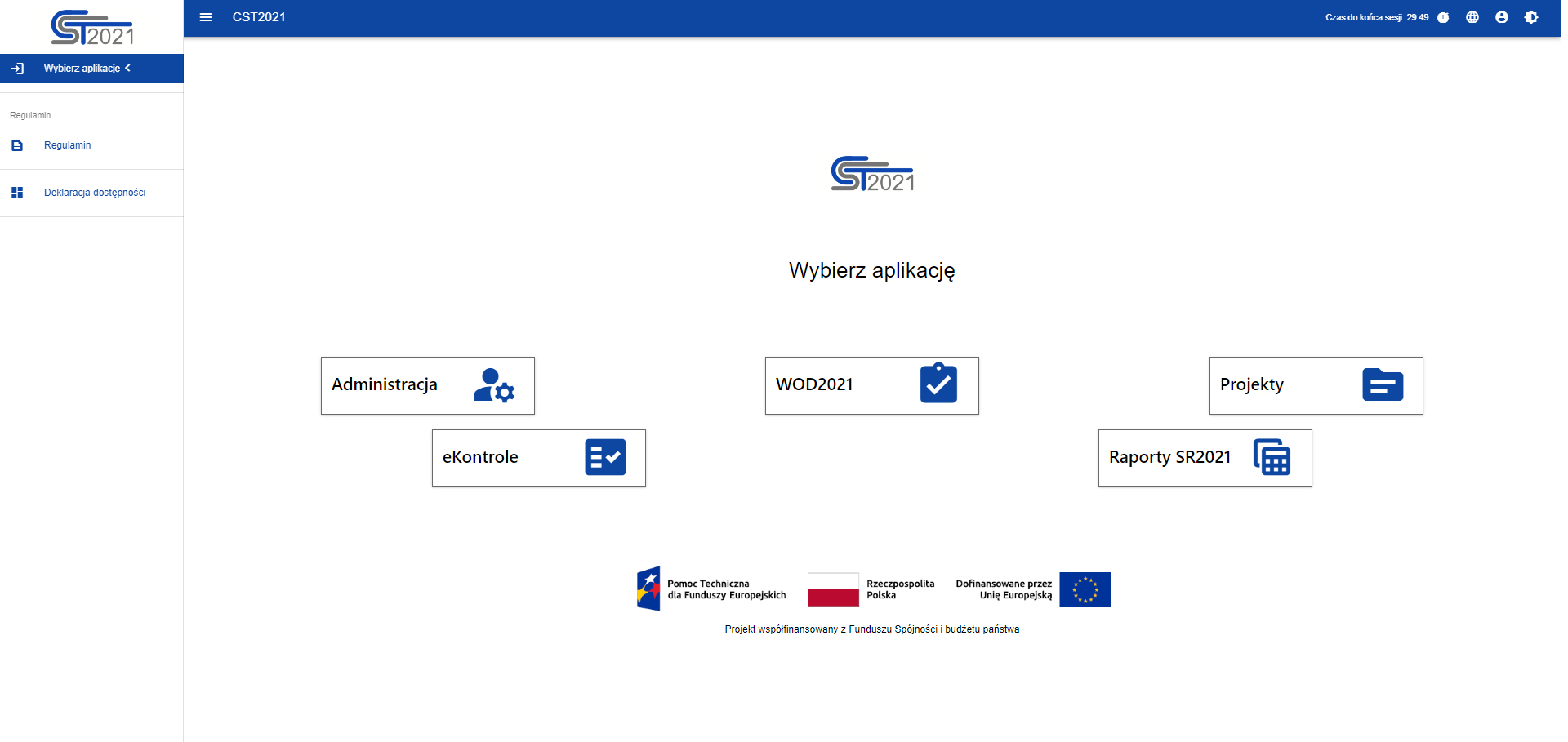


Po zamknięciu tego komunikatu, system wyświetli okno *Zmiana hasła*. Dopóki nie zatwierdzisz zmiany hasła, system nie pozwoli Ci na przejście do żadnego innego ekranu w aplikacji.

Po pomyślnej zmianie hasła, system wyświetla komunikat *Zmieniłeś hasło*.



Po zalogowaniu i ewentualnej zmianie hasła zostaniesz przekierowany na stronę wyboru aplikacji. Kliknij kafelek z nazwą aplikacji, aby rozpocząć w niej pracę.



Treści na stronach aplikacji SZT (dla zalogowanego użytkownika) są prezentowane w języku wskazanym jako domyślny w ramach konta użytkownika. Jednak niezależnie od domyślnego języka masz możliwość zmiany wersji językowej aplikacji na czas otwarcia przeglądarki. Proces ten przebiega w taki sam sposób, jak zostało to opisane w rozdziale 2. *Zmiana języka aplikacji dla niezalogowanego użytkownika*. Po ponownym otwarciu przeglądarki i zalogowaniu do aplikacji ponownie obowiązuje domyślny język przypisany do konta użytkownika.

### Logowanie przy włączonym uwierzytelnianiu dwuetapowym – wprowadzenie

Aby zwiększyć ochronę swojego konta, możesz włączyć dodatkową metodę potwierdzania tożsamości podczas logowania.

Potwierdzanie tożsamości jest nazywane uwierzytelnianiem lub autentykacją. Aby włączyć dodatkowy mechanizm uwierzytelniania, powinieneś zainstalować specjalną aplikację na swoim telefonie komórkowym. Jest wiele aplikacji tego typu. Zwykle mają one w nazwie słowo „Authenticator” od angielskiego słowa „authentication” oznaczającego uwierzytelnianie. Przykładowe aplikacje znanych firm, z których można bezpłatnie korzystać to np. Microsoft Authenticator, Oracle Mobile Authenticator czy Google Authenticator.

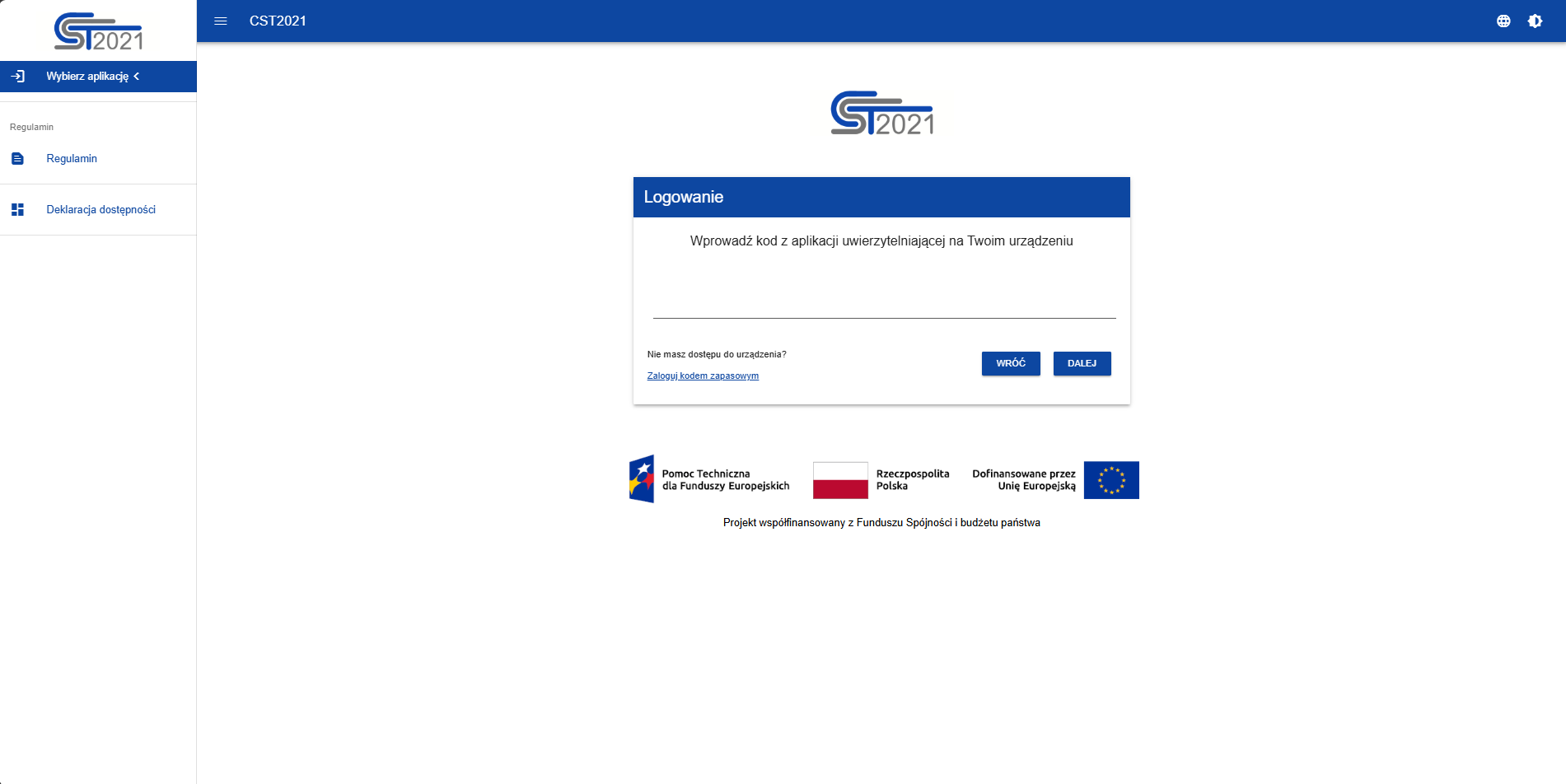
Z punktu widzenia uwierzytelniania dwuetapowego (w skrócie: 2FA) kiedy się logujesz ma miejsce jeden z czterech głównych scenariuszy:

1. Nie masz włączonego 2FA. Wtedy logowanie przebiega tak, jak opisano to powyżej.
2. Nie masz włączonego 2FA, ale Administrator zobowiązał Cię, abyś je sobie włączył. W takiej sytuacji zalogujesz się do CST2021 loginem i hasłem, ale system natychmiast przekieruje Cię na ekran edycji profilu i dopóki nie włączysz sobie na nim 2FA, nie będziesz mógł wejść do żadnej aplikacji. Rozdział 10 tej instrukcji opisuje, co zrobić w takiej sytuacji – czyli jak włączyć 2FA na swoim koncie.
3. Masz włączone 2FA w formie kodu przepisywanego z aplikacji uwierzytelniającej (wymaga to dowolnej aplikacji obsługującej algorytm generowania jednorazowych kodów TOTP – Time-based One-Time Password).
4. Masz włączone 2FA w formie powiadomienia akceptowanego w aplikacji uwierzytelniającej (wymaga aplikacji Oracle Mobile Authenticator oraz połączenia z internetem telefonu komórkowego, na którym jest zainstalowana).

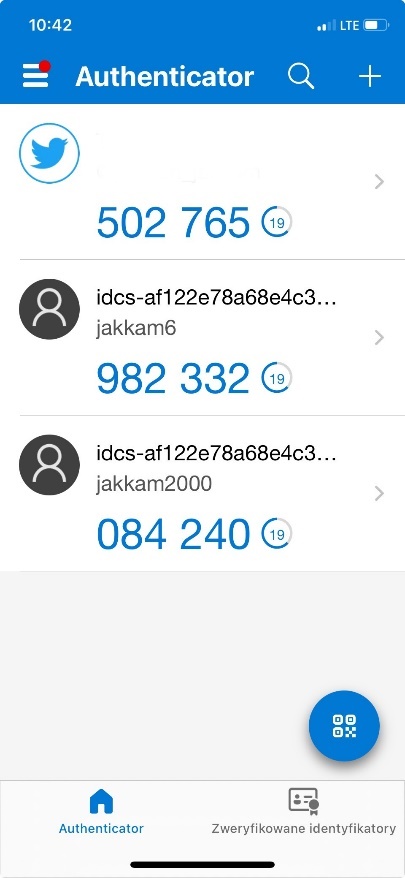
Poniżej opisano dwie ostatnie sytuacje. Opis zakłada, że masz już włączone i skonfigurowane 2FA zarówno w CST2021 jak i w aplikacji uwierzytelniającej. Jak możesz sobie je włączyć, skonfigurować i wyłączyć, przeczytasz w rozdziale 10 tej instrukcji.

### Logowanie za pomocą kodu

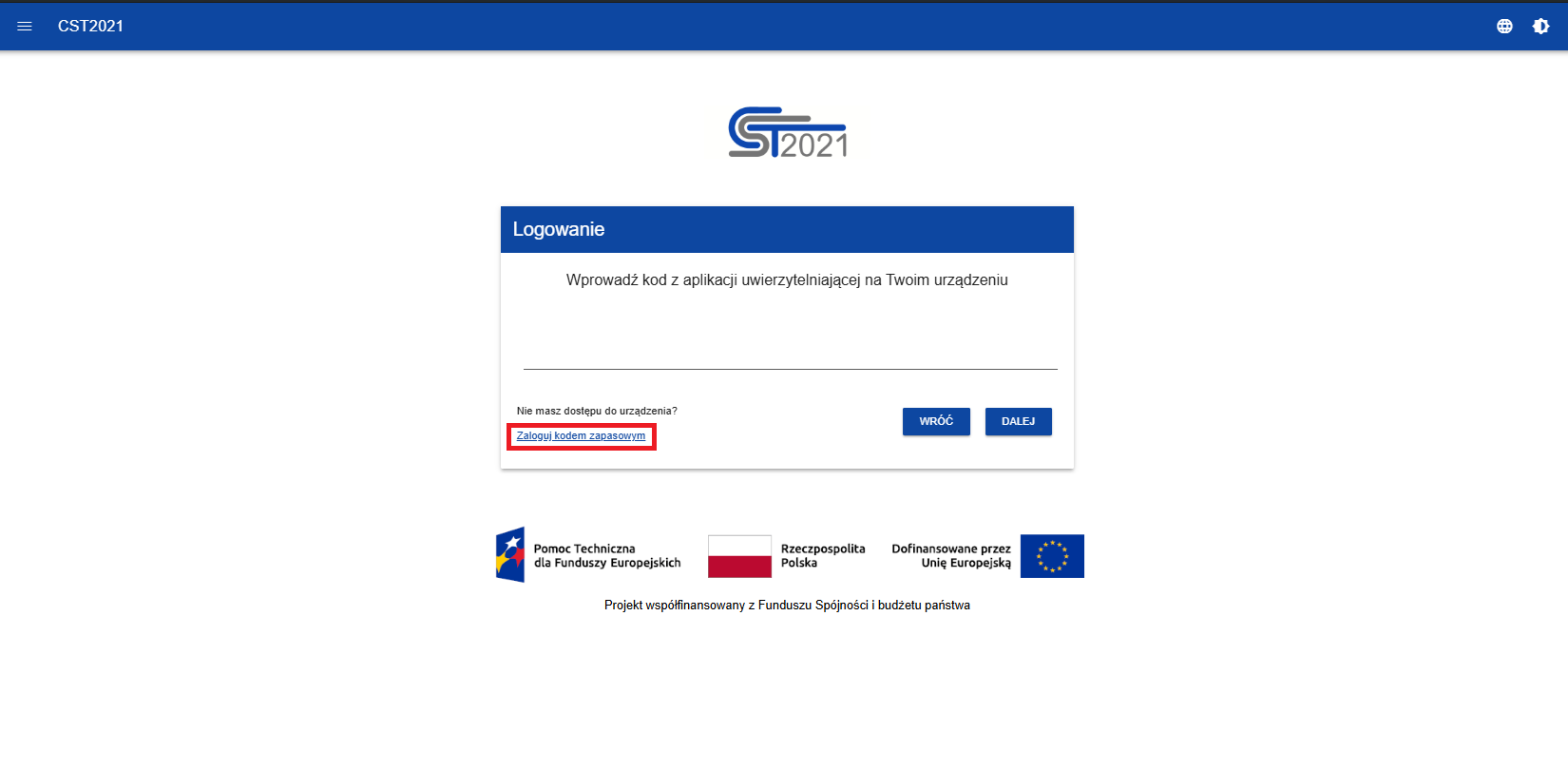
Kiedy wpiszesz login i poprawne hasło, system rozpozna że masz włączone 2FA w formie kodu TOTP i poprosi o przepisanie kodu z aplikacji uwierzytelniającej.



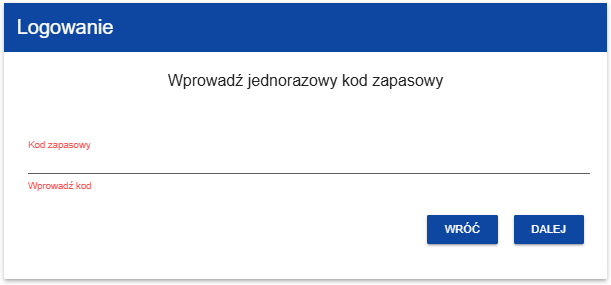
Otwórz aplikację w swoim telefonie. Przykładowe ekrany z aplikacji uwierzytelniającej pokazano w rozdziale 10 tej instrukcji. Jeśli poprawnie dodałeś w niej swoje konto w CST2021 podczas włączania 2FA, wiesz już jak wygląda taka aplikacja. Od razu po jej otwarciu powinna pokazywać się lista kont, z aktualnym kodem przy każdym koncie. Odnajdź właściwe konto i przepisz kod do formularza w CST2021. Kliknij „Dalej” – jeśli wpisałeś właściwy kod logowanie zakończy się sukcesem.



Jeśli nie masz dostępu do urządzenia z aplikacją uwierzytelniającą, kliknij w link Zaloguj kodem zapasowym:



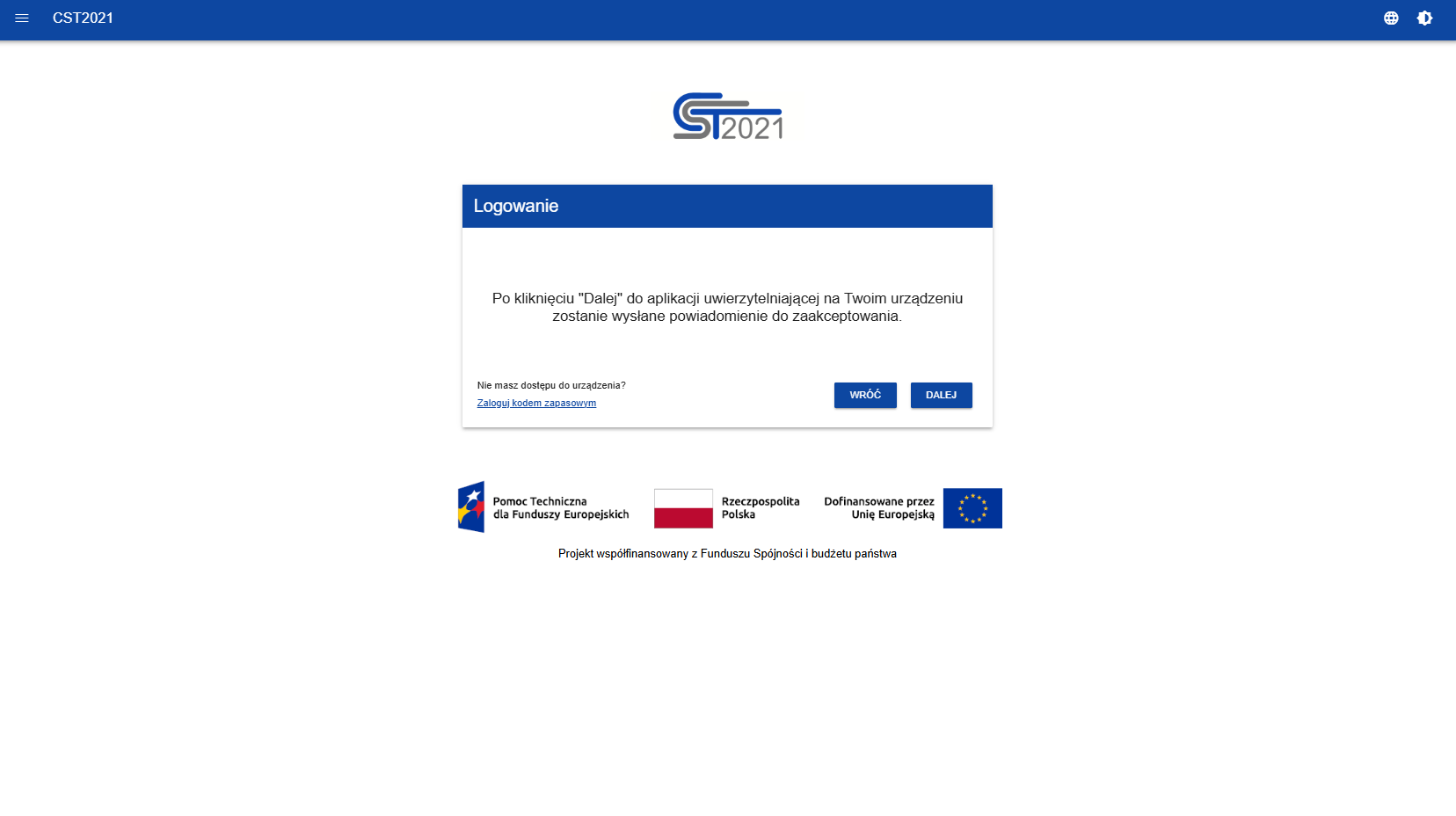
System wyświetli okno z możliwością wprowadzenia jednorazowego kodu zapasowego. Wpisz go i kliknij „Dalej” - jeśli wpisałeś właściwy kod logowanie zakończy się sukcesem a system CST2021 pokaże Ci nowy kod zapasowy. Zapisz go w bezpiecznym miejscu zamiast poprzedniego.



Jeśli nie pamiętasz kodu zapasowego i nie masz dostępu do urządzenia z aplikacją uwierzytelniającą, nie będziesz mógł się zalogować. W takiej sytuacji musisz poprosić Administratora o wyłączenie 2FA na Twoim koncie.

### Logowanie za pomocą powiadomienia

Kiedy wpiszesz login i poprawne hasło, system rozpozna że masz włączoną opcję 2FA w formie powiadomień i poprosi o dodatkowe potwierdzenie logowania w aplikacji Oracle Mobile Authenticator.



Kliknij „Dalej” i otwórz aplikację Oracle Mobile Authenticator w swoim telefonie. Poczekaj, aż na jej ekranie wyświetli się powiadomienie do zaakceptowania. Powinno to trwać kilka sekund. Jeśli powiadomienie się nie wyświetla, kliknij ikonę dzwonka w prawym górnym rogu listy kont. Aktualne powiadomienia będą widoczne w zakładce „Oczekujące”. Kliknij „Zezwól” na powiadomieniu aby potwierdzić logowanie.

|  |  |  |
| --- | --- | --- |
|  |  |  |

Tak samo jak przy logowaniu kodem TOTP, masz również dostępny link do zalogowania kodem zapasowym – na wypadek sytuacji, w której potrzebujesz się zalogować a nie masz dostępu do urządzenia z aplikacją uwierzytelniającą.

# Akceptacja Regulaminu

Konieczność zaakceptowania regualminu CST2021 zachodzi w przypadku:

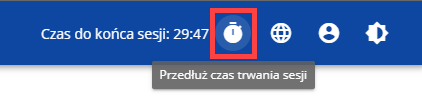
* Pierwszego logowania po zarejestrowaniu konta użytkownika. Regulamin do akceptacji wyświetlany jest jako ostatnia (obowiązująca) wersja w domyślnym języku zalogowanego użytkownika, a jeśli nie ma wersji regulaminu w tym języku to w języku polskim.
* Logowania następującego po dodaniu w Systemie nowej wersji regulaminu (który zaczął już obowiązywać), o ile dodany regulamin jest w wersji językowej zgodnej z językiem wskazanym domyślnie dla konta użytkownika lub dla domyślnego języka przypisanego do konta użytkownika nie ma żadnej wersji regulaminu, a nowododana wersja jest w języku polskim.
* Zmiany przez zalogowanego użytkownika aktualnie wybranego języka interfejsu aplikacji, o ile użytkownik nie zaakceptował wcześniej obowiązującej wersji regulaminu dla tego języka.

Regulamin jest wspólny dla różnych aplikacji objętych SZT, dlatego okno akceptacji regulaminu prezentowane jest w SZT po zalogowaniu, a przed wyświetleniem ekranu wyboru aplikacji.

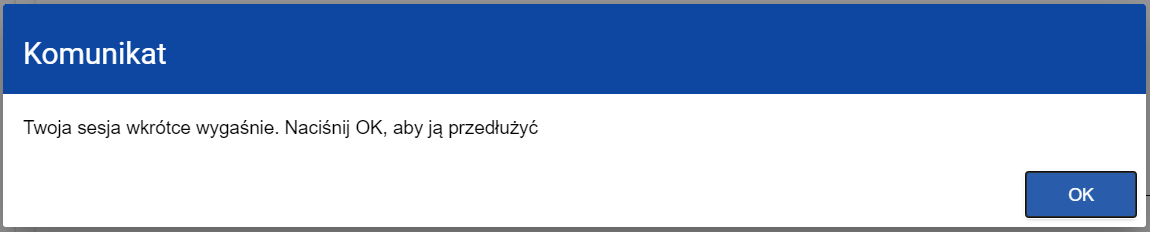
W celu zaakceptowania regulaminu musisz kliknąć przycisk *Zaakceptuj*, który staje się widoczny po przewinięciu na sam dół treści regulaminu. Kliknięcie przycisku *Anuluj* oznacza brak akceptacji treści regulaminu i skutkuje wylogowaniem użytkownika z SZT uniemożliwiając tym samym dalszą pracę.

# Przedłużanie sesji

Po udanym zalogowaniu rozpoczyna się sesja, która pozwala na korzystanie z systemu przez 30 min. Czas pozostały do końca sesji widać obok ikony *Menu użytkownika* w prawej części górnego menu.



Na 5 minut przed wygaśnięciem sesji system wyświetla komunikat, którego potwierdzenie wydłuża czas sesji o kolejne 30 minut.

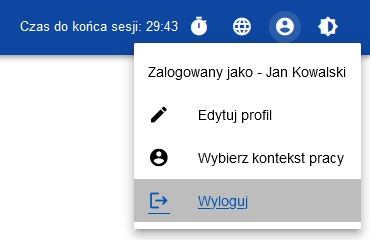


Niepodjęcie żadnego działania prowadzi do wygaśnięcia sesji i automatycznego wylogowania. Aby przedłużyć sesję w trakcie jej trwania, zanim pojawi się komunikat o bliskim wygaśnięciu sesji, kliknij na ikonę zegara umieszczoną obok prezentowanego czasu do końca sesji. Czas sesji jest wydłużany automatycznie przy każdorazowym przeładowaniu strony.

Uwaga: wprowadzenie funkcjonalności sesji wynika z zasad bezpieczeństwa. Jeśli aktywnie pracujesz w systemie, sesja nie stanowi ograniczenia, możesz ją przedłużać.

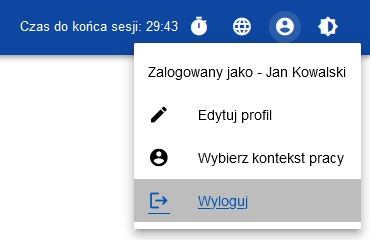
# Wylogowanie z aplikacji

Aby wylogować się z Administracji kliknij ikonę *Menu użytkownika* w prawym górnym rogu ekranu oraz wybierz przycisk *Wyloguj*.

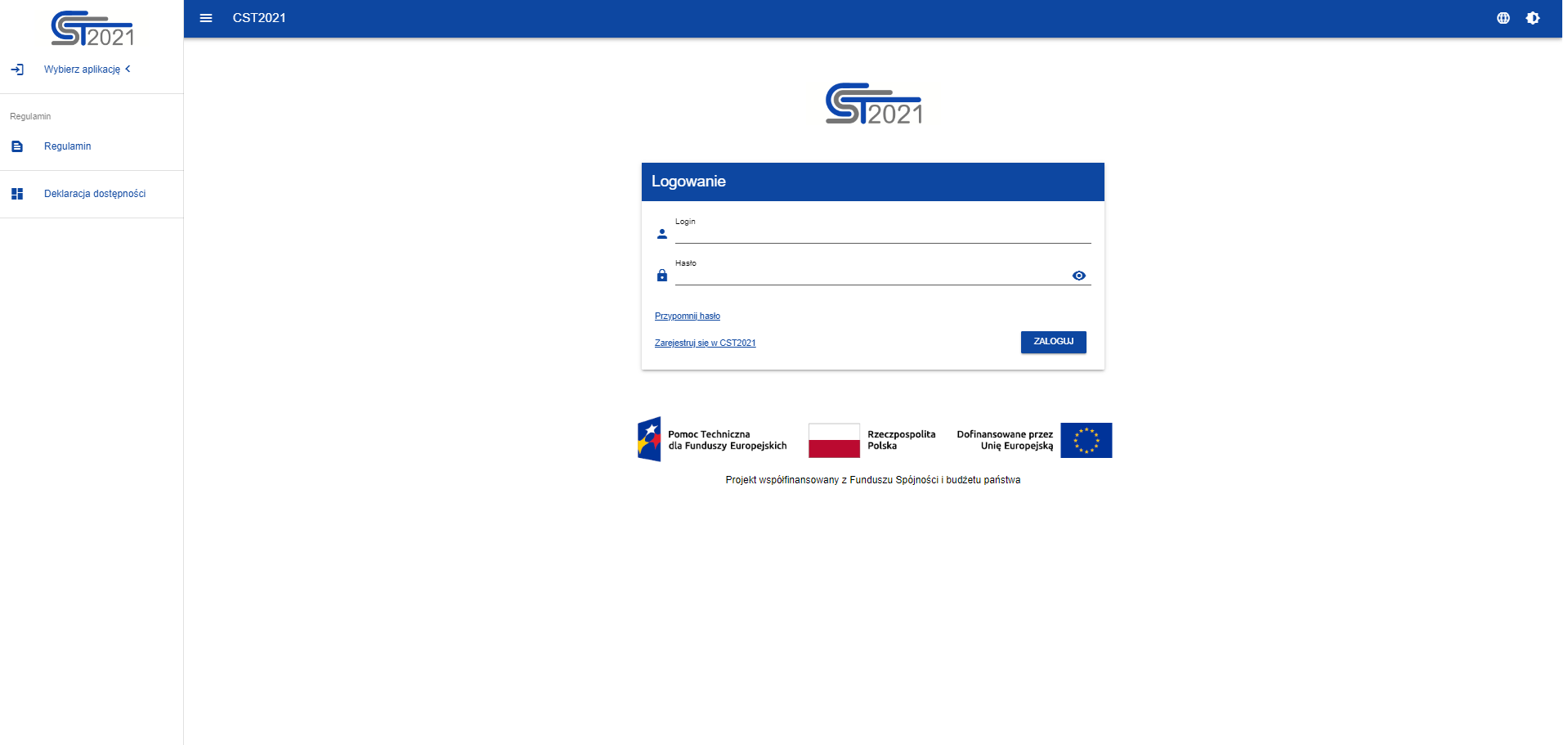


Zostaniesz przekierowany do aplikacji SZT, gdzie zobaczysz ekran *Wybierz aplikację* z linkami do aplikacji, do których masz nadany dostęp (o ile nie wygasła globalna sesja).

Z poziomu SZT będziesz mógł wylogować się z całego systemu CST2021, korzystając z przycisku *Wyloguj.*

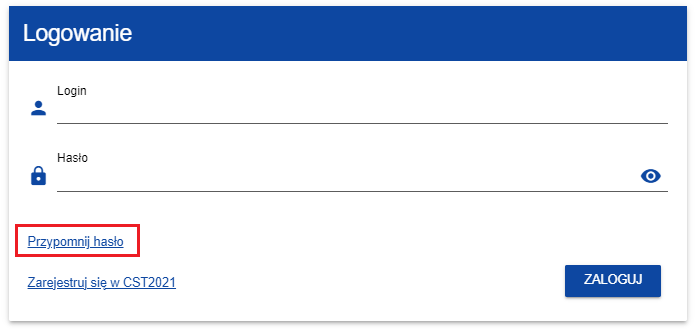
**

Po wylogowaniu bezpośrednio z aplikacji SZT zaprezentowany zostanie komunikat *Zostałeś wylogowany*, a po jego zamknięciu ekran logowania.

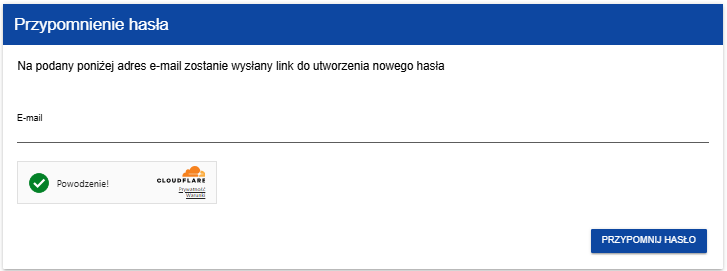


# Przypomnienie hasła

W celu przypomnienia hasła do swojego konta skorzystaj z funkcji *Przypomnij hasło* dostępnej na stronie logowania SZT.



Wybór funkcji *Przypomnij hasło* powoduje wyświetlenie okna *Przypomnienia hasła.*



Pod polem *E-mail* widoczny widżet usługi zabezpieczającej Cloudflare Turnstile:



Wskazuje on status przeprowadzonego testu. Jeśli prezentowana jest informacja „Powodzenie!”, możesz przystąpić do operacji przypomnienia hasła do konta.

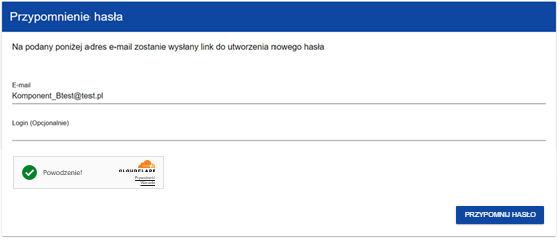
W oknie podaj swój adres mailowy przypisany do konta, następnie wybierz przycisk *Przypomnij hasło*.

Jeśli wprowadzony adres nie zostanie odnaleziony w aplikacji jako przypisany do jednego z kont, aplikacja wyświetli komunikat o błędzie.

Jeśli wprowadzony adres mailowy jest poprawny, system wyświetli komunikat *Na ten e-mail w ciągu 10 minut otrzymasz link do zresetowania hasła.* Na wskazany adres email otrzymasz wiadomość z linkiem do utworzenia nowego hasła do konta.

Dalej proces przebiega zgodnie z opisem w punkcie 3.2 Określenie hasła.

Jeśli podczas operacji przypominania hasła zostanie rozpoznane na serwerze tożsamości więcej niż jedno konto przypisane do podanego adresu email, aplikacja wyświetli komunikat *Dla podanego adresu e-mail rozpoznano więcej niż jedno konto. Wymagane jest podanie dodatkowo Loginu.* Dodatkowo aplikacja wyświetli zmieniony wygląd okna przypomnienia hasła. W oknie podaj adres mailowy oraz login przypisane do konta, następnie wybierz przycisk *Przypomnij hasło*.

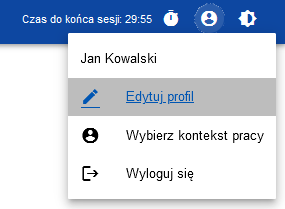


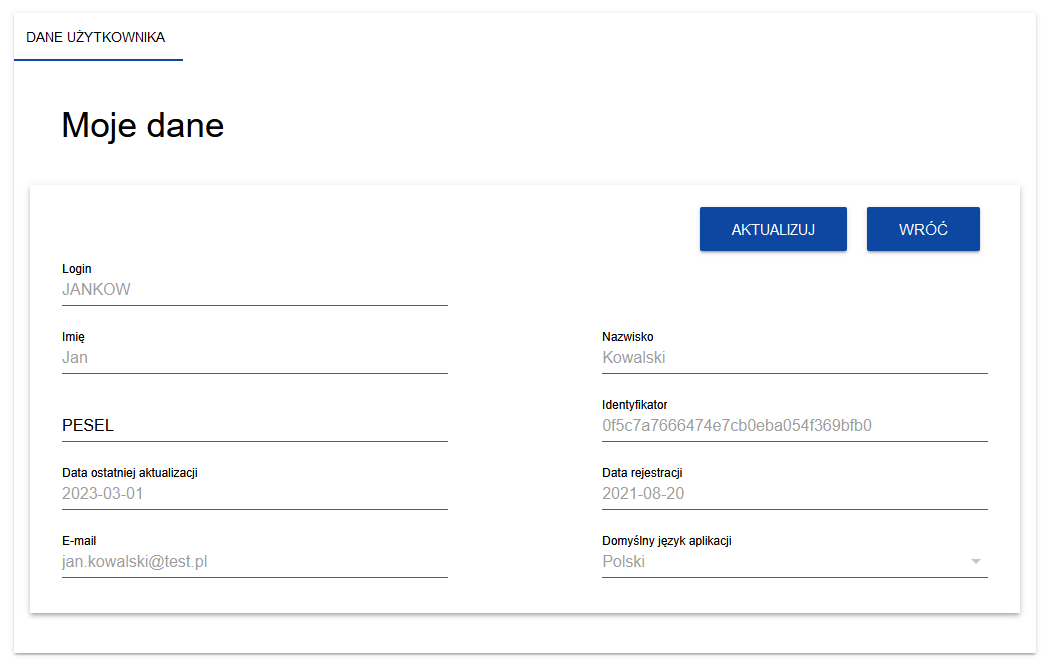
Jeśli wprowadzone dane są poprawne, system podobnie jak w przypadku opisanym wyżej wyświetli komunikat *Na ten e-mail w ciągu 10 minut otrzymasz link do zresetowania hasła.* Na wskazany adres email otrzymasz wiadomość z linkiem do utworzenia nowego hasła do konta.

Dalej proces przebiega zgodnie z opisem w punkcie 3.2 Określenie hasła.

# Edycja własnych danych oraz zmiana hasła

Po zalogowaniu możesz przeglądać dane przypisane do Twojego konta. Kliknij ikonę *Menu użytkownika* znajdującą się w prawej części górnego menu oraz wybierz przycisk *Edytuj profil*. System wyświetli ekran *Moje dane* z danymi użytkownika.



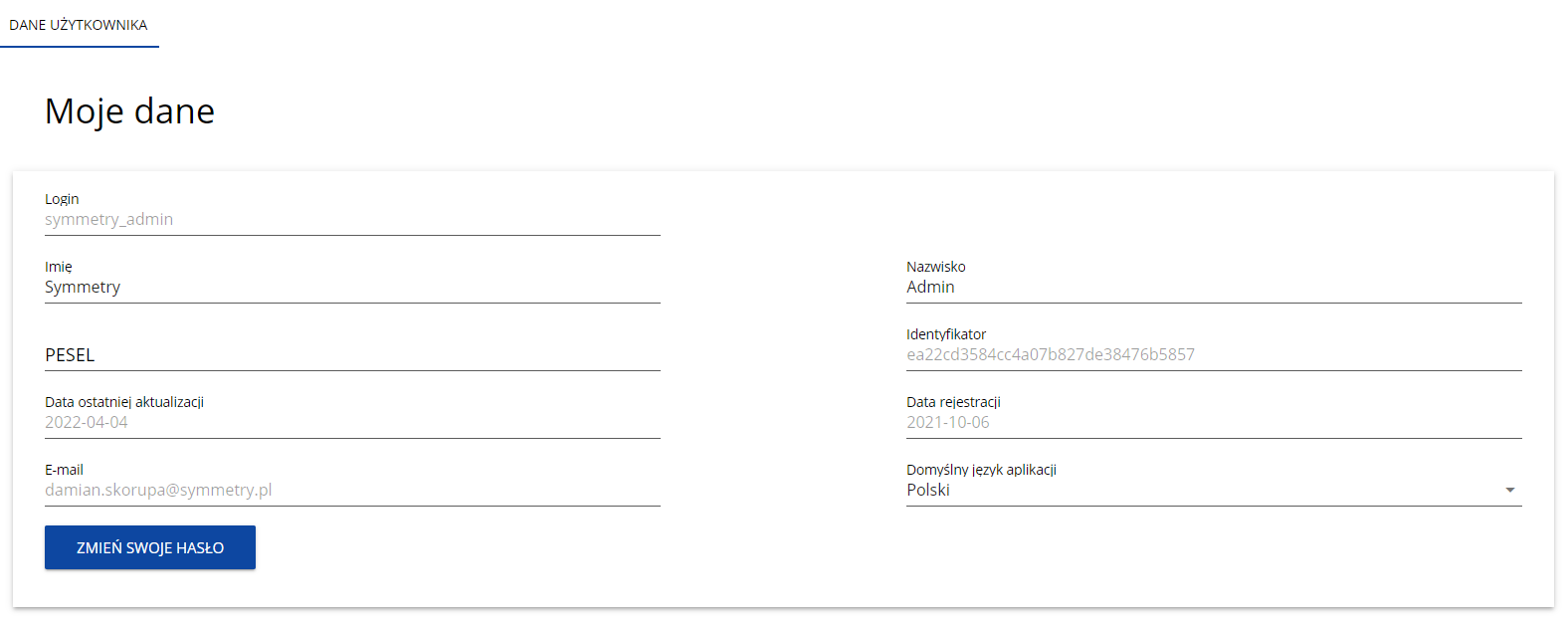


Na ekranie *Moje dane* dostępne są dwa przyciski: *Aktualizuj* i *Wróć.*

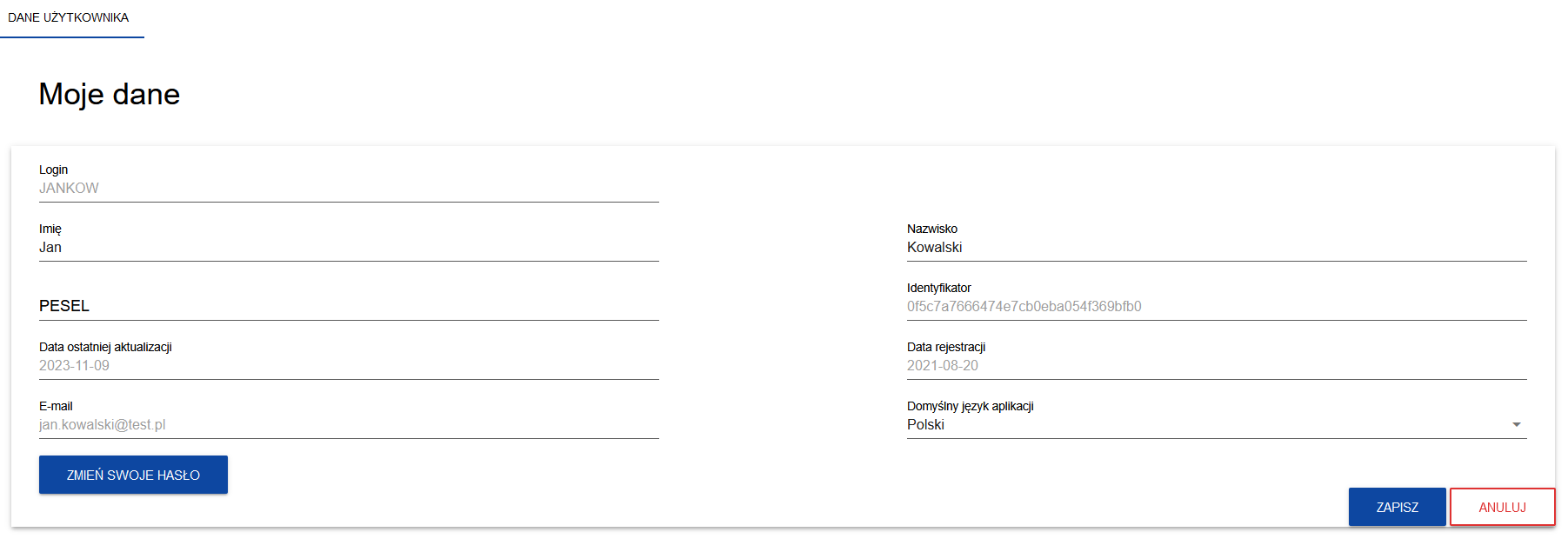
Wybór przycisku *Wróć* powoduje przekierowanie do ekranu, z poziomu którego użytkownik wybrał funkcję *Edytuj profil* (ekran wyświetlany przed przejście do ekranu *Moje dane*).

Wybór przycisku *Aktualizuj* umożliwia edycję pól:

* Imię,
* Nazwisko,
* PESEL,
* Domyślny język aplikacji.



Aplikacja wyróżni kolorem czerwonym oraz wyświetli podpowiedź prawidłowej wartości dla pól, które zawierają niedozwoloną wartość.



Oprócz aktualizacji podstawowych informacji o użytkowniku ekran *Moje dane* umożliwia edycję domyślnego języka aplikacji, wskazanego podczas rejestracji. W tym celu należy wybrać odpowiedni język z listy.

Aby zatwierdzić wprowadzone zmiany wybierz przycisk *Zapisz*. System wyświetli komunikat *Twoje dane zostały zapisane*.

Tryb edycji danychumożliwia również zmianę hasła. Wybierz przycisk *Zmień swoje hasło,* aby uruchomić proces opisany w punkcie 3.2 Określenie hasła.

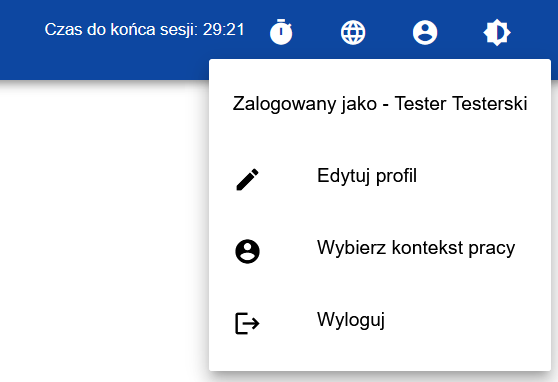
Po uzupełnieniu pól *Stare hasło*, *Nowe hasło* oraz *Powtórz hasło* zatwierdź zmianę hasła przyciskiem *Zapisz.* Poprawne utworzenie nowego hasła system potwierdzi komunikatem *Zmieniłeś hasło.* Na adres mailowy otrzymasz wiadomość potwierdzającą ustawienie nowego hasła.

Jeśli wprowadzone stare hasło jest niepoprawne, system wyświetli komunikat *Wprowadź poprawne stare hasło*.

# Zarządzanie ustawieniami uwierzytelniania dwuetapowego (2FA)

Aby zwiększyć ochronę swojego konta, możesz włączyć dodatkową metodę potwierdzania tożsamości podczas logowania. Takie potwierdzanie tożsamości jest nazywane również uwierzytelnianiem lub autentykacją. Aby włączyć dodatkowy mechanizm uwierzytelniania, powinieneś zainstalować specjalną aplikację na swoim telefonie komórkowym. Jest wiele aplikacji tego typu. Zwykle mają one w nazwie słowo „Authenticator” od angielskiego słowa „authentication” oznaczającego uwierzytelnianie. Przykładowe aplikacje znanych firm, z których można bezpłatnie korzystać to np. Microsoft Authenticator, Oracle Mobile Authenticator czy Google Authenticator.

Aby włączyć 2FA wybierz funkcję *Edytuj profil* pod ikoną ludzika w prawym górnym rogu ekranu.

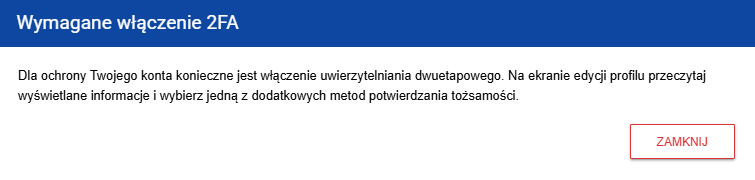


Ekran podglądu i edycji danych Twojego konta składa się z dwóch bloków. W pierwszym, u góry, widzisz swoje dane osobowe. Drugi blok, poniżej pierwszego, zawiera krótką instrukcję, informacje nt. statusu 2FA na Twoim koncie oraz przyciski umożliwiające zarządzanie ustawieniami 2FA:

Obraz zawierający tekst, Czcionka, zrzut ekranu, linia

Zawartość wygenerowana przez AI może być niepoprawna.

Jeżeli Administrator włączył dla Twojego konta wymuszenie uwierzytelniania dwuetapowego, po zalogowaniu zostaniesz przekierowany na ekran edycji profilu, a system wyświetli następujący komunikat:



Zamknięcie komunikatu spowoduje, że zostaniesz przekierowany do edycji swojego profilu gdzie powinieneś włączyć 2FA. Ekran edycji profilu, który widzisz po wymuszeniu włączenia 2FA, jest taki sam jak wtedy, kiedy wchodzisz na niego dobrowolnie. Masz do wyboru dwa przyciski, odpowiadające dwóm dostępnym metodom:



|  |  |  |
| --- | --- | --- |
|  | Używanie powiadomienia jest wygodniejsze, ponieważ podczas logowania może wymagać nawet tylko jednego kliknięcia w aplikacji uwierzytelniającej na telefonie. Kod trzeba przepisać z telefonu do formularza pokazanego przez system CST2021. Są jednak dwa ograniczenia powiadomień w porównaniu z kodem:   1. Powiadomienie (po lewej stronie) wymaga aplikacji Oracle Mobile Authenticator, podczas gdy kod może być generowany w dowolnej aplikacji obsługującej algorytm TOTP (po prawej stronie). Być może masz już zainstalowaną jedną taką aplikację i nie chcesz instalować kolejnej. 2. Powiadomienie wymaga połączenia telefonu z internetem.   Zastanów się przez chwilę, która metoda będzie Ci bardziej odpowiadać. **Możesz ją później łatwo zmienić tylko uważaj, aby najpierw wyłączyć starą metodę w systemie CST2021 a dopiero później usunąć z aplikacji w telefonie!** W sklepie z aplikacjami na swoim telefonie wyszukaj odpowiedni autentykator, zainstaluj go i otwórz. Następnie kliknij przycisk wyboru odpowiedniej metody w CST2021.  Niezależnie od wybranej metody, w następnym kroku zobaczysz kod QR który powinieneś zeskanować w aplikacji na telefonie. W zależności od wybranej metody, komunikat pokazany z kodem QR będzie się nieco różnił. |  |

### Konfiguracja kodu

Jeśli wybrałeś Kod, zobaczysz poniższy komunikat. Zeskanuj wyświetlony kod QR za pomocą wybranej aplikacji uwierzytelniającej:



Sposób skanowania kodu będzie się nieco różnić zależnie od wybranej aplikacji. Zwykle trzeba rozpocząć od znalezienia w aplikacji funkcji dodania nowego konta. Dla aplikacji Microsoft jest to znak „+” na obrazku poniżej po lewej stronie. Aplikacja może następnie zapytać o typ konta. W przypadku aplikacji Microsoft najlepiej wybrać „Inne” ponieważ okno, które się wtedy pojawia, umożliwia również ręczne wprowadzenie kodu QR, gdyby wystąpiły problemy z jego zeskanowaniem.

Wyceluj aparat telefonu w kod QR pokazany w CST2021. Po udanym zeskanowaniu (lub wprowadzeniu ręcznym) w aplikacji na telefonie zobaczysz nowe konto wraz z nowym kodem.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

Jeśli nie możesz zeskanować kodu QR, kliknij w link podświetlony poniżej:

**

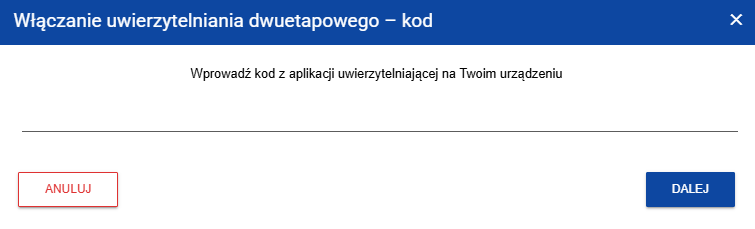
Zobaczysz kolejny komunikat, którego najważniejszą częścią jest ciąg znaków odpowiadający kodowi QR:

|  |  |
| --- | --- |
|  |  |

Uważnie przepisz ten ciąg znaków do odpowiedniego pola w aplikacji uwierzytelniającej (autentykatorze). W polu na nazwę konta wpisz coś, co pozwoli Ci odróżniać to konto od innych, z których korzystasz w tej aplikacji. Kiedy zapiszesz te dwie informacje, w autentykatorze pojawi się nazwa nowego konta wraz z kodem TOTP. Wpisz ten kod na powyższym formularzu CST2021 i kliknij „Dalej”.

Uwaga! Jeżeli prawidłowo przepisujesz kod z autentykatora, a mimo to w CST2021 widzisz błąd „Błędny kod uwierzytelniający” to prawdopodobnie pomyliłeś się przepisując ciąg znaków zastępujący kod QR. Jeśli ten ciąg znaków choć w jednym miejscu był inny, konto w autentykatorze nie zostało powiązane z kontem w CST2021. Upewnij się na ekranie edycji profilu, że tak faktycznie jest, po czym usuń konto z autentykatora i dodaj je ponownie.

Jeśli zeskanowałeś kod QR w aplikacji na telefonie, w CST2021 kliknij *Dalej.* Zobaczysz poniższy komunikat, na którym ostatecznie potwierdzisz włączenie 2FA, wpisując aktualny kod widoczny w Twoim telefonie przy nowo dodanym koncie.



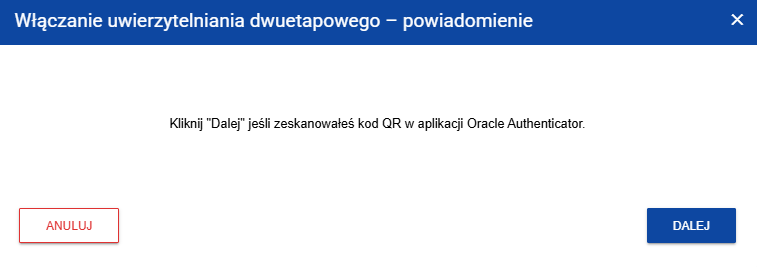
Po zakończeniu konfiguracji wyświetlony zostanie kod zapasowy. Zapisz go od razu w bezpiecznym miejscu, na wypadek jakbyś utracił dostęp do konta w aplikacji uwierzytelniającej. Po kliknięciu „Dalej” zostaniesz automatycznie wylogowany. Przy następnym logowaniu będziesz już musiał użyć kodu z aplikacji uwierzytelniającej lub kodu zapasowego.

### Konfiguracja powiadomienia

Jeśli wybrałeś Powiadomienie, zobaczysz poniższy komunikat. W aplikacji Oracle Mobile Authenticator kliknij znak „+” aby dodać nowe konto. Od razu powinno otworzyć się okno skanowania kodu QR. Wyceluj aparat telefonu w kod QR na komunikacie.



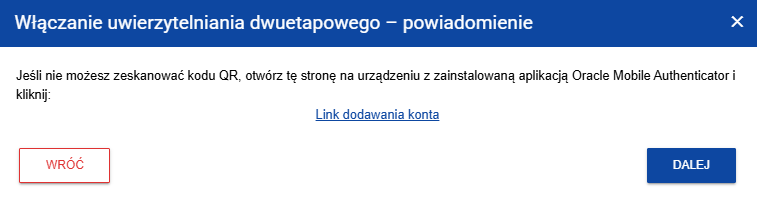
Po zeskanowaniu kodu, kliknij *Dalej* na kolejnym komunikacie:



**Jeśli nie możesz zeskanować kodu QR, wyloguj się z CST2021 na komputerze i zaloguj w przeglądarce internetowej na telefonie komórkowym, na którym masz zainstalowaną aplikację Oracle Mobile Authenticator.** Powtórz proces włączania 2FA, a kiedy zobaczysz poniższy komunikat, kliknij na podświetlony link:



Pojawi się kolejny komunikat – z linkiem do dodawania konta. Po kliknięciu na ten link aplikacja uwierzytelniająca powinna automatycznie się otworzyć i zarejestrować dodawane konto.



Przełącz się z widoku aplikacji Oracle do przeglądarki, w której masz otwarte CST2021 i kliknij *Dalej* na powyższym komunikacie. System wyświetli kod zapasowy. Zapisz go od razu w bezpiecznym miejscu, na wypadek jakbyś utracił dostęp do konta w aplikacji uwierzytelniającej. Po kolejnym kliknięciu „Dalej” zostaniesz automatycznie wylogowany. Przy następnym logowaniu będziesz już musiał zaakceptować powiadomienie lub użyć kodu zapasowego.

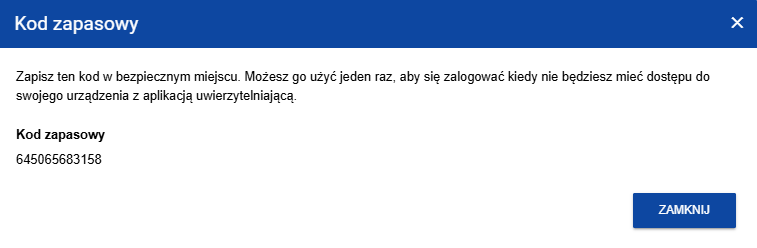
Uwaga! Przy korzystaniu z powiadomień w aplikacji Oracle Mobile Authenticator zwróć uwagę na dwie rzeczy:

1. Aplikacja generuje i wyświetla również kody TOTP dla Twojego konta w CST2021. Jednak możesz mieć włączoną tylko jedną domyślną metodę 2FA więc nie możesz z tych kodów korzystać. Po prostu je ignoruj i oczekuj na pojawienie się w autentykatorze powiadomienia o próbie logowania.
2. Jeśli powiadomienie nie wyświetli się w aplikacji w ciągu kilku sekund od wywołania go przez CST2021, kliknij na ikonę dzwonka w prawym górnym rogu ekranu (obrazek po lewej stronie). Zostaniesz przeniesiony do ekranu powiadomień. Aktualne powiadomienie powinno pokazać się w zakładce „Oczekujące”. Kliknij na nie aby w następnym kroku móc je zaakceptować albo odrzucić.

|  |  |
| --- | --- |
|  |  |

### Kod zapasowy

Po udanym włączeniu 2FA, CST2021 pokaże Ci kod zapasowy, który pozwoli na jednokrotne zalogowanie się do systemu jeżeli nie będziesz mieć dostępu do swojego urządzenia z aplikacją uwierzytelniającą. Kiedy go wykorzystasz podczas logowania system automatycznie pokaże Ci komunikat z nowym kodem, który znowu powinieneś zapisać w bezpiecznym miejscu.



Uwaga! Ze względów bezpieczeństwa kodu zapasowego nie możesz drugi raz zobaczyć w aplikacji. Nie ma funkcji jego podglądu, jest jedynie funkcja jego zmiany:



Kiedy klikniesz przycisk jej uruchomienia zobaczysz nowy kod a poprzedni przestanie działać. Pamiętaj wtedy aby go zastąpić w miejscu, gdzie był zapisany. Jeśli nie wiesz gdzie przechowujesz swój aktualny kod zapasowy, wygeneruj nowy i zapisz w miejscu, o którym nie zapomnisz.

### Zmiana nazwy konta w aplikacji uwierzytelniającej

|  |  |  |
| --- | --- | --- |
| W większości aplikacji uwierzytelniających powinieneś mieć możliwość zmiany wyświetlanej nazwy systemu, którego dotyczy dane konto. Domyślnie Twoje konto zapisze się z nazwą będącą długim ciągiem znaków (technicznym identyfikatorem zewnętrznej usługi zarządzania tożsamością, z której korzystamy). Aby zmienić ją na bardziej przyjazną, wejdź w szczegóły konta i poszukaj jego ustawień. Na pokazanym obok ekranie z aplikacji Microsoft Authenticator ustawienia te znajdują się pod ikoną „koła zębatego” . Wprowadź nazwę, która będzie kojarzyć się z systemem CST2021. |  |  |

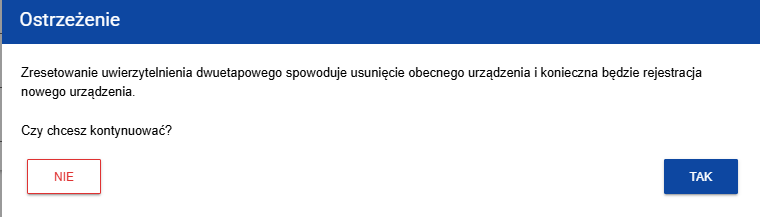
### Wyłączanie i resetowanie uwierzytelniania dwuetapowego (2FA)

Po tym, jak włączysz sobie uwierzytelnianie dwuetapowe, na ekranie edycji profilu w CST2021 znikną przyciski do wyboru metody 2FA. Zamiast tego pojawi się przycisk *Wyłącz 2FA* albo – jeżeli włączono dla Ciebie zobowiązanie do korzystania z uwierzytelniania dwuetapowego – przycisk *Resetuj 2FA*.

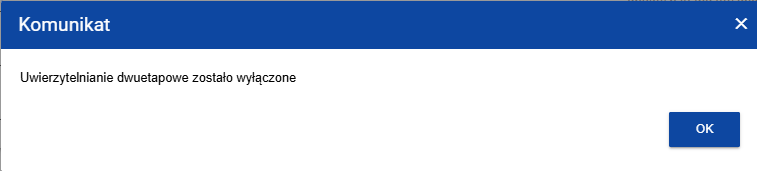
Uwaga! Zmiana metody, aplikacji uwierzytelniającej lub urządzenia z tą aplikacją odbywa się poprzez wyłączenie a następnie ponowne włączenie 2FA. Pamiętaj, żeby zawsze najpierw usuwać 2FA z CST2021 a dopiero potem ze swojej aplikacji uwierzytelniającej. Jeśli usuniesz konto z autentykatora a w CST2021 pozostanie informacja, że 2FA jest włączone, przy logowaniu będziesz musiał użyć kodu zapasowego lub poprosić Administratora systemu o wyłączenie 2FA dla Twojego profilu.

Kliknięcie „Wyłącz 2FA” powoduje rezygnację z dodatkowego zabezpieczenia oraz wylogowanie użytkownika.

Kliknięcie „Resetuj 2FA” również, przy czym najpierw pojawi się ostrzeżenie, że system wymusi (po wylogowaniu i ponownym zalogowaniu) ponowne włączenie 2FA:



Wybór przycisku *Tak* powoduje wyłączenie wybranej metody uwierzytelniania dwuetapowego oraz wyświetlenie komunikatu potwierdzającego, po którym nastąpi wylogowanie:



Włączenie 2FA zwiększa bezpieczeństwo Twojego konta. Nawet jeśli system umożliwia Ci pracę bez niego i nie wymusza ponownego włączenia po tym, jak je sobie wyłączysz, i tak warto je ponownie ustawić po najbliższym zalogowaniu.

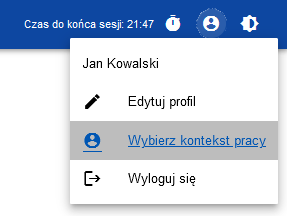
# Wybór kontekstu pracy

Jeśli pracujesz dla różnych organizacji, lub dla jednej organizacji w różnych rolach (np. instytucji oraz beneficjenta) zakres danych które zobaczysz w systemie zależy od tego, w kontekście której organizacji i jakiej jej roli jesteś zalogowany.

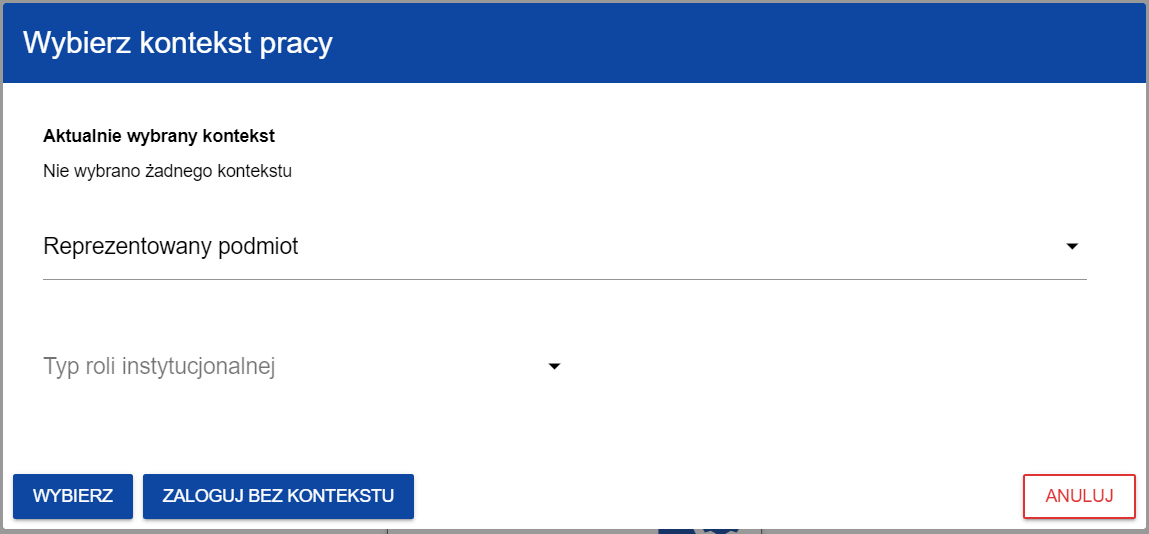
Jeżeli posiadasz tylko jeden kontekst pracy, czyli pracujesz dla jednej organizacji w jednej jej roli, system już przy Twoim pierwszym logowaniu automatycznie wybierze za Ciebie ten kontekst.

Jeżeli posiadasz kilka kontekstów pracy, możesz przełączać się między nimi.

Kliknij ikonę *Menu użytkownika* w prawym górnym rogu ekranu a następnie przycisk *Wybierz kontekst pracy*.



Aplikacja wyświetli nowe okno *Wybierz kontekst pracy.*



W oknie wyboru kontekstu pokazują się tylko aktualne reprezentacje, czyli takie, których termin ważności (nadany przez właściwego Administratora) nie upłynął.

Kontekst wprowadzony przez użytkownika jest zapamiętywany, a następnie wykorzystywany przy ponownym uruchomieniu aplikacji.

W polu *Aktualnie wybrany kontekst* pokazuje się informacja o aktualnie wybranym kontekście pracy lub komunikat *Nie wybrano żadnego kontekstu*. Okno zawiera pola, które należy uzupełnić by wskazać nowy kontekst pracy:

* reprezentowany podmiot – pole typu lista rozwijalna, użytkownik wybiera z listy jeden podmiot;
* typ roli instytucjonalnej – pole typu lista rozwijalna, użytkownik wybiera z listy jeden typ roli instytucjonalnej. Pole jest niedostępne do edycji, jeśli nie został wskazany żaden podmiot w polu *Reprezentowany podmiot*.

Jeżeli na listach nie masz żadnych pozycji do wyboru, oznacza to prawdopodobnie, że Administrator nie przydzielił jeszcze uprawnień lub że Twoje uprawnienia wygasły.

W celu zatwierdzenia wyboru nowego kontekstu pracy, po uzupełnieniu wymienionych powyżej pól kliknij przycisk *Wybierz*. Zmianę kontekstu system potwierdza wyświetleniem komunikatu *Zmieniono kontekst*.

W przypadku nieuzupełnienia któregoś z pól *Reprezentowany podmiot* i/lub *Typ roli instytucjonalnej*, zmiana kontekstu nie zostanie przeprowadzona, a pod nieuzupełnionym polem system wyświetli komunikat wskazujący na konieczność uzupełnienia tego pola.

W ramach okna dostępne są dwa inne przyciski *Zaloguj bez kontekstu* oraz *Anuluj*.

Wybór przycisku *Zaloguj bez kontekstu* powoduje rezygnację z obowiązującego kontekstu i rozpoczęcie pracy bez wskazanego kontekstu. Tylko nieliczni użytkownicy (np. Administratorzy IK UP) mogą posiadać role indywidualne, umożliwiające pracę bez kontekstu. Pozostali użytkownicy po wyborze tej opcji nie będą mogli wykonać w aplikacji żadnych czynności poza edycją danych przy własnym koncie.

Na potwierdzenie dokonanej zmiany system prezentuje komunikat *Zmieniono kontekst*.



Wybór przycisku *Anuluj* powoduje zamknięcie okna *Wybierz kontekst pracy* i powrót do ekranu, z którego wybrałeś wcześniej opcję *Wybierz kontekst pracy*.

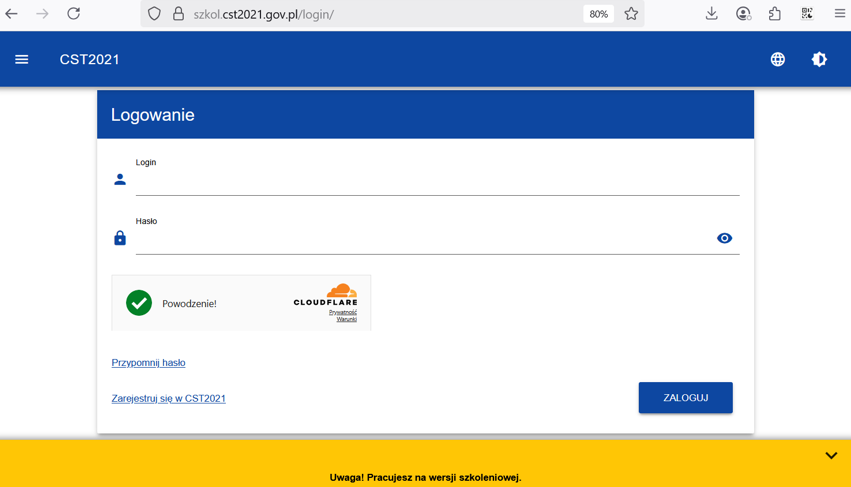
# 

# Komunikaty informacyjne

W SZT mogą być prezentowane komunikaty z ważnymi informacjami dla Użytkowników. Komunikaty są wyświetlane na żółtym pasku umieszczonym na dole poszczególnych ekranów SZT. Brak żółtego paska oznacza, że w danym momencie nie ma dodanych żadnych komunikatów dla Użytkowników.

Komunikaty mogą zawierać linki przenoszące do innych stron. Linki otwierane są w nowych kartach przeglądarki.

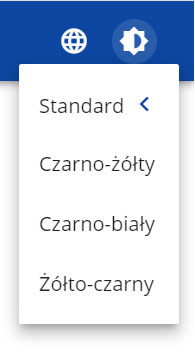
Po zapoznaniu z treścią komunikatów możesz zwinąć pasek, aby nie zasłaniał części ekranu. W celu zwinięcia paska kliknij w ikonę strzałki skierowanej w dół , która znajduje się w prawym górnym rogu żółtego paska. Zwinięty pasek możesz w każdej chwili ponownie rozwinąć klikając w ikonę strzałki skierowanej w górę , która znajduje się po prawej stronie zwiniętego paska.



# Responsywność i dostępność

Wygląd i układ stron dostosowują się automatycznie do rozmiaru okna urządzenia, na którym uruchamiasz aplikacje. Strony są uniwersalne i wyświetlają się prawidłowo zarówno na dużych jak i małych ekranach, na urządzeniach stacjonarnych oraz mobilnych.

Osoby słabowidzące mogą dostosować kontrast do swoich potrzeb. W celu zmiany kontrastu wybierz ikonę zmiany kontrastu w prawym górnym rogu ekranu. Do wyboru są typy z listy:



Wybór jednej z opcji powoduje odpowiednią zmianę kontrastu ekranu. Dla przykładu wybór żółto-czarnej opcji zmieni wygląd ekranu w następujący sposób:

