mMedica

Moduły eRejestracja i eRejestracja+ – instalacja i konfiguracja

Wersja 9.0.0

asseco POLAND

2023-02-15

Spis treści

1. WSTĘP 7

2. ARCHITEKTURA ORAZ WYMAGANIA 9

2.1. MIGRACJA Z WERSJI .NET CORE 3.1 DO .NET 6.0 9

2.2. PUBLIKOWANIE PORTALU 10

2.3. ROZWIĄZANIE PROSTE 10

2.4. ROZWIĄZANIE Z JEDNYM SERWEREM WEBOWYM 11

2.5. ROZWIĄZANIE ROZPROSZONE 11

2.6. WYMAGANIA SPRZĘTOWE ORAZ PROGRAMOWE 12

2.7. ZASADY KOMPATYBILNOŚCI WERSJI OPROGRAMOWANIA 13

2.8. ZASADA DZIAŁANIA ASP .NET CORE Z SERWERAMI WWW 14

2.8.1. Hosting w procesie 14

2.8.2. Hosting poza procesem 14

2.9. KOMPONENT MMDAB 15

3. INSTALACJA DLA WINDOWS 16

3.1. INSTALACJA W SYSTEMACH WINDOWS 16

3.2. WYMAGANIA 16

3.3. INSTALACJA SERWERA IIS 17

3.4. INSTALACJA ASP .NET CORE WRAZ Z MODUŁEM IIS 20

3.5. INSTALACJA IIS PO INSTALACJI ASP .NET CORE 23

3.6. KB2533623 DLA WINDOWS 8.1, WINDOWS SERVER 2012 R2 24

3.7. KB3118401 DLA WINDOWS 8.1 25

3.8. INSTALACJA ZA POMOCĄ INSTALATORA 25

3.9. INSTALACJA DODATKOWYCH MODUŁÓW/KOMPONENTÓW 32

3.10. INSTALACJA MANUALNA 34

3.11. KONFIGURACJA NAZWY APLIKACJI 44

3.12. WERYFIKACJA INSTALACJI 45

3.13. DODATKOWA KONFIGURACJA IIS 47

3.13.1. Konfiguracja typów MIME w IIS 47

3.13.2. Konfiguracja certyfikatu SSL 49

3.13.3. Zaawansowana konfiguracja witryn 50

3.13.4. Zaawansowana konfiguracja aplikacji 52

3.14. DOINSTALOWANIE KOMPONENTÓW 55

3.15. RESTARTOWANIE I ZATRZYMYWANIE KOMPONENTÓW 56

3.16. AKTUALIZACJA MODUŁU 56

3.17. ZMIANA SPOSOBU HOSTINGU 57

4. INSTALACJA W DYSTRYBUCJACH LINUX 58

4.1. WYMAGANIA ... 58
4.2. INSTALACJA ... 58
4.3. INSTALACJA BAZY DANYCH EREJESTRACJA ... 58
4.4. INSTALACJA WYMAGANEGO OPROGRAMOWANIA ... 59
4.5. KONFIGURACJA SERWERA ORAZ INSTALACJA MODUŁU ... 60
4.6. KONFIGURACJA NAZWY APLIKACJI ... 62
4.7. KONFIGURACJA ADRESU APLIKACJI ... 63
4.8. WERYFIKACJA INSTALACJI ... 63
4.9. KONFIGURACJA DODATKOWA APACHE ... 66
4.9.1. Konfiguracja typów MIME ... 66
4.9.2. Konfiguracja certyfikatu SSL ... 66
4.9.3. Zaawansowana konfiguracja witryn ... 67
4.10. DOINSTALOWANIE KOMPONENTÓW ... 69
4.11. KONFIGURACJA WIELU PORTALI NA JEDNYM SERWERZE ... 69
4.12. RESTARTOWANIE I ZATRZYMYWANIE KOMPONENTÓW ... 70
4.13. AKTUALIZACJA MODUŁU ... 70
4.14. POMOC ... 70

5. KONFIGURACJA APLIKACJI ... 72

5.1. KONFIGURACJA POŁĄCZENIA Z BAZAMI DANYCH ... 72
5.2. ZABEZPIECZENIE PRZED UŻYCIEM IFRAME ... 72
5.3. KONFIGURACJA NAZWY ORAZ ADRESU APLIKACJI ... 73
5.4. KONFIGURACJA STRONY OFFLINE ... 73
5.5. KONFIGURACJA PULI PORTÓW DLA MODUŁÓW WEWNĘTRZNYCH MMDAB ... 74
5.6. ZAAWANSOWANA KONFIGURACJA MODUŁÓW WEWNĘTRZNYCH MMDAB ... 74
5.7. PRZEKIEROWANIE NAGŁÓWKÓW Z PROXY ... 74
5.8. URUCHAMIANIE WIELU MODUŁÓW WEWNĘTRZNYCH TEGO SAMEGO TYPU PRZEZ MMDAB ... 75

6. ZARZĄDZANIE ORAZ KOPIE ZAPASOWE BAZ DANYCH ... 77

6.1. KOPIE BAZY DANYCH ... 77
6.1.1. Wykonywanie kopii bazy danych ... 77
6.1.2. Odtwarzanie bazy danych ... 77
6.1.3. Operacje na zdalnym serwerze PostgreSQL ... 78
6.1.4. Uproszczenie wykonywania kopii ... 78

7. BEZPIECZEŃSTWO MODUŁU ... 80

7.1. INFRASTRUKTURA ... 80
7.1.1. Zewnętrzny hosting lub VPS ... 80
7.1.2. Protokół SSL ... 80
7.1.3. VPN ... 81
7.2. OPROGRAMOWANIE ... 81

7.2.1. Konta użytkowników ... 81
7.2.2. Oprogramowanie antywirusowe ... 81
7.2.3. Firewall ... 81
7.2.4. Nieużywane protokoły TCP IP oraz protokoły serwera WWW ... 82
7.2.5. Poczta wychodząca ... 83
7.3. KONFIGURACJA MODUŁU ... 83
7.4. ZABEZPIECZENIA MODUŁU ... 83
7.4.1. Token bezpieczeństwa ... 83
7.4.2. Blokowanie adresów IP oraz kont ... 84
7.4.3. Zabezpieczenie przed spamem ... 84
7.4.4. Inne ... 84
7.5. FILTROWANIE KOMUNIKACJI Z WYBRANYMI ADRESAMI IP ... 85
7.5.1. Filtrowanie komponentów ... 85
7.5.2. Filtrowanie logowania administratora ... 86
7.6. WYMUSZENIE KORZYSTANIA Z PROTOKOŁU HTTPS ... 88
7.7. POZOSTAŁE ZALECENIA ... 89

8. KONFIGURACJA W PORTALU ... 90

8.1. PIERWSZE URUCHOMIENIE ... 90
8.1.1. Konfiguracja programu mMedica ... 93
8.1.2. Dodawanie świadczeniodawcy do Portalu ... 94
8.2. MOJE KONTO ... 94
8.2.1. ZMIEŃ DANE ... 95
8.2.2. Zmiana hasła ... 96
8.2.3. Weryfikacja dwuskładnikowa ... 96
8.2.4. Powiąż z ePUAP\PZ ... 98
8.2.5. Sesje użytkownika ... 99
8.3. ZARZĄDZANIE ... 101
8.3.1. Świadczeniodawcy ... 102
8.3.2. Dziennik systemowy ... 105
8.3.3. Rejestr użytkowników ... 112
8.3.4. Personel medyczny ... 124
8.3.5. Rejestr zablokowanych IP ... 126
8.3.6. Grafik dla trybu offline ... 127
8.3.7. Masowe wiadomości ... 128
8.3.8. Kopie zapasowe bazy danych ... 133
8.3.9. Konfiguracja ... 134
8.3.10. Zawartość strony ... 158
8.3.11. Zarządzanie podmiotami ... 173
8.3.12. Statystyki ... 189

8.4. NIEZGODNOŚĆ WERSJI BAZY DANYCH Z WERSJĄ APLIKACJI 212
8.5. KONFIGURACJA EPUAP\PZ 213
8.5.1. Podmiot publiczny ePUAP oraz uprawnienia dla środowiska produkcyjnego 214
8.5.2. Konfiguracja w Portalu eRejestracja 215

9. PERSONEL 216

9.1. DODANIE DO PORTALU I PIERWSZE LOGOWANIE 216
9.2. MOJE KONTO 216
9.2.1. Zmień dane 216
9.2.2. Zmień hasło 217
9.2.3. Weryfikacja dwuskładnikowa 217
9.3. WOLNE TERMINY 218
9.4. PLAN WIZYT 220

10. KOMUNIKACJA ORAZ SYNCHRONIZACJA DANYCH 226

10.1. MODELE KOMUNIKACJI MMEDICA 226
10.2. MODEL KOMUNIKACJI Z EARCHIWUM 228
10.3. MODEL KOMUNIKACJI Z CHMURĄ DLA ZDROWIA 228
10.4. DIAGNOSTYKA KOMUNIKACJI 229
10.5. ZASADY SYNCHRONIZACJI DANYCH Z BAZĄ MMEDICA 229

11. POBIERANIE DANYCH DIAGNOSTYCZNYCH 231
12. ROZWIĄZANIA CZĘSTYCH PROBLEMÓW 231

12.1. NIEPRAWIDŁOWE HASŁO USŁUG SIECIOWYCH (TOKEN) 231
12.2. PROBLEM Z BRAKIEM LICENCJI NA MODUŁ 231
12.3. NIE POBIERAJĄ SIĘ WOLNE TERMINY 232
12.4. BRAK TERMINÓW W GRAFIKU OFFLINE 232
12.5. BRAK SPECJALNOŚCI 232
12.6. BRAK PERSONELU 232
12.7. NIEPRAWIDŁOWE NAZWY SPECJALNOŚCI 232
12.8. PROBLEM Z DODANIEM LUB ODŚWIEŻENIEM ŚWIADCZENIODAWCY 232
12.9. ZAPOMNIANE HASŁO DO KONTA ADMINISTRATORA 233
12.10. PROBLEM Z WYSYŁANIEM WIADOMOŚCI E-MAIL (SMTP) 233
12.11. PROBLEM Z WYSYŁANIEM WIADOMOŚCI SMS 233
12.12. PROBLEM Z UTWORZENIEM UŻYTKOWNIKA W PORTALU Z POZIOMU MMEDICA 233
12.13. PROBLEM Z WYKONANIEM PROCEDURY SERWISOWEJ 233
12.14. MAPY NIE WYŚWIETLAJĄ SIĘ POPRAWNIE 234
12.15. WYŁĄCZANIE POWIADOMIEŃ SMS 234
12.16. ZDUPLIKOWANY PERSONEL 234
12.17. ZDUPLIKOWANE SPECJALNOŚCI 234
12.18. ZMIANA TREŚĆ WIADOMOŚCI E-MAIL LUB SMS 234

12.19. Zmiana nazwy świadczeniodawcy ... 234
12.20. Nieprawidłowe ustawienia Portalu – odtwórz. kopii bazy danych eRejestracji ... 235
12.21. Biała strona komponentu po instalacji przez instalator na IIS ... 235
12.22. Błąd 403.4 na localhost lub na adresie komponentu na IIS ... 235
12.23. Błąd 500.21 w IIS ... 235
12.24. Błąd 502.19 w IIS ... 235
12.25. Błąd 502.5 w IIS ... 236
12.26. Polecenie dotnet nie jest rozpoznawalne – Linux ... 236
12.27. Status serwisu Main process exited – Linux ... 236
12.28. Invalid command 'ProxyPreserveHost' – Linux ... 237
12.29. Brak portu w statusie usługi – Linux ... 237
12.30. Strona jest widoczna wyłącznie z komputera lokalnego ... 237
12.31. Błąd podczas zapisu strony offline ... 237
12.32. Błąd podczas zapisu własnego stylu strony ... 237
12.33. Przekroczenie czasu realizacji operacji na bazie danych (timeout) ... 238
12.34. Problem z podpisem kwalifikowanym – Java ... 238
12.35. Problem z mMDAB i mMWS na IIS ... 239
12.36. Brak pliku api-ms-win-crt-runtime-l1-1-0 – Windows ... 241
12.37. Błąd „Unspecified certificate from client” w mMedica ... 241

1. Wstęp

Niniejsza instrukcja opisuje architekturę, proces instalacji oraz konfiguracji modułów eRejestracja i eRejestracja+. Dokument dostarcza również informacji dotyczących bezpieczeństwa.

Moduły eRejestracja i eRejestracja+ są nowoczesnymi systemami, nazywanymi popularnie rejestracją internetową, umożliwiającymi umawianie się na wizyty drogą elektroniczną bez konieczności wychodzenia z domu. To bezpieczne i skuteczne rozwiązanie, które przynosi korzyści zarówno pacjentowi, jak i placówce. Co najważniejsze, systemy eRejestracja i eRejestracja+ są zgodne z wymogami Ministerstwa Zdrowia określonymi w Rozporządzeniu MZ z dnia 19 kwietnia 2013 r. Dzięki temu wdrożenie rejestracji internetowej pozwala spełnić ustawowy obowiązek określony w artykule 23a Ustawy z dnia 27 sierpnia 2004 r.

Moduły eRejestracja i eRejestracja+ mogą być stosowane nie tylko w celu realizacji ustawowego obowiązku udostępniania takiej metody umawiania się na wizyty. Dzięki zastosowaniu zaawansowanych rozwiązań stworzono narzędzie uniwersalne, a przy tym niezwykle bezpieczne. Internetowa część aplikacji została skutecznie oddzielona od głównej bazy danych mMedica. Za synchronizowanie informacji o dokonanych rejestracjach i aktualizację danych o dostępności poszczególnych terminów, odpowiada specjalnie w tym celu zaprojektowany system komunikacji.

Najistotniejsze jest, że moduły eRejestracja i eRejestracja+ w pełnym zakresie współpracują z terminarzem i harmonogramami zdefiniowanymi w mMedica, jednocześnie pozwalając na swobodne decydowanie, które terminarze będą dostępne w Internecie, a które tylko lokalnie. Oczywiście aktualizacja informacji o dostępnych i zarezerwowanych terminach jest w pełni automatyczna i nie wymaga wykonywania żadnych dodatkowych działań. Zastosowanie modułów eRejestracja i eRejestracja+ może istotnie ułatwić pracę w rejestracji i umożliwić pacjentom samodzielne planowanie wizyt w najbardziej dostosowanych do ich potrzeb terminach.

Moduły eRejestracja i eRejestracja+ dają możliwość umówienia się na wizytę do lekarza drogą elektroniczną bez konieczności wychodzenia z domu. Rejestracja on-line jest dostępna 24 godziny na dobę 7 dni w tygodniu, dzięki czemu pacjent może dokonać rejestracji na wizytę w dogodnym dla siebie czasie i miejscu, mając jedynie dostęp do Internetu. Pacjent po zalogowaniu na własne konto, ma możliwość wyszukiwania wolnych terminów do interesujących go specjalistów i przeglądania listy własnych rezerwacji, oraz ich modyfikacji. Użytkownicy eRejestracji mogą także dokonywać szybkich rezerwacji, zmieniać je lub odwoływać bez logowania na konto. Ponadto pacjenci korzystający z leków stale podawanych mogą zamawiać recepty drogą internetową. Na portalu da się także wyświetlać: skierowania, eSkierowania, eZlecenia na wyroby medyczne, udostępnione dokumenty, eRecepty, planowane i wykonane szczepienia oraz zalecenia lekarskie.

Oprócz tego, pacjenci mają możliwość wysyłania wniosków. Użytkownicy eRejestracji mogą korzystać również z funkcjonalności dla teleporad, związanych z wykonywaniem wizyt poprzez wyznaczone do tego kanały komunikacji.

Korzyści wynikające z używania modułów eRejestracja i eRejestracja+ dla podmiotu leczniczego są bezsporne. Kluczowym atutem jest oszczędność czasu personelu oraz zmniejszenie prawdopodobieństwa wystąpienia pomyłek podczas rejestracji pacjenta. Rejestracja internetowa znacząco wpływa na zmniejszenie kolejek w przychodni, dzięki czemu pracownicy rejestracji mogą skupić się na bieżących sprawach i problemach pacjentów znajdujących się w placówce.

Na usprawnienie pracy w przychodni wpływa również funkcjonalność automatycznego przenoszenia rezerwacji do Terminarza w mMedica, co skutkuje brakiem konieczności ich powtórnego rejestrowania. Ponadto, każda osoba zakładająca konto na portalach eRejestracji lub eRejestracji+, jest automatycznie wprowadzana do kartoteki pacjentów, dzięki czemu personel weryfikuje jedynie tożsamość pacjenta podczas jego wizyty w przychodni. Kolejnym udogodnieniem jest możliwość wysyłania masowych wiadomości e-mail przez administratora Portalu, w celu przekazania pacjentom ważnych informacji dotyczących np. funkcjonowania poradni.

Elastyczność i duże możliwości dostosowania do indywidualnych potrzeb pozwalają na stosowanie systemów eRejestracja i eRejestracja+ w gabinetach i przychodniach o bardzo zróżnicowanym zakresie realizowanych świadczeń.

2. Architektura oraz wymagania

Moduł eRejestracja (eR) składa się z trzech komponentów oraz dedykowanej bazy danych. W skład modułu wchodzą:

- Portal – aplikacja webowa, która łączy się z bazą danych eR, zawiera w sobie usługę sieciową eRWS,
- mMWS – usługa sieciowa pośrednicząca w dostępie do bazy danych mMedica,
- mMDAB – usługa sieciowa, która zarządza i uruchamia inne usługi sieciowe pośredniczące w dostępie do bazy danych mMedica np. mMWS.

Portal jest stroną internetową dla użytkowników (pacjentów oraz administratorów), z kolei mMWS (zawarty w mMDAB) zapewnia komunikację pomiędzy modułem eRejestracja a oprogramowaniem mMedica. Wszystkie komponenty eRejestracji mogą być uruchamiane za pomocą platformy .NET firmy Microsoft na wspieranych systemach operacyjnych Microsoft Windows oraz wybranych dystrybucjach systemów opartych o jądro Linux.

Jedna instancja Portalu przypada na jedną bazę danych eR. Z kolei usług sieciowych mMWS musi być tyle, ile jest podłączonych baz danych mMedica. Innymi słowy, liczba usług mMWS jest determinowana przez liczbę podłączonych baz mMedica do Portalu. W zależności od wymagań oraz możliwości klienta, eR może zostać skonfigurowana na wiele sposobów.

2.1. Migracja z wersji .NET Core 3.1 do .NET 6.0

Migracja do .NET 6.0 wymaga od użytkownika zainstalowania nowej wersji środowiska uruchomieniowego ASP .NET Core 6.0. W przypadku instalacji mModułów pod IIS, należy zainstalować wersję Bundle-Hosting\WindowsHosting - odnośnik. W trybie aktualizacji instalator mModułów jest w stanie sam pobrać i zainstalować nową wersję ASP .NET Core 6.0, jeśli taka nie została wcześniej zainstalowana. Proces instalacji oraz aktualizacji odbywa się w bardzo zbliżony sposób do poprzednich wersji. Odpowiednie kroki zostały opisane w działach *3. Instalacja dla Windows* oraz *4. Instalacja w dystrybucjach Linux*.

Wraz z wprowadzeniem .NET 6.0 zakończone zostało wsparcie dla przeglądarki Internet Explorer.

Uwaga: Przed wykonaniem procesu migracji, należy bezwzględnie wykonać kopię bazy danych modułu eRejestracja.

Uwaga: Istnieje możliwość posiadania jednocześnie zainstalowanego środowiska uruchomieniowego .NET Core 3.1 oraz .NET 6.

2.2. Publikowanie Portalu

Portal należy w uproszczeniu traktować jako stronę internetową, co oznacza, że podlega ona takim samym zasadom udostępniania w sieci Internet za pomocą serwerów WWW. Serwer WWW to oprogramowanie pozwalające opublikować stronę internetową w taki sposób, aby mogła ona być widoczna dla przeglądarek internetowych, które są zainstalowane na innych komputerach. Serwer WWW może być zainstalowany zarówno na komputerze użytkowym (np. wykorzystującym oprogramowanie mMedica), jak i specjalnie do tego dedykowanym. Komponenty modułu będą widoczne dla innych komputerów tak długo, jak komputer będzie uruchomiony i podłączony do sieci internetowej. Wymogiem, aby komponenty były widoczne w sieci Internet, jest posiadanie publicznego (najlepiej stałego) adresu IP. Jednym z rozwiązań jest skorzystanie z usług hostingowych lub wirtualnych prywatnych serwerów (VPS), czyli zazwyczaj odpłatnych usług, w których firma zewnętrzna umieszcza w swoich zasobach strony internetowe oraz usługi sieciowe.

Komponenty eRejestracji mogą mieć adres domenowy, czyli przyjazną do zapamiętania nazwę, po wpisaniu której zostaną one wyświetlone. Adres domenowy może zostać wykupiony (często w pakiecie z usługą hostingową) poprzez zewnętrzny podmiot. Bez wykorzystywania adresu domenowego dostęp do komponentów możliwy jest przez adres IP komputera, na którym zostały zainstalowane komponenty modułu. Aby móc korzystać z bezpiecznego, szyfrowanego połączenia internetowego (HTTPS) należy dokonać zakupu certyfikatu SSL u zaufanego dostawcy.

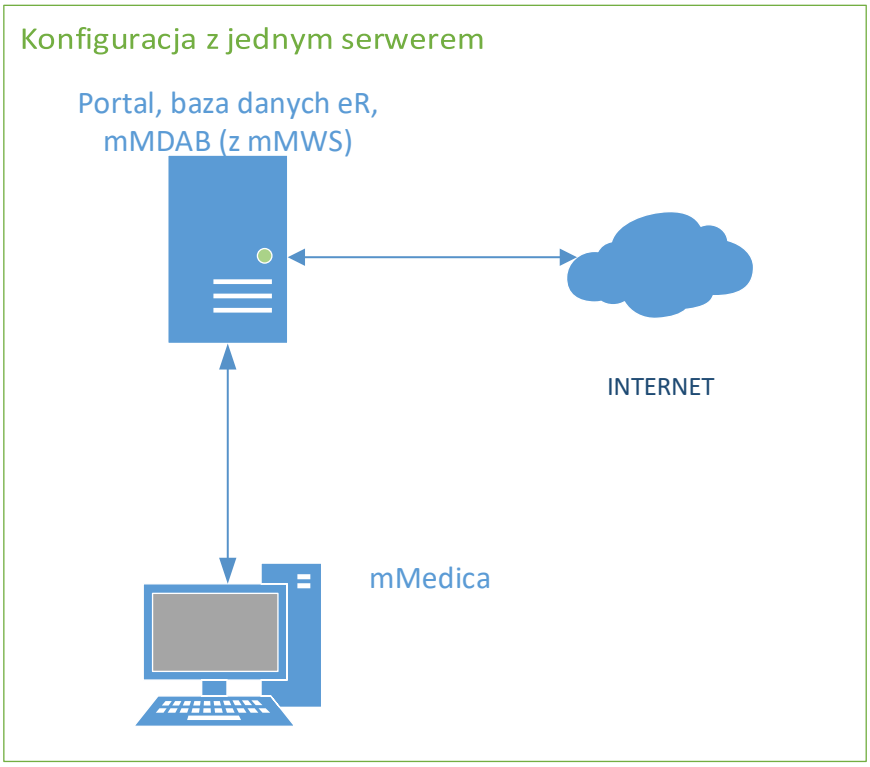
Instalacja oraz konfiguracja nieodpłatnych serwerów WWW, konfiguracji SSL oraz adresów domenowych została opisana w rozdziale *3. Instalacja dla Windows* oraz *4. Instalacja w dystrybucjach Linux.* Zalecenia dotyczące bezpieczeństwa oraz korzyści związanych z wykorzystywaniem SSL zostały opisane w rozdziale *7. Bezpieczeństwo modułu.*

2.3. Rozwiązanie proste

Najprostszą konfiguracją jest instalacja programu mMedica wraz z bazą danych oraz modułem eR na jednym komputerze. Jest to najprostsza, ale jednocześnie najbardziej obciążająca system konfiguracja. Dodatkowo jest ona niezalecana ze względów bezpieczeństwa.

2.4. Rozwiązanie z jednym serwerem webowym

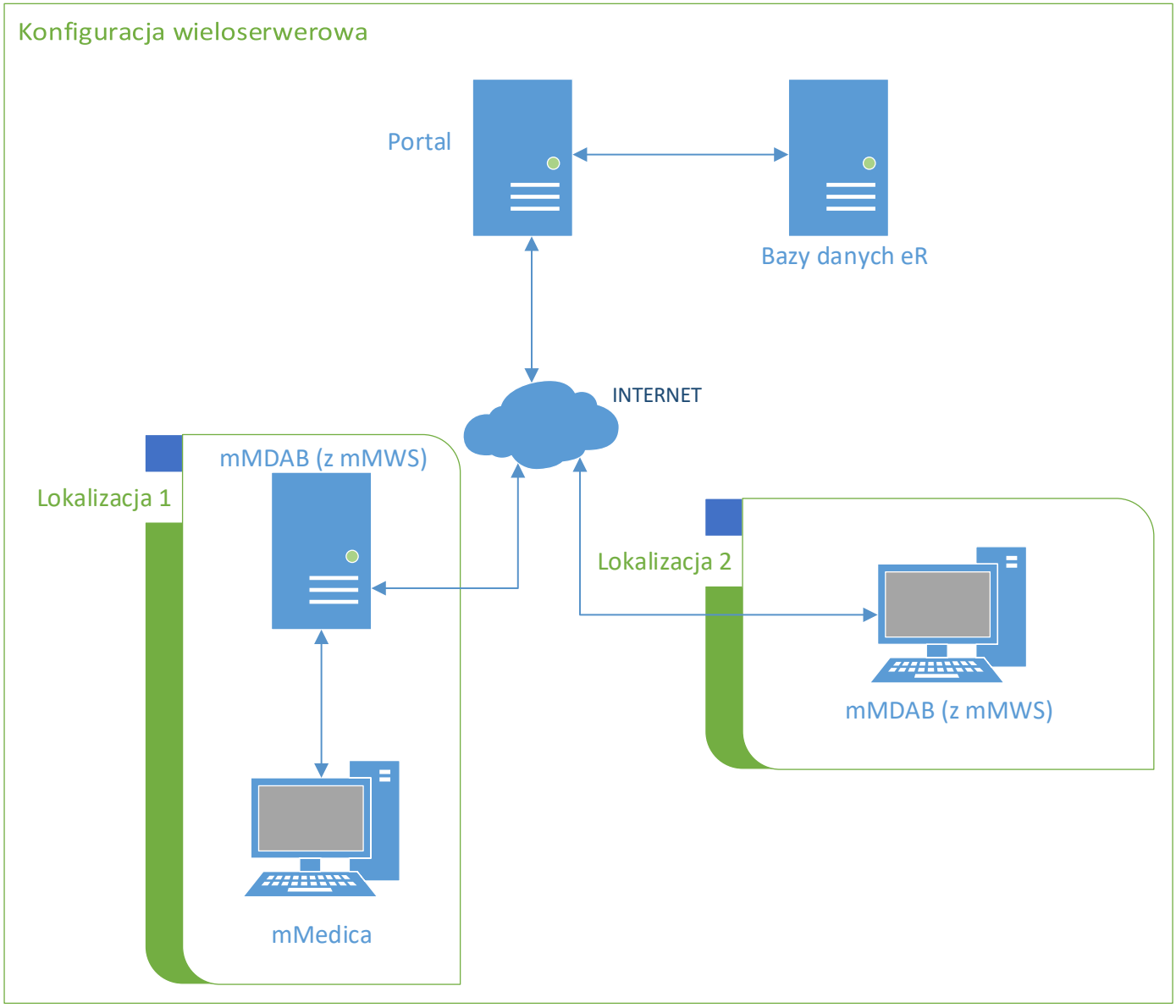
Konfiguracja zakłada zainstalowanie modułu eRejestracji na dedykowanym do tego serwerze (*Rysunek 1*). Serwer, z punktu widzenia sieci Internet, udostępnia wyłącznie Portal, natomiast mMDAB (zawierający mMWS) nie są widoczne z zewnątrz. Baza mMedica jest zainstalowana na komputerze i udostępniona tylko w sieci wewnętrznej z uwzględnieniem serwera WWW.



Rysunek 1: Konfiguracja jednego serwera webowego

2.5. Rozwiązanie rozproszone

Architektura przedstawia przykładowe rozwiązanie w przypadku użycia wielu świadczeniodawców podpiętych do jednego Portalu (*Rysunek 2*). W tej konfiguracji dla bazy danych eRejestracji jest utworzony dedykowany serwer, który nie jest dostępny dla sieci Internet. Każda z lokalizacji zawiera własną bazę danych mMedica oraz mMDAB (z mMWS), który jest dostępny z Internetu. Portal jest dostępny z Internetu.



Rysunek 2: Konfiguracja wieloserwerowa

2.6. Wymagania sprzętowe oraz programowe

Nie jest możliwe precyzyjne określenie wymagań sprzętowych modułu eRejestracja. Wynika to m.in. z obciążenia ruchem Portalu, liczby komponentów, różnych rozwiązań architektonicznych oraz innych usług zainstalowanych na komputerze.

Wymagania programowe są zależne od systemu operacyjnego, z tego powodu zostały one umieszczone w rozdziałach instalacji dla każdego z systemów operacyjnych.

Uwaga: Komponenty mogą być instalowane na różnych systemach operacyjnych, np. Portal na dystrybucji Linux, z kolei mMDAB na systemie z rodziny Microsoft Windows.

Uwaga: Wszystkie systemy operacyjne, na których są zainstalowane komponenty eRejestracji oraz serwery baz danych, powinny mieć ustawioną tę samą strefę czasową i możliwie maksymalnie zbliżoną datę oraz czas.

2.7. Zasady kompatybilności wersji oprogramowania

Wersje komponentów eRejestracji powinny być zawsze takie same. Z kolei wersje oprogramowania mMedica oraz eRejestracja muszą być ze sobą kompatybilne, czyli w możliwie równych wersjach. Wbudowane mechanizmy blokują komunikację pomiędzy oprogramowaniem, gdy dwie pierwsze liczby wersji różnią się. Przykład zamieszczono w tabeli poniżej:

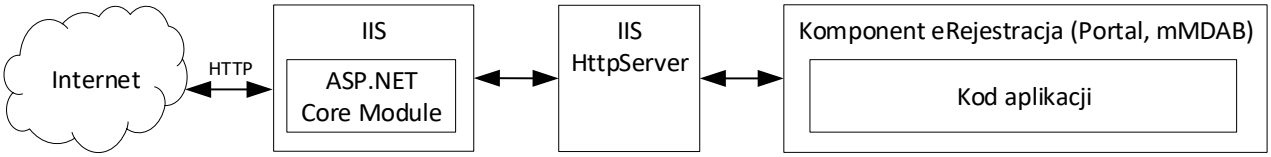
Wersja mMedica	Wersja eRejestracja	Kompatybilność
5.8.0	**5.8**.0	Tak
5.7.2	**5.7**.0	Tak
5.8.0	**5.7**.0	Nie

2.8. Zasada działania ASP .NET Core z serwerami WWW

Każdy z komponentów eR może działać w jednym z dwóch trybów.

2.8.1. Hosting w procesie

Tryb ten dotyczy jedynie systemów Windows oraz serwera IIS. W trybie tym komponenty eR uruchamiane są wewnątrz procesu IIS. Wyeliminowanie komunikacji poprzez serwer proxy pozwala na zapewnienie większej wydajności.

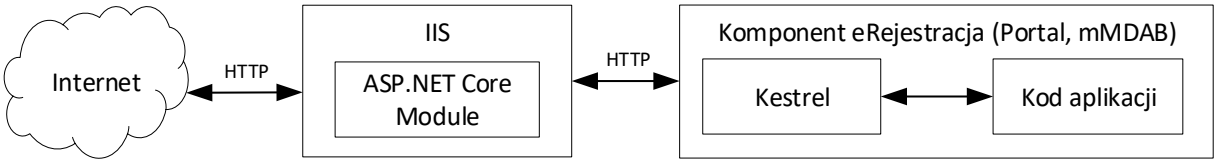


Rysunek 3: Hosting w procesie

2.8.2. Hosting poza procesem

Pliki każdego z komponentów eR zawierają wbudowany serwer WWW o nazwie Kestrel, którego zadaniem jest uruchamianie komponentów oraz pośredniczenie w ruchu pomiędzy nimi a właściwym serwerem WWW. Kestrel w domyślnej konfiguracji nasłuchuje wyłącznie ruchu sieciowego w obrębie lokalnego komputera. Ze względu bezpieczeństwa oraz znaczących ograniczeń, Kestrel nie powinien mieć upublicznionego połączenia do sieci Internet bez właściwego serwera WWW.

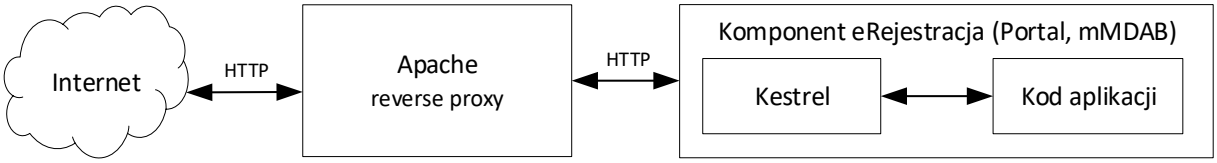
W przypadku instalacji dla systemów rodziny Windows, zalecanym serwerem jest Internet Information Services (w skrócie IIS), a uogólniony schemat z Kestrel został przedstawiony na *Rysunek 4*.



Rysunek 4: Kestrel - połączenie z IIS

Domyślnie jedynie komponent mMDAB uruchamiany jest w tym trybie na systemach Windows.

Dla dystrybucji Linux zalecanym serwerem WWW jest Apache. Połączenie Apache z Kestrel zostało opisane na *Rysunek 5*.

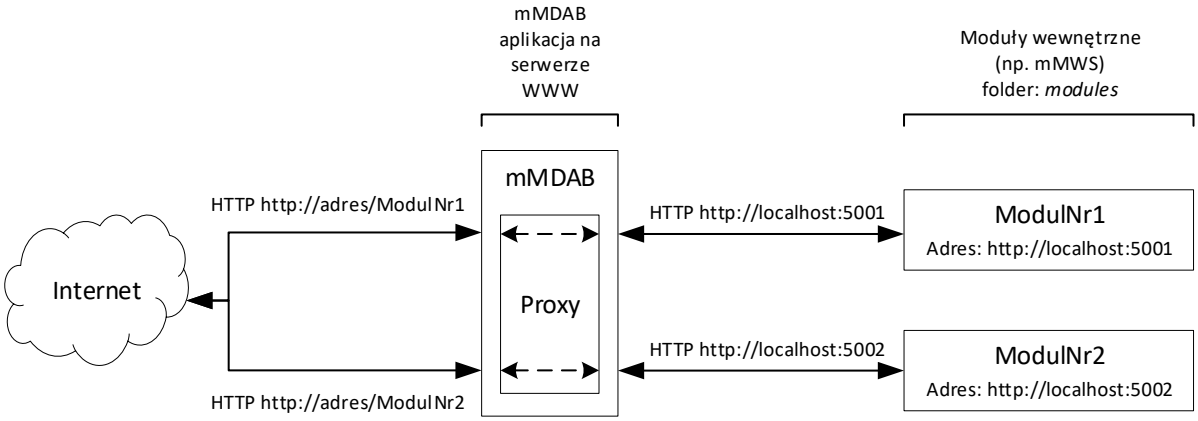


Rysunek 5: Kestrel - połączenie z Apache

Szczegóły instalacji oraz konfiguracji wymaganego oprogramowania zostały przedstawione w rozdziałach: *3. Instalacja dla Windows* oraz *4. Instalacja w dystrybucjach Linux*.

2.9. Komponent mMDAB

Komponent ma za zadanie ułatwić dodawanie nowych usług sieciowych (modułów wewnętrznych), które komunikują się z bazą danych mMedica. Aplikacja uruchamia podczas startu wewnętrzne moduły znajdujące się w jej strukturze katalogów (katalog *modules*) takie jak np. mMWS. Moduły wewnętrzne są uruchamiane tak, że akceptują wyłącznie ruch sieciowy wewnątrz komputera. mMDAB jest pośrednikiem w komunikacji do modułów wewnętrznych, tzn. przekierowuje do nich zgodnie z zasadą, że komunikacja na adres http://adres.szyny/PrzykladowyModul jest przekierowana do modułu wewnętrznego o nazwie PrzykladowyModul.



Rysunek 6: Zasada działania mMDAB

Konsekwencją takiego rozwiązania jest to, że skonfigurowany w aplikacji serwera WWW musi być wyłącznie mMDAB, a nie wszystkie moduły wewnętrzne.

3. Instalacja dla Windows

3.1. Instalacja w systemach Windows

Proces instalacji modułów mMedica w systemach Microsoft Windows może zostać wykonany za pomocą dedykowanego instalatora, który zainstaluje bazę danych oraz wszystkie komponenty modułu wraz z ich uruchomieniem na serwerze WWW Menedżer internetowych usług sieciowych (IIS). Możliwa jest również manualna instalacja oraz konfiguracja modułu z wykorzystaniem plików eRejestracji. W takim przypadku instalator modułu jest wykorzystywany wyłącznie do instalacji bazy danych.

Instalator mModuły nie tylko instaluje moduł, ale również dokonuje procesu aktualizacji plików oraz bazy danych modułu. Aktualizacja dotyczy wyłącznie komponentów, które zostały zainstalowane za pomocą instalatora.

3.2. Wymagania

Przed przystąpieniem do instalacji modułów mMedica należy sprawdzić, czy zostały zainstalowane następujące elementy:

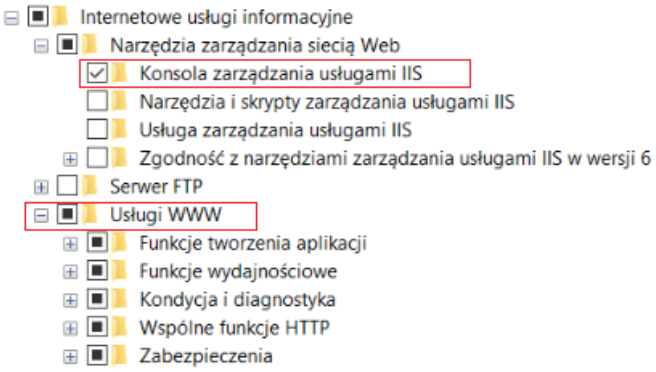
- System operacyjny (32 lub 64-bitowy): Windows 8.1, Windows Server 2012 R2, Windows 10, Windows Server 2016, Windows Server 2019, Windows 11, Windows Server 2022 (więcej informacji: https://docs.microsoft.com/pl-pl/dotnet/core/install/windows?tabs=net60).
- Dla systemu Windows 8.1 wymagany jest pakiet KB3118401 (więcej informacji: *3.7 25KB3118401 dla Windows 8.1*).
- Java Runtime Environment (JRE) w wersji 1.8 (zaleca się instalacje wersji 64-bitowej dystrybucji Oracle JRE lub RedHat OpenJDK).
- VC ++ Redistributable.
- Universal C Runtime w najnowszej dostępnej wersji (więcej informacji: https://support.microsoft.com/pl-pl/help/2999226/update-for-universal-c-runtime-in-windows).
- Serwer WWW: Menedżer internetowych usług sieciowych (w skrócie IIS, angielska nazwa: Internet Information Services) w wersji 7 lub wyższej – opis instalacji w *3.3. Instalacja serwera IIS*).
- ASP .NET Core Runtime w wersji 6.0 wraz z modułem dla IIS (patrz: *3.4. Instalacja ASP .NET Core wraz z modułem* IIS).

Uwaga: System operacyjny wraz z jego składnikami powinien być zaktualizowany do najnowszej dostępnej wersji, np. za pomocą funkcjonalności automatycznych aktualizacji.

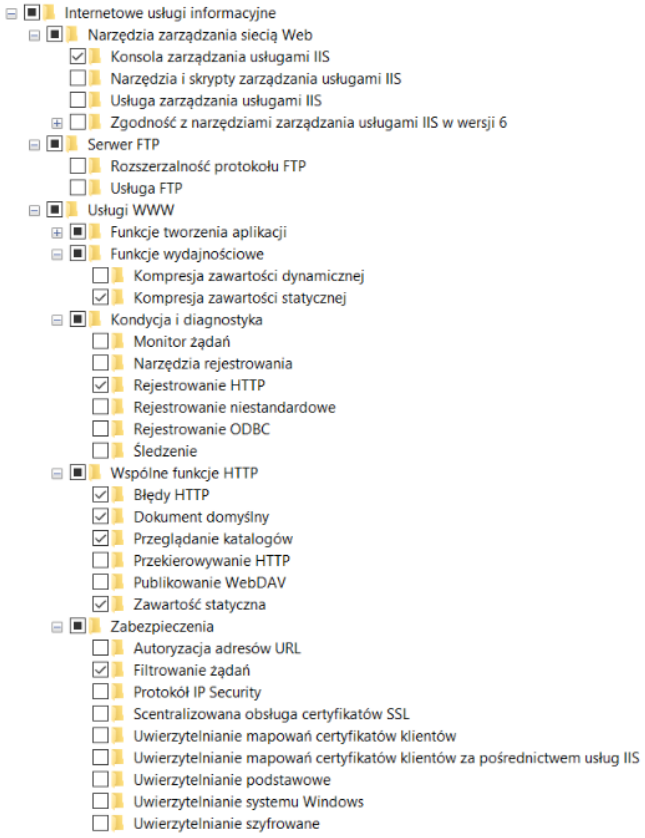
3.3. Instalacja serwera IIS

Niezbędnym krokiem jest przeprowadzenie instalacji serwera WWW. Proces instalacji został opisany poniżej:

1. Uruchomić okno „Włącz lub wyłącz funkcje systemu Windows” - można to zrobić na dwa sposoby:
   a) Menu Start\Panel sterowania\Programy i funkcje, z menu po lewej wybrać „Włącz lub wyłącz funkcje systemu Windows”,
   b) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „optionalfeatures” i zatwierdzić klawiszem Enter.
2. Rozwinąć drzewo funkcji punktu „Internetowe usługi informacyjne”, a następnie zaznaczyć oznaczone kolorem czerwonym zgodnie z *Rysunek 7*:



Rysunek 7: Wymagane komponenty IIS

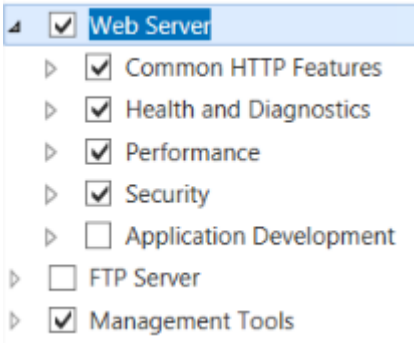


Rysunek 8: Wymagane komponenty IIS - szczegóły

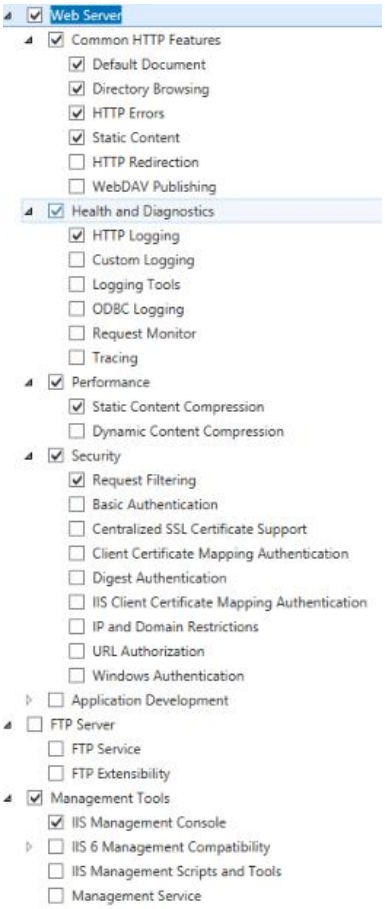
Zatwierdzić okno. Jeżeli wyświetlony zostanie komunikat o konieczności ponownego uruchomienia komputera, należy to wykonać.

Niektóre systemy serwerowe mogą mieć nieco odmienny interfejs włączania funkcji systemu Windows. Po uruchomieniu opcji „Włącz lub wyłącz funkcje systemu Windows” może pojawić się „Kreator dodawania ról i funkcji” (można to również uruchomić z poziomu „Menedżera serwera” – „Dodaj role i funkcje”). Następnie:

a) po lewej stronie wybrać „Wybieranie serwera”, gdzie należy upewnić się, że został zaznaczony właściwy serwer,
b) po lewej stronie wybrać „Role serwera” i na liście zaznaczyć „Web Server (IIS)”, zatwierdzić okno potwierdzenia,
c) z menu po lewej wybrać „Usługi ról” i zaznaczyć odpowiadające pozycje zgodnie z *Rysunek 9*:



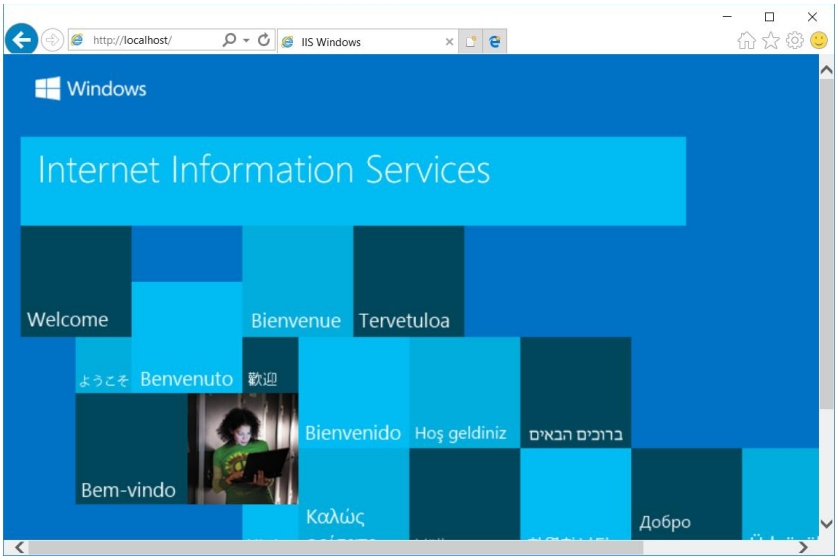
Rysunek 9: Komponenty IIS - Windows Server



Rysunek 10: Wymagane komponenty IIS - Windows Server - szczegóły

d) wybrać ponownie „Potwierdzenie” po lewej stronie (lub nacisnąć przycisk „Dalej >”), a następnie zainstalować komponenty wybierając przycisk „Zainstaluj”.

3. Zweryfikować, czy po wpisaniu „http://localhost” w adres przeglądarki internetowej wyświetli się strona powitalna.



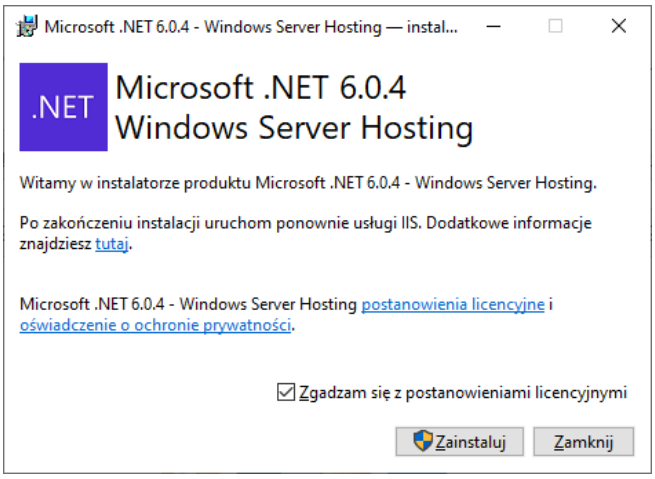
Rysunek 11: Przykładowa strona powitalna IIS

3.4. Instalacja ASP .NET Core wraz z modułem IIS

Uwaga: Po zainstalowaniu środowiska uruchomieniowego ASP .NET Core 6.0 na administratora spada obowiązek aktualizacji tego oprogramowania. Najnowsza wersja środowiska uruchomieniowego ASP .NET Core 6.0 wraz z modułem IIS znajduje na stronie Microsoft: https://dotnet.microsoft.com/en-us/download/dotnet/6.0 (należy wybrać pakiet Hosting Bundle z sekcji ASP.NET Core Runtime w wersji 6.0.X, gdzie X oznacza dowolną podwersję systemu 6.0).

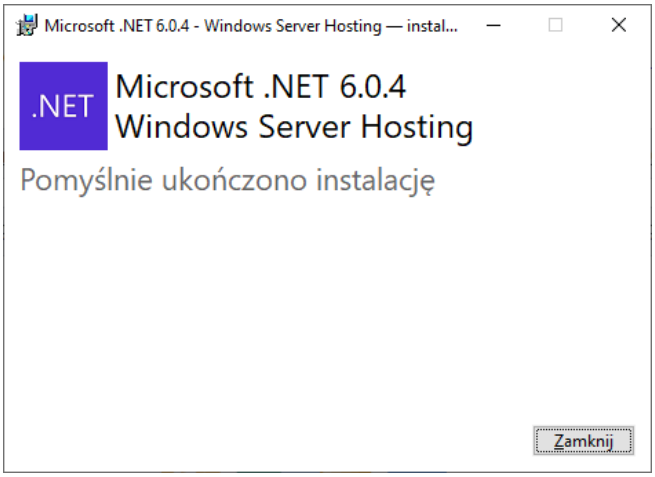
Do działania programu eRejestracja wymagana jest platforma ASP .NET Core w wersji 6.0 wraz modułem IIS o nazwie AspNetCoreModuleV2. Całość jest dostępna w pakiecie instalacyjnym:
https://mmedica-download.asseco.pl/inst/mModuly/dotnet-hosting-win.exe
Proces instalacji pakietu wygląda następująco:

1. Uruchomić pobrany plik z uprawnieniami administratora.
2. Zaznaczyć pole związane z akceptacją licencji i warunków („Zgadzam się…”). Warunki licencji są dostępne po naciśnięciu niebieskich odnośników. Nacisnąć przycisk „Zainstaluj”.



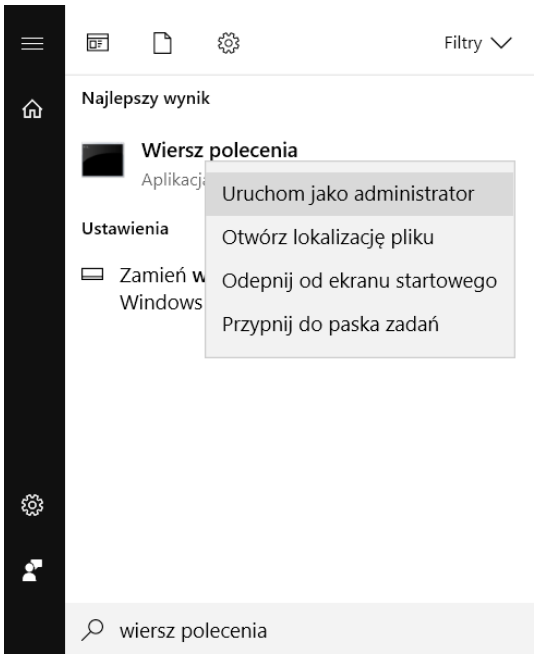
Rysunek 12: Instalacja .NET Core

3. Po instalacji wybrać przycisk „Zamknij”.



Rysunek 13: Instalacja .NET Core - potwierdzenie instalacji

4. W celu uruchomienia modułu dla IIS należy zrestartować serwer IIS (co spowoduje chwilowe zatrzymanie udostępniania witryn). Restart serwera IIS można wykonać poprzez ponowne uruchomienie systemu operacyjnego lub wykonanie poniższych kroków:
    a) uruchomić Wiersz polecenia w trybie administratora,



Rysunek 14: Uruchomienie Wiersz polecenia w trybie administratora - Windows 10

b) zatrzymać usługę IIS wpisując poniże polecenie i zatwierdzając klawiszem Enter,

```
net stop was /y
```

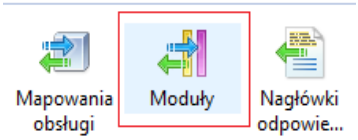
c) uruchomić usługę IIS wpisując poniże polecenie i zatwierdzając klawiszem Enter,

```
net start w3svc
```

d) dokonać weryfikacji instalacji modułu IIS uruchamiając panel zarządzania IIS w jeden z poniższych sposobów:

- Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
- Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).

e) w oknie środkowym odnaleźć opcję „Moduły”,



Rysunek 15: IIS - moduły

f) jeśli na liście znajduje się pozycja o nazwie „AspNetCoreModuleV2” oznacza to, że moduł dedykowany dla .NET Core został zainstalowany pomyślnie.

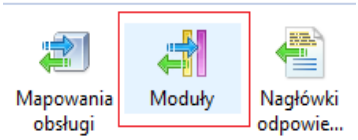
Rysunek 16: Moduł IIS - weryfikacja

Uwaga: .NET może być zainstalowany równolegle z .NET Framework.

3.5. Instalacja IIS po instalacji ASP .NET Core

W przypadku, w którym w pierwszej kolejności został zainstalowany ASP .NET Core, a następnie IIS, należy doinstalować moduł AspNetCoreModuleV2 oraz zarejestrować jego obsługę w IIS. Proces instalacji wygląda następująco:

1. Uruchomić ponownie instalator ASP.NET Core z Windows Hosting (patrz: *3.4. Instalacja ASP .NET Core wraz z modułem* IIS). W przypadku, gdy w systemie zainstalowana jest nowsza wersja ASP.NET Core z Windows Hosting, należy posłużyć się instalatorem w nowszej wersji.
2. Wybrać w instalatorze opcję: „Repair".
3. Uruchomić panel zarządzania IIS na jeden z poniższych sposobów:
   a) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr" i zatwierdzić klawiszem Enter,
   b) Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
4. W oknie środkowym odnaleźć opcję „Moduły":



Rysunek 17: IIS - moduły

5. Jeśli na liście znajduje się pozycja o nazwie „AspNetCoreModuleV2" oznacza to, że moduł dedykowany dla .NET Core został zainstalowany pomyślnie. W przeciwnym razie trzeba przejść do kolejnych kroków.

Rysunek 18: Sprawdzanie modułu dla .NET Core w IIS

6. W oknie „Moduły" z menu „Akcje" po lewej stronie należy wybrać „Konfiguruj moduły macierzyste…".
7. Jeśli na liście w nowym oknie jest dostępny moduł „AspNetCoreModuleV2", należy go oznaczyć. Jeśli moduł na liście nie występuje, należy wybrać przycisk „Zarejestruj", a następnie uzupełnić:
   a) Nazwa: AspNetCoreModuleV2
   b) Ścieżka: %ProgramFiles%\IIS\Asp.Net Core Module\V2\aspnetcorev2.dll

   Zatwierdzić okno przyciskiem „OK", a następnie oznaczyć go na liście dostępnych modułów.

8. Wybrać przycisk „OK” zatwierdzając wybór modułu.
9. Wykonać restart serwera IIS, można go wykonać poprzez ponowne uruchomienie systemu operacyjnego lub wykonanie poniższych kroków:
   a) uruchomić Wiersz polecenia w trybie administratora,
   b) zatrzymać usługę IIS wpisując poniże polecenie i zatwierdzając klawiszem Enter,

```
net stop was /y
```

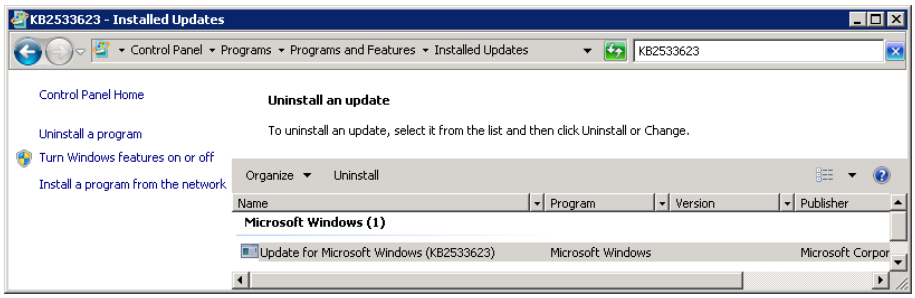
   c) uruchomić usługę IIS wpisując poniższe polecenie i zatwierdzając klawiszem Enter.

```
net start w3svc
```

3.6. KB2533623 dla Windows 8.1, Windows Server 2012 R2

Systemy operacyjne Windows 8.1, Windows Server 2012 R2 wymagają instalacji pakietu KB2533623 dostarczanego przez firmę Microsoft. W przypadku włączonych automatycznych aktualizacji systemu paczka powinna zostać automatycznie zainstalowana. Istnieje możliwość weryfikacji, czy podany pakiet został zainstalowany w następujący sposób:

1. Otworzyć Panel Sterowania.
2. Wybrać opcję „Programy i funkcje”.
3. Wybrać z menu po lewej stronie „Wyświetl zainstalowane aktualizacje”.
4. Wpisać w górnym pasku wyszukiwania „KB2533623”.
5. Jeśli na liście znajduje się wpis informujący o aktualizacji (patrz: *Rysunek 19*) oznacza to, że pakiet został już zainstalowany.



Rysunek 19: Weryfikacja instalacji KB2533623

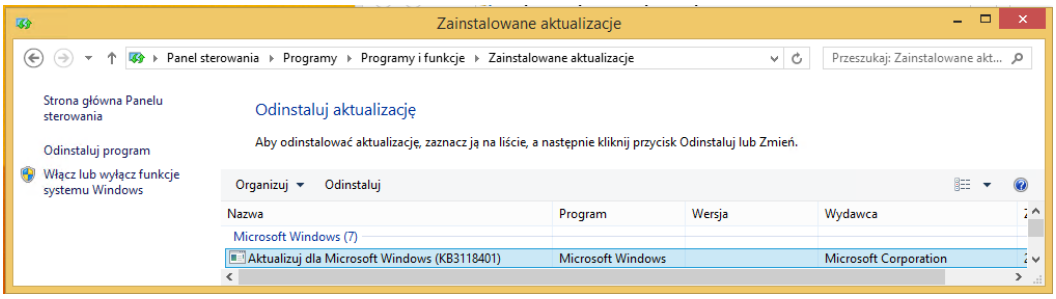
Składnik może zostać również pobrany ze strony: https://support.microsoft.com/en-us/help/2533623/microsoft-security-advisory-insecure-library-loading-could-allow-remot.

3.7. KB3118401 dla Windows 8.1

System operacyjny Windows 8.1 wymaga instalacji pakietu KB3118401 dostarczanego przez firmę Microsoft. W przypadku włączonych automatycznych aktualizacji systemu paczka powinna zostać automatycznie zainstalowana. Istnieje możliwość weryfikacji, czy podany pakiet został zainstalowany w następujący sposób:

1. Otworzyć Panel Sterowania.
2. Wybrać opcję „Programy i funkcje”.
3. Wybrać z menu po lewej stronie „Wyświetl zainstalowane aktualizacje”.
4. Wpisać w górnym pasku wyszukiwania „KB3118401”.

Jeśli na liście znajduje się wpis informujący o aktualizacji (patrz: *Rysunek 20*) oznacza to, że pakiet został już zainstalowany.



Rysunek 20 Weryfikacja instalacji KB3118401

Składnik może zostać również pobrany ze strony: https://www.microsoft.com/en-ph/download/details.aspx?id=51106.

3.8. Instalacja za pomocą instalatora

Przedstawiony w tym rozdziale proces instalacji uwzględnia najprostszy przypadek, w którym wszystkie komponenty modułu eRejestracja, baza danych modułu eRejestracja oraz baza danych programu mMedica, mają się znajdować na tym samym komputerze.

Pełen proces instalacji można przedstawić za pomocą następujących podpunktów:

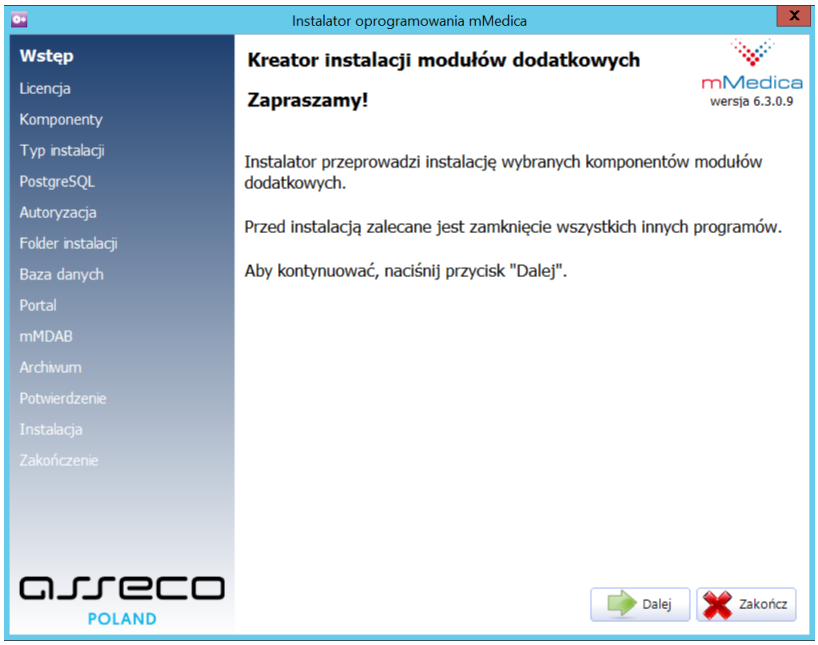
1. Instalacja niezbędnego oprogramowania związanego z wymaganiami.
2. Instalacja serwera WWW (*3.3. Instalacja serwera IIS*).
3. Instalacja ASP .NET Core (*3.4. Instalacja ASP .NET Core wraz z modułem* IIS).
4. Instalacja modułu przez instalator (baza danych oraz komponenty).
5. Weryfikacja instalacji.

6. Dodatkowa konfiguracja serwera WWW.
7. Weryfikacja instalacji (*3.12. Weryfikacja instalacji*).
8. Dodatkowa konfiguracja serwera WWW (*3.13. Dodatkowa konfiguracja IIS*).

Uwaga: Instalator może zainstalować wyłącznie jeden komponent danego typu. W przypadku chęci instalacji większej liczby komponentów należy posłużyć się informacjami zawartymi w *3.14. Doinstalowanie komponentów* lub posłużyć się instrukcją instalacji manualnej (patrz: *3.10. Instalacja manualna*).

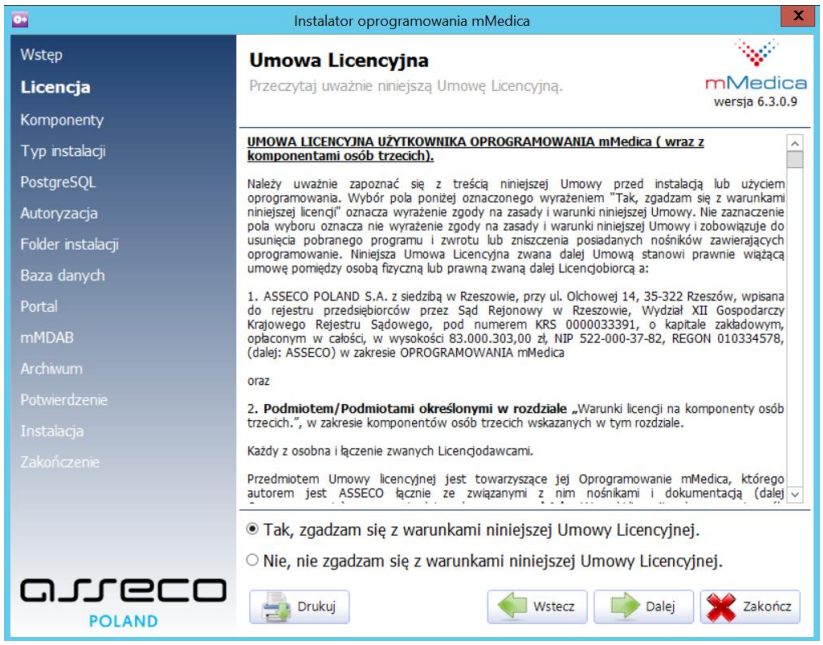
Proces instalacji:

1. Uruchomić plik instalatora modułów mMedica, który wyświetli formatkę powitalną. Przycisk strzałki w prawo pozwala przejść dalej (dotyczy to wszystkich kroków instalacji).



Rysunek 21: Formatka powitalna instalatora modułu

2. Zapoznać się z Umową Licencyjną. Aby ją zaakceptować należy zaznaczyć „Tak, zgadzam się z warunkami niniejszej Umowy Licencyjnej”.



Rysunek 22: Akceptacja umowy licencyjnej w instalatorze

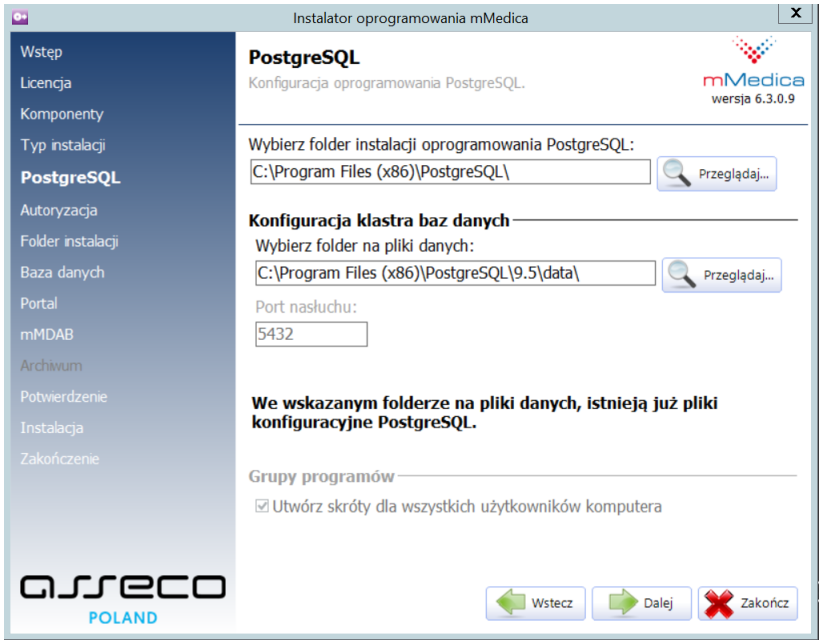
3. Wybrać komponenty, które mają zostać zainstalowane.

Rysunek 23: Wybór komponentów do instalacji

4. Zaznaczyć typ instalacji bazy danych (lokalna lub zdalna instalacja). Dla celów instruktażowych instalacja zostanie wykonana lokalnie. W przypadku zdalnej instalacji należy podać adres IP lub nazwę serwera oraz port komputera, na którym jest zainstalowany serwer bazy danych PostgreSQL. W takim przypadku serwer PostgreSQL musi być tak skonfigurowany, aby zezwalać na komunikację z zewnątrz oraz sam port musi być odblokowany do komunikacji przychodzącej w oprogramowaniu typu firewall.

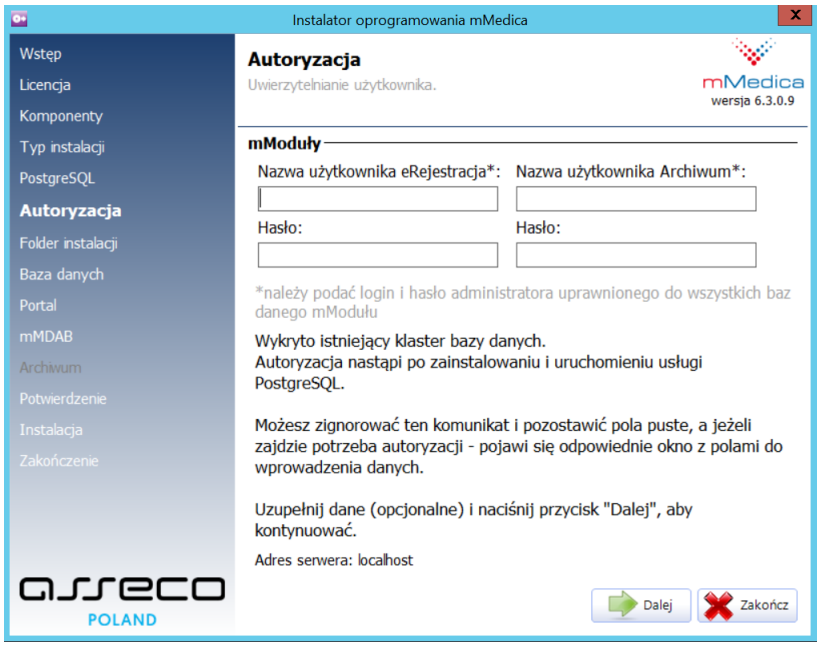
Rysunek 24: Wybór typu instalacji modułu

5. Wybrać miejsce instalacji oprogramowania bazy danych oraz miejsce składowania plików danych.



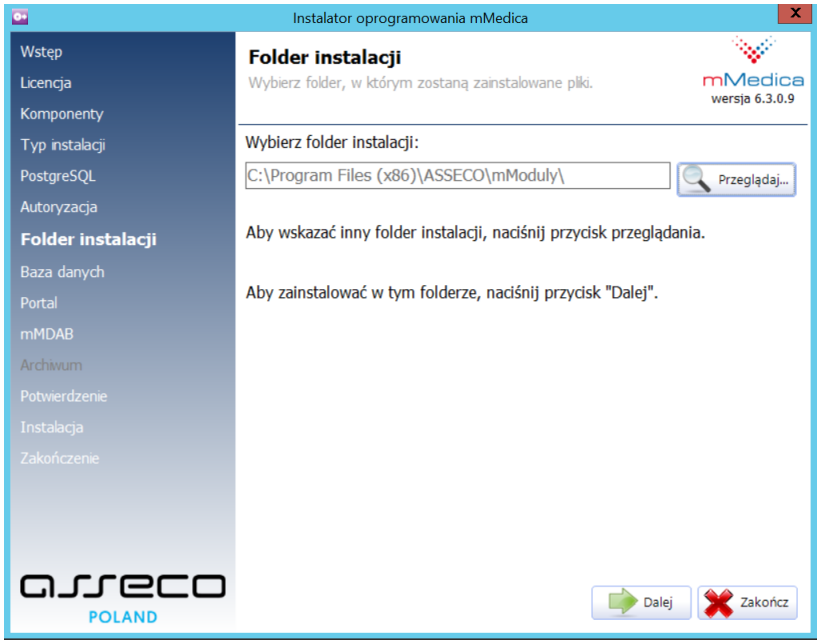
Rysunek 25: Konfiguracja instalacji serwera bazy danych

6. Opcjonalnie dokonać uwierzytelnienia do baz danych mModułów. Jeśli na komputerze nie są zainstalowane żadne bazy modułów eRejestracja lub Archiwum należy ten krok pominąć wybierając przycisk „Dalej”.



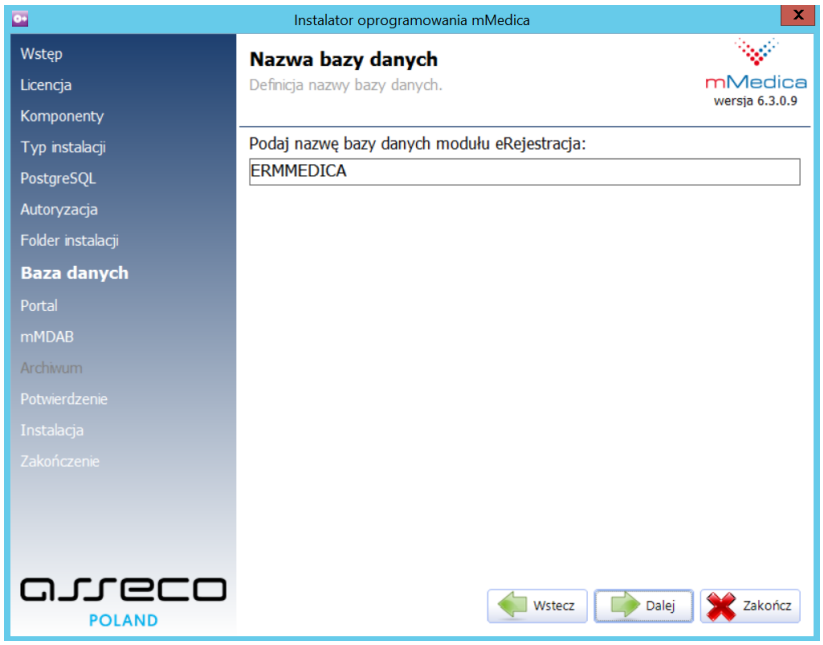
Rysunek 26: Opcjonalna autoryzacja dostępu do bazy danych

7. Wybrać folder, gdzie mają zostać zainstalowane zaznaczone komponenty (Portal, mMDAB + mMWS).



Rysunek 27: Wybór miejsca instalacji komponentów

8. Podać nazwę bazy danych eRejestracji.

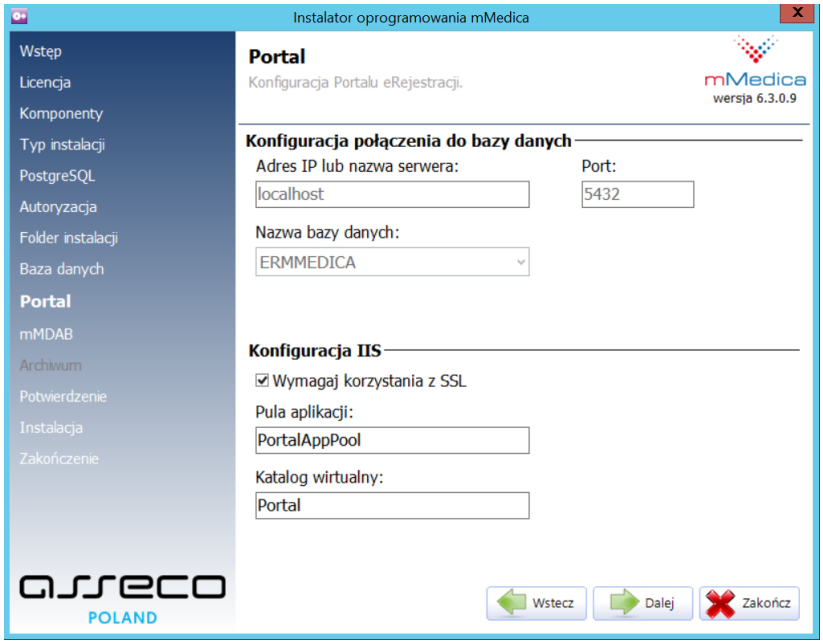


Rysunek 28: Wybór nazwy bazy danych eRejestracji

9. W formatce konfiguracji Portalu możemy wybrać, czy Portal ma wykorzystywać SSL, jaką nazwę ma mieć pula aplikacji oraz katalog wirtualny w IIS (więcej informacji znajduje się w *7.1.2. Protokół SSL*).

Uwaga: SSL można również uruchomić po instalacji komponentów. Zaznaczenie wykorzystywania SSL bez importu i skonfigurowania certyfikatu na serwerze IIS, spowoduje wyświetlenie białej strony w przeglądarce internetowej.

Uwaga: Możliwa jest zmiana adresu IP oraz nazwy bazy danych po instalacji komponentu. Więcej informacji w rozdziale *5.1. Konfiguracja połączenia z bazami danych*.

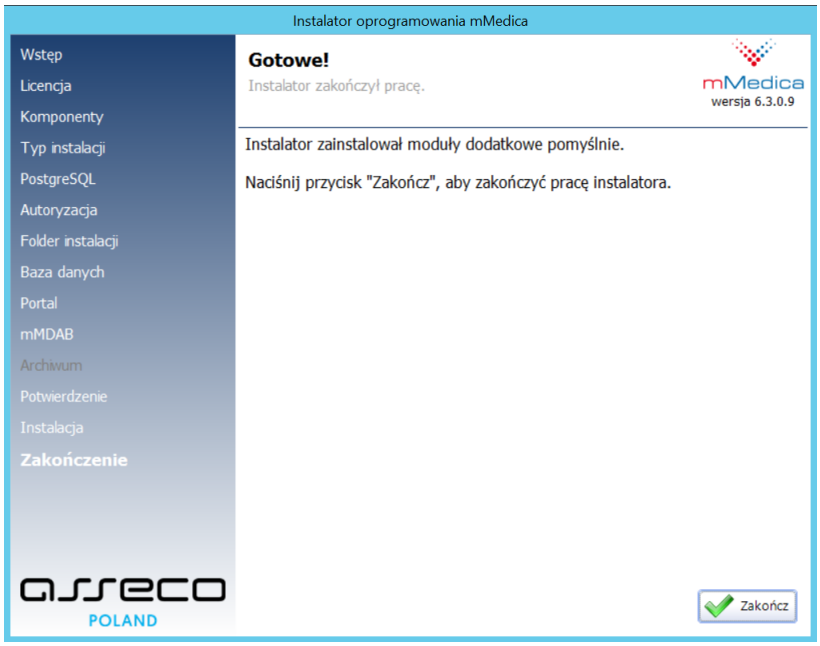


Rysunek 29: Konfiguracja instalacji Portalu

10. W ustawieniach instalacji mMDAB (mMWS) należy podać adres serwera bazy danych PostgreSQL, w którym znajduje się baza danych mMedica. Pozostałe opcje konfiguracji są analogiczne jak w przypadku innych komponentów.

Rysunek 30: Ustawienia instalacji mMDAB (mMWS)

11. Zatwierdzić instalację oraz poczekać na jej zakończenie.



Rysunek 31: Zakończenie instalacji modułu

3.9. Instalacja dodatkowych modułów/komponentów

W przypadku wcześniejszej instalacji tylko wybranych modułów/komponentów możliwe jest doinstalowanie pozostałych przy pomocy instalatora.

1. Uruchomić plik instalatora modułów mMedica, który zostanie uruchomiony w trybie serwisowym. Wybrać opcję Zarządzaj modułami dodatkowymi.

Rysunek 32: Tryb serwisowy instalatora

2. Wybrać komponenty, które mają zostać zainstalowane. W tym kroku można również doinstalować moduł Archiwum.

Rysunek 33: Wybór instalowanych komponentów

3. W dalszy krokach należy postępować podobnie jak jest to opisane w dziale *3.8 Instalacja za pomocą instalatora*.

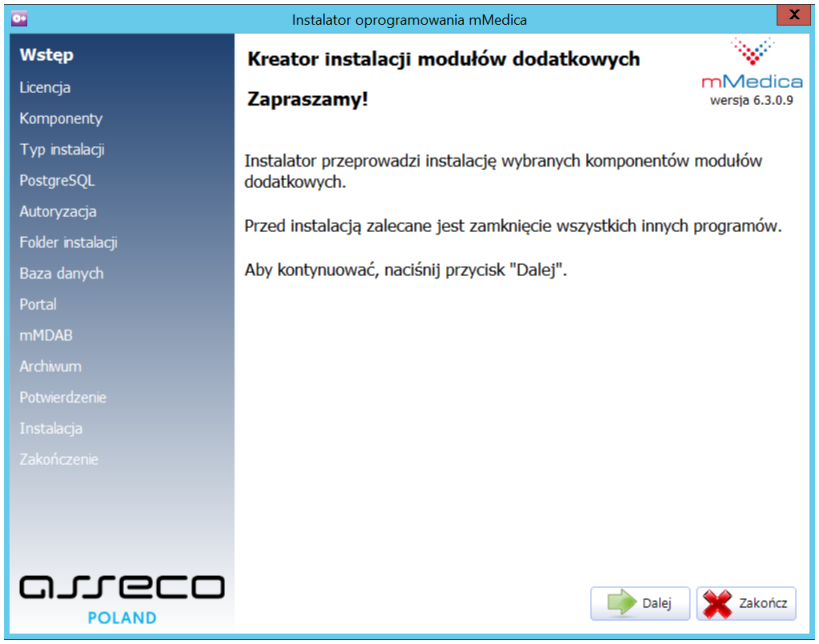
3.10. Instalacja manualna

Instalacja manualna to proces, który można sprowadzić do następujących kroków:

1. Instalacja niezbędnego oprogramowania związanego z wymaganiami.
2. Instalacja serwera WWW (*3.3. Instalacja serwera IIS*).
3. Instalacja ASP .NET Core (*3.4. Instalacja ASP .NET Core wraz z modułem* IIS*)*.
4. Instalacja bazy danych przez instalator (poniższy proces instalacji).
5. Konfiguracja podstawowa serwera WWW (poniższy proces instalacji).
6. Skopiowanie plików poszczególnych komponentów (poniższy proces instalacji).
7. Konfiguracja połączenia z bazami danych dla komponentów (*5.1. Konfiguracja połączenia z bazami danych*).
8. Konfiguracja nazw aplikacji (*3.11. Konfiguracja nazwy aplikacji*).
9. Weryfikacja instalacji (*3.12.* Weryfikacja instalacji).
10. Dodatkowa konfiguracja serwera WWW (*3.13. Dodatkowa konfiguracja IIS*).

Proces instalacji:

1. Uruchomić plik instalatora eRejestracji, który wyświetli formatkę powitalną. Przycisk strzałki w prawo pozwala przejść dalej (dotyczy to wszystkich kroków instalacji).



Rysunek 34: Formatka powitalna instalatora modułu

2. Zapoznać się z Umową Licencyjną. Aby ją zaakceptować należy zaznaczyć „Tak, zgadzam się z warunkami niniejszej Umowy Licencyjnej”.

Rysunek 35: Akceptacja umowy licencyjnej w instalatorze

3. Wybrać wyłącznie komponent „Baza danych”.

Rysunek 36: Wybór komponentu Bazy danych do instalacji

4. Zaznaczyć typ instalacji bazy danych (lokalna lub zdalna instalacja). Dla celów instruktażowych instalacja zostanie wykonana lokalnie. W przypadku zdalnej instalacji należy podać adres IP lub nazwę

serwera oraz port komputera, na którym jest zainstalowany serwer bazy danych PostgreSQL. W takim przypadku serwer PostgreSQL musi być tak skonfigurowany, aby zezwalać na komunikację z zewnątrz oraz sam port musi być odblokowany do komunikacji przychodzącej w oprogramowaniu typu firewall.

Rysunek 37: Wybór typu instalacji modułu

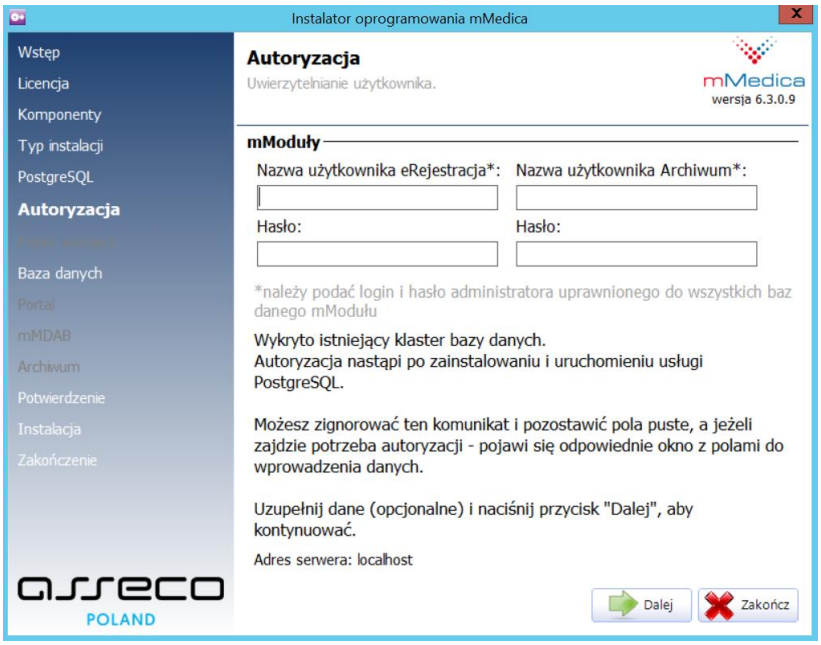
5. Wybrać miejsce instalacji oprogramowania bazy danych oraz miejsce składowania plików danych.

Rysunek 38: Konfiguracja instalacji serwera bazy danych

6. Opcjonalnie dokonać uwierzytelnienia do baz danych mModułów. Jeśli na komputerze nie są zainstalowane żadne bazy modułów eRejestracja lub Archiwum należy ten krok pominąć wybierając przycisk „Dalej”.

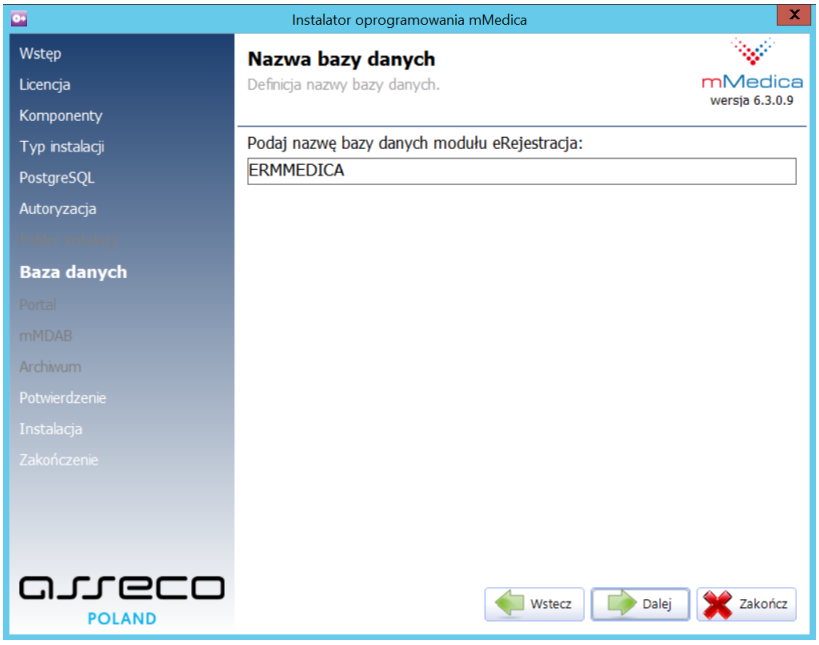
   Domyślne dane do logowania do bazy eRejestracji:

   - nazwa użytkownika: **admin**
   - hasło: **test2013**



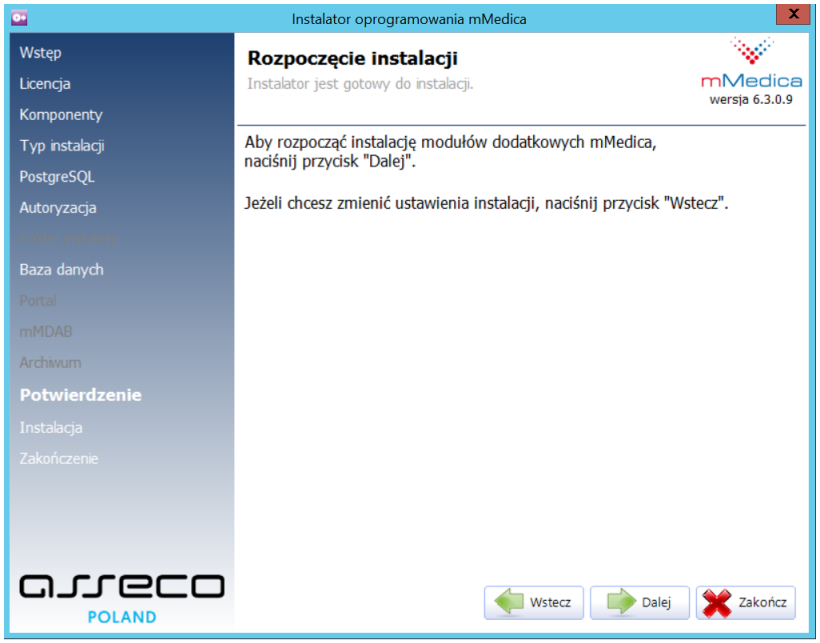
Rysunek 39: Opcjonalna autoryzacja dostępu do bazy danych

7. Podać nazwę bazy danych eRejestracji.



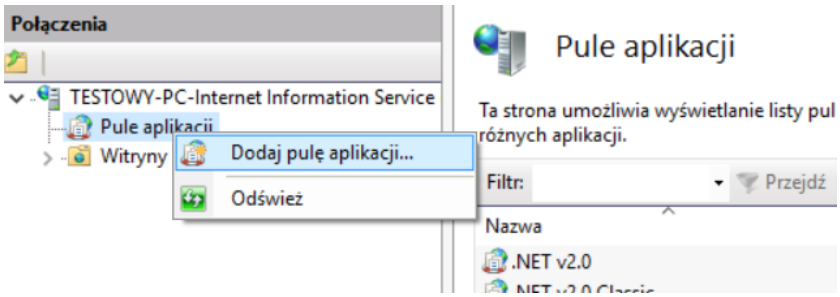
Rysunek 40: Wybór nazwy bazy danych eRejestracji

8. Zatwierdzić instalację oraz poczekać na jej zakończenie. Po zakończeniu pojawi się okno informujące o liczbie zainstalowanych baz danych eRejestracji.



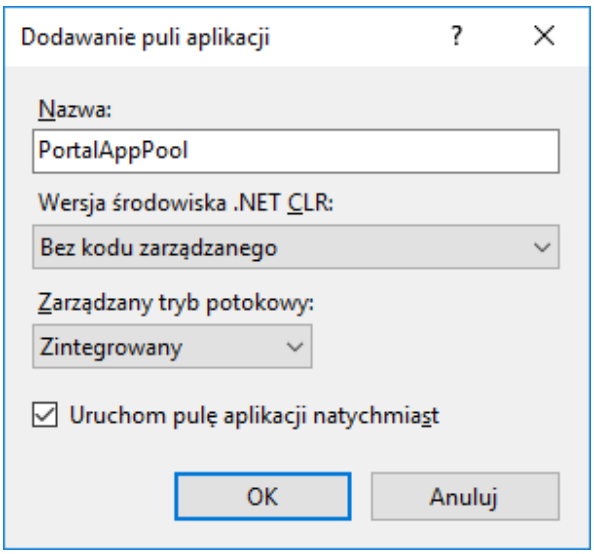
Rysunek 41: Potwierdzenie instalacji modułu

9. Uruchomić Menedżer internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
   a) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
   b) Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
10. Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera, następnie kliknąć prawym przyciskiem myszy na ikonę podpisaną „Pule aplikacji” i wybrać opcję „Dodaj pulę aplikacji…”.



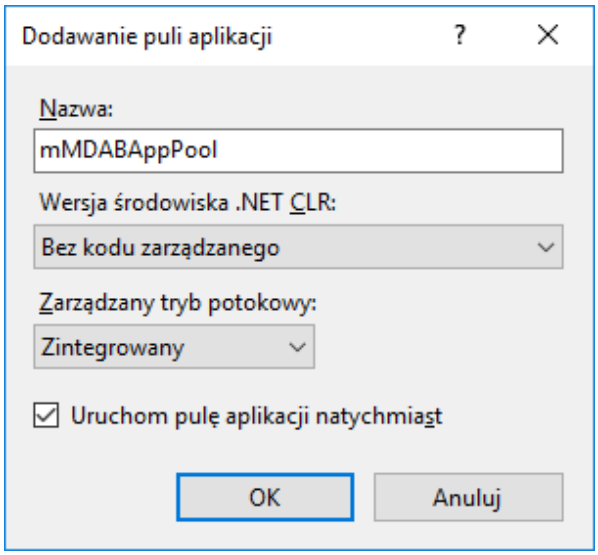
Rysunek 42: Tworzenie nowej puli aplikacji w programie IIS

11. Po wybraniu powyższej opcji powinno pojawić się okno, które należy uzupełnić jak poniżej. Nazwa puli aplikacji może być dowolna.



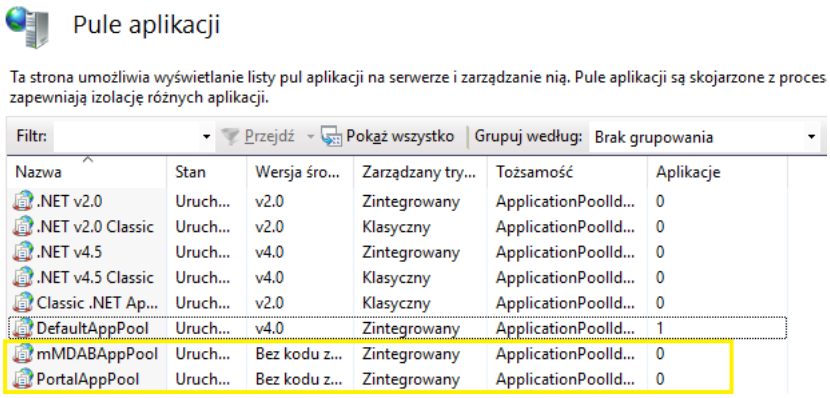
Rysunek 43: Tworzenie nowej puli aplikacji – ustawienia

12. Operację „Dodaj pulę aplikacji…" należy wykonać jeszcze raz dla mMDAB, tak jak na poniższym zrzucie ekranu:



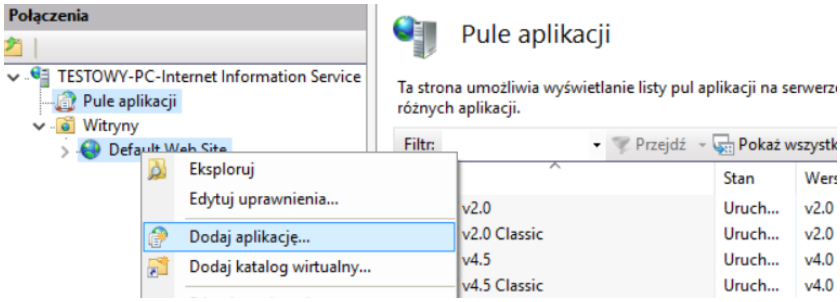
Rysunek 44: Tworzenie puli aplikacji dla mMDAB

13. Po wykonaniu tych operacji należy zweryfikować, czy konfiguracja przedstawia się identycznie, jak na poniższym zrzucie ekranu (kolumna „Tożsamość" może się różnić wartościami):



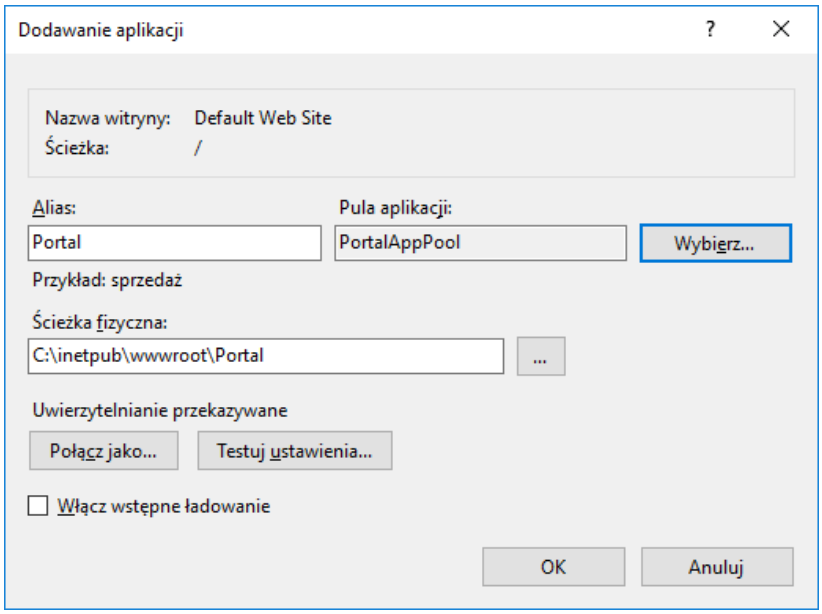
Rysunek 45: Widok pul aplikacji

14. Kliknąć prawym przyciskiem myszy na „Default Web Site” i wybrać opcję „Dodaj aplikację…”.



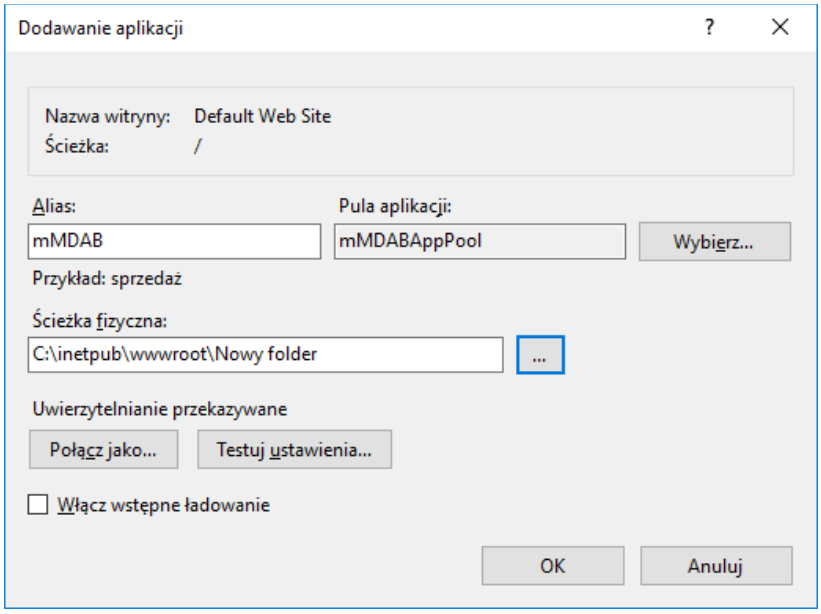
Rysunek 46: Dodawanie nowej aplikacji

15. Uzupełnić okno według zrzutu przedstawionego poniżej. Przy wybieraniu dowolnej fizycznej ścieżki do folderu, do którego w późniejszym etapie zostaną skopiowane pliki komponentu, można posłużyć się przyciskiem „…”. Pliki komponentu można skopiować do wybranego folderu po dodaniu aplikacji. Za pomocą przycisku „Wybierz…” należy wybrać zdefiniowaną wcześniej pulę aplikacji.



Rysunek 47: Dodawanie nowej aplikacji

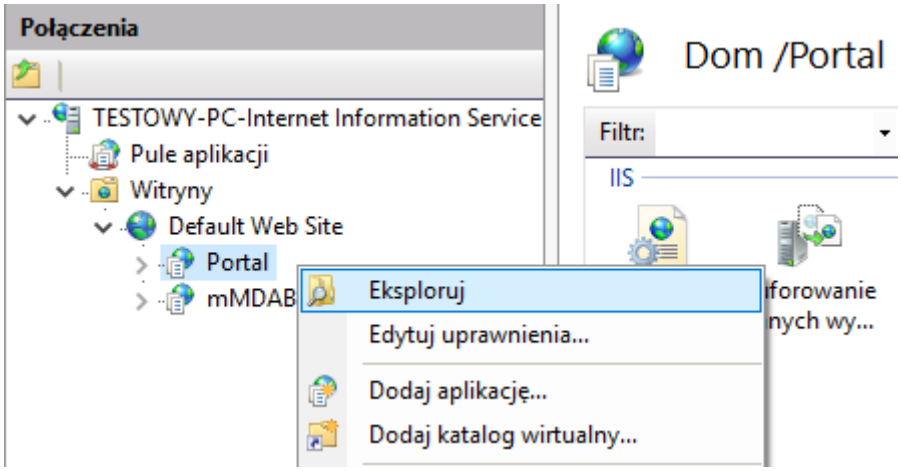
16. Operację dodawania aplikacji do „Default Web Site” powtórzyć również dla mMDAB. Proszę pamiętać przy tym o wyborze przez przycisk „Wybierz…” odpowiedniej puli aplikacji.



Rysunek 48: Dodawanie nowej aplikacji dla mMDAB

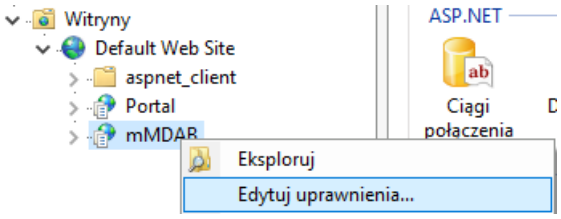
17. Pobrać pliki komponentów – odnośnik. Skopiować z dostarczonego archiwum pliki Portalu, mMDAB, mMWS, do odpowiednich folderów (poniżej przykład dla ścieżek użytych na zrzutach ekranu):
    - Zawartość folderu Portal przenieść do *C:\inetpub\wwwroot\Portal*
    - Zwartość katalogu mMDAB przenieść do *C:\inetpub\wwwroot\mMDAB*
    - Zwartość folderu mMWS przenieść do *C:\inetpub\wwwroot\mMDAB\modules\mMWS*

Dla ułatwienia odszukania właściwego katalogu możliwe jest użycie opcji „Eksploruj”. Pojawia się ona do wyboru po naciśnięciu prawego przycisku myszy na dowolną aplikację (np. Portal) oknie „Połączenia”.



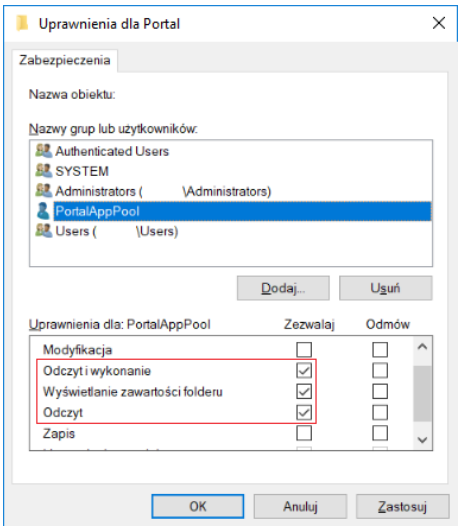
Rysunek 49: Otworzenie katalogu aplikacji

18. Zaleca się umieszczanie plików komponentów w ścieżce C:\inetpub\wwwroot\, gdyż jest to folder przeznaczony do przechowywania plików IIS. Jeśli pliki komponentów zostały skopiowane do innego katalogu, możliwe jest wyświetlenie w oknie przeglądarki błędu 502.5 w procesie weryfikacji instalacji. W takim przypadku wymagane jest dodatkowe nadanie uprawnień, które zezwolą puli aplikacji na odczyt plików z danej ścieżki. Proces nadawania uprawnień (należy go wykonać dla Portal oraz mMDAB):
    a) Przejść do ścieżki pliku lub folderu komponentu. Następnie kliknąć prawym przyciskiem myszy na plik lub folder, wybrać z menu kontekstowego „Właściwości". Można również posłużyć się opcją „Edytuj uprawnienia…" dostępną w menu kontekstowym po wybraniu odpowiedniej aplikacji w IIS (patrz: *Rysunek 50: Edycja uprawnień do katalogu w IIS*).



Rysunek 50: Edycja uprawnień do katalogu w IIS

    b) Przejść do górnej zakładki „Zabezpieczenia".
    c) Wybrać przycisk „Edytuj".
    d) W oknie nadawania uprawnień wybrać przycisk „Dodaj".
    e) W dolnym polu tekstowym wpisać nazwę IIS APPPOOL\[Nazwa puli aplikacji], czyli dla przykładu:
        - Dla folderu Portalu: IIS APPPOOL\PortalAppPool,
        - Dla foleru mMDAB: IIS APPPOOL\mMDABAppPool
    f) Następnie kliknąć opcję sprawdzania nazwy „Sprawdź nazwy" oraz zatwierdzić przyciskiem „OK". Jeśli nazwa została odnaleziona, zostanie podkreślona.
    g) Zaznaczyć dodanego użytkownika (podaną wcześniej nazwę) kliknięciem myszy. W dolnym polu nadać użytkownikowi uprawnienia: „Odczyt i wykonywanie", „Wyświetlenie zawartości folderu", „Odczyt". Zatwierdzić zmianę przyciskiem OK.



Rysunek 51: Nadawanie uprawnień odczytu dla użytkownika puli IIS

19. Nadać uprawnienia do zapisu dla:

- folderu: *[Ścieżka do Portalu]\Views\Shared\Custom*

  dla przykładowej instalacji: *C:\inetpub\wwwroot\Portal\Views\Shared\Custom*
- pliku: [Ścieżka do Portalu]\wwwroot\content\css\custom-site.min.css

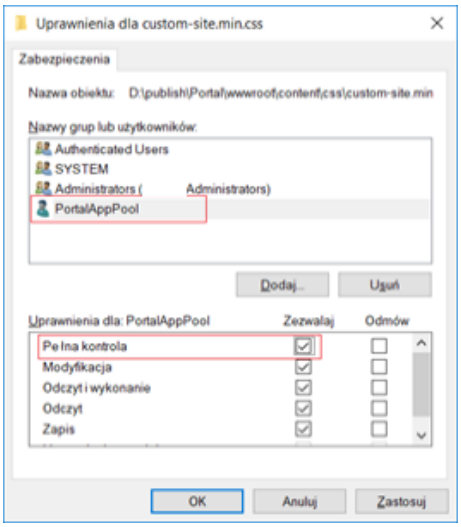
  dla przykładowej instalacji: *C:\inetpub\wwwroot\Portal*\wwwroot\content\css\custom-site.min.css
- pliku: [Ścieżka do Portalu]\application.log

  dla przykładowej instalacji: *C:\inetpub\wwwroot\Portal*\application.log
- pliku: [Ścieżka do mMDAB]\modules.xml

  dla przykładowej instalacji: *C:\inetpub\wwwroot\mMDAB*\modules.xml
- pliku: [Ścieżka do mMDAB]\application.log

  dla przykładowej instalacji: *C:\inetpub\wwwroot\mMDAB*\application.log

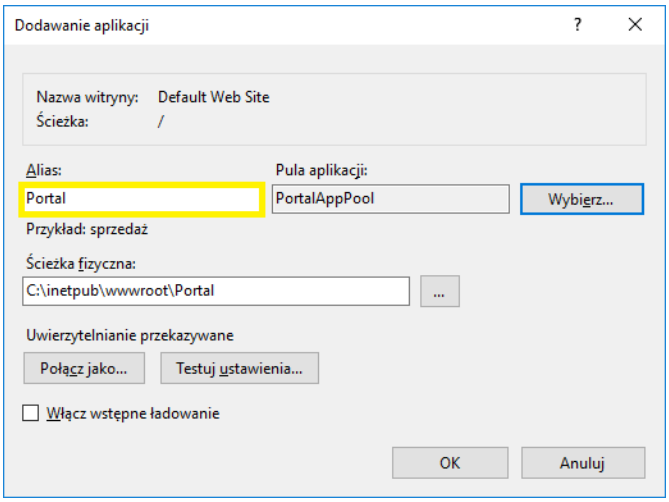
Dla każdego z wyżej wymienionych plików oraz folderu należy nadać uprawnienia „Pełna kontrola” dla użytkownika przypisanego do puli aplikacji zgodnie z punktem *18*:

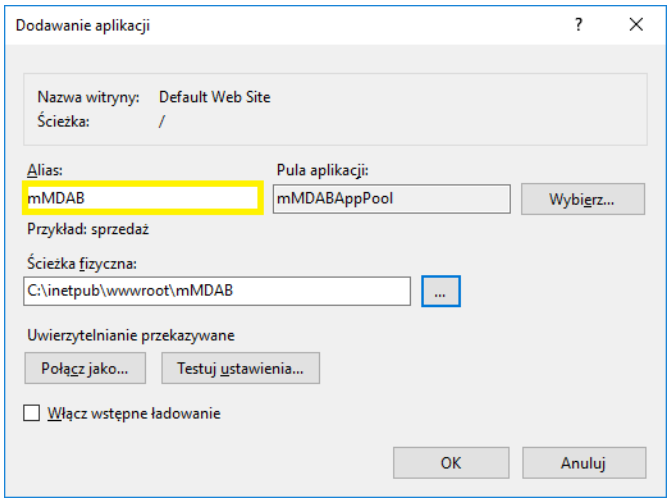


Rysunek 52: Dodanie pełnych uprawnień dla IIS

3.11. Konfiguracja nazwy aplikacji

Jeśli komponenty (Portal oraz mMDAB) nie mają swojego własnego adresu domenowego, to w pliku appsettings.json znajdującym się w katalogu każdej z aplikacji, należy wprowadzić nazwę aplikacji. Nazwa ta nie jest dowolna. Należy wprowadzić dokładnie tę samą nazwę, która zostanie wykorzystana do konfiguracji serwera IIS. Nazwa ta znajduje się w zaznaczonych miejscach:





Rysunek 53: Identyfikacja nazwy aplikacji

Nazwę tą należy umieścić w sekcji ApplicationName, dla przykładowej konfiguracji:

a. Portalu:

```
"ApplicationName": "Portal"
```

b. mMDAB:

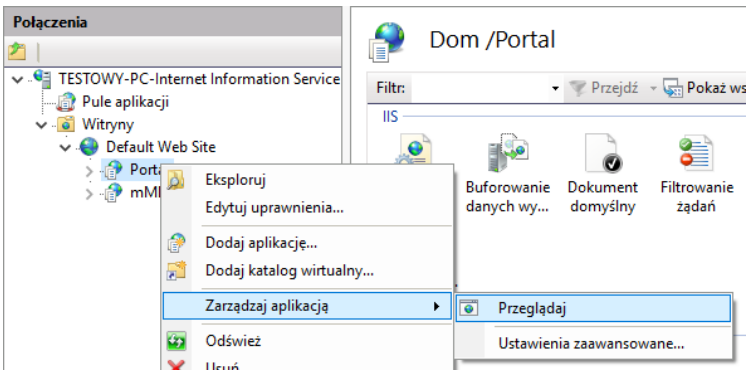
```
"ApplicationName": "mMDAB"
```

Nazwy powinny być unikalne w ramach jednego serwera WWW.

3.12. Weryfikacja instalacji

Po instalacji przez instalator jak i instalacji manualnej należy zweryfikować, czy instalacja została przeprowadzona poprawnie. Proces weryfikacji wygląda następująco:

1. Uruchomić Menedżer internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
   a. Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr" i zatwierdzić klawiszem Enter,
   b. Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
2. Rozwinąć drzewo połączeń tak, aby widoczna była aplikacja, którą należy zweryfikować. Klikając prawym przyciskiem myszy na wybraną aplikację należy wybrać Zarządzaj aplikacją\Przeglądaj, co spowoduje uruchomienie aplikacji w przeglądarce internetowej.



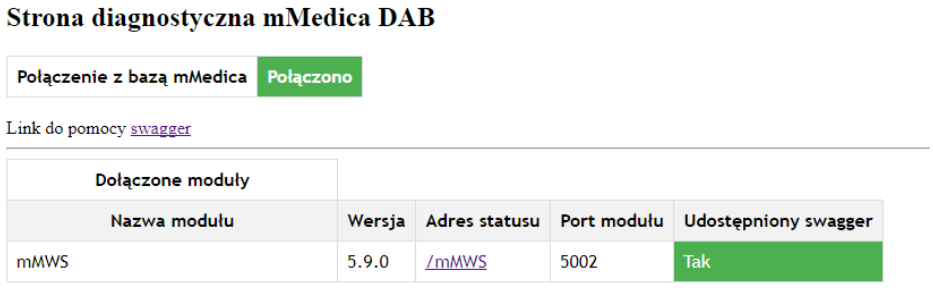
Rysunek 54: Podgląd aplikacji z poziomu IIS

3. W przypadku, w którym uruchomioną aplikacją jest Portal, powinien on zostać od razu wyświetlony. Po uruchomieniu, strona w przeglądarce internetowej powinna się prezentować jak poniżej (lub podobnie):

Rysunek 55: Portal podczas pierwszego uruchomienia

Błąd 500.21 oznacza problem z modułem .NET dla IIS – rozwiązanie zostało poruszone w rozdziale *12.23. Błąd 500.21 w IIS.*

4. Z kolei w przypadku, w którym rozmyślnie wybrano wymaganie SSL i zostanie wyświetlona zostanie biała strona lub błąd 403.4, należy skonfigurować SSL zgodnie z *3.13.2. Konfiguracja certyfikatu SSL*. Jeżeli wymaganie SSL zostało zaznaczone błędnie, jest możliwość jego wyłączenia zgodnie z podrozdziałem *12.21. Biała strona komponentu po instalacji przez instalator na IIS*.
5. Weryfikacja usługi sieciowej mMDAB odbywa się poprzez wejście na stronę statusową usługi. Adres usługi dla przykładowej konfiguracji to: http://localhost/mMDAB. Wyświetlona zostanie strona statusowa z informacjami o dołączonych modułach takich jak mMWS oraz wystąpieniu dokumentu z dostępnymi metodami.



Rysunek 56: Weryfikacja mMDAB

6. Weryfikacja usługi sieciowej mMWS odbywa się poprzez wejście na stronę usługi, która kończy się frazą „mMWS”. Adres mMWS dla przykładowej konfiguracji to: http://localhost/mMDAB/mMWS. Wyświetlona zostanie strona statusowa dla aplikacji mMWS. Poprzez stronę statusową można zweryfikować, czy nawiązane zostało połączenie z bazą mMedica oraz z eRWS. Rezultat poprawnej komunikacji wygląda następująco:

Strona diagnostyczna eRejestracja mMWS

Status	OK
Wersja mMWS	6.3.0
Wersja mMedica	6.3.0
Połączenie z bazą danych	Tak
Baza mMedica w stanie aktualizacji	Nie
Licencja na moduł eRejestracja	Tak
Licencje na dodatkowe moduły	eRejestracja+, Archiwum
Kompatybilność wersji	Tak
Uwagi dotyczące kompatybilności	OK
Data z serwera aplikacji	20.09.2019 12:44:05
Data z serwera bazy danych mMedica	20.09.2019 12:44:05
Połączenie z eRWS	Tak

Rysunek 57: Weryfikacja mMWS

Uwaga: Na tym etapie możliwe jest wystąpienie błędu w połączenia z eRWS, gdyż adres eRWS będzie konfigurowany w oprogramowaniu mMedica w późniejszym etapie.

W przypadku problemów zostanie wyświetlony komunikat o błędzie. Możliwe problemy:

- nieprawidłowy adres serwera bazy danych, port lub nieprawidłowa nazwa bazy danych mMedica,
- brak komunikacji z serwerem bazy danych (zapora ogniowa lub konfiguracja serwera PostgreSQL).
- baza danych mMedica w stanie aktualizacji,
- brak licencji na moduł eRejestracja,
- brak połączenia z eRWS (nieprawidłowy adres eRWS w mMedica),
- niekompatybilna wersja oprogramowania mMedica oraz modułu eRejestracja.

Uwaga: Najczęściej pojawiające się problemy zostały opisane w rozdziale *11. Pobieranie danych diagnostycznych*

Możliwe jest pobieranie danych diagnostycznych w formie XML lub JSON dotyczących działania komponentów mModułów. Zakres danych do pobrania jest tożsamy z danymi wyświetlanymi na stronach statusowych. Opis techniczny znajduje się w dokumencie pod odnośnikiem.

Rozwiązania częstych problemów.

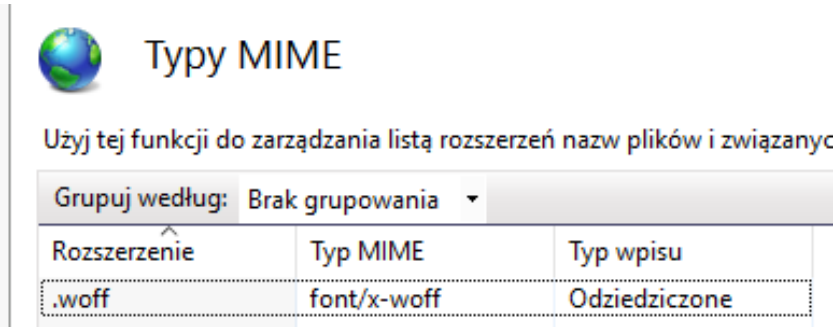
3.13. Dodatkowa konfiguracja IIS

3.13.1. Konfiguracja typów MIME w IIS

W przypadku instalacji manualnej należy dodać odpowiednie typy MIME do IIS. W pierwszym kroku należy zweryfikować, czy poniżej podane typy nie zostały już wcześniej zdefiniowane:

Rozszerzenie	Typ MIME
.woff	font/x-woff
.woff2	application/font-x-woff2
.ttf	application/x-font-ttf

Można to zweryfikować klikając lewym przyciskiem myszy na wybraną witrynę (domyślnie „Default Web Site"), a następnie w oknie po lewej stronie wybrać ikonę z podpisem „Typy MIME". Należy zwrócić uwagę, by zaznaczyć opcję widoku na „Widok funkcji" (na dole formatki). W typach MIME powinna wyświetlić się następująca pozycja (na przykładzie typu o rozszerzeniu .woff):



Rysunek 58: Podgląd typów MIME

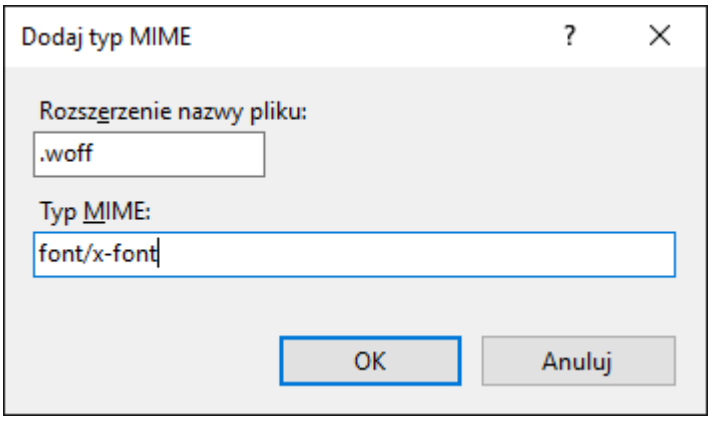
Należy również sprawdzić, czy wpis rejestrujący typ MIME nie znajduje się również w pliku C:\inetpub\wwwroot\web.config (o ile istnieje) w poniższej formie:

```
<mimeMap fileExtension="[rozszerzenie]" mimeType="[Typ MIME]" />
```

Przykład dla rozszerzenia .woff:

```
<mimeMap fileExtension=".woff" mimeType="font/x-woff" />
```

Sprawdzenia należy dokonać dla każdego podanego wyżej typu MIME. Jeśli dany plik nie istnieje, należy go dodać za pomocą opcji „Dodaj…" znajdującej się po prawej stronie listy Akcje, a następnie uzupełnić ją według poniższego wzoru:

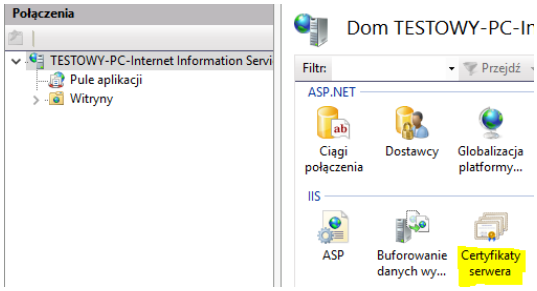


Rysunek 59: Tworzenie nowego typu MIME

3.13.2. Konfiguracja certyfikatu SSL

Konfiguracja certyfikatu SSL wygląda następująco:

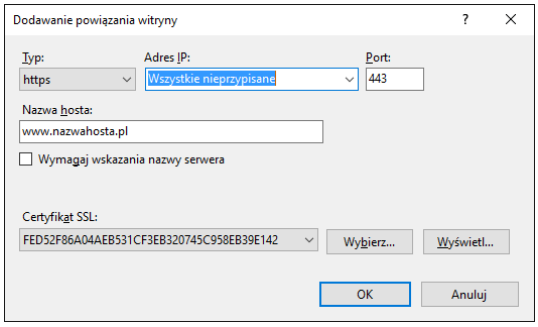
1. Zainstalować otrzymany certyfikat w systemie operacyjnym zgodnie z instrukcją dostarczoną przez dystrybutora.
2. Otworzyć Menedżer internetowych usług sieciowych (IIS).
3. Wybrać z głównego okna opcję „Certyfikaty serwera”.



Rysunek 60: Dodawanie certyfikatów SSL

4. W otwartym oknie wybrać z menu po prawej stronie „Ukończ żądanie certyfikatu...”.
5. Wybrać certyfikat za pomocą przycisku „…”, nadać nazwę (do celów administracyjnych może być dowolna) oraz wybrać opcję „Osobisty” (dla pojedynczych certyfikatów SSL) lub „Usługa hosta sieci Web” dla certyfikatów z wykorzystaniem SNI). Zatwierdzić okno.
6. W menu po lewej stronie należy kliknąć prawym przyciskiem myszy na wybraną witrynę (domyślnie „Default Web Site”) i wybrać z menu kontekstowego opcję „Edytuj powiązania…”.
7. W otwartym oknie należy wybrać opcję „Dodaj…”.

8. Wybrać typ jako „https”, port zostawić na 443, ustawić odpowiedni adres domenowy w „Nazwa hosta” oraz wybrać certyfikat SSL z listy rozwijanej. Zatwierdzić okno.
9. Opcjonalnie można również usunąć powiązanie dla protokołu http na porcie 80.



Rysunek 61: Konfiguracja certyfikatu SSL dla witryny

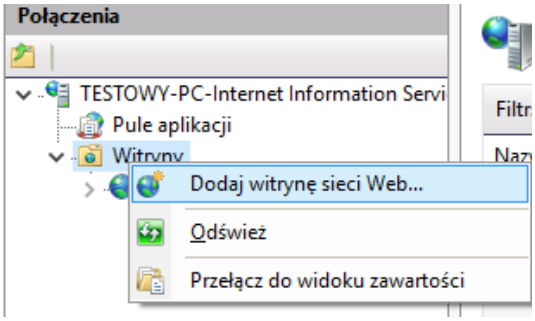
10. Istnieje również możliwość wymuszenia korzystania z protokołu https poprzez zaznaczenie wybranej witryny, wybór z panelu środkowego „Ustawienia protokołu SSL”, w którym należy zaznaczyć opcję „Wymagaj protokołu SSL”.

3.13.3. Zaawansowana konfiguracja witryn

Numery portów komunikacji oraz wybór certyfikatu definiuje się na poziomie witryn IIS. W skład witryn wchodzą aplikacje, które dziedziczą ustawienia z witryny. Może zajść konieczność dodania nowej witryny (np. komponenty mogą pracować na innych portach lub pod innym certyfikatem). W tym rozdziale została opisana procedura dodawania nowej witryny oraz edycja powiązań witryn.

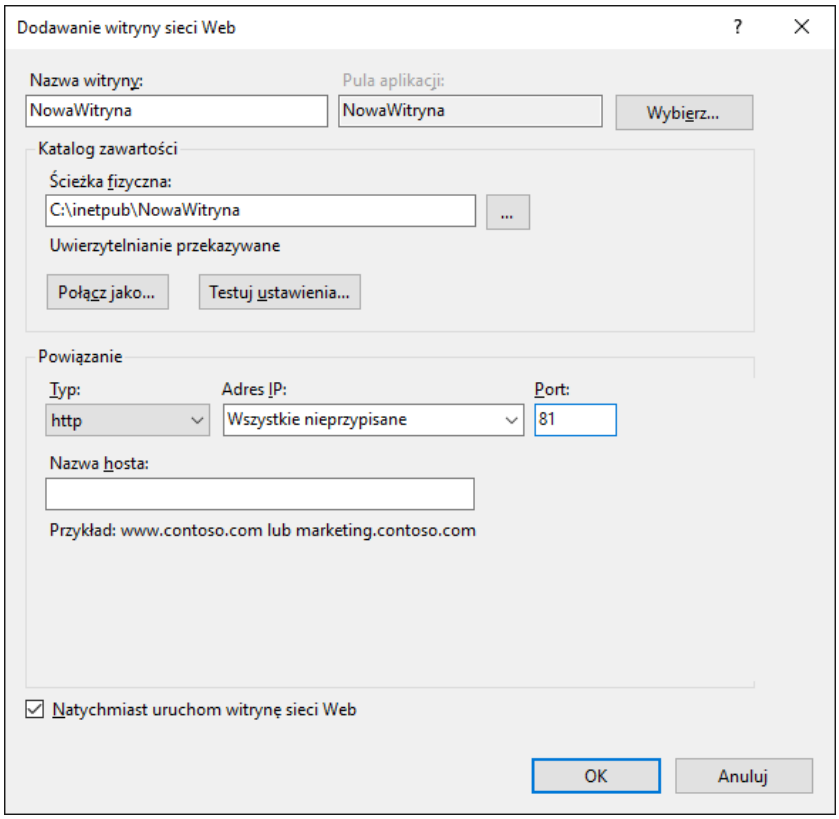
Dodawanie nowej witryny:

1. Uruchomić manager IIS.
2. Dodać nową pulę aplikacji (patrz: *3.10. Instalacja manualna*).
3. Kliknąć prawym przyciskiem myszy na „Witryny” i wybrać „Dodaj witrynę sieci Web…”.



Rysunek 62: Dodawanie nowej witryny

4. W otwartym oknie nadać dowolną nazwę witryny, za pomocą „Wybierz” wybrać stworzoną pulę aplikacji. Następnie przez przycisk „…” podać ścieżkę fizyczną do folderu, w którym znajdą się pliki aplikacji. Ostatnim etapem jest konfiguracja powiązania, która została opisana w dalszej części podrozdziału.



Rysunek 63: Okno dodawania nowej witryny

5. Do nowej witryny można dodawać nowe aplikacje oraz komponenty modułu, tak jak zostało to opisane w *3.10. Instalacja manualna*.

Edycja powiązań (zmiana: portu, nazwy hosta, certyfikatu, powiązania IP):

1. Uruchomić manager IIS.
2. Na wybranej witrynie kliknąć prawym przyciskiem „Edytuj powiązania…”.
3. W oknie zaznaczyć istniejące powiązanie (domyślnie http na porcie 80) i wybrać przycisk „Edytuj…” lub przycisk „Dodaj…”.
4. W oknie „Edytowanie powiązań witryny” można zdefiniować typ, nazwę hosta oraz port. Dodatkowo istnieje możliwość przypisania konkretnego adresu IP, z którego będzie dostępna witryna (opcja „Wszystkie nieprzypisane” oznacza dostępność dla wszystkich dostępnych adresów IP).

Uwaga: Każda z witryn, która nie posiada przypisanego adresu domenowego musi mieć unikalne numery portów.

Uwaga: W przypadku wykorzystywania innych portów niż 80 (dla http) oraz 443 (dla https) należy posługiwać się adresem zawierającym port np. http://localhost:81 (dla portu 81).

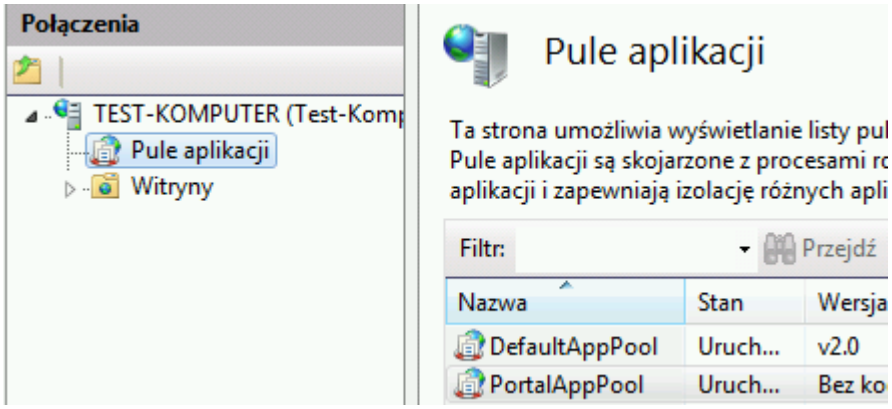
Poniżej zaprezentowano przykładową konfigurację wykorzystującą dodatkowe witryny oraz zdefiniowane numery portów:

Komponent	Witryna	Adres		Typ	Port	Domena	Przypisanie IP
Portal, eRWS	Default Web Site	Portal	http://www.er.domena.pl/	http	80	www.er.domena.pl	Nieprzypisane
		eRWS	http://www.er.domena.pl/eRWS				
		Portal	https://www.er.domena.pl/	https	443		
		eRWS	https://www.er.domena.pl/eRWS				
mMDAB	eR.mMDAB	mMDAB	http://localhost:1099/	http	1099	brak	IP z sieci VPN
		mMWS	http://localhost:1099/mMWS/				

3.13.4. Zaawansowana konfiguracja aplikacji

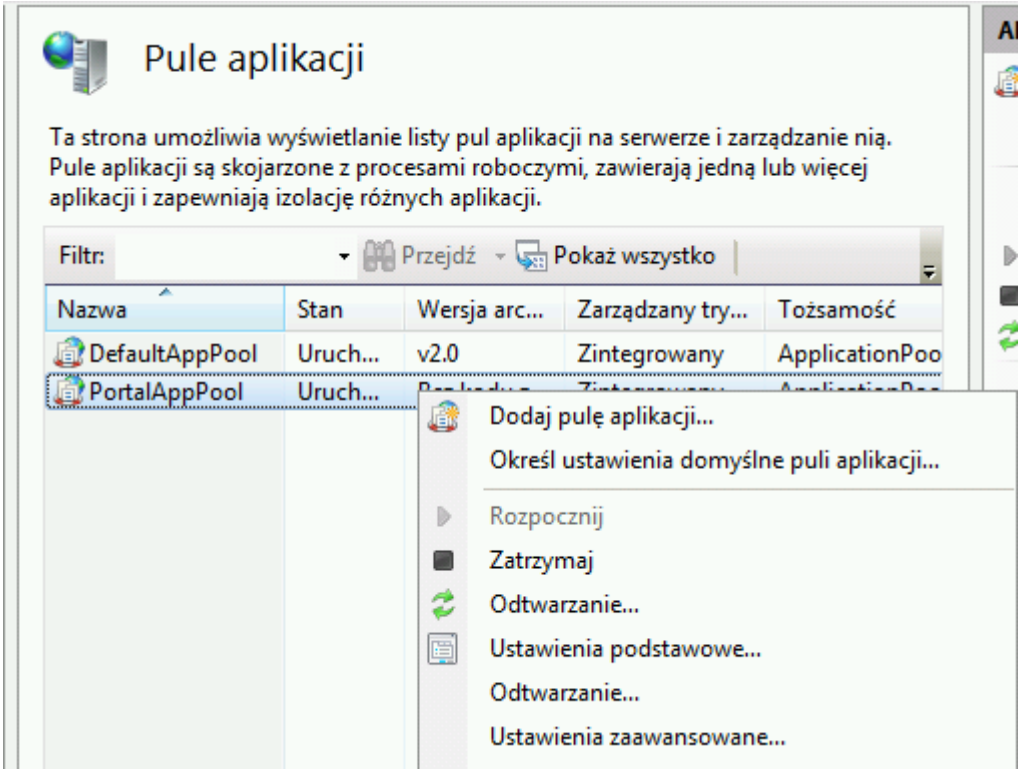
W celu wydłużenia czasu usypiania aplikacji w środowisku IIS należy uruchomić Menedżer internetowych usług informacyjnych.

Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera i wybrać opcję „Pule aplikacji”.



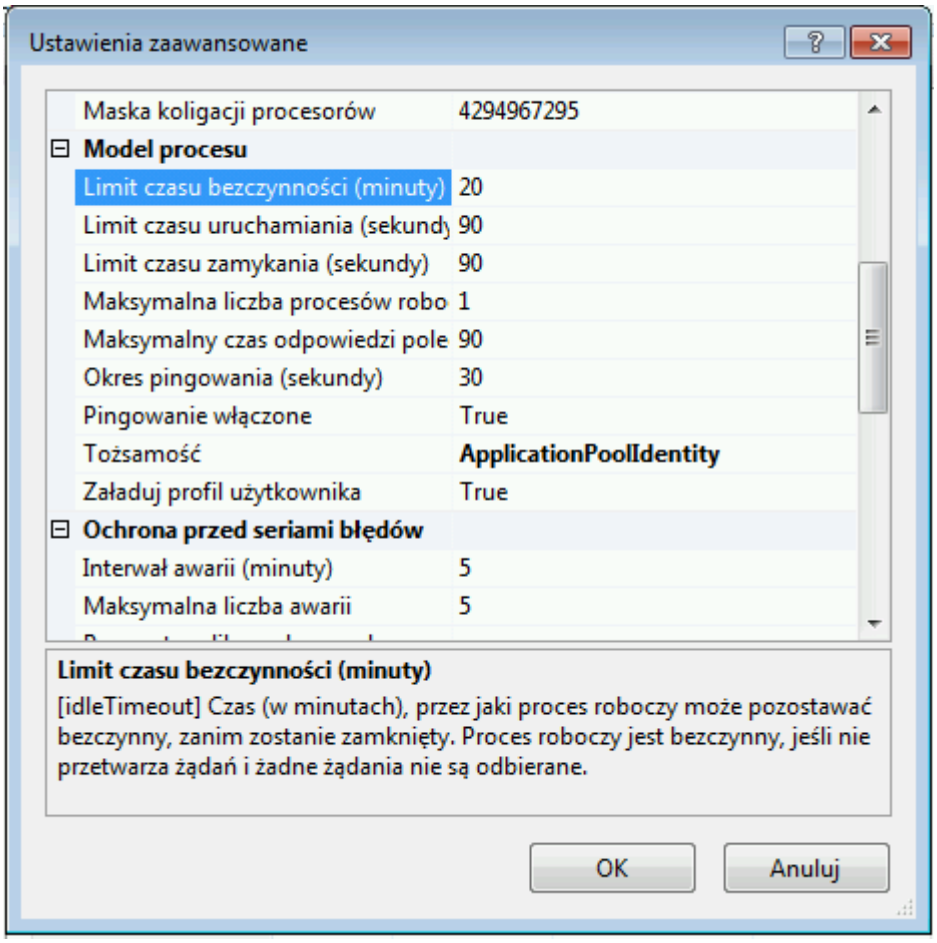
Rysunek 64: Drzewko "Połączenia" w aplikacji IIS Manager

Po wybraniu powyższej opcji po prawej stronie pojawi się okno do zarządzania pulami aplikacji. Z listy dostępnych pul należy wybrać interesującą nas pulę, kliknąć na nią prawym przyciskiem myszy i wybrać opcję „Ustawienia zaawansowane…”.



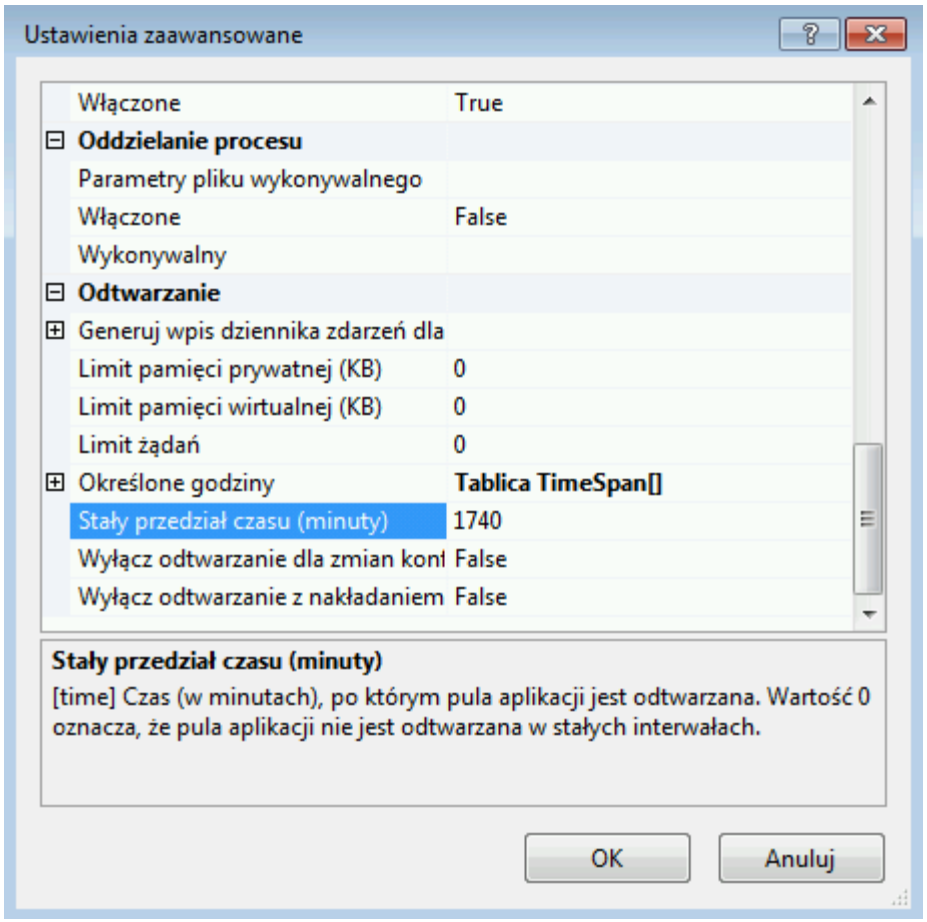
Rysunek 65: Okno zarządzania pulami aplikacji

Po wybraniu opcji pojawi się okno konfiguracji.



Rysunek 66: Okno konfiguracji - "Ustawienia zaawansowane": Limit czasu bezczynności (minuty)

Modyfikowanie wartości w polu „Limit czasu bezczynności (minuty)” pozwala na wydłużenie/skrócenie czasu, po którym aplikacja przejdzie w stan uśpienia. Ustawienie wartości 0 pozwala na skonfigurowania aplikacji tak, aby nie była ona usypiana.



Rysunek 67: Okno konfiguracji - "Ustawienia zaawansowane": Stały przedział czasu (minuty)

Kolejnym parametrem jest „Stały przedział czasu (minuty)”. Pozwala on na określenie czasu, po jakim pula aplikacji powinna ulec zrestartowaniu. Parametr ten również można ustawić na wartość 0. Spowoduje to, że pula aplikacji nie będzie restartowana. Nie jest to zalecane ze względu na zużywanie pamięci przez aplikację, gdyż w przypadku wykorzystania zbyt dużej ilości zasobów może dojść do błędów.

3.14. Doinstalowanie komponentów

Zarówno dla instalacji z pełnym wykorzystaniem instalatora, jak i w przypadku instalacji manualnej, możliwe jest doinstalowanie dodatkowych komponentów modułu. Jeśli konieczne jest zainstalowanego nowego komponentu (który nie jest zainstalowany) to można to zrobić z instalatora zgodnie z opisem w rozdziale *3.9. Instalacja dodatkowych modułów/komponentów*. Istnieje też możliwość posiadania na jednym serwerze kilku komponentów tego samego typu, np. dwóch Portali Archiwum. W tym celu należy zapoznać się z rozdziałem *3.10. Instalacja manualna*. Proces dodawania nowego komponentu wygląda następująco:

1. Dodać nową witrynę, jeżeli jest to konieczne – *3.13.3. Zaawansowana konfiguracja witryn*.

2. Dodać nową pulę aplikacji dla aplikacji komponentu.
3. Dodać nową aplikację wybierając utworzoną pulę aplikacji oraz ścieżkę fizyczną do folderu, który będzie przechowywać pliki komponentu.
4. Dodać bazę danych za pomocą instalatora. W przypadku pierwszego użycia instalatora należy dodać bazę danych tak, jak zostało to opisane w *3.10. Instalacja manualna*. W przypadku, w którym użyto już wcześniej instalatora do instalacji bazy danych lub dowolnego komponentu, należy przeprowadzić proces dodawania nowej bazy zgodnie z rozdziałem *6. Zarządzanie oraz kopie zapasowe baz danych*.
5. Skopiować do folderu z punktu 2. pliki komponentu – odnośnik lub wykonać kopię plików komponentu zainstalowanych przez instalator.
6. Skonfigurować połączenie z bazą danych dla komponentu (patrz: *5.1. Konfiguracja połączenia z bazami danych*).
7. Skonfigurować nazwy aplikacji (*3.11. Konfiguracja nazwy aplikacji*).
8. Zweryfikować instalację (*3.12.* Weryfikacja instalacji).

3.15. Restartowanie i zatrzymywanie komponentów

Komponenty zawierają wewnętrzną pamięć podręczną i może istnieć potrzeba jej wyczyszczenia za pomocą zrestartowania komponentu. Takim przypadkiem, w którym należy zrestartować komponent, jest odtworzenie kopii zapasowej bazy danych lub problem z brakiem licencji na moduł eRejestracja mimo jego istnienia (w takim przypadku konieczne jest zrestartowanie mMDAB zawierającego mMWS).
Możliwe jest zrestartowanie komponentów na dwa sposoby:

1. Zatrzymać pracę usługi IIS. Opcja jest dostępna w IIS z menu „Akcje” (Zarządzanie serwerem) z poziomu przycisk „Zatrzymaj”. Ponowne uruchomienie serwera IIS możliwe jest również z poziomu menu „Akcje” wybierając przycisk „Rozpocznij”.
2. Zatrzymanie witryny w IIS, w której znajdują się komponenty do zatrzymania. Z poziomu IIS rozwinąć po prawej stronie z okna „Połączenia” katalog „Witryny” i zaznaczyć wybraną witrynę, następnie z menu po prawej stronie o nazwie „Zarządzanie witryną sieci Web” należy wybrać przycisk „Zatrzymaj”. Aby ponownie uruchomić witryny należy wybrać opcję „Rozpocznij”.

3.16. Aktualizacja modułu

W przypadku instalacji za pomocą instalatora w celu aktualizacji należy uruchomić najnowszy instalator modułu eRejestracja. Instalator wykryje istniejącą instalacje eRejestracja i zaktualizuje pliki, które zostały

wcześniej utworzone przez instalator. Instalator równocześnie zaktualizuje instalacje modułu Archiwum, jeśli takowa istnieje.

W przypadku instalacji manualnej należy podmienić wszystkie pliki komponentów oraz przenieść ustawienia z wcześniej skonfigurowanych plików appsettings.json do nowych. Nie zaleca się podmiany plików na wcześniej skonfigurowane, gdyż struktura pliku konfiguracyjnego może ulegać zmianie.

Dla każdego z powyższych sposobów instalacji instalator aktualizuje wszystkie dostępne na serwerze bazy danych eRejestracji. Zaleca się tworzenie kopii bazy danych eRejestracji przed wykonaniem aktualizacji modułu.

Proces aktualizacji powinien być wykonywany na zatrzymanych komponentach eR w IIS (całym serwerze lub witrynie, w której znajdują się instalacje). Po aktualizacji należy uruchomić ponownie komponent na serwerze WWW. W przypadku aktualizacji przez instalator proces zatrzymywania i uruchamiania serwera jest dokonywany przez instalator. Z kolei w przypadku instalacji manualnej należy posłużyć się opisem znajdujących się w rozdziale *3.15. Restartowanie i zatrzymywanie komponentów*.

3.17. Zmiana sposobu hostingu

W celu zmiany trybu konieczne jest edycja wartości atrybutu „hostingModel” w pliku web.config znajdującego się wewnątrz katalogów poszczególnych komponentów:

- Portal: [Ścieżka do Portalu]\web.config
  dla przykładowej instalacji: *C:\inetpub\wwwroot\Portal*\web.config
- mMDAB: [Ścieżka do mMDAB]\web.config
  dla przykładowej instalacji: *C:\inetpub\wwwroot\mMDAB*\web.config

Do wyboru są dwa tryby:

- „inprocess” - hosting w procesie,
- „outofprocess” - hosting poza procesem

Domyślne konfiguracje to:

- Portal:

```
<aspNetCore processPath="dotnet" arguments=".\mMedica.eR.Portal.dll" stdoutLogEn-
abled="false" stdoutLogFile=".\logs\stdout" hostingModel="inprocess" />
```

- mMDAB:

```
<aspNetCore processPath="dotnet" arguments=".\mMedica.mMDAB.dll" stdoutLogEna-
bled="false" stdoutLogFile=".\logs\stdout" hostingModel="outofprocess">
```

Tryby hostingu zostały opisane w dziale *2.8 Zasada działania ASP .NET Core z serwerami* WWW.

4. Instalacja w dystrybucjach Linux

4.1. Wymagania

Instalacja modułu eRejestracja możliwa jest na dystrybucji Linux, jeżeli jest możliwa instalacja poniższego oprogramowania:

- serwer WWW Apache2,
- libunwind8,
- Java Runtime Environment (JRE) w wersji 1.8 (zaleca się instalację wersji 64-bitowej),
- ASP .NET Core Runtime (więcej informacji: https://docs.microsoft.com/pl-pl/dotnet/core/install/linux).

4.2. Instalacja

Proces instalacji dla przypadku instalacji wszystkich komponentów oraz serwera bazy danych na jednym komputerze można opisać za pomocą następujących kroków:

1. Instalacja i przygotowanie bazy danych (*4.3. Instalacja bazy danych eRejestracja*).
2. Instalacja niezbędnego oprogramowania (*4.4. Instalacja wymaganego oprogramowania*).
3. Skopiowanie plików komponentów (*4.5. Konfiguracja serwera oraz instalacja modułu*).
4. Konfiguracja serwera Apache (*4.5. Konfiguracja serwera oraz instalacja modułu*).
5. Konfiguracja nazw aplikacji (*4.6. Konfiguracja nazwy aplikacji*).
6. Konfiguracja adresów aplikacji (*4.7. Konfiguracja adresu aplikacji*).
7. Konfiguracji połączenia z bazami danych dla komponentów (*5.1. Konfiguracja połączenia z bazami danych*).
8. Weryfikacja instalacji (*4.8. Weryfikacja instalacji*).
9. Konfiguracja dodatkowa serwera WWW (*4.9 Konfiguracja dodatkowa Apache*).

4.3. Instalacja bazy danych eRejestracja

Pierwszym etapem jest zainstalowanie serwera bazy danych PostgreSQL zgodnie z instrukcją: https://mmedica.asseco.pl/assets/Dokumentacja/mM-Instalacja-programu-mMedica.pdf (identycznie jak w przypadku oprogramowania mMedica). Drugim etapem jest zainstalowanie bazy danych poprzez uruchomienie instalatora eRejestracji z poziomu stacji roboczej z systemem Windows.

4.4. Instalacja wymaganego oprogramowania

UWAGA: Do przeprowadzenia procesu instalacji wymagana jest podstawowa znajomość systemów operacyjnych opartych o jądro Linux.

Poniżej przedstawiono procedurę instalacji wymaganego przez moduł oprogramowania na przykładzie Ubuntu Server 20.04 z poziomu konsoli:

1. Pobranie listy pakietów z repozytorium:

```
sudo apt-get update
```

2. Instalacja serwera WWW Apache:

```
sudo apt-get install apache2
```

3. Instalacja pakietu libcurl4-openssl-dev:

```
sudo apt-get install libcurl4-openssl-dev
```

4. Instalacja pakietu libunwind8:

```
sudo apt-get install libunwind8
```

5. Instalacja oprogramowania Java:

```
sudo apt-get install default-jre
```

6. Instalacja ASP .NET Core 6.0:

   a) Rejestracja produktu Microsoft:

```
wget https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft-
prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb
```

UWAGA: Podczas realizacji tych komend najlepiej znajdować się w katalogu domowym, tak aby posiadać pełne uprawnienia do katalogów.

Na stronie https://docs.microsoft.com/pl-pl/dotnet/core/install/linux w poszczególnych działach, znajdują się instrukcje dla innych popularnych wersji systemu.

   b) Aktualizacja listy pakietów z repozytorium:

```
sudo apt-get update
```

   c) Instalacja pakietu apt-transport-https:

```
sudo apt-get install apt-transport-https
```

   d) Aktualizacja listy pakietów z repozytorium:

```
sudo apt-get update
```

e) Instalacja pakietu ASP .NET Core:

```
sudo apt-get install aspnetcore-runtime-6.0
```

UWAGA: Do prawidłowego działania modułu wymagana jest instalacja aspnetcore-runtime w wersji 6.0. Alternatywnie możliwa jest instalacja dotnet-sdk w wersji 6.0.

Proces instalacji dla innych dystrybucji Linux został opisany pod adresem: https://docs.microsoft.com/pl-pl/dotnet/core/install/ w poszczególnych działach.

4.5. Konfiguracja serwera oraz instalacja modułu

W niniejszym rozdziale omówiono najprostszą konfigurację serwera Apache. Procedura wygląda następująco:

1. Do katalogu /var/www (domyślny katalog stron dla Apache) należy przekopiować katalogi ze źródłami: mMDAB, Portal, mMWS. Zawartość katalogu mMWS musi zostać umieszczona w katalogu /var/www/mMDAB/modules/mMWS.
2. Należy przeprowadzić wstępną konfigurację opisaną w punktach *4.6. Konfiguracja nazwy aplikacji* oraz *4.7. Konfiguracja adresu aplikacji.*
3. Jeżeli w katalogu /var/www znajduje się plik index.html należy go usunąć lub przenieść w inne miejsce.
4. Skonfigurować plik witryny /etc/apache2/sites-available/default (lub 000-default.conf) lub plik z konfiguracją SSL:

```
<VirtualHost *:80>
  ServerName localhost
  ProxyPreserveHost On
  ProxyPass /Portal http://localhost:4999/
  ProxyPassReverse /Portal http://localhost:4999/
  ProxyPass /mMDAB http://localhost:5001/
  ProxyPassReverse /mMDAB http://localhost:5001/
</VirtualHost>
```

Opis:

- ServerName – nazwa lub adres serwera,
- ProxyPass oraz ProxyPassReverse zapewniają dwukierunkową komunikację. Pierwszym elementem jest adres routingu (jest on bezpośrednio powiązany z Konfiguracja nazwy aplikacji), drugi element to adres aplikacji, na który przekierowany ma zostać ruch (parametr powiązany z Konfiguracja adresu aplikacji).

Powyższy plik konfiguracyjny (dla protokołu http) definiuje wykorzystanie domyślnego portu 80 do komunikacji oraz wskazuje aplikacje, na jakie przekierowywany ma być ruch. Apache pełni tu rolę serwera pośredniczącego, dlatego konieczne jest zezwolenie serwerowi na tego typu operacje:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_balancer
sudo a2enmod proxy_http
sudo a2enmod headers
```

Apache domyślnie przekierowuje oryginalny adres IP żądania do aplikacji. Automatyczne przekierowanie protokołu z (http lub https) możliwe po dodaniu do pliku konfiguracji witryny wpisu:

```
RequestHeader set "X-Forwarded-Proto" expr=%{REQUEST_SCHEME}
```

5. Skonfigurować połączenie komponentów z bazami danych według opisu z rozdziału *5.1. Konfiguracja połączenia z bazami danych*.
6. Zrestartować serwer Apache:

```
sudo service apache2 restart
```

7. Utworzyć skrypty uruchomieniowe:
   a) Utworzyć plik Portal.sh o zawartości:

```
#!/bin/sh
cd /var/www/Portal
dotnet ./mMedica.eR.Portal.dll
```

   b) Utworzyć plik mMDAB.sh o zawartości:

```
#!/bin/sh
cd /var/www/mMDAB
dotnet ./mMedica.mMDAB.dll
```

   c) Nadać tym plikom uprawnienia do wykonywania:

```
sudo chmod +x Portal.sh mMDAB.sh
```

8. Dodać aplikacje do serwisów:
   a) Utworzyć plik mMedica.eR.Portal.service w katalogu /etc/systemd/system o zawartości:

```
[Unit]
Description = mMedica eRejestracja Portal
[Service]
ExecStart=/var/www/Portal.sh
WorkingDirectory=/var/www/Portal
Restart=always
RestartSec=10
SyslogIdentifier=mMedica-eR-Portal
User=user
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=Multi-user.target
```

b) Utworzyć plik mMedica.mMDAB.service w katalogu /etc/systemd/system o zawartości:

```
[Unit]
Description = mMedica mMDAB
[Service]
ExecStart=/var/www/mMDAB.sh
WorkingDirectory=/var/www/mMDAB
Restart=always
RestartSec=10
SyslogIdentifier=mMedica-mMDAB
User=user
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=Multi-user.target
```

gdzie w pole User należy wprowadzić nazwę istniejącego w systemie użytkownika, na którym uruchomiony zostanie serwis (nie zaleca się stosowanie użytkownika root).

c) Udostępnić serwisy:

```
sudo systemctl enable mMedica.eR.Portal.service
sudo systemctl enable mMedica.mMDAB.service
```

d) Uruchomić serwisy:

```
sudo systemctl start mMedica.eR.Portal.service
sudo systemctl start mMedica.mMDAB.service
```

9. Nadać uprawnienia do plików i folderów:

a) Nadać uprawnienia do modyfikowania pliku modules.xml

```
sudo chmod 666 /var/www/mMDAB/modules.xml
```

b) Nadać uprawnienia do modyfikowania pliku custom-site.min.css

```
sudo chmod 666 /var/www/Portal/wwwroot/content/css/custom-site.min.css
```

c) Nadać uprawnienia do zapisu dla katalogu Custom

```
sudo chmod +w /var/www/Portal/Views/Shared/Custom
```

d) Nadać uprawnienia do zapisu pliku application.log

```
sudo chmod +w /var/www/Portal/application.log
sudo chmod +w /var/www/mMDAB/application.log
sudo chmod +w /var/www/mMDAB/modules/mMWS/application.log
```

4.6. Konfiguracja nazwy aplikacji

Jeśli komponenty (tj. Portal lub mMDAB) nie posiadają własnego adresu domenowego, to w pliku appsettings.json znajdującym się w katalogu każdej z aplikacji, należy wprowadzić nazwę aplikacji. Nazwa ta nie jest dowolna. Należy wprowadzić dokładnie tę samą nazwę, która zostanie wykorzystana do konfiguracji serwera apache. Nazwa ta znajduje się w zaznaczonych miejscach:

```
<VirtualHost *:80>
  ServerName localhost
  ProxyPreserveHost On
  ProxyPass /Portal http://localhost:4999/
  ProxyPassReverse /Portal http://localhost:4999/
  ProxyPass /mMDAB http://localhost:5001/
  ProxyPassReverse /mMDAB http://localhost:5001/
</VirtualHost>
```

Nazwę tą należy umieścić w sekcji ApplicationName, dla przykładowej konfiguracji:

a) Portal:

```
"ApplicationName": "Portal"
```

b) mMDAB:

```
"ApplicationName": "mMDAB"
```

Nazwy powinny być unikalne w ramach jednego serwera WWW.

4.7. Konfiguracja adresu aplikacji

Poprzez konfigurację sekcji ApplicationUrl w pliku appsettings.json zmieniać można adres, pod jakim widoczna będzie aplikacja. Adres dla przykładowej konfiguracji:

a) Portal:

```
"ApplicationUrl": "http://localhost:4999"
```

b) mMDAB:

```
"ApplicationUrl": "http://localhost:5001"
```

Port powinien być unikalny w ramach całego serwera.

4.8. Weryfikacja instalacji

W przypadku wykorzystywania systemu bez środowiska graficznego, pomocne jest skorzystanie z drugiego komputera w celu wyświetlenia zawartości komponentów w przeglądarce internetowej (należy wtedy pamiętać o wpisaniu odpowiedniego adresu IP zamiast localhost). Proces weryfikacji wygląda następująco:

1. Otworzyć w przeglądarce internetowej stronę Portalu (dla przykładowej konfiguracji: http://localhost/Portal). Po otwarciu strona powinna prezentować się tak jak zostało to przedstawione poniżej lub podobnie:

Rysunek 68: Weryfikacja działania Portalu po instalacji

W przypadku, w którym strona się nie otwiera należy sprawdzić, czy usługa Apache działa:

```
service apache2 status
```

W wyniku powinien zostać wyświetlony status jako „active (running)”. Jeżeli usługa nie jest uruchomiona należy ją uruchomić:

```
sudo service apache2 start
```

Jeżeli strona nadal się nie wyświetla a status Apache jest poprawny, należy sprawdzić status serwisów mMedica.eR.Portal oraz mMedica.mMDAB. Status tych serwisów można sprawdzić stosując komendy:

```
sudo systemctl status mMedica.eR.Portal.service
sudo systemctl status mMedica.mMDAB.service
```

W wyniku powinien zostać wyświetlony status jako „active (running)”. Jeżeli usługi nie są uruchomione, należy je uruchomić i ponownie sprawdzić ich status. W przypadku, gdy status się nie zmieni, należy sprawdzić czy pliki konfiguracyjne zawierają dobre dane, pliki skryptowe oraz konfiguracji serwisów zawierają odpowiednią treść.

2. Weryfikacja usługi sieciowej mMDAB odbywa się poprzez wejście na stronę statusową usługi. Adres usługi dla przykładowej konfiguracji to: http://localhost/mMDAB. Wyświetlona zostanie strona statusowa z informacjami o dołączonych modułach takich jak mMWS oraz wystąpieniu dokumentu z dostępnymi metodami.

Strona diagnostyczna mMedica DAB

Połączenie z bazą mMedica	Połączono

Link do pomocy swagger

Dołączone moduły				
Nazwa modułu	Wersja	Adres statusu	Port modułu	Udostępniony swagger
mMWS	5.9.0	/mMWS	5002	Tak

Rysunek 69: Weryfikacja działania mMDAB

3. Weryfikacja usługi sieciowej mMWS odbywa się poprzez wejście na stronę usługi, która kończy się frazą „mMWS". Adres mMWS dla przykładowej konfiguracji to: http://localhost/mMDAB/mMWS. Wyświetlona zostanie strona statusowa dla aplikacji mMWS. Poprzez stronę statusową można zweryfikować czy nawiązane zostało połączenie z bazą mMedica oraz z eRWS. Rezultat poprawnej komunikacji wygląda następująco:

Strona diagnostyczna eRejestracja mMWS

Status	OK
Wersja mMWS	7.2.0
Wersja mMedica	7.2.0
Połączenie z bazą danych mMedica	Tak
Baza mMedica w stanie aktualizacji	Nie
Licencja na moduł eRejestracja	Tak
Licencje na dodatkowe moduły	eRejestracja+, eArchiwum, MIAM, Teleporada, Medicover, Moduł Integracji eRepozytorium w Chmurze
Kompatybilność wersji	Tak
Uwagi dotyczące kompatybilności	OK
Data z serwera aplikacji	17.08.2021 14:23:18
Data z serwera bazy danych mMedica	17.08.2021 14:23:18
Połączenie z eRWS	Tak

Rysunek 70: Efekt poprawnej komunikacji mMWS z bazą danych mMedica

Uwaga: Na tym etapie możliwe jest wystąpienie błędu w połączenia z eRWS, gdyż adres eRWS będzie konfigurowany w oprogramowaniu mMedica w późniejszym etapie.

W przypadku problemów zostanie wyświetlony komunikat o błędzie. Możliwe problemy:

- nieprawidłowy adres serwera bazy danych, port lub nieprawidłowa nazwa bazy danych mMedica,
- brak komunikacji z serwerem bazy danych (zapora ogniowa lub konfiguracja serwera PostgreSQL).

- baza danych mMedica w stanie aktualizacji,
- brak licencji na moduł eRejestracja,
- brak połączenia z eRWS (nieprawidłowy adres eRWS w mMedica),
- niekompatybilna wersja oprogramowania mMedica oraz modułu eRejestracja.

Uwaga: Najczęściej pojawiające się problemy zostały opisane w rozdziale *11. Pobieranie danych diagnostycznych*

Możliwe jest pobieranie danych diagnostycznych w formie XML lub JSON dotyczących działania komponentów mModułów. Zakres danych do pobrania jest tożsamy z danymi wyświetlanymi na stronach statusowych. Opis techniczny znajduje się w dokumencie pod odnośnikiem.

Rozwiązania częstych problemów.

4.9. Konfiguracja dodatkowa Apache

4.9.1. Konfiguracja typów MIME

Należy dodać do Apache obsługę następujących typy plików MIME (MIME type):

- typ: application/x-font-woff (o rozszerzeniu woff)
- typ: application/x-font-woff2 (o rozszerzeniu woff2)
- typ: application/x-font-ttf (o rozszerzeniu ttf)

W tym celu należy otworzyć plik zawierający konfigurację typów MIME mime.types, który w zależności od dystrybucji znajduje się najczęściej pod ścieżką: /etc/mime.types lub /usr/local/etc/httpd/conf/mime.types. Następnie sprawdzić, czy w pliku znajdują się powyższe wpisy, w przypadku ich braku należy je dodać. Konwencja dodawania wpisów jest następująca:

typ rozszerzenie rozszerzenie rozszerzenie

Przykładowe wpisy:

application/x-font-woff woff

application/x-font-woff2 woff2

Po edycji pliku należy go zapisać, a także zrestartować usługę Apache:

```
sudo service apache2 restart
```

4.9.2. Konfiguracja certyfikatu SSL

Proces konfiguracji certyfikatu SSL wygląda następująco:

1. Uruchomić moduł „ssl” dla Apache (zazwyczaj jest on już uruchomiony):

```
sudo a2enmod ssl
```

2. Uruchomić moduł „headers” dla Apache:

```
sudo a2enmod headers
```

3. Skopiować pliki zawierające certyfikat serwera (crt), certyfikat pośredni (crt) oraz klucz prywatny (key) do katalogu, z którego serwer Apache będzie dokonywał ich odczytu, np.: /etc/ssl/certs/.
4. Otworzyć istniejący plik konfiguracyjny witryny (domyślnie default-ssl.conf) lub dodać nowy, a następnie dodać (modyfikując ścieżki do plików z punktu 2.) elementy oznaczone kolorem zielonym:

```
<VirtualHost *:443>
  ServerName localhost
  ProxyPreserveHost On
  ProxyPass /Portal http://localhost:4999/
  ProxyPassReverse /Portal http://localhost:4999/
  ProxyPass /mMDAB http://localhost:5001/
  ProxyPassReverse /mMDAB http://localhost:5001/
  SSLEngine on
  Header edit Set-Cookie ^(.*)$ $1;Secure
  SSLProtocol +TLSv1.2
  SSLCertificateFile /etc/ssl/certs/certyfikat_serwera.crt
  SSLCertificateKeyFile /etc/ssl/private/klucz_prywatny.key
  SSLCertificateChainFile /etc/ssl/certs/certyfikat_posredni.crt
 . . .
```

Uwaga: Należy zwrócić uwagę na numer portu, domyślnie SSL wykorzystuje port 443.

Akceptowane protokoły są definiowane w „SSLProtocol”. Alternatywnie można zezwolić na wszystkie protokoły:

```
SSLProtocol all
```

5. Zrestartować serwer Apache:

```
sudo service apache2 restart
```

6. Na stronie http://httpd.apache.org/docs/current/mod/mod_ssl.html znajdują się wskazówki dotyczącej zaawansowanej konfiguracji SSL.

4.9.3. Zaawansowana konfiguracja witryn

Możliwe jest dodawanie nowych witryn do usługi Apache. Na poziomie witryny konfigurowany jest m.in. port komunikacji, adres domenowy, alias, certyfikat SSL, zakres IP z jakiego jest widoczna witryna. Możliwe jest działanie wielu witryn na tym samym porcie komunikacji. Pojedyncza witryna jest definiowana w pliku o rozszerzeniach „conf" w ścieżce /etc/apache2/sites-available/. Poniżej przedstawiono przykładową konfigurację:

Komponent	Witryna	Adres		Typ	Port	Domena	Przypisanie IP
Portal	s1.conf	Portal	http://www.er.domena.pl/	http	80	www.er.domena.pl	Nieprzypisane
		eRWS	http://www.er.domena.pl/eRWS				
	s1_ssl.conf	Portal	https://www.er.domena.pl/	https	443		
		eRWS	https://www.er.domena.pl/eRWS				
mMDAB	s2.conf	mMDAB	http://10.10.10.2:1099/	http	1099	brak	10.10.10.2
		mMWS	http://10.10.10.2:1099/mMWS				

Przykładowa zawartość dla pliku s1.conf:

```
<VirtualHost *:80>
  ServerName www.er.domena.pl
  ServerAlias er.domena.pl
  ProxyPreserveHost On
  ProxyPass /Portal http://localhost:4999/
  ProxyPassReverse /Portal http://localhost:4999/
</VirtualHost>
```

Powyższa konfiguracja posiada przypisany adres domenowy www.er.domena.pl oraz alias.

Przykładowa zawartość plik s2.conf:

```
<VirtualHost 10.10.10.2:1099>
  ServerName 10.10.10.2
  <Location /mMDAB>
    Deny from all
    Allow from 10.10.10.1/24
    ProxyPass http://localhost:5001/
    ProxyPassReverse http://localhost:5001/
  </Location>
</VirtualHost>
```

W pliku s2.conf witryna jest przypisana do adresu 10.10.10.2 i tylko pod takim będzie widoczna. Z kolei „Allow from” pozwala zdefiniować zakres adresów IP, z których jest widoczna strona. Domyślnie ma on wartość „all” oznaczający brak ograniczeń.

Po utworzeniu pliku z konfiguracja witryny w ścieżce /etc/apache2/sites-available/ należy wykonać polecenie:

```
sudo a2ensite NAZWA_PLIKU_KONFIGURACJI.conf
```

Przykład:

```
sudo a2ensite s1.conf
```

Następnie należy przeładować konfigurację usługi Apache:

```
sudo service apache2 reload
```

4.10. Doinstalowanie komponentów

Instalacja nowych komponentów polega na:

1. Skopiowaniu nowych plików komponentów do pożądanych ścieżek.
2. Dodaniu bazy danych za pomocą instalatora. W przypadku pierwszego użycia instalatora należy dodać bazę danych zgodnie z *4.3. Instalacja bazy danych eRejestracja*. W przypadku, w którym użyto już wcześniej instalatora do instalacji bazy danych lub dowolnego komponentu, należy przeprowadzić proces dodawania nowej bazy zgodnie z *6. Zarządzanie oraz kopie zapasowe baz danych*.
3. Skonfigurowaniu połączenia do bazy danych (*5.1. Konfiguracja połączenia z bazami danych)*.
4. Skonfigurowaniu nazw aplikacji (*4.6. Konfiguracja nazwy aplikacji*).
5. Skonfigurowaniu adresów aplikacji (*4.7. Konfiguracja adresu aplikacji*).
7. Konfiguracji serwera oraz instalacji modułu (*4.5. Konfiguracja serwera oraz instalacja modułu).*
6. Weryfikacji instalacji (*4.8. Weryfikacja instalacji*).
7. Konfiguracji dodatkowej serwera WWW (*4.9. Konfiguracja dodatkowa Apache*).

4.11. Konfiguracja wielu Portali na jednym serwerze

W przypadku, kiedy na jednym serwerze Apache udostępniony jest więcej niż jeden Portal eRejestracji, należy poczynić dodatkowe kroki konfiguracyjne. Utworzyć dla każdego z portali osobny katalog, w którym znajdować się będą pliki aplikacji. Wymagana jest zmiana portu, na jakim dana aplikacja będzie udostępniona, dlatego należy w pliku appsettings.json każdej aplikacji zmienić adres aplikacji.

Uwaga: Ważne, aby każdy z Portali miał unikalny atrybut „ApplicationUrl” oraz „ApplicationName” w ramach jednego serwera WWW.

Konieczne jest ponowne dokonanie kroków opisanych w punkcie *4.5. Konfiguracja serwera oraz instalacja modułu*.

4.12. Restartowanie i zatrzymywanie komponentów

Komponenty zawierają wewnętrzną pamięć podręczną i może istnieć potrzeba jej wyczyszczenia za pomocą zrestartowania komponentu. Takim przypadkiem, w którym należy zrestartować komponent, jest odtworzenie kopii zapasowej bazy danych lub problem z brakiem licencji na moduł eRejestracja, mimo jego istnienia (w takim przypadku konieczne jest zrestartowanie mMDAB zawierającego mMWS). Możliwe jest zrestartowanie komponentów w następujący sposób:

1. Wyłączyć usługę mMDAB w serwisach:

```
sudo systemctl stop mMedica.mMDAB.service
```

2. Uruchomić usługę ponownie po odczekaniu około 1 min., wykorzystując polecenie:

```
sudo systemctl start mMedica.mMDAB.service
```

Do zatrzymania komponentu Portalu (zmieniając nazwę serwisu), można wykorzystać dokładnie te same komendy.

Uwaga: Nie zaleca się stosowania komendy restart ze względu na czas wymagany na prawidłowe wyłączenie mMDAB.

4.13. Aktualizacja modułu

Należy podmienić wszystkie pliki komponentów oraz przenieść ustawienia z wcześniej skonfigurowanych plików appsettings.json do nowych. Nie zaleca się podmiany plików na wcześniej skonfigurowane, gdyż struktura pliku konfiguracyjnego może ulegać zmianie.

Dla każdego z powyższych sposobów instalacji, instalator aktualizuje wszystkie dostępne na serwerze bazy danych eRejestracji. Zaleca się tworzenie kopii bazy danych eRejestracji przed wykonaniem aktualizacji modułu.

Proces aktualizacji powinien być wykonywany na zatrzymanych komponentach eR w dystrybucjach Linux. Po aktualizacji należy uruchomić ponownie komponent w systemie. Do aktualizacji komponentów należy posłużyć się opisem znajdujących się w rozdziale *4.12. Restartowanie i zatrzymywanie komponentów.*

4.14. Pomoc

W razie problemów można skorzystać z pomocy pod następującymi adresami internetowymi:

1. http://httpd.apache.org/docs/
2. http://httpd.apache.org/docs/current/mod/mod_ssl.html
3. https://docs.microsoft.com/en-us/dotnet/core/linux-prerequisites?tabs=netcore1x
4. https://docs.microsoft.com/en-us/aspnet/core/publishing/apache-proxy

5. Konfiguracja aplikacji

5.1. Konfiguracja połączenia z bazami danych

W przypadku instalacji manualnej w systemach operacyjnych Microsoft Windows, dystrybucjach systemów opartych o jądro Linux oraz w przypadku doinstalowania komponentów, konieczna jest konfiguracja połączenia z bazami danych w komponentach. Możliwa jest również edycja parametrów połączeń, które zostały utworzone przez instalator. Każdy z komponentów posiada plik appsettings.json, w którym znajdują się parametry połączenia z bazą danych, tj. adres serwera bazy danych, port oraz nazwa bazy danych.
Konfiguracja połączenia z bazą danych wygląda następująco:

1. Otworzyć plik appsettings.json z prawami administratora do edycji.
2. Wyszukać fragment (identyczny lub podobny) dla:
   a. Portal:

```
"ConnectionString": "Server=localhost,5432;Database=ERMMEDICA;"
```

   b. mMDAB:

```
"ConnectionString": "Server=localhost,5432;Database=MMEDICA;"
```

3. Zmienić według wzoru: „Server=localhost,5432;Database=NAZWA_BAZY" – baza danych o nazwie NAZWA_BAZY znajduje się na komputerze, na którym działa komponent (localhost) na porcie 5432. W przypadku innej nazwy bazy danych należy zmienić właściwość „Database" na odpowiednią. Dla innego adresu, na którym znajduje się baza, należy zmienić parametr Server.
4. Zapisać plik i zrestartować komponent zgodnie z *3.15.* Restartowanie i zatrzymywanie komponentów (Windows) lub *4.12. Restartowanie i zatrzymywanie komponentów* (Linux).

5.2. Zabezpieczenie przed użyciem IFRAME

Atak na strony internetowe typu clickjacking polega na przechwyceniu kliknięć nieświadomego użytkownika na spreparowanej stronie internetowej, a następnie wykonanie określonych operacji na innej stronie internetowej, uwierzytelniając ją danymi użytkownika. Metoda wykorzystuje element języka HTML o nazwie IFRAME (ramka) poprzez zagnieżdżenia na stronie spreparowanej zawartości strony, do której mają zostać przekierowane akcje. W celu zabezpieczenia się przez atakiem tego typu, należy w pliku appsettings.json (znajdującym się w katalogu Portalu) umieścić następujący jeden z poniższych wpisów:

a) Portal eRejestracji może być wyświetlany w IFRAME tylko jeżeli pochodzi z tego samego miejsca, co strona zagnieżdżająca:

```
"AllowShowPortalInIframe": true,
"AllowShowPortalInIframeOnlyFromURL": ""
```

b) Żadna strona nie może wyświetlać strony eRejestracji w ramce:

```
"AllowShowPortalInIframe": false,
"AllowShowPortalInIframeOnlyFromURL": ""
```

c) Strona eRejestracji może być wyświetlana w ramce, jeżeli strona zagnieżdżająca pochodzi z podanego adresu:

```
"AllowShowPortalInIframe": true,
"AllowShowPortalInIframeOnlyFromURL": "ADRES"
```

UWAGA: Przykładowy plik appsettings.json zawiera konfigurację typu DENY.

5.3. Konfiguracja nazwy oraz adresu aplikacji

Konfiguracja ta została opisana osobno dla systemu Windows (w dziale *3.11. Konfiguracja nazwy aplikacji*) oraz Linux (w działach 4.6. Konfiguracja nazwy aplikacji oraz *4.7. Konfiguracja adresu aplikacji*).

5.4. Konfiguracja strony offline

Strona offline jest uruchamiana w przypadku braku połączenia z bazą danych eRejestracji. Opis nadawania zawartości strony znajduje się w *8.3.10.1. Treści*. Punkt dotyczy wyłącznie przypadku, w którym administrator chce wyświetlać na żądanie zdefiniowaną stronę offline w Portalu (opcjonalnie). Poprawne działanie strony offline wymaga odpowiedniej konfiguracji pliku appsettings.json w Portalu:

8. Ustawienie powodujące wyświetlanie strony offline w przypadku, gdy baza danych eRejestracji jest niedostępna:

```
„ShowOfflinePageWhenERDBIsOffline": true
```

9. Wymuszenie wyświetlenia strony offline:

```
„ShowOfflinePageNow": true
```

Uwaga: Zmiany dokonane w appsettings.json widoczne będą w aplikacji dopiero po zrestartowaniu aplikacji.

5.5. Konfiguracja puli portów dla modułów wewnętrznych mMDAB

Konfiguracja ta jest dostępna jedynie w mMDAB w pliku appsettings.json. Określa pulę portów, na których uruchomione mogą zostać poszczególne moduły wewnętrzne takie jak np. mMWS. Przykładowa konfiguracja:

```
„ModulesPortStartIndex”: „5002”,
„ModulesPortEndIndex”: „5500”
```

5.6. Zaawansowana konfiguracja modułów wewnętrznych mMDAB

Każdy moduł wewnętrzny taki jak mMWS znajdujący się wewnątrz katalogu *modules* komponentu mMDAB, posiada własny plik konfiguracyjny appsettings.json. W konfiguracji przykładowej wykorzystane zostały ustawienia domyślne, tzn. wszystkie wymagane ustawienia przekazywane są przez komponent mMDAB. Możliwe jest jednak nadpisanie tych ustawień poprzez wprowadzenie zmian do pliku konfiguracyjnego modułu wewnętrznego. Do przywrócenia ustawień domyślnych wystarczy wyczyścić pola, tak aby nie znajdował się w nich żaden ciąg znaków (””). Opis ustawień zostanie wytłumaczony w poniższych podpunktach:

a) Konfiguracja połączenia z bazą danych

   Konfiguracje połączenia z bazą danych przeprowadza się tak jak w opisanym punkcie *5.1. Konfiguracja połączenia z bazami danych.*

b) Konfiguracja nazwy aplikacji

   Konfiguracja tej opcji nie jest zalecana, gdy moduł wewnętrzny uruchamiany jest przez komponent mMDAB.

c) Konfiguracja adresu aplikacji

   Konfiguracja tej opcji odbywa się w sposób podobny do opisanego w punkcie *4.7. Konfiguracja adresu aplikacji,* niezależnie od systemu operacyjnego. Komponent mMDAB postara się uruchomić moduł wewnętrzny na wskazanym adresie. W przypadku gdy port będzie zajęty, modułowi wewnętrznemu zostanie przydzielony pierwszy wolny z puli dostępnych portów.

5.7. Przekierowanie nagłówków z proxy

W przypadku, w którym komponent taki jak Portal lub mMDAB zainstalowany na IIS (system rodziny Windows) dostępny jest poprzez proxy lub reverse-proxy, należy odpowiednio skonfigurować plik appsettings.json. Uruchomienie obsługi proxy polega na edycji sekcji w pliku appsettings.json danego komponentu poprzez zmianę wartości klucza *ProxyWindowsEnable*:

Ustawienie domyślne (proxy wyłączone):

```
"ProxyWindowsEnable": false
```

Włączona obsługa proxy:

```
"ProxyWindowsEnable": true
```

Mechanizm automatycznie obsługuje proxy, które jest uruchomione na tym samym systemie co komponent (adres lokalny). Jeśli proxy znajduje się pod innym adresem niż adres lokalny, należy jego adres IP wpisać w kluczu *ProxyIPs* (w przypadku wielu proxy należy wpisać adresy po średniku), przykład:

```
"ProxyIPs": "192.168.137.1;192.168.137.2;192.168.137.3"
```

Na środowisku opartym o jądro Linux ruch do komponentów przekierowywany jest z Apache do odpowiednich usług komponentów. Jednak komponenty Portal oraz mMDAB automatycznie obsługują odpowiednie nagłówki z proxy dla Linux. Podobnie jak w przypadku komponentów zainstalowanych w systemie Windows, o ile proxy jest na adresie lokalnym, nie wymaga on dodatkowej konfiguracji. W innym przypadku konfiguracja odbywa się na takich samych zasadach jak dla instalacji pod Windows (edycja klucza *ProxyIPs*).

Do prawidłowego działania mechanizmu przekazywania nagłówków http z proxy konieczne jest, aby proxy obsługiwało nagłówek HTTP X-Forwarded-For, w którym przekazywany jest oryginalny adres IP pochodzący z żądania.

Brak odpowiedniej konfiguracji proxy będzie skutkowało odczytem nieprawidłowych adresów IP z żądań, co z kolei może spowodować nieprawidłowe działanie mechanizmu blokad IP podczas logowania w Portalu jak i mechanizmie blokad dostępowych do komponentów.

5.8. Uruchamianie wielu modułów wewnętrznych tego samego typu przez mMDAB

Komponent mMDAB daje możliwość uruchamiania wielu modułów wewnętrznych tego samego typu, tzn. możliwe jest uruchomienie np. trzech modułów mMWS. W celu uruchomienia wielu modułów wewnętrznych przez mMDAB konieczne jest umieszczanie kolejnych jego instancji w osobnych folderach o nazwach według następującego wzorca: typModułu_dodatkowaNazwa. Jeżeli chodzi o typ modułu to musi być on dokładnie taki sam jak rodzaj modułu, który będzie uruchamiany np. mMWS. Dodatkowa nazwa pozwala identyfikować moduł wewnętrzny, przykładem może być nazwa Test. Ważne jest to, aby typ modułu odseparować od nazwy dodatkowej separatorem jakim jest „_”, jest to konieczne w celu prawidłowego działania aplikacji. Dodatkowym obostrzeniem jest, aby nazwa folderu nie zawierała żadnego dodatkowego znaku specjalnego poza pojedynczym znakiem separującym wspomnianym wcześniej. Każdy z modułów mMWS powinien zostać skonfigurowany poprzez plik appsettings.json znajdującym się w folderze każdego modułu w celu poprawnego łączenia się z bazą danych mMedica.

Przykładowa konfiguracja dla modułów wewnętrznych typu mMWS:

1. Utworzyć wewnątrz katalogu „modules” komponentu mMDAB dwa foldery o nazwie mMWS_Test oraz mMWS_Test2.
2. Umieścić pliki aplikacji mMWS wewnątrz tych folderów.
3. Uruchomić aplikację zgodnie z wersją wykorzystywanego systemu Windows (*3.15 Restartowanie i zatrzymywanie komponentów*) lub Linux *(4.12 Restartowanie i zatrzymywanie komponentów).*
4. Po uruchomieniu moduły będą dostępne pod adresami http://adresmMDAB/mMWS_Test oraz http://adresmMDAB/mMWS_Test2.

6. Zarządzanie oraz kopie zapasowe baz danych

6.1. Kopie bazy danych

Wykonywanie kopii baz danych eRejestracji oraz ich odtwarzanie możliwe jest za pomocą aplikacji mMBackup.exe, która jest częścią składową oprogramowania mMedica. Podobnie jak w przypadku wykonywania kopii bazy danych mMedica, stan bazy danych jest zapisywany do pliku o rozszerzeniu ZIP, który w nazwie zawiera informacje o dacie, godzinie i nazwie bazy danych.

6.1.1. Wykonywanie kopii bazy danych

Aby wykonać kopię bazy należy z poziomu wiersza poleceń systemu Windows (Menu Start\Uruchom – skrót: klawisz Windows + r, następnie wpisać „cmd” i zatwierdzić) wpisać:

```
„[Ścieżka do mMedica]\mMBackup.exe” [Baza danych eRejestracji] backup
```

Przykład wykonywania kopii dla domyślnej ścieżki instalacji i bazy danych o nazwie „ERMMEDICA”:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ERMMEDICA backup
```

Następnie w oknie podać miejsce zapisu kopii bazy danych oraz nazwę użytkownika z uprawnieniami administratora w Portalu (domyślnie „admin”), hasło oraz nacisnąć przycisk „Start”.

6.1.2. Odtwarzanie bazy danych

Odtworzenie kopii bazy danych wygląda w bardzo zbliżony sposób. Również z poziomu wiersza poleceń należy wpisać:

```
„[Ścieżka do mMedica]\mMBackup.exe” [Baza danych eRejestracji] restore
```

Przykład odtwarzania kopii dla domyślnej ścieżki instalacji i bazy danych o nazwie „ERMMEDICA”:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ERMMEDICA restore
```

W oknie należy wybrać ścieżkę do pliku kopii bazy danych i nacisnąć przycisk „Start” (nie jest wymagane ponowne podawanie nazwy użytkownika oraz hasła). W oknie odzyskiwania danych można również zmienić adres serwera bazy danych oraz odczytać wersję bazy danych. Kopia bazy danych może zostać odtworzona pod inną nazwą niż pierwotna.

6.1.3. Operacje na zdalnym serwerze PostgreSQL

Wykonywanie kopii lub odtwarzanie bazy danych na zdalnym serwerze PostgreSQL wymaga dodatkowej konfiguracji. W tym celu należy:

1. Otworzyć do edycji plik DBXCONNECTIONS.INI znajdujący się w katalogu programu mMedica.
2. Dodać lub zmienić wpisy według poniższego wzoru:

```
[ERMMEDICA_LNX]
DriverName=PostgreSQL
Database=10.3.4.138:5432/ERMMEDICA
```

   „[ERMMEDICA_LNX]" oznacza alias jaki będzie podawany w poleceniu mMBackup.exe.

   W „Database" określa się kolejno adres IP oraz port nasłuchu serwera PostgreSQL, a po ukośniku nazwę bazy danych modułu.

3. Zapisać plik.
4. Wykonać polecenie wykonania lub odtworzenia kopii, dla powyższego przykładu:
   a. Wykonanie kopii bazy danych „ERMMEDICA_LNX":

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ERMMEDICA_LNX backup
```

   b. Odtworzenie kopii bazy danych „ERMMEDICA_LNX":

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ERMMEDICA_LNX restore
```

Istnieje również możliwość utworzenia nowej bazy danych na podstawie istniejącej kopii (odtworzenie bazy pod inną nazwą) na zdalnym serwerze. Aby dokonać takiej operacji należy:

1. Wykonać polecenie odtwarzania kopii bazy danych „ERMMEDICA_LNX:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ERMMEDICA2_LNX restore
```

   „ERMMEDICA2_LNX" będzie nazwą dla nowej bazy danych.

2. W oknie programu mMBackup w polu serwer należy podać adres IP zdalnego serwera PostgreSQL.

Uwaga: Serwer PostgreSQL musi zezwalać na zdalną komunikację, a oprogramowanie typu firewall musi zezwalać na komunikacje na wybranym porcie.

6.1.4. Uproszczenie wykonywania kopii

Możliwe jest również utworzenie skrótu do mMBackup.exe, który będzie wykonywał kopię lub odzyskiwanie bazy danych. W tym celu należy wejść do katalogu domyślnej instalacji oprogramowania mMedica (domyślnie: C:\Program Files\Asseco\mMedica lub C:\Pliki programów (x86)\Asseco\mMedica), zaznaczyć

prawym przyciskiem myszy plik mMBackup.exe i wybrać pozycję „Utwórz skrót”, a następnie umieścić go w żądanym miejscu. Następnie kliknąć prawym przyciskiem myszy na skrót i wybrać opcję „Właściwości” i zmodyfikować pole „Element docelowy” tak, aby zawierało ono polecenie „backup” lub „restore” dla wybranej bazy danych:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ERMMEDICA restore
```

7. Bezpieczeństwo modułu

Rozdział opisuje jedynie najczęściej stosowane praktyki zapewnienia bezpieczeństwa informacji. Ostateczna decyzja dotycząca wprowadzenia zabezpieczeń należy do administratora. Ponadto obowiązkiem administratora jest aktualizacja zabezpieczeń zgodnie z powstającymi nowymi standardami bezpieczeństwa oraz zmianami w obowiązującym prawie.

7.1. Infrastruktura

7.1.1. Zewnętrzny hosting lub VPS

Komponenty eRejestracji mogą być instalowane zarówno we własnej infrastrukturze jak i za pośrednictwem usług firm zewnętrznych (hosting lub VPS). VPS, czyli wirtualny, prywatny serwer daje więcej możliwości konfiguracyjne i pozwala na zarządzanie jak zwykłym komputerem. Rekomenduje się, aby moduł eRejestracja (szczególnie w przypadku jednostanowiskowej infrastruktury) nie był zainstalowany na komputerze przeznaczonym do zadań użytkowych np. pracy biurowej. Minimalizuje to ryzyko związane z ingerencją złośliwego oprogramowania, jak i spadków wydajności komputera czy połączenia sieciowego.

7.1.2. Protokół SSL

Wysoce zalecane jest stosowanie protokołu SSL, który zapewnia szyfrowanie transmitowanych danych. Dzięki temu przesyłane dane, w przypadku przechwycenia, nie zostaną odczytane ani zmodyfikowane. Dla pełnego bezpieczeństwa protokół powinien zostać użyty dla wszystkich elementów modułu eRejestracja, w tym również dla usług mMDAB.

Protokół będzie spełniał swoją rolę wyłącznie, gdy wszędzie będą używane adresy internetowe wykorzystujące ten protokół. Z tego powodu nie zaleca się ustawienia podwójnego protokołu dostępu HTTP oraz HTTPS na serwerach WWW. Sposób konfiguracji SSL powinien zostać dostarczony przez dostawcę certyfikatu.

W przypadku zastosowania protokołu SSL dla Portalu, użytkownicy będą informowani przez przeglądarkę internetową o istnieniu bezpiecznego połączenia ze stroną, co pozwala użytkownikowi na wykrycie przypadku phishingu, czyli podmiany strony na łudząco podobną, służącą do wyłudzenia danych osobowych lub autoryzacyjnych.

7.1.3. VPN

W przypadku, w którym architektura komponentów eRejestracji, aplikacji mMedica oraz baz danych jest rozproszona, warto rozważyć zastosowanie tunelu VPN pomiędzy poszczególnymi elementami modułu eRejestracja. Zastosowanie VPN pozwala na utworzenie prywatnej, wirtualnej sieci o ograniczonym dostępnie, do której mogą być podłączone komputery z bazami danych oraz wszystkimi modułami eRejestracji. W takiej konfiguracji zasadne jest ustawienie udostępniania na adresie publicznym wyłącznie Portalu. Zaleca się takie podejście szczególnie w przypadku, w którym nie jest możliwe zastosowanie SSL dla komponentów mMDAB.

7.2. Oprogramowanie

7.2.1. Konta użytkowników

Komputer, na którym zainstalowane są komponenty eRejestracji, powinien posiadać aktualny system operacyjny oraz aktualne oprogramowanie wspierające bezpieczeństwo (np. oprogramowanie antywirusowe).

Dostęp do systemu operacyjnego powinien być zabezpieczony hasłem poprzez indywidualne konto dla każdego użytkownika systemu. Ponadto hasło powinno podlegać przymusowej zmianie co ściśle określony interwał czasu.

Należy również rozważnie konfigurować oraz korzystać z usług zdalnych połączeń do komputera (usługi typu RDP). W celu zwiększenia stopnia bezpieczeństwa poleca się stosowanie szyfrowanych nośników do przechowywania baz danych eRejestracji.

7.2.2. Oprogramowanie antywirusowe

Dodatkowo zaleca się stosowanie ochrony antywirusowej wraz z aktualną bazą definicji szkodliwego oprogramowania. Ochrona antywirusowa powinna mieć skonfigurowane okresowe skanowanie systemu oraz włączoną ochronę w czasie rzeczywistym.

7.2.3. Firewall

Kolejnym ważnym aspektem jest instalacja i konfiguracja zapory ogniowej (firewall). Zapora powinna zezwalać wyłącznie na ruch usług, które są świadomie uruchomione na komputerze. W przypadku komponentów eRejestracji wymaga się odblokowania portu HTTP (80) lub/oraz HTTPS (443) lub innych w zależności

od konfiguracji serwera WWW, portu do serwera bazy danych (jeżeli jest to wymagane, domyślnie 5432), a także portu do komunikacji z serwerem poczty wychodzącej.

Przy konfiguracji zapory ogniowej rekomenduje się stosowanie podejścia, w którym punktem wyjścia jest blokada komunikacji, a następnie świadome dodawanie pojedynczych reguł zezwalających dla komunikacje dla usług, aplikacji oraz na numerach portów. Takie podejście jest zalecane wyłącznie osobom posiadającym wiedzę techniczną, gdyż istnieje ryzyko zablokowania komunikacji, która jest wymagana do prawidłowego i bezpiecznego działania systemu operacyjnego oraz zainstalowanych aplikacji czy usług.

7.2.4. Nieużywane protokoły TCP IP oraz protokoły serwera WWW

Zaleca się wyłącznie na serwerze obsługi protokołów TCP, której nie są używane (np. IPv6). Brak takich działań może skutkować negatywnie m.in. w przypadku, w którym administrator zapomni o odpowiednim skonfigurowaniu zapory ogniowej dla nieużywanego protokołu lub w aplikacji serwera WWW (IIS, Apache).
Instrukcja wyłączenia IPv6 dla Windows:

1. Przejść do „Panelu Sterowania”.
2. Uruchomić „Centrum sieci i udostępniania”.
3. Wybrać „Zmień ustawienia karty sieciowej”.
4. Kliknąć prawym przyciskiem myszy i wybrać z menu kontekstowej „Właściwości” po kolei na każda z aktywnych kart (fizyczne oraz wirtualne), które komunikują się z siecią.
5. Odznaczyć w oknie „Internet Protocol Version 6 (TCP/IPv6)”.
6. Zapisać zmiany.

Serwery WWW (IIS, Apache) również powinny zostać skonfigurowane tak, aby udostępniać wyłącznie aktywne protokoły komunikacji (np.: http, https, ftp) i to wyłącznie na aktywnych protokołach TCP (IPv4, IPv6).
Instrukcja wyłączania protokołów dla IIS:

1. Uruchomić IIS.
2. W menu „Połączenia” prawym przyciskiem myszy uruchomić menu kontekstowe witryny, której ustawienia należy zmienić (np. Default Web Site).
3. Z menu kontekstowego wybrać opcję „Edytuj powiązania…”.
4. W oknie powiązań zostaną wyświetlone wszystkie uruchomione protokoły komunikacji aplikacji (typy) oraz przypisane adresy IP (symbol * oznacza wszystkie adresy), które wynikają z aktywnych protokołów TCP.

5. Za pomocą opcji „Edytuj…” można zmienić już istniejące w tabeli wpisy. Wpisy można również dodać lub usunąć za pomoc przycisków kolejno „Dodaj…” oraz „Usuń”.
6. Po wprowadzeniu zmian okno „Powiązania witryny” można zamknąć za pomocą przycisku „Zamknij”.

7.2.5. Poczta wychodząca

Serwer poczty wychodzącej (SMTP), który jest konieczny do wysyłania wiadomości email z eRejestracji, powinien działać z wykorzystaniem protokołu TLS oraz posiadać logowania za pomocą nazwy użytkownika oraz hasła. Wyjątkiem może być sytuacja, w której serwer SMTP jest zainstalowany na tym samym komputerze, co reszta komponentów eRejestracji.

7.3. Konfiguracja modułu

Dobrą praktyką jest utworzenie dodatkowego konta administratora, które umożliwi dostęp do Portalu, w przypadku zablokowania lub utracenia hasła do konta domyślnego.

W przypadku użycia protokołu HTTPS lub/oraz VPN, należy posługiwać się właściwymi dla wymienionych technologii adresami w:

- mMedica: właściwe adresy mMWS oraz eRWS w konfiguracji modułu eRejestracja,
- eRejestracja: konfiguracja adresów mMWS oraz adresu Portalu w konfiguracji podstawowej.

W konfiguracji wielostanowiskowej zaleca się wprowadzenie ograniczenia na adresy IP, jakie mogą łączyć się z serwerem bazy danych. W katalogu „data” w ścieżce instalacji bazy danych znajduje się plik pg_hba.conf, który pozwala na podanie zakresu adresów IP lub konkretnego adresu IP (dotyczy to również adresów VPN). Pełną specyfikację konfiguracji dostępu do bazy danych można odnaleźć na stronie producenta bazy danych PostgreSQL.

7.4. Zabezpieczenia modułu

7.4.1. Token bezpieczeństwa

Komunikacja pomiędzy poszczególnymi komponentami eRejestracji a aplikacją jest autoryzowana przy udziale hasła usług sieciowych, na podstawie którego powstaje token bezpieczeństwa. Nie jest więc możliwe połączenie komponentów bez wspólnego hasła usług sieciowych.

7.4.2. Blokowanie adresów IP oraz kont

Portal zawiera mechanizm blokowania adresów IP komputerów, z których dochodzi do wielokrotnej nieudanej próby logowania na nieistniejącego użytkownika. W przypadku, w którym dochodzi do nagminnej próby nieprawidłowego logowania na istniejące konto, następuje jego blokada. Administrator ma możliwość konfiguracji dopuszczalnej liczby niepoprawnych logowań, jak i usunięcia adresu IP oraz odblokowania użytkownika. Powyższe funkcjonalności mają za zadanie ograniczać możliwość logowania do Portalu za pomocą używania metod siłowych (brute force).

Usługa eRWS posiada również swój własny mechanizm blokowania adresów IP komputerów, z których następuje wielokrotna próba zalogowania się do usługi przy użyciu nieprawidłowego hasła usług sieciowych. Administrator również ma możliwość osobnej dla eRWS konfiguracji dopuszczalnej liczby niepoprawnych logowań, jak i odblokowania adresu IP.

7.4.3. Zabezpieczenie przed spamem

Adres kontaktowy email do administratora (definiowany z konfiguracji) jest zabezpieczony przed możliwością jego przechwycenia przez roboty wysyłające SPAM. Dodatkowo istnieje możliwość konfiguracji zabezpieczenia reCAPTCHA, które pojawi się w momencie tworzenia nowych kont.

7.4.4. Inne

Portal posiada bezpieczny mechanizm resetowania hasła na żądanie użytkowników, w którym na adres email użytkownika nie trafia hasło, lecz specjalny kod, który pozwala na stronie Portalu dokonać nadania nowego hasła. Portal posiada mechanizm zbierania informacji o błędach oraz ewentualnych próbach włamań do dziennika systemowego umieszczonego w Portalu. Dziennik systemowy umożliwia administratorowi Portalu eksport wpisów z dziennika systemowego do zaszyfrowanego pliku, który może zostać wysłany do analizy Serwisu mMedica.

Zaimplementowany mechanizm autoryzacji zapewnia rozdzielenie poziomu wyświetlanej treści (niezalogowany użytkownik, zalogowany użytkownik, administrator). Walidacja pól w formularzach odbywa się zarówno po stronie przeglądarki, jak i serwera.

Dostęp do bazy danych eRejestracji jest zabezpieczony przed możliwością bezpośredniej (z pominięciem oprogramowania mMedica) ingerencji w bazę danych. Wszystkie newralgiczne dane, które są przechowywane po stronie bazy danych eRejestracji są zapisywane w formie niejawnej tj. z wykorzystaniem funkcji mieszających lub nowoczesnych algorytmów szyfrowania.

7.5. Filtrowanie komunikacji z wybranymi adresami IP

7.5.1. Filtrowanie komponentów

Dla każdego z komponentów możliwe jest poprzez plik konfiguracyjny appsettings.json ustawienie filtrowania komunikacji z wybranymi adresami IP. Dostępne są dwa tryby pracy:

- W pierwszym dostęp do zasobów strony jest odmawiany wszystkim użytkownikom o wskazanych adresach.
- W drugim dostęp do zasobów jest udostępniony jedynie użytkownikom o wskazanym adresie IP.

Proces konfiguracji filtrowania komunikacji z wybranymi adresami IP wygląda następująco:

1. Otworzyć plik appsettings.json z prawami administratora do edycji.
2. Wyszukać fragmenty (identyczne lub podobne) lub utworzyć następujące sekcje:
   a. Portal:

```
"IpFilteringOptionPortal": 0,
"SetOfIpAddressesPortal": "192.168.137.1;192.168.137.10-192.168.20",

"IpFilteringOptioneRWS": 0,
"SetOfIpAddresseseRWS": "192.168.137.1;192.168.137.10-192.168.20"
```

Uwaga: Pierwsze dwa parametry odpowiadają za konfigurację filtrowania komunikacji z wybranymi adresami IP na portalu eRejestracja, a dokładniej za możliwość zalogowania się na konto administratora jedynie z wybranych adresów IP.
Kolejne dwa parametry odpowiadają za konfiguracje komunikacji z modułem eRWS.

   b. mMDAB:

```
"IpFilteringOption": 0,
"SetOfIpAddresses": "192.168.137.1;192.168.137.10-192.168.20"
```

   c. mMWS:

```
"IpFilteringOption": 0,
"SetOfIpAddresses": "192.168.137.1;192.168.137.10-192.168.20"
```

Opis parametrów:

"IpFilteringOption": 0 – parametr ten można ustawić na trzy sposoby. Ustawiając jego wartość na 0 wyłączone zostanie filtrowanie komunikacji. Wartość 1 spowoduje blokowanie komunikacji z adresami zdefiniowanymi w sekcji "*SetOfIpAddresses*". Z kolei ustawienie na wartość 2 pozwoli na dostęp do zasobów jedynie użytkownikom o wskazanych w sekcji "*SetOfIpAddresses*" adresach IP.

"SetOfIpAddresseseRWS": "192.168.137.1;192.168.137.10-192.168.20" – w sekcji tej podaje się adresy IP, które mają być brane pod uwagę. Adresy można podawać na dwa sposoby:

- Jako pojedyncze adresy 192.168.137.1,
- Jako pule adresów 192.168.137.10-192.168.20. Pule adresów należy odczytywać jako zakres adresów np. pula 192.168.137.10-192.168.20 oznacza adresy 192.168.137.10, 192.168.137.11, 192.168.137.12 … aż do 192.168.137.20.

Kolejne pojedyncze adresy bądź pule adresów należy rozdzielać separatorem „;".

3. Zrestartować moduły. W zależności od systemu odpowiednio Windows (*3.15 Restartowanie i zatrzymywanie komponentów*) lub Linux (*4.12 Restartowanie i zatrzymywanie komponentów*).

7.5.2. Filtrowanie logowania administratora

Na podobnej zasadzie jak filtrowanie IP dla komponentów (poprzedni podrozdział) istnieje możliwość filtrowania z jakich adresów IP użytkownik może lub nie może zalogować się na użytkownika z grupy administratorów lub konkretne konto administratora.

Konfiguracja odbywa się przez dodanie lub edycję elementu „IpFilteringPortalLogon" w pliku Portal\appsettings.json. Należy pamiętać, że elementy na tym samym poziomie zagnieżdżenia w pliku appsettings.json muszą być rozdzielone przecinkiem (zgodnie z formatem JSON). Przykład wpisu wraz z opisem:

```
"IpFilteringPortalLogon": {
  "Admins": {
    "Option": 2,
    "Addresses": "192.168.137.1-192.168.140.138",
    "Users": [
      {
        "Login": "admin",
        "Option": 2,
        "Addresses": "192.168.137.1"
      },
      {
        "Login": "admin2",
        "Option": 2,
        "Addresses": "192.168.137.1-192.168.137.254"
      }
    ]
  }
}
```

Poziom	Nazwa elementu	Krotność	Opis
1	Admins	1	Konfiguracja dla grupy administratorów
2	Option	1	Rodzaj filtrowania dla grupy: 0 – wyłączona funkcja, 1 – blokowania dla wskazanego adresu/adresów IP, 2 – dopuszczenie wyłącznie blokowania dla wskazanego adresu/adresów IP.
2	Addresses	1	Adres IP lub lista adresów IP lub zakres zakresów IP.
3	Users	0 lub 1	Tablica skonfigurowanych użytkowników. Element opcjonalny.
4	Element tablicy Users	Od 0 do N	Konfiguracja wybranego konta administratora.
5	Login	1	Nazwa konta administratora.
5	Option	1	Rodzaj filtrowania dla użytkownika: 0 – wyłączona funkcja, 1 – blokowania dla wskazanego adresu/adresów IP, 2 – dopuszczenie wyłącznie blokowania dla wskazanego adresu/adresów IP
5	Addresses	1	Adres IP lub lista adresów IP lub zakres zakresów IP.

Definiowanie filtrowania dla poszczególnych użytkowników jest opcjonalne (element „Users”). Jeśli nie zdefiniowano filtrowania dla wybranego konta to mechanizm filtrowania uwzględni konfigurację dla grupy.

Konfiguracja dla konta użytkownika zawsze ma pierwszeństwo nad konfiguracją dla grupy administratorów. W przypadku wielokrotnego wpisu dotyczącego danego konta administratora, mechanizm uwzględni wyłącznie pierwszy wpis. Definiowanie rodzaju filtrowania w elemencie „Options” oraz adresu/adresów IP w element „Addresses” jest takie samo jak filtrowaniu IP dla komponentów.

Przykład dla filtrowania IP wyłącznie dla grupy z dopuszczeniem logowania dla lokalnego adresu IPv4:

```
"IpFilteringPortalLogon": {
  "Admins": {
    "Option": 2,
    "Addresses": "127.0.0.1"
  }
}
```

Poniżej przedstawiono przykład z filtrowaniem dla grupy po zakresie IP (logowanie dopuszczone dla 192.168.1.1 – 192.168.1.254) oraz dopuszczenie logowania dla adresów IP 192.168.1.2 oraz 192.168.1.5 na użytkownika „admin”, z jednoczesnym blokowaniem logowania dla adresu IP 192.168.1.5 na użytkownika „admin2”:

```
"IpFilteringPortalLogon": {
  "Admins": {
    "Option": 2,
    "Addresses": "192.168.1.1-168.168.1.254",
    "Users": [
      {
        "Login": "admin",
        "Option": 2,
        "Addresses": "192.168.1.2;192.168.1.5"
      },
      {
        "Login": "admin2",
        "Option": 1,
        "Addresses": "192.168.1.5"
      }
    ]
  }
}
```

7.6. Wymuszenie korzystania z protokołu HTTPS

Dla Portalu możliwe jest wymuszenie korzystania z połączeń zaszyfrowanych za pomocą SSL poprzez plik konfiguracyjny appsettings.json. W tym celu wykorzystywany jest atrybut Strict-Transport-Security. Aby aktywować atrybut należy wykonać następujące kroki:

1. Otworzyć plik appsettings.json z prawami administratora do edycji.
2. Wyszukać fragment (identyczny lub podobny) i usunąć poprzedzające go ukośniki „//” . Jeśli fragment nie został odnaleziony należy utworzyć następującą sekcję:

```
"StrictTransportSecurity": "max-age=31536000; includeSubDomains",
```

Opis parametrów:

- "max-age=31536000" – obowiązkowy parametr wskazujący czas, w którym przeglądarka ma zapamiętać informacje o tym, że dane żądania są wysyłane za pomocą

zabezpieczonego protokołu. Jednostką, w której podawany jest czas, jest sekunda. Podany w przykładzie czas to jeden rok.

- "includeSubDomains" – opcjonalny parametr informujący przeglądarkę o tym czy należy uwzględnić subdomeny.
- Kolejne parametry należy rozdzielać separatorem „;”.

3. Zrestartować moduł Portalu. W zależności od systemu odpowiednio Windows (*3.15 Restartowanie i zatrzymywanie komponentów*) lub Linux (*4.12 Restartowanie i zatrzymywanie komponentów*).

7.7. Pozostałe zalecenia

Wszystkie używane hasła (np. do kont administracyjnych, usług sieciowych oraz połączenia do SMTP) powinny być silne, tj. rekomenduje się użycie haseł, które zawierają zarówno małe, jak i wielkie litery, cyfry oraz znaki specjalne. Hasło nie powinno również zawierać fraz słownikowych (np. imiona) i fraz związanych bezpośrednio z rodzajem prowadzanej działalności (np. nazwa świadczeniodawcy). Minimalna wymagana długość haseł:

a) hasło do konta administratora: 12 znaków (zalecana minimalna długość 16 znaków),
b) hasło usług sieciowych: 20 znaków.

Lista osób mających dostęp do infrastruktury oraz użytkowników administracyjnych Portalu powinna być ściśle określona, a konta dostępowe powinny być indywidualne.

Osoba odpowiedzialna za infrastrukturę i oprogramowanie powinna okresowo wykonywać sprawdzenia wydajności komputerów, zużycie łącza internetowego oraz przeprowadzać wykonywanie kopii bazy danych eRejestracji. Kopie bazy danych eRejestracji nie powinny być składowane na komputerze, na którym zainstalowany jest serwer bazy danych. Rekomenduje się stosowanie szyfrowanych nośników do przechowywania kopii baz danych. Stanowczo odradza się trzymanie kopii baz danych w katalogach serwerów WWW.

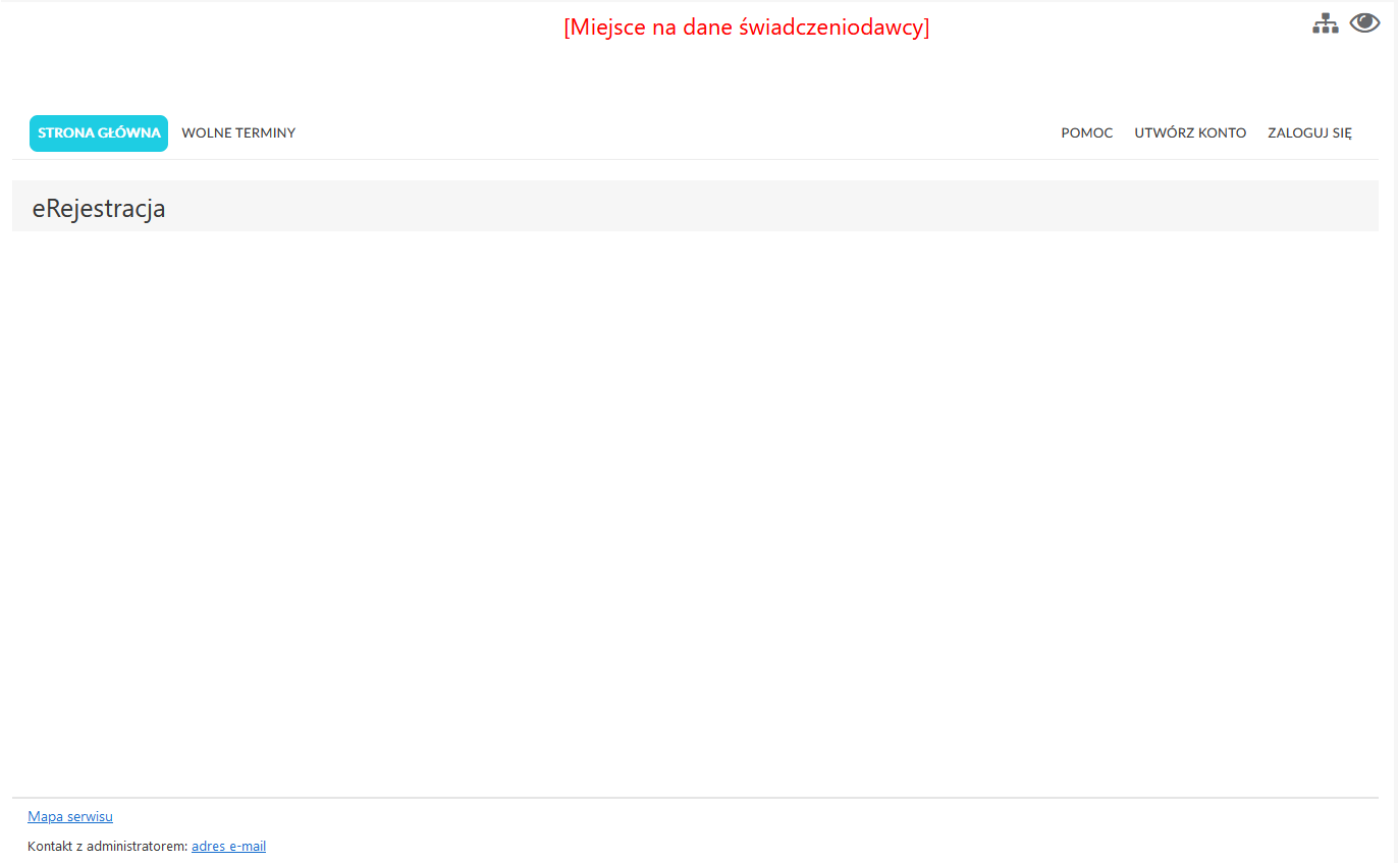
Wszelkie sytuacje, które mogą świadczyć o ingerencji osób nieupoważnionych w infrastrukturę (np. do serwera WWW) wymagają natychmiastowej reakcji. W takim przypadku należy niezwłocznie zmienić hasła dostępowe i – jeżeli to możliwe – dokonać rozłączenia połączonych użytkowników.

8. Konfiguracja w Portalu

8.1. Pierwsze uruchomienie

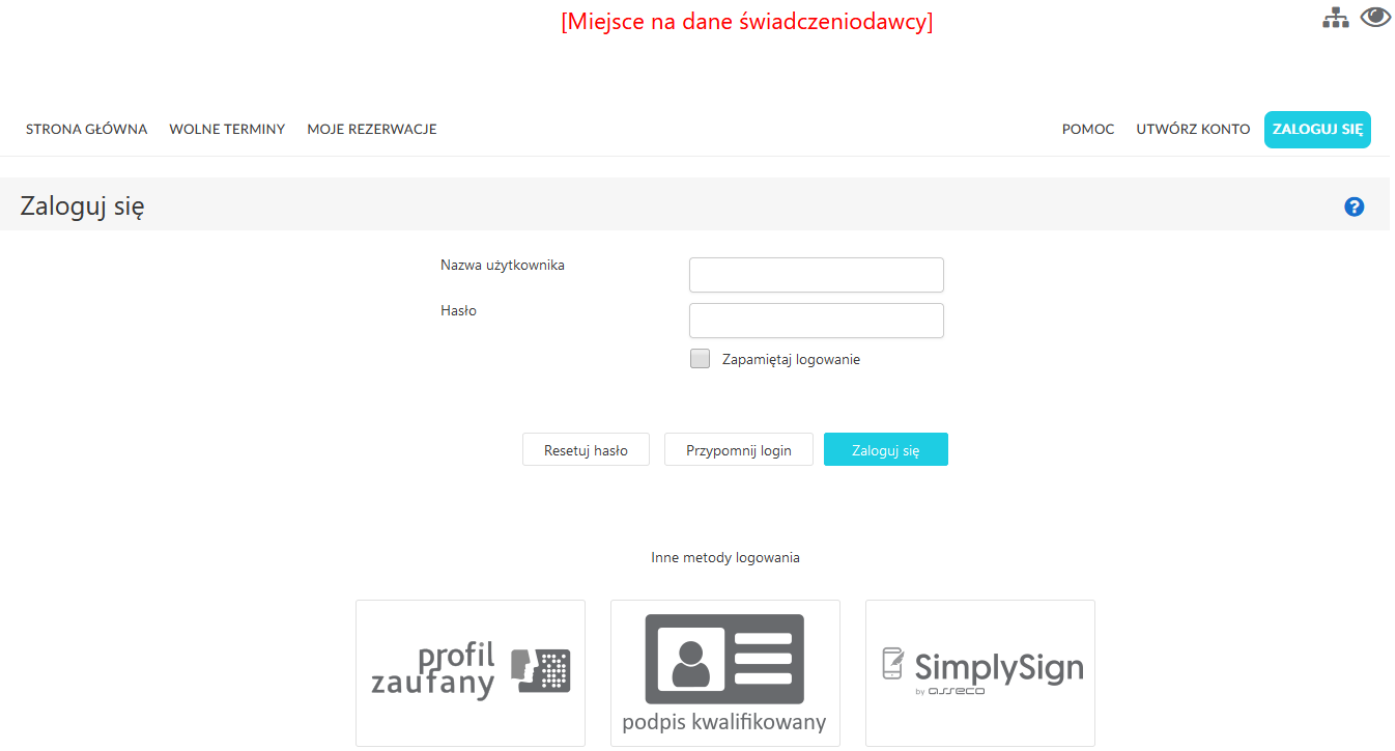
Uwaga: Należy się upewnić, czy systemy operacyjne, na których są zainstalowane komponenty eRejestracji oraz serwery baz danych, mają ustawioną tą samą strefę czasową i możliwie maksymalnie zbliżoną datę oraz czas.

Po otworzeniu Portalu w przeglądarce internetowej powinna zostać wyświetlona strona jak poniżej:



Rysunek 71: Strona główna Portalu

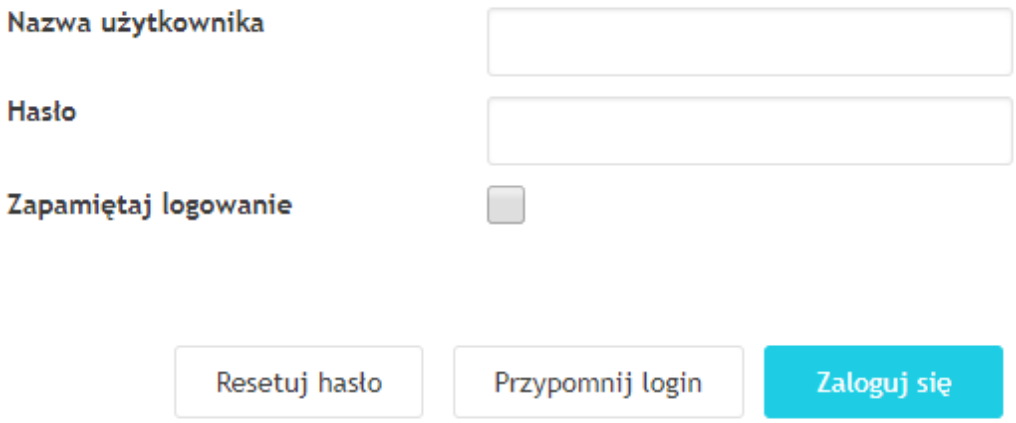
Po wybraniu z prawego, górnego menu opcji „Zaloguj się” pojawi się formatka wyboru logowania.



Rysunek 72: Domyślne metody logowania portalu eRejestracja

Administrator początkowo posiada możliwość zalogowania się poprzez metodę „Logowanie z wykorzystaniem nazwy użytkownika i hasła”. Domyślne dane logowania dla administratora są następujące:

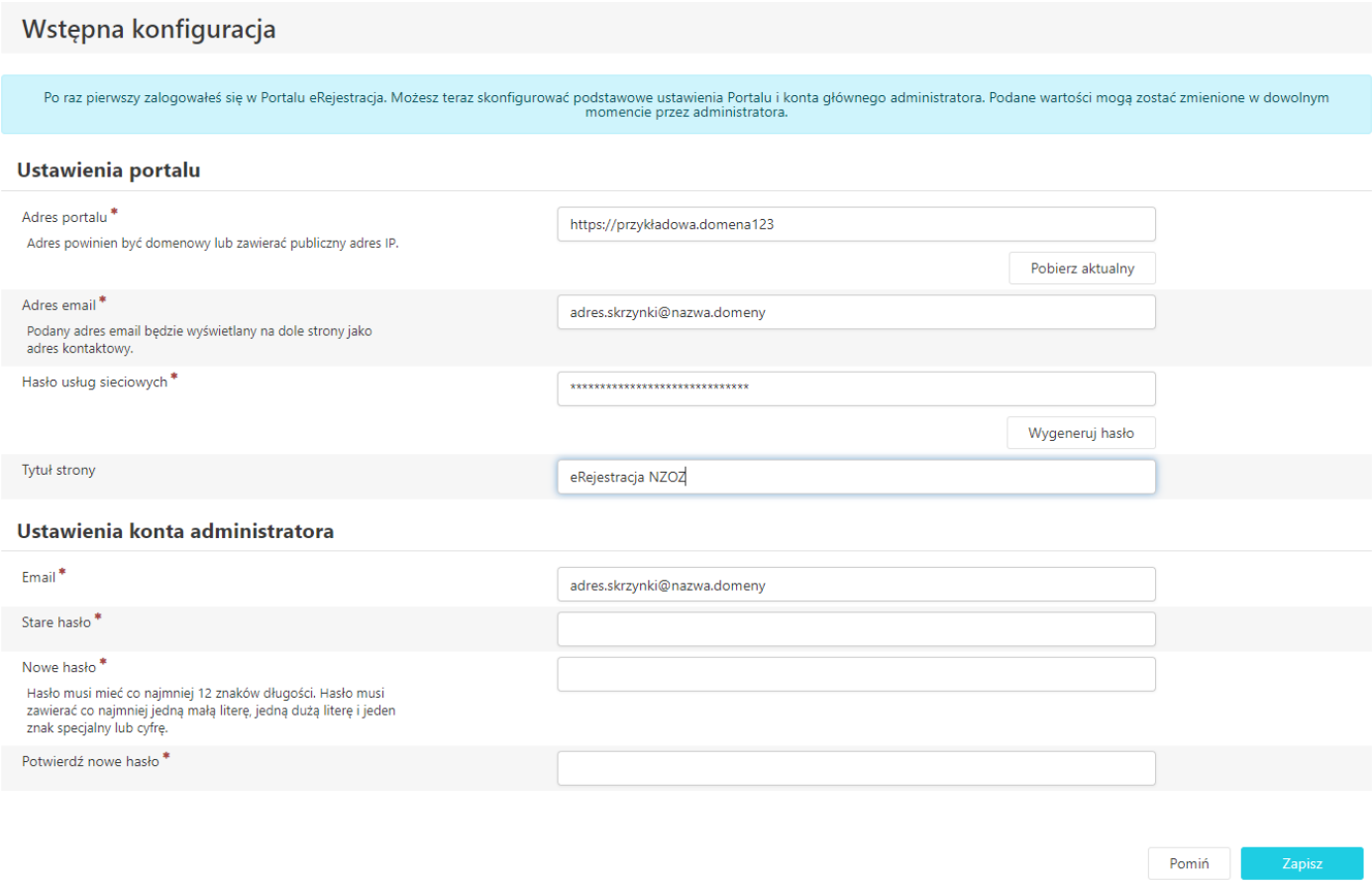
- **nazwa użytkownika:** admin
- **hasło:** test2013



Rysunek 73: Logowanie tradycyjne

Proces logowania nastąpi po wpisaniu danych logowania w odpowiednich polach oraz kliknięciu przycisku „Zaloguj się”. Po dokonaniu tej czynności administrator zostanie zalogowany i przeniesiony na stronę główną portalu.

Po pierwszym logowaniu administratora do Portalu wyświetlona zostaje konfiguracja startowa. Formularz zawiera najważniejsze ustawienia portalu eRejestracja, takie jak jego adres, kontaktowy email, hasło usług sieciowych. Umożliwia także zmianę domyślnego hasła administratora.



Rysunek 74: Konfiguracja po pierwszym zalogowaniu administratora

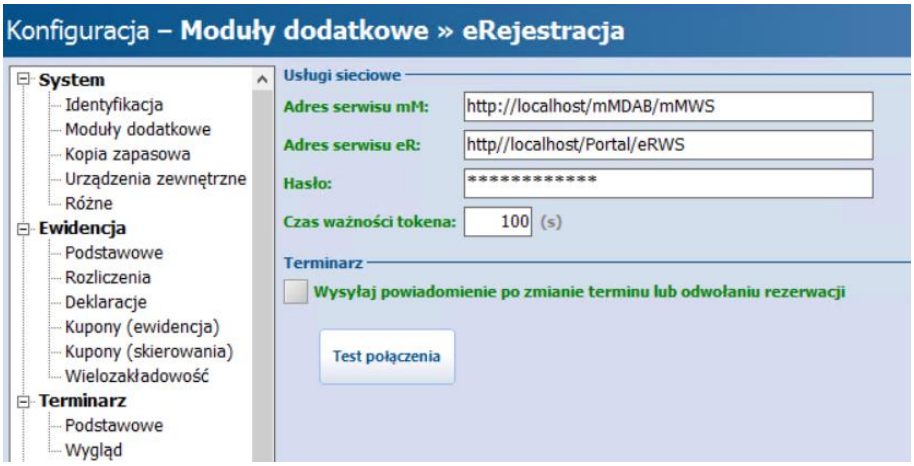
Uwaga: Należy zwrócić dużą uwagę na wpisywane hasło usług sieciowych, gdyż będzie ono wymagane podczas konfigurowania programu mMedica.

Po uzupełnieniu formularza należy zapisać dane naciskając przycisk „Wyślij”. Po zatwierdzeniu nastąpi możliwość skonfigurowania połączenia z serwerem poczty wychodzącej (opis znajduje się w *8.3.9.1.3. Konfiguracja SMTP*). Konfigurację startową można pominąć poprzez wylogowanie się, wejście na stronę główną (przycisk menu) lub naciśnięcie przycisku „Pomiń”. Należy jednak pamiętać, że strona konfiguracji startowej zostaje wyświetlona tylko w przypadku pierwszego logowania domyślnego administratora.

Pełna konfiguracja portalu znajduje się w menu Konfiguracja (*8.2.4. Powiąż z ePUAP\PZ*), natomiast zmianę danych logowania administratora zawarto w menu Moje konto (*8.2. Moje konto*). Zmiana adresu email administratora dokonywana jest poprzez edycję danych administratora z poziomu listy użytkowników (*8.3.3. Rejestr użytkowników*).

8.1.1. Konfiguracja programu mMedica

W programie mMedica należy skonfigurować parametry połączenia z eRejestracja. W Zarządzanie/Konfiguracja/Konfigurator (w kontekście systemu) należy po lewej stronie z sekcji „Moduły dodatkowe” wybrać „eRejestracja”.



Rysunek 75: Przykładowa konfiguracja połączenia z modułem eRejestracja w mMedica

W „Adres serwisu mM” należy wpisać adres usług mMWS (powinien kończyć się frazą „/mMWS”), z kolei w polu „Adres serwisu eR” należy podać adres eRWS (powinien kończyć się frazą „/eRWS”). W kolejnym kroku należy wpisać w pole „Hasło” hasło usług sieciowych, które musi być takie samo jak zdefiniowane w eRejestracji. Pole „Czas ważności tokena” definiuje maksymalny czas ważności tokena bezpieczeństwa, który jest generowany na podstawie hasła usług sieciowych. Celem weryfikacji konfiguracji można posłużyć się przyciskiem „Test połączenia”.

Po konfiguracji adresów w aplikacji mMedica należy sprawdzić ich poprawność wchodząc na stronę statusu mMWS. W przypadku poprawnej konfiguracji adresu eRWS „Połączenie z eRWS” powinno mieć wartość „Tak” (patrz*: 3.12. Weryfikacja instalacji* (Windows) oraz *4.8.* Weryfikacja instalacji (Linux)). W przypadku wyświetlenia komunikatu błędu należy ponownie sprawdzić adres eRWS w Konfiguratorze mMedica.

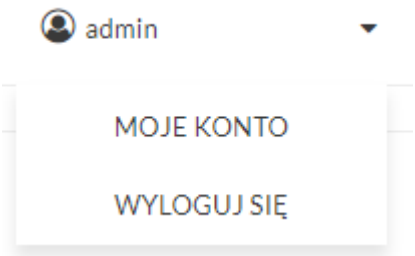
Uwaga: Adres mMWS to http.*adres-mMDAB*/mMWS. Z kolei eRWS znajduje się po adresem http.*adres-Portalu*/eRWS. Wpisane adresy mMWS oraz eRWS powinny rozpoczynać się od typu protokołu tj. „http” lub „https”.

8.1.2. Dodawanie świadczeniodawcy do Portalu

Połączenie oprogramowania mMedica i eRejestracji odbywa się poprzez dodawanie świadczeniodawcy, który polega na dodaniu adresu mMWS w Portalu. Proces został opisany rozdziale *8.3.11. Zarządzanie podmiotami*. Po dodaniu świadczeniodawcy istnieje połączenie eRejestracji z zasobami bazy danych mMedica.

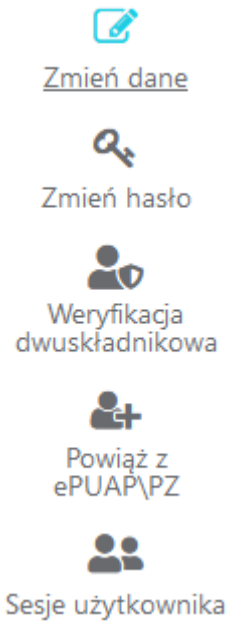
8.2. Moje konto

Po zalogowaniu administratora do portalu, w rozwijanym menu po prawej stronie aplikacji zostanie wyświetlony przycisk „Moje konto". Przycisk ten otwiera stronę zarządzania kontem administratora. Przycisk „Wyloguj się", wylogowuje administratora z konta.



Rysunek 76: Menu rozwijane administratora

Strona zarządzania kontem administratora zawiera trzy główne funkcje: zmianę hasła, ustawienia weryfikacji dwuskładnikowej dla konta oraz możliwość powiązania/odłączenia konta z ePUAP\PZ. Dodatkowo, może znajdować się tam również strona umożliwiająca zarządzanie aktywnymi sesjami użytkownika. Aby móc korzystać z tej opcji, należy wcześniej włączyć ją zaznaczając checkbox obok pola „Informuj o sesjach użytkownika" w zakładce „Zarządzanie" -> „Konfiguracja" -> „Podstawowa" –> „Ogólna". Każda z powyższych funkcji została szczegółowo opisana poniżej.

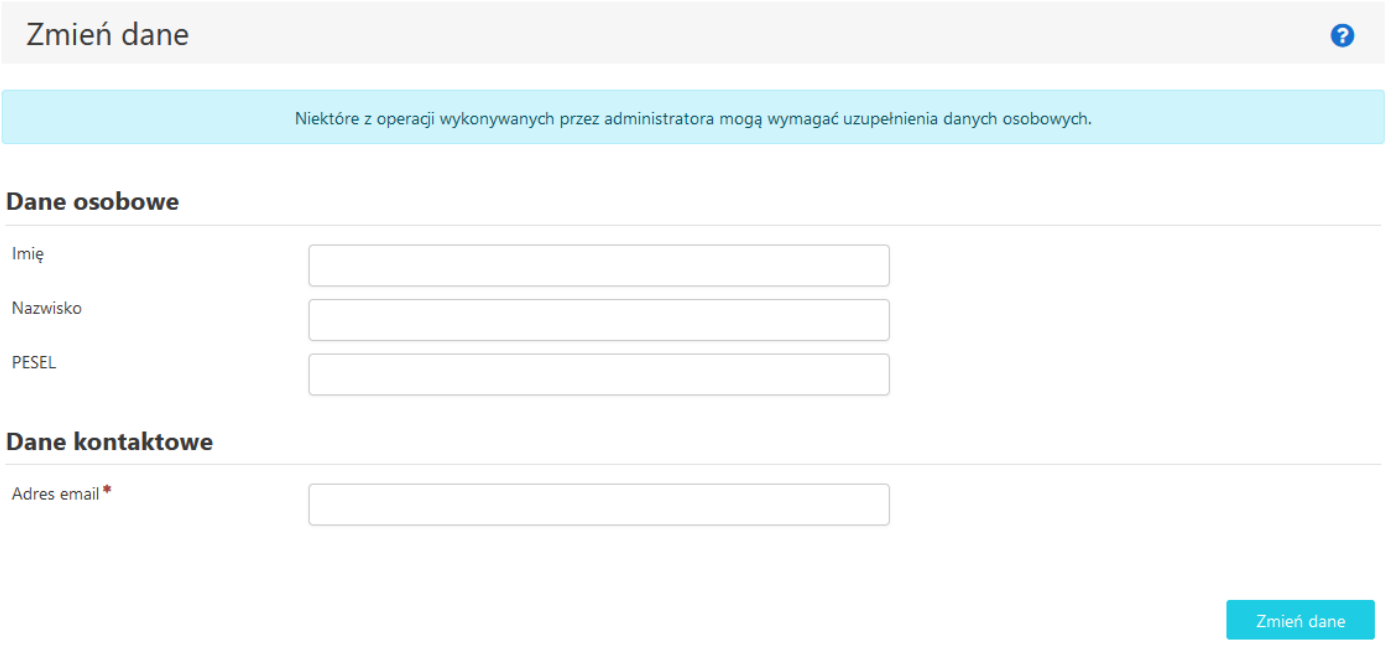


Rysunek 77: Funkcje zarządzania kontem administratora

8.2.1. Zmień dane

Administrator ma możliwość edycji swoich danych z poziomu menu Moje konto/Zmień dane. Na formatce istnieje możliwość uzupełnienia danych osobowych administratora (pola nieobowiązkowe). Dodatkowo istnieje możliwość edycji adresu e-mail w sekcji dane kontaktowe.

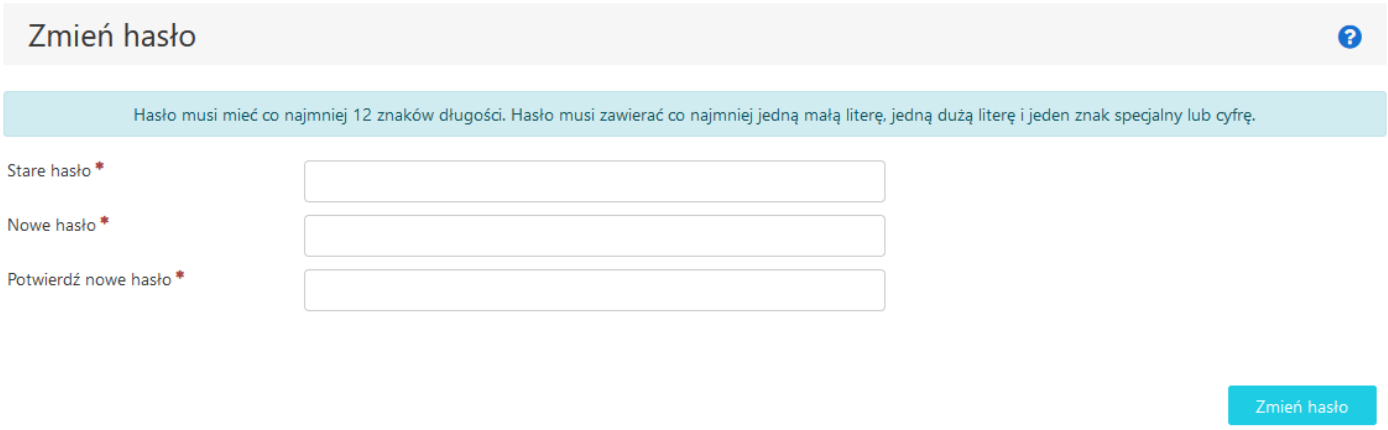
Część funkcjonalności aplikacji może wymagać, aby administrator uzupełnił dane osobowe. W takim przypadku administrator zostanie poinformowany o konieczności uzupełnienia danych.



Rysunek 78: Zmiana danych administratora

8.2.2. Zmiana hasła

W celu zmiany hasła należy zalogować się na konto, a następnie wejść w menu Moje konto/Zmień hasło i wypełnić formularz. Jeśli dane zostaną uzupełnione poprawnie, po naciśnięciu przycisku „Zmień dane” wyświetli się komunikat potwierdzający dokonanie zmiany. Od tej pory administrator może logować się za pomocą zmienionego hasła.



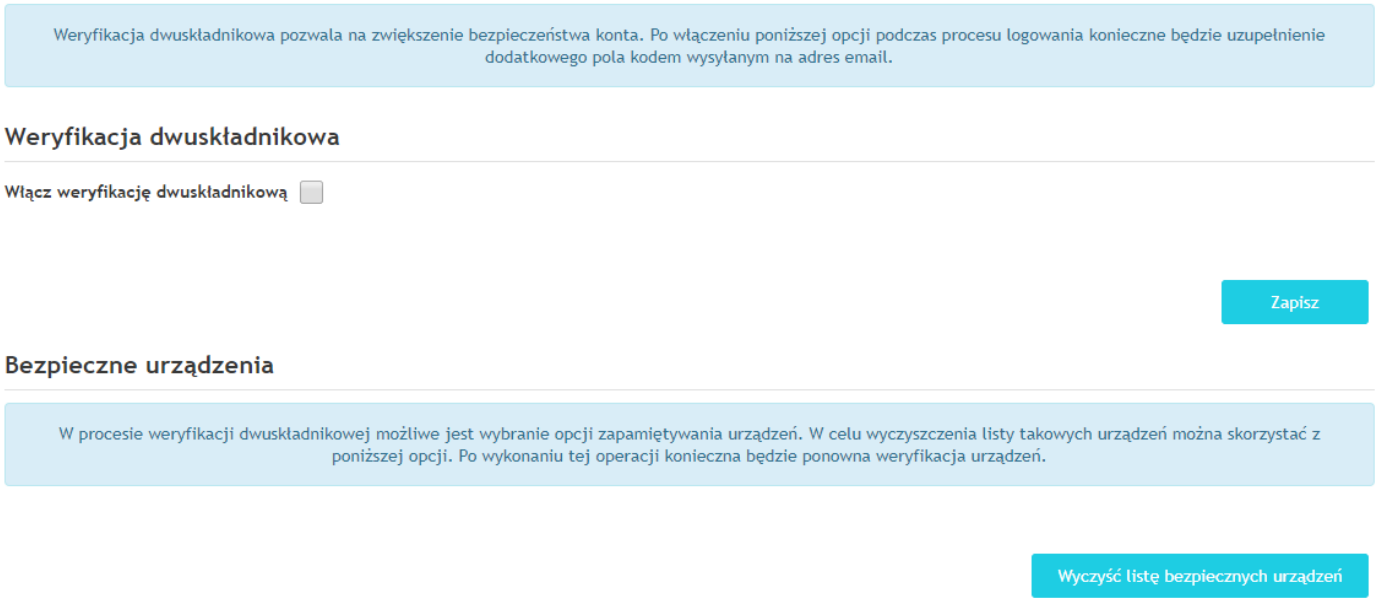
Rysunek 79: Formularz zmiany hasła

8.2.3. Weryfikacja dwuskładnikowa

Weryfikacja dwuskładnikowa jest dodatkową formą zabezpieczenia podczas logowania się na konto. Po włączeniu tej opcji podczas procesu logowania konieczne będzie uzupełnienie dodatkowego pola kodem wysłanym na adres email.

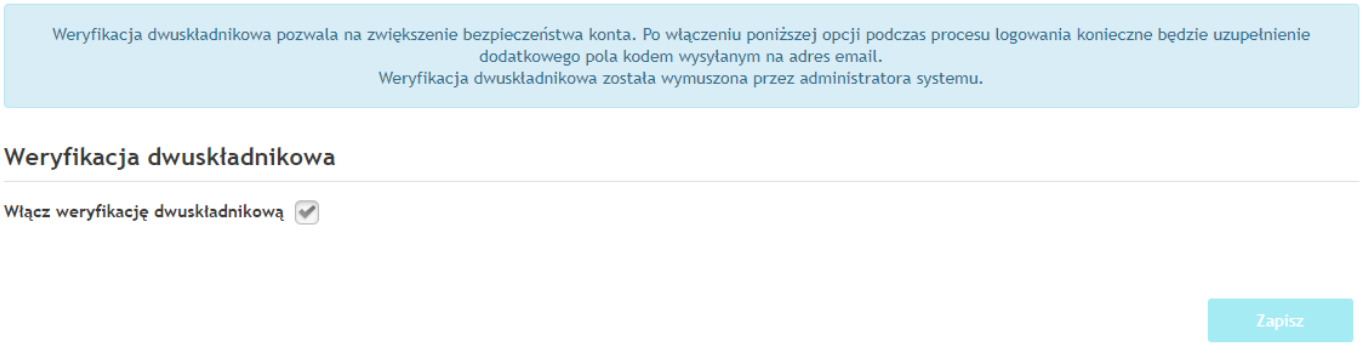
W Portalu eRejestracja użytkownik sam decyduje czy chce mieć włączoną usługę weryfikacji dwuskładnikowej. W tym celu należy odpowiednio zaznaczyć/odznaczyć checkbox przy funkcji „Włącz weryfikację dwuskładnikową” i kliknąć przycisk „Zapisz”.

Dodatkowo podczas logowania istnieje możliwość wybrania opcji zapamiętywania urządzeń. Wówczas logowanie się na takim urządzeniu będzie pomijało dodatkową weryfikację, nawet jeśli będzie ona zaznaczona w polu „Włącz weryfikację dwuskładnikową”. Aby wyczyścić listę bezpiecznych urządzeń, należy kliknąć przycisk „Wyczyść listę bezpiecznych urządzeń”. Po wykonaniu tej operacji konieczna będzie ponowna weryfikacja urządzeń.



Rysunek 80: Strona „Weryfikacja dwuskładnikowa”

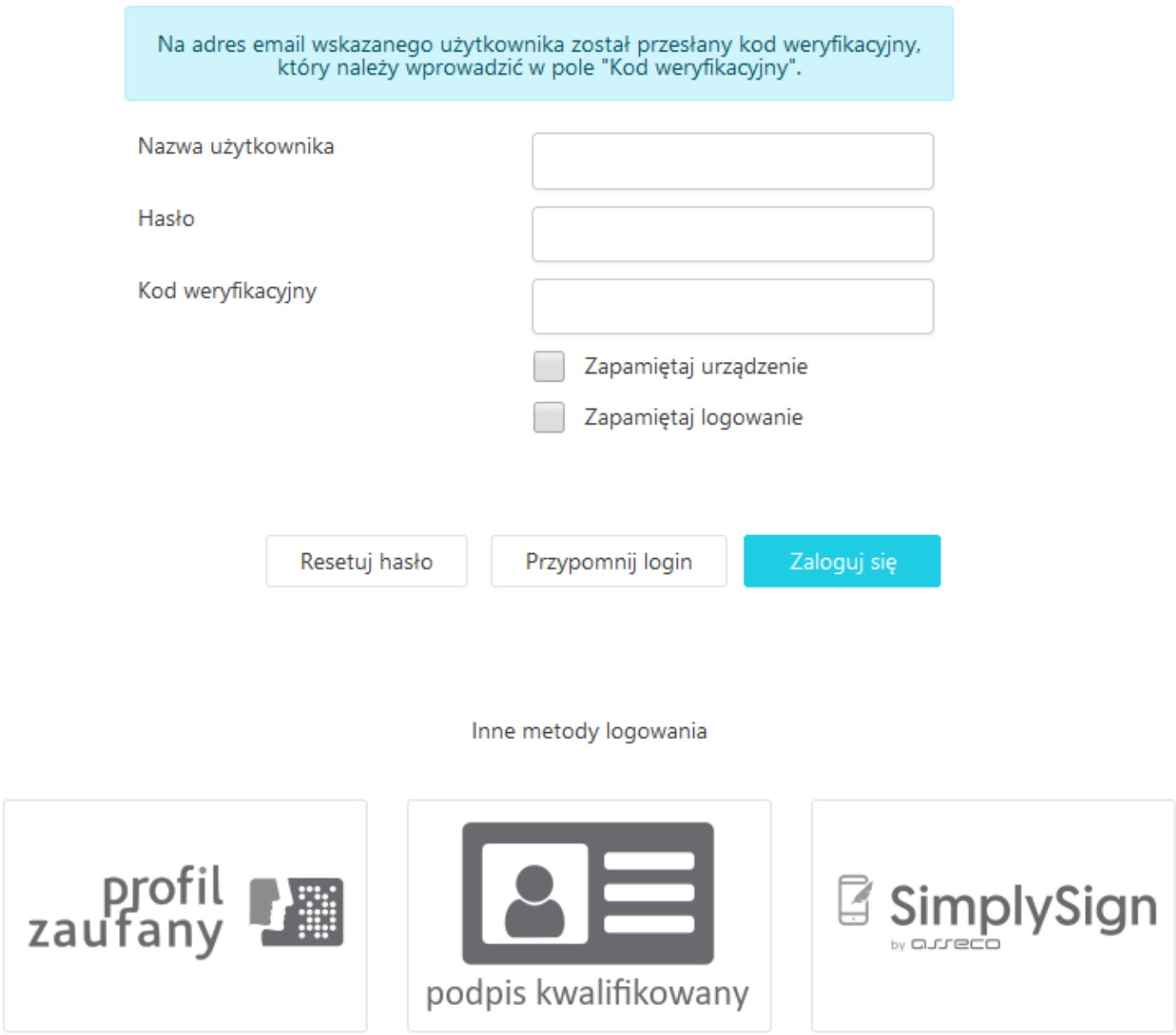
Administrator i/lub personel medyczny może mieć zablokowaną opcję wyłączenia weryfikacji dwuskładnikowej, jeśli wcześniej w zakładce „Zarządzanie” -> „Konfiguracja” -> „Podstawowa” -> „Ogólna”, w dziale „Konta użytkowników” została zaznaczona opcja „Wymuszanie weryfikacji dwuskładnikowej dla administratorów” i/lub „Wymuszenie weryfikacji dwuskładnikowej dla personelu”.



Rysunek 81: Strona „Weryfikacja dwuskładnikowa” – wymuszona weryfikacja dwuskładnikowa dla administratorów

Jeśli użytkownik ma włączoną/wymuszoną opcję weryfikacji dwuskładnikowej, wówczas po poprawnym wypełnieniu pól w formularzu logowania tradycyjnego, pojawi się dodatkowe pole: „Kod weryfikacyjny”. W polu tym należy wpisać kod wysłany na adres e-mail użytkownika.

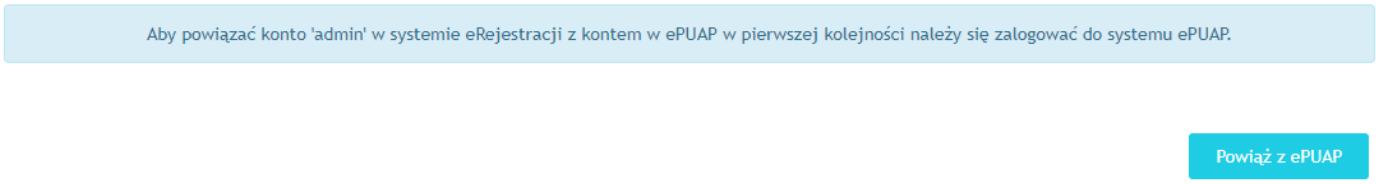
Dodatkowo pojawiła się również opcja „Zapamiętaj urządzenie”, której zaznaczenie powoduje wpisanie urządzenia na listę bezpiecznych urządzeń. Po wpisaniu urządzenia na taką listę pomijana będzie na nim weryfikacja dwuskładnikowa.



Rysunek 82: Weryfikacja dwuskładnikowa

8.2.4. Powiąż z ePUAP\PZ

Funkcjonalność pozwala połączyć konto z serwisem ePUAP (Profil Zaufany). Powiązanie można utworzyć dla kont tradycyjnych (login i hasło) oraz wykorzystujących podpis kwalifikowany.



Rysunek 83: Powiązanie z ePUAP

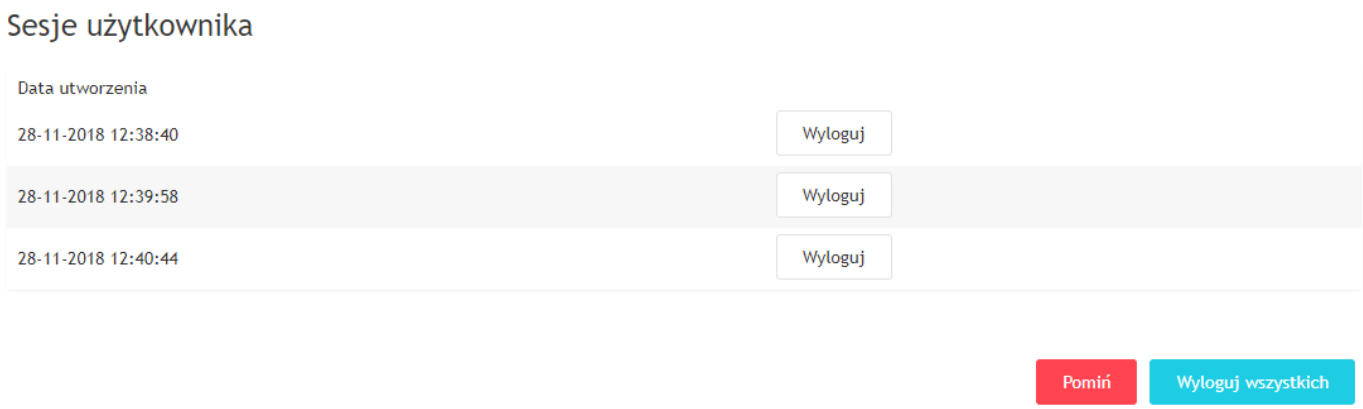
Powiązanie konta następuje po naciśnięciu przycisku „Powiąż z ePUAP” dostępnego na stronie Moje Konto/Powiąż z ePUAP\PZ. Przycisk ten przenosi użytkownika na stronę ePUAP, gdzie jest on proszony o zalogowanie się na konto PZ. Po zalogowaniu użytkownik zostanie ponownie przekierowany na stronę eRejestracji, gdzie zostaje poinformowany o rezultacie połączenia kont. Jeśli utworzenie powiązania zakończyło się sukcesem, od tej pory użytkownik może logować się do systemu eRejestracja za pomocą konta ePUAP\PZ.

8.2.5. Sesje użytkownika

Może zdarzyć się sytuacja, gdy użytkownik nie wyloguje się z konta, po czym zaloguje się na innym urządzeniu/w innej przeglądarce. Aby ułatwić użytkownikowi kontrolę nad takim zdarzeniem, wprowadzona została funkcja powiadamiania użytkownika o tym, że jest zalogowany w innej sesji/sesjach.

Gdy użytkownik zaloguje się w kolejnej sesji, automatycznie otworzy się strona, na której będzie miał możliwość zarządzania obecnymi sesjami.

Na stronę można wejść przez menu użytkownika, klikając „MOJE KONTO”, a następnie otwierając zakładkę „Sesje użytkownika”.

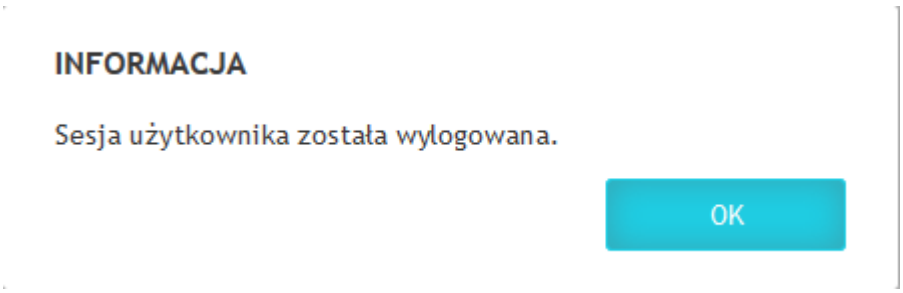


Rysunek 84: Okno zarządzania sesjami użytkownika

Okno zarządzania sesjami użytkownika zawiera listę aktywnych sesji. Po lewej stronie znajduje się data i godzina utworzenia poszczególnych sesji. Po prawej stronie, znajdują się przyciski umożliwiające wylogowanie z konkretnych sesji. Pod listą umieszczone są dwa przyciski:

- „Pomiń” – kliknięcie nie wylogowywuje użytkownika z żadnej aktywnej sesji,
- „Wyloguj wszystkich” – kliknięcie wylogowywuje użytkownika z wszystkich aktywnych sesji (z wyjątkiem bieżącej).

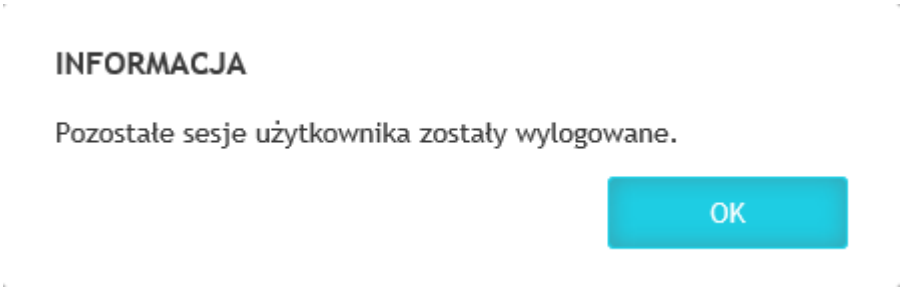
W przypadku, gdy użytkownik kliknie przycisk „Wyloguj” przy konkretnej sesji, wyświetlony zostanie komunikat, informujący o wylogowaniu go z danej sesji.



Rysunek 85: Okno informujące o wylogowaniu sesji użytkownika

Po zatwierdzeniu komunikatu kliknięciem przycisku „OK”, następuje ponowne przekierowanie do okna zarządzania sesjami użytkownika, aż do momentu wylogowania ze wszystkich aktywnych sesji bądź kliknięcia przycisku „Pomiń”.

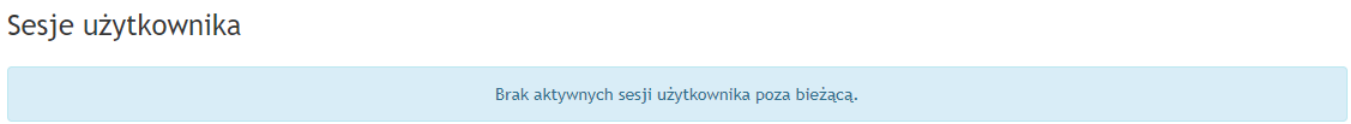
W przypadku kliknięcia przycisku „Wyloguj wszystkich”, wyświetlony zostanie następujący komunikat:



Rysunek 86: Okno informujące o wylogowaniu wszystkich pozostałych sesji użytkownika

Po zatwierdzeniu komunikatu kliknięciem przycisku „OK”, następuje przekierowanie do strony głównej Portalu.

Jeśli użytkownik jest zalogowany tylko w jednej sesji, po wejściu na stronę „Sesje użytkownika” wyświetli mu się komunikat o braku aktywnych sesji poza bieżącą.

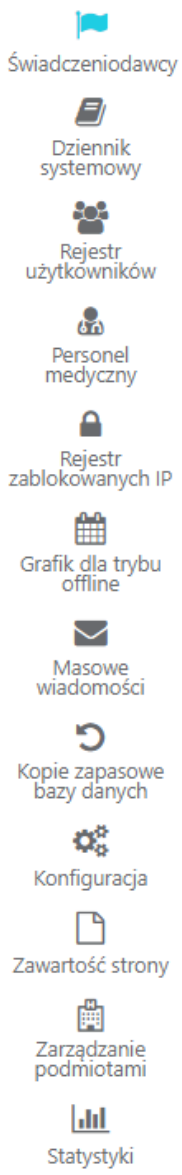


Rysunek 87: Komunikat o braku aktywnych sesji użytkownika poza bieżącą

Aby móc korzystać z zakładki „Sesje użytkownika”, należy wcześniej włączyć ją zaznaczając checkbox obok pola „Informuj o sesjach użytkownika” w zakładce „Zarządzanie” -> „Konfiguracja” -> „Podstawowa” –> „Ogólna”.

8.3. Zarządzanie

Menu „Zarządzanie” zawiera szereg opcji umożliwiających zarządzanie eRejestracja. Poza możliwością dostosowania wyglądu strony głównej, tworzenia newsów czy regulaminu, zawiera informacje diagnostyczne odnośnie połączenia ze słownikami świadczeniodawców, grafik trybu offline, narzędzia umożliwiające zarządzanie personelem oraz statystyki dotyczące m.in. liczby rejestracji kont, logowań, blokad, rezerwacji terminów.



Rysunek 88: Opcje zarządzania

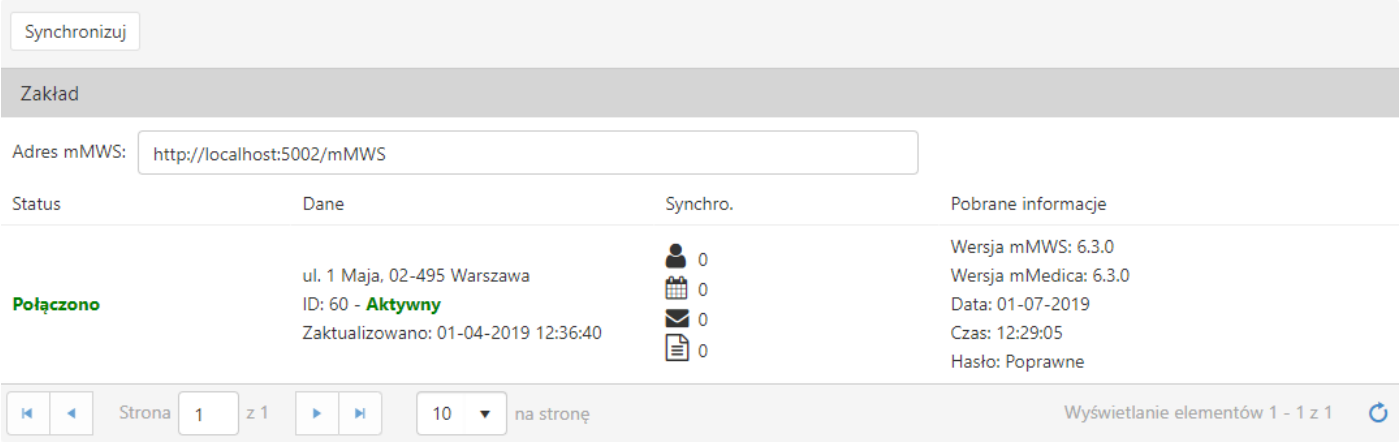
8.3.1. Świadczeniodawcy

Przejście do strony statusów świadczeniodawców następuje poprzez wybranie z menu „Zarządzanie” opcji „Świadczeniodawcy”. Widok ten wyświetla informacje diagnostyczne dotyczące dodanych świadczeniodawców. Tabela, poza danymi identyfikującymi świadczeniodawcę, zawiera informacje o jego:

- adresie URL słownika świadczeniodawcy (mMWS),
- adresie,
- identyfikatorze i aktywności,
- ostatniej aktualizacji,

- liczbie użytkowników, terminów, wysłanych SMSów oraz wniosków, które muszą zostać synchronizowane dla danego świadczeniodawcy,
- wersji mMWS i mMedica,
- dacie i godzinie pobrania informacji,
- poprawności hasła usług sieciowych,
- statusie połączenia z danym świadczeniodawcą.

Strona pozwala również zmienić adres mMWS świadczeniodawcy.



Rysunek 89: Statusy świadczeniodawców

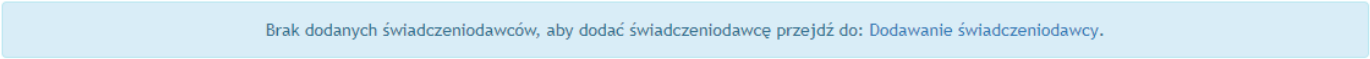
Na stronie statusów świadczeniodawców pobierane są także dane o wersji mMWS, wersji programu mMedica, dacie oraz czasie serwera bazy danych mMedica. Przycisk „Synchronizuj" pozwala na wymuszenie synchronizacji danych do mMedica. Możliwe stany statusów:

- Połączono – konfiguracja jest poprawna;
- Brak połączenia z serwisem – adres URL od świadczeniodawcy jest błędny lub nie ma połączenia z serwisem mMWS;
- Brak połączenia z bazą – istnieje połączenie z serwisem mMWS, jednak konfiguracja bazy jest niepoprawna lub baza nie działa;
- Wersja bazy danych mMedica nie odpowiada wersji mMWS – istnieje połączenie z serwisem mMWS, jednak wersja mMWS nie jest zgodna z wersją programu mMedica;
- Wersja mMWS powinna być taka sama jak wersja Portalu – istnieje niezgodność wersji portalu eRejestracja oraz wersji usług sieciowych mMWS;
- Trwają prace serwisowe w mMedica – na bazie mMedica wykonywane są prace serwisowe np. związane z aktualizacją oprogramowania. Należy poczekać na ich zakończenie.

- Brak połączenia z serwisem - wystąpił błąd z kodem HTTP: 404 (Not Found) - adres URL od świadczeniodawcy jest błędny.

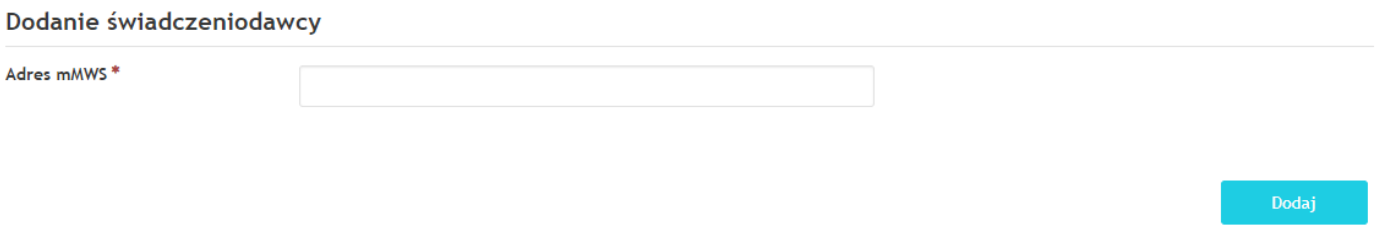
Jeśli z Portalem eRejestracja nie jest powiązany żaden świadczeniodawca (mógł nie zostać jeszcze dodany lub mógł zostać usunięty jedyny powiązany świadczeniodawca), wówczas strona „Świadczeniodawcy" jest niedostępna. Niedostępne są również strony: „Personel medyczny", „Grafik dla trybu offline" oraz zakładka „Import użytkowników z mMedica" na stronie „Rejestr użytkowników".

W miejscu strony zostaje wyświetlony komunikat zawierający link do formularza dodawania świadczeniodawcy.



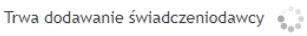
Rysunek 90: Komunikat o braku powiązanego świadczeniodawcy

Aby dodać świadczeniodawcę należy kliknąć w link („Dodawanie świadczeniodawcy"), po czym nastąpi przekierowanie do formularza dodawania świadczeniodawcy.



Rysunek 91: Formularz dodawania świadczeniodawcy

Po wypełnieniu pola „Adres mMWS" i kliknięciu przycisku „Dalej" rozpocznie się dodawanie świadczeniodawcy.



Rysunek 92: Dodawanie świadczeniodawcy

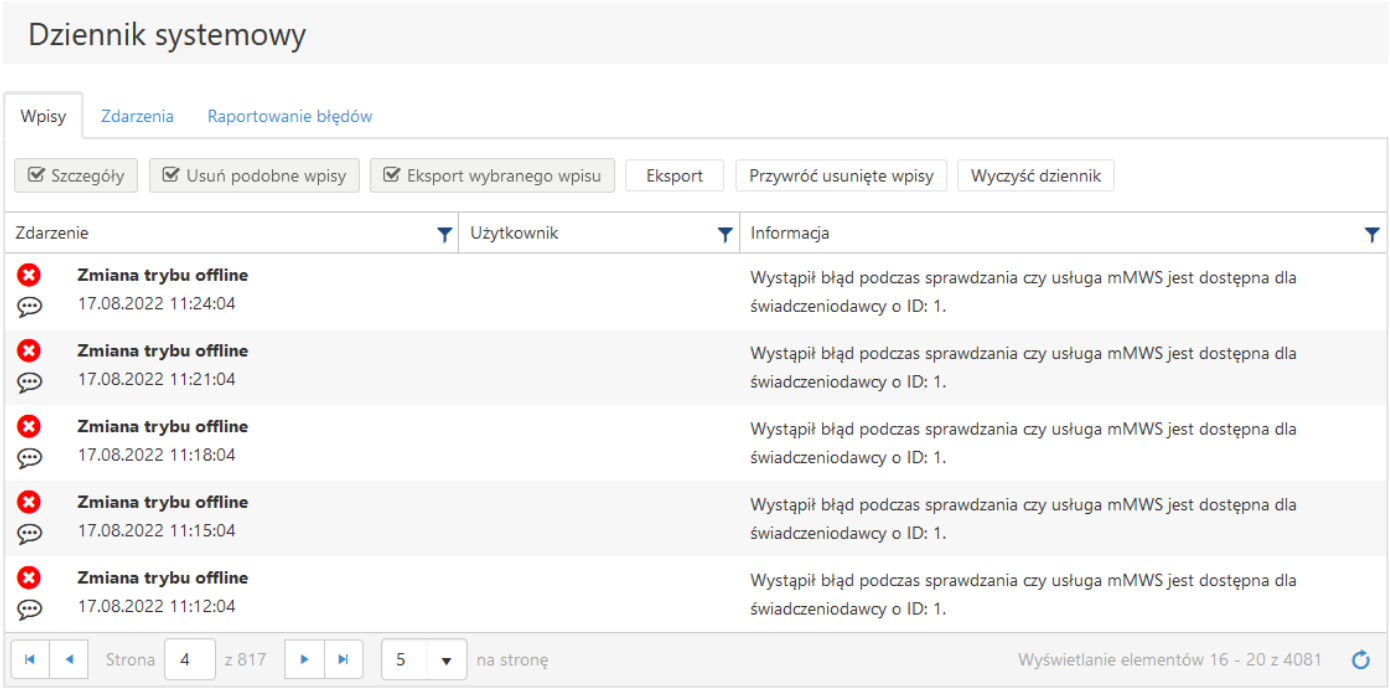
Po zakończeniu dodawania świadczeniodawcy strona „Świadczeniodawcy" będzie już dostępna.

8.3.2. Dziennik systemowy

Weryfikacja dziennika systemowego następuje poprzez wejście z menu "Zarządzanie" w „Dziennik systemowy”. Dziennik systemowy składa się z trzech zakładek: „Wpisy”, „Zdarzenia” oraz „Raportowanie błędów”.

8.3.2.1. Wpisy

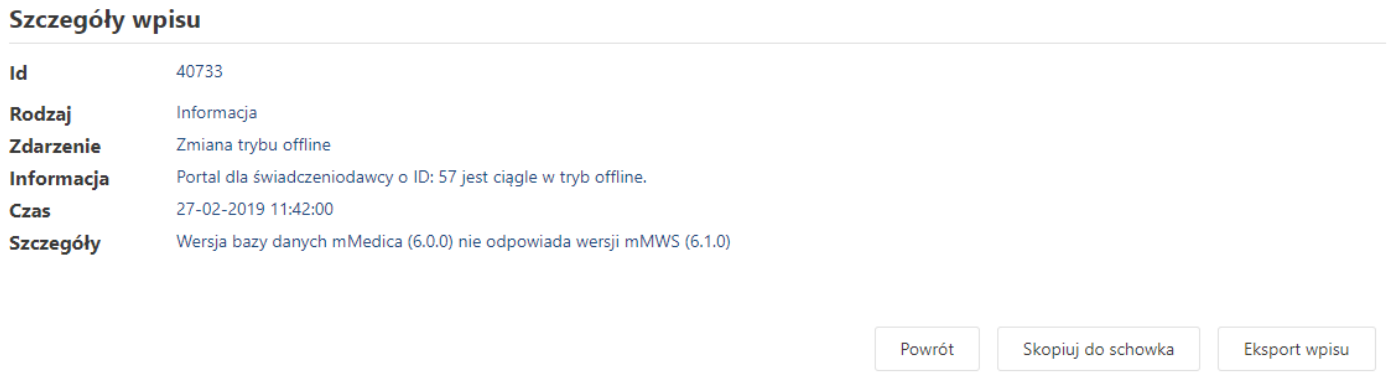
W pierwszej z nich znajdują się wszystkie zdarzenia, które wystąpiły w systemie wraz z najistotniejszymi informacjami.



Rysunek 93: Dziennik systemowy

Kolumny wpisów dziennika systemowego mogą być sortowane poprzez naciśnięcie na ich nazwę, oraz filtrowane za pomocą przycisku filtra.

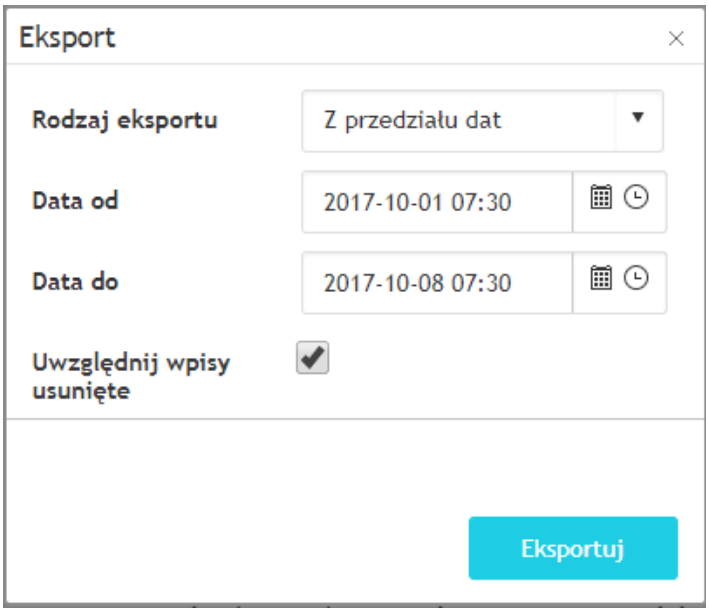
Dziennik zawiera dane o ID zdarzenia, czasie wystąpienia zdarzenia, rodzaju zdarzenia, nazwie zdarzenia oraz jego opisie. Jeśli zdarzenie zostało wywołane przez użytkownika, zapisywany jest jego login. Dodatkowo, w przypadku, gdy znane są szczegóły błędu, można je wyświetlić poprzez zaznaczenie wpisu i naciśnięciu przycisku „Szczegóły”. Wywoła to przekierowanie na stronę wyświetlającą dokładne informacje o zdarzeniu. Jeśli przycisk szczegółów zostaje nieaktywny, oznacza to brak informacji dodatkowych odnośnie zaznaczonego wpisu.



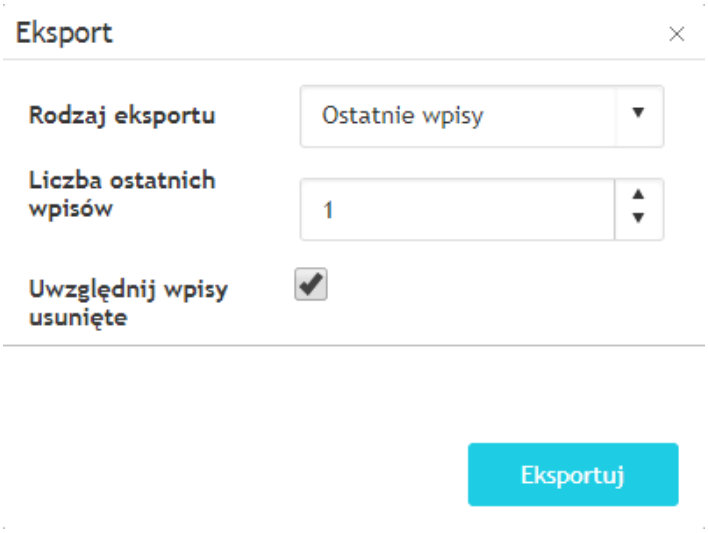
Rysunek 94: Informacje szczegółowe zawarte w Dzienniku systemowym

Przycisk „Skopiuj do schowka” kopiuje wszystkie zawarte w szczególe wpisu dane. Dzięki temu możliwe jest wklejenie danych informacji do edytora tekstowego. Można zrobić to za pomocą kliknięcia prawego przycisku myszy i wybrania opcji „Wklej” lub za pomocą skrótów klawiszowych Ctrl + v.

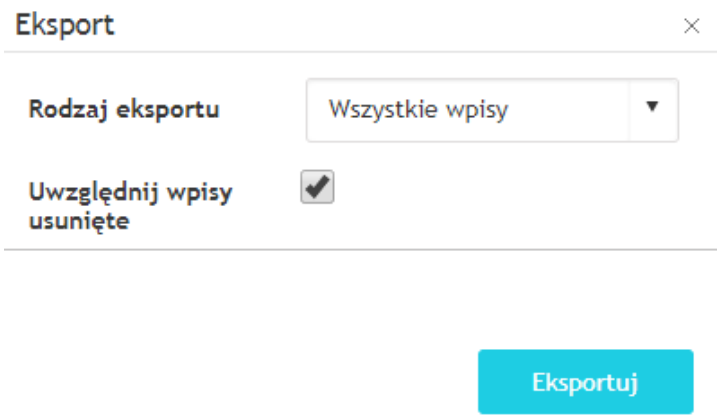
Eksport wpisów z dziennika systemowego pozwala na zapis poszczególnych wpisów do pliku *.csv. Przycisk „Eksport” otwiera okno zawierające opcje eksportu. Rozwijana lista „Rodzaj eksportu” umożliwia eksport wpisów na podstawie wybranego przedziału dat, ostatnich wpisów (wymaga podania liczby ostatnich wpisów do eksportu) lub wszystkich wpisów dziennika systemowego. Przycisk „Eksport wybranego wpisu” pozwala na zapis pojedynczego, zaznaczonego na liście wpisu. Jest on dostępny również z poziomu informacji szczegółowych wpisu.



Rysunek 95: Eksport wpisów dziennika systemowego z wybranego okresu czasu



Rysunek 96: Eksport dziennika systemowego dla ostatnich wpisów

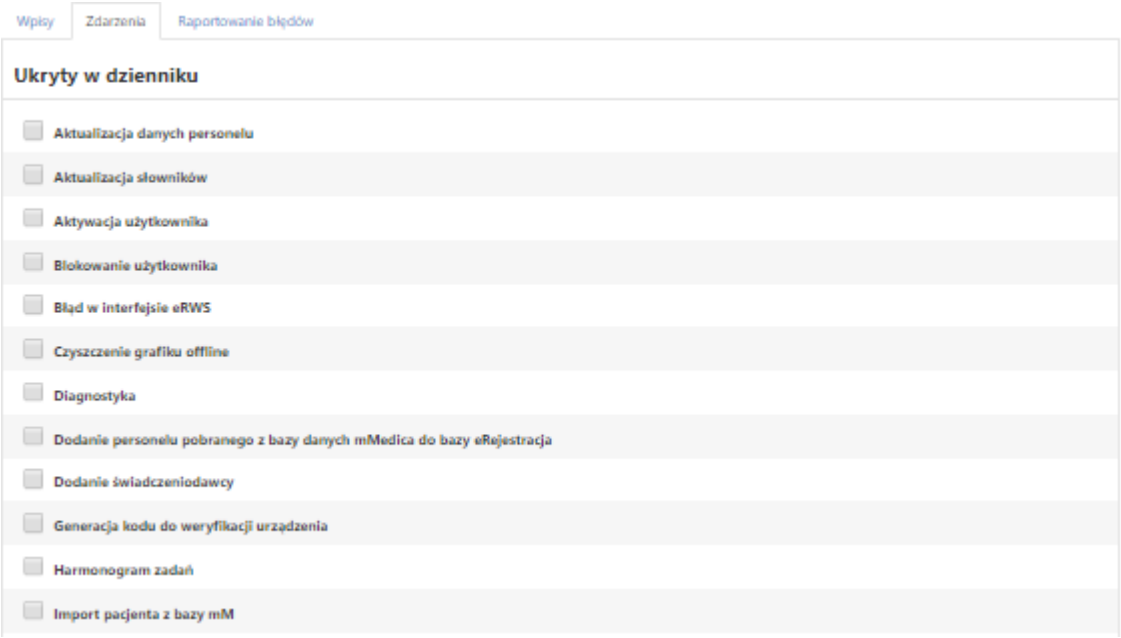


Rysunek 97: Eksport wszystkich wpisów z dziennika systemowego

Dodatkowo zakładka wpisów pozwala na usuwanie wszystkich wpisów za pomocą opcji „Wyczyść dziennik”. Istnieje również możliwość usunięcia podobnych wpisów (takie samo zdarzenie i informacja) do zaznaczonego poprzez skorzystanie z przycisku „Usuń podobne wpisy” . W przypadku obu tych opcji wpisy nie są fizycznie usuwane z bazy danych i mogą zostać przywrócone za pomocą przycisku „Przywróć usunięte wpisy”.

8.3.2.2. Zdarzenia

Druga zakładka „Zdarzenia” pozwala wybrać typy zdarzeń, które mają być ukryte w Dzienniku systemowym. Ukrycie typu zdarzenia można zmienić zaznaczając/odznaczając pole wyboru przy wybranym typie zdarzenia.


Wpisy
Zdarzenia
Raportowanie błędów
Ukryty w dzienniku
Aktualizacja danych personelu
Aktualizacja słowników
Aktywacja użytkownika
Blokowanie użytkownika
Błąd w interfejsie eRWS
Czyszczenie grafiku offline
Diagnostyka
Dodanie personelu pobranego z bazy danych mMedica do bazy eRejestracja
Dodanie świadczeniodawcy
Generacja kodu do weryfikacji urządzenia
Harmonogram zadań
Import pacjenta z bazy mM

- [ ] Konfiguracja ePUAP\PZ
- [ ] Logowanie poprzez ePUAP\PZ
- [ ] Logowanie przy pomocy SimplySign
- [ ] Logowanie za pomocą podpisu elektronicznego
- [ ] Nieobsłużony wyjątek
- [ ] Obsługa moich dokumentów
- [ ] Odblokowanie użytkownika
- [ ] Odpięcie subkont
- [ ] Odwołanie rezerwacji
- [ ] Odwołanie terminu poza kartoteką
- [ ] Pobieranie danych konfiguracji połączenia z bramką SMS z mMedica
- [ ] Pobieranie danych profilu użytkownika z ePUAP\PZ
- [ ] Pobieranie eRecept z bazy mM
- [ ] Pobieranie grafików trybu offline z bazy mM
- [ ] Pobieranie harmonogramu lekarza z bazy mM
- [ ] Pobieranie leków z bazy mM
- [ ] Pobieranie moich dokumentów z bazy Archiwum
- [ ] Pobieranie moich rezerwacji z bazy mM
- [ ] Pobieranie personelu z bazy mM
- [ ] Pobieranie rezerwacji poza kartoteką z bazy mM
- [ ] Pobieranie skierowań z bazy mM
- [ ] Pobieranie szczegółów zaleceń lekarskich z bazy mM
- [ ] Pobieranie szczepień z bazy mM
- [ ] Pobieranie wniosków pacjenta z bazy mM
- [ ] Pobieranie wolnych terminów z bazy mM
- [ ] Pobieranie zaleceń lekarskich z bazy mM
- [ ] Pobieranie zamówionych leków pacjenta z bazy mM
- [ ] Pobieranie zawartości dokumentu z bazy Archiwum
- [ ] Pobranie danych pacjenta z bazy mM
- [ ] Podpięcie subkonta
- [ ] Rejestracja personelu
- [ ] Rejestracja użytkownika
- [ ] Rezerwacja poza kartoteką
- [ ] Rezerwacja terminu
- [ ] Rezerwacja wizyty receptowej
- [ ] Rezygnacja z zamówionej wizyty receptowej
- [ ] SimplySign
- [ ] Statystyki
- [ ] Strona serwisowa online
- [ ] Synchronizacja wniosków pacjenta

- [ ] Synchronizacja wysłanych SMSów do bazy mM
- [ ] Synchronizacja zgody pacjenta
- [ ] Szyfrowana komunikacja
- [ ] Szyfrowanie adresów email
- [ ] Usunięcie personelu
- [ ] Usunięcie świadczenia
- [ ] Usunięcie świadczeniodawcy
- [ ] Usunięcie użytkownika
- [ ] Wstawianie eRecept do bazy eR
- [ ] Wstawianie harmonogramu lekarza do bazy eR
- [ ] Wstawianie leków do bazy eR
- [ ] Wstawianie moich dokumentów do bazy eR
- [ ] Wstawianie moich rezerwacji do bazy eR
- [ ] Wstawianie skierowań do bazy eR
- [ ] Wstawianie szczepień do bazy eR
- [ ] Wstawianie terminów poza kartoteką do bazy eR
- [ ] Wstawianie wolnych terminów do bazy eR
- [ ] Wstawianie zaleceń lekarskich do bazy eR
- [ ] Wstawianie zamówionych recept do bazy eR
- [ ] Wycofywanie wniosku
- [ ] Wygenerowanie PIN do rejestracji w systemie IM
- [ ] Wykonanie procedury serwisowej
- [ ] Wylogowywanie ePUAP
- [ ] Wyrejestrowanie z systemu IM
- [ ] Wysłanie maila
- [ ] Wysłanie zgody na komunikacje z IM
- [ ] Wysyłanie danych pacjenta do bazy mM
- [ ] Wysyłanie rezerwacji offline do bazy mM
- [ ] Wysyłanie SMS
- [ ] Wysyłanie wycofania zgody na komunikacje z IM
- [ ] Zgody
- [ ] Złożenie/Wycofanie zgody
- [ ] Zmiana kanału komunikacji dla teleporady
- [ ] Zmiana parametru konfiguracyjnego
- [ ] Zmiana sposobu logowania użytkownika
- [ ] Zmiana stanu blokady śmierci
- [ ] Zmiana terminu
- [ ] Zmiana trybu offline
- [ ] Zmiana uwagi do terminu

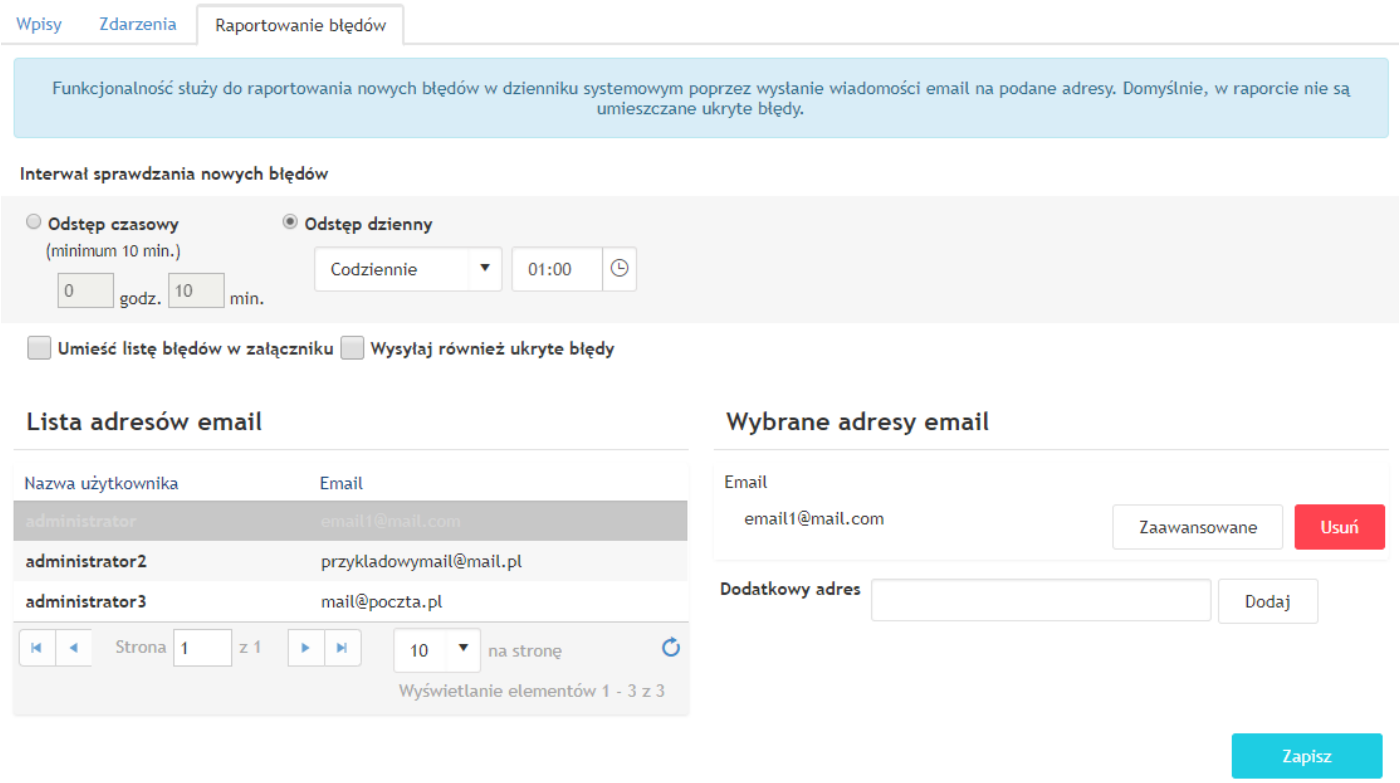
Zapisz

Rysunek 98: Zakładka „Zdarzenia” w Dzienniku systemowym

8.3.2.3. Raportowanie błędów

Ostatnia zakładka „Raportowanie błędów” odpowiada za konfigurację dostarczania raportów zawierających najnowsze błędy z dziennika systemowego. Raporty wysyłane są na podane adresy email, które mogą być wybrane spośród adresów administratorów portalu lub dodane jako dodatkowe adresy. Należy również ustawić interwał sprawdzania nowych błędów: czasowy lub dzienny. Interwał czasowy pozwala na aktualizację co podany odstęp w godzinach i/lub minutach, a interwał dzienny umożliwia wykonanie aktualizacji w konkretnym dniu tygodnia (lub codziennie) o podanej porze. W przypadku, kiedy od daty ostatniego raportu nie pojawiły się nowe błędy, żadna wiadomość email nie jest wysyłana.

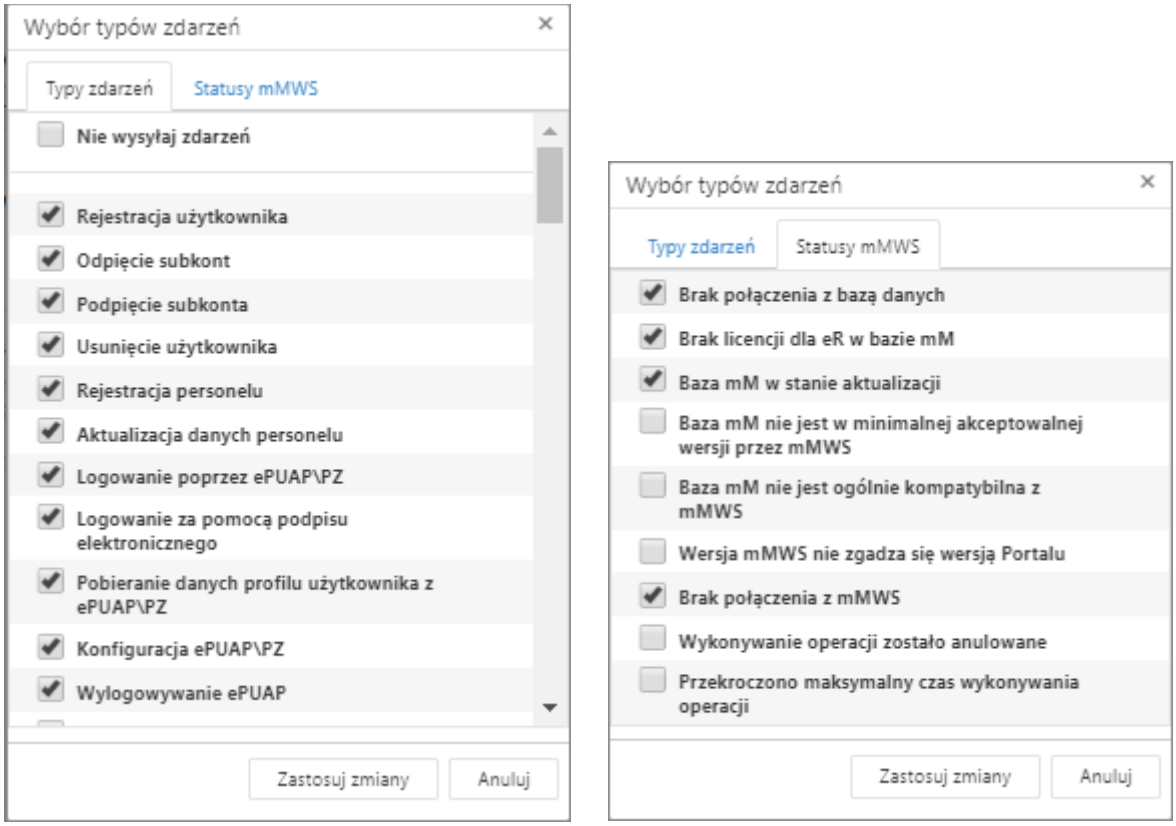
Opcja „Umieść listę błędów w załączniku” pozwala na dołączenie raportu w postaci pliku *.html jako załącznika do wiadomości email. W sytuacji, gdy opcja ta jest odznaczona, tabela z błędami wyświetlana jest jako treść wiadomości. Wybór ustawienia „Wysyłaj również ukryte błędy” powoduje, że w raporcie umieszczane są również błędy skonfigurowane jako „ukryte”.



Rysunek 99: Zakładka „Raportowanie błędów” w Dzienniku systemowym

Po wybraniu adresów email można zdecydować jakie typy zdarzeń mają być wysyłane na poszczególne z nich. Można tego dokonać wchodząc w ustawienia zaawansowane dla każdego adresu email. W ustawieniach zaawansowanych istnieje również możliwość włączenia powiadamiania poprzez wiadomości email

o stanie połączenia portalu eRejestracja z modułem mMWS jak i wybraniu o jakich statusach wybrana osoba ma być informowana.

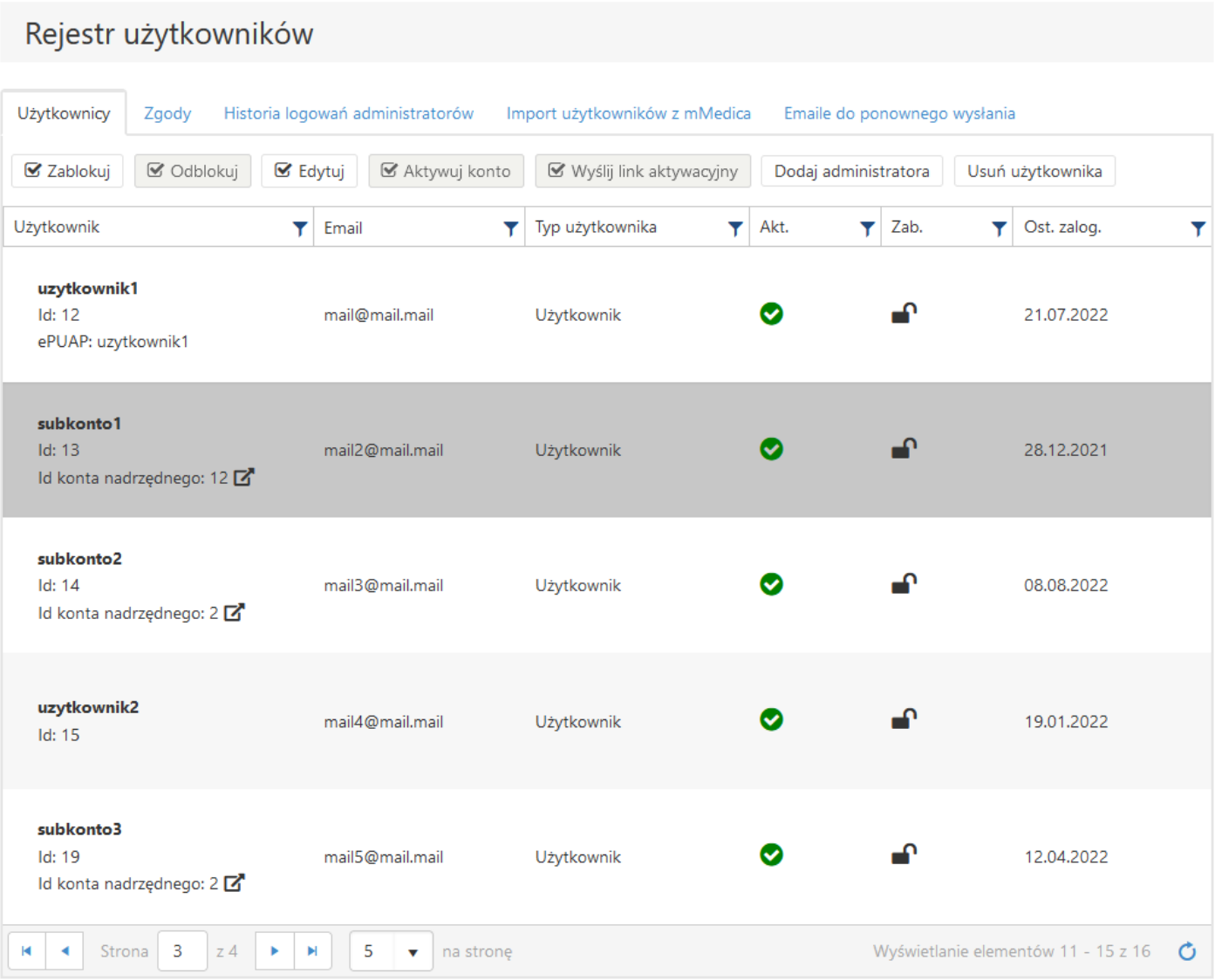


Rysunek 100: Zaawansowana konfiguracja typów zdarzeń oraz statusów połączenia Portalu z mMWS wysyłanych na email

8.3.3. Rejestr użytkowników

8.3.3.1. Użytkownicy

Lista użytkowników znajduje się w menu „Zarządzanie” pod zakładką „Rejestr użytkowników”. Wyświetlona na stronie tabela zawiera listę użytkowników posiadających konto w systemie eRejestracja.



Rysunek 101: Lista użytkowników

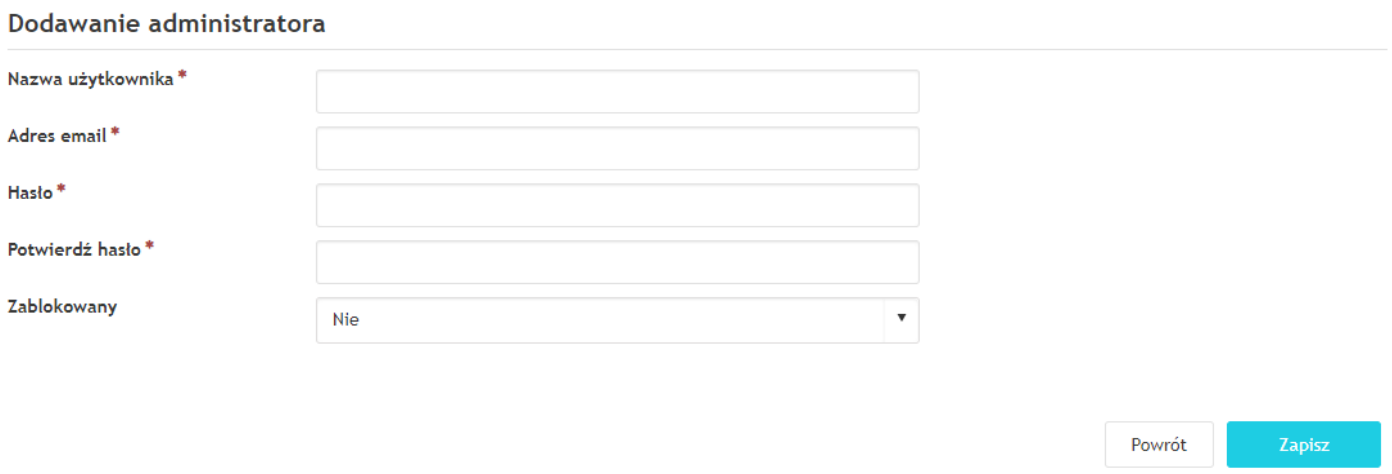
W pierwszej kolumnie tabeli wyświetlane są nazwy użytkowników eRejestracja, z ich numerami Id. Dodatkowo dla subkont wyświetlane są numery Id konta nadrzędnego, obok którego znajduje się przycisk przekierowujący do widoku edycji danych konta nadrzędnego.

W czwartej oraz piątej kolumnie tabeli wyświetlane są statusy konta użytkownika. Informują one o aktywności konta oraz jego ewentualnym zablokowaniu. Poniżej opisano znaczenie symboli:

- Użytkownik nie jest zablokowany, posiada możliwość logowania się do portalu;
- Użytkownik jest zalogowany, nie posiada możliwości logowania się do portalu;
- Użytkownik jest aktywny;
- Użytkownik nie jest aktywny.

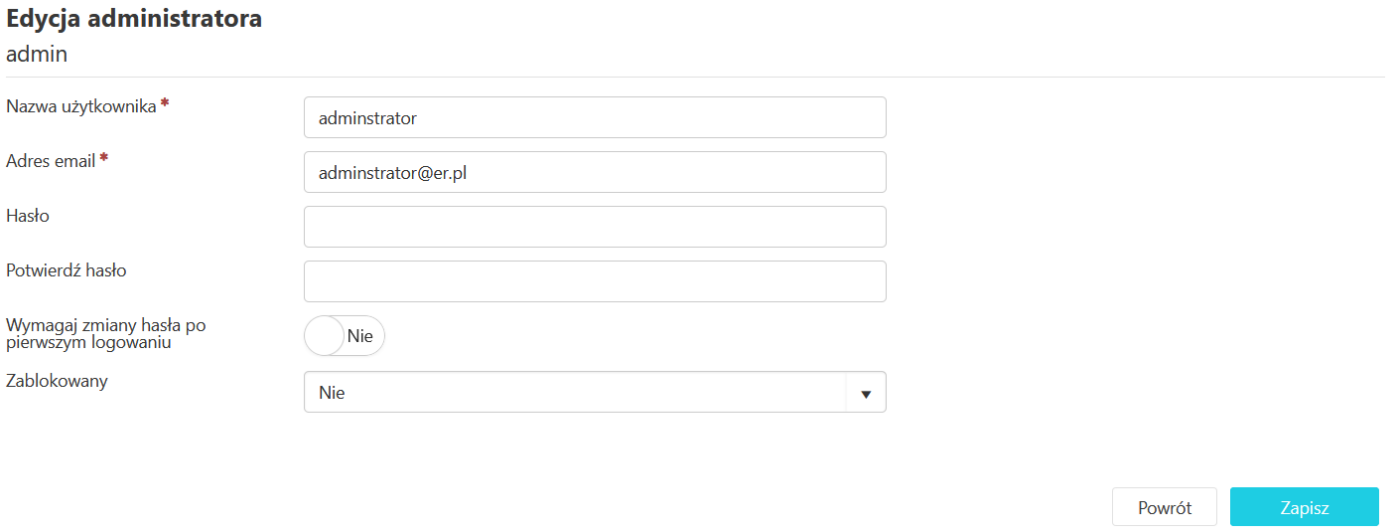
W górnym poziomym menu aplikacji znajdują się przyciski pozwalające zarządzać kontem użytkownika. Służą one do zmiany statusu użytkownika. Poniżej opisano działanie każdego z nich:

- Zablokuj – aktywny po zaznaczeniu niezablokowanego użytkownika,
- Odblokuj – aktywny po zaznaczeniu zablokowanego użytkownika,
- Edytuj,
- Wyślij link aktywacyjny – przycisk dostępny tylko dla nieaktywnego konta,
- Aktywuj konto – przycisk dostępny tylko dla nieaktywnego konta,
- Dodaj administratora,
- Usuń użytkownika – usuwa użytkownika z bazy danych eRejestracji (wraz ze wszelką jego aktywnością związaną z tym użytkownikiem) oraz usuwa jego login eRejestracja we wszystkich podpiętych poprzez mMWS bazach danych mMedica. Dodatkowo nazwa użytkownika trafia na listę zablokowanych nazw uniemożliwiając ponowne stworzenie konta (użytkownik może ponownie utworzyć konto na swoich danych, ale na innej nazwie użytkownika).



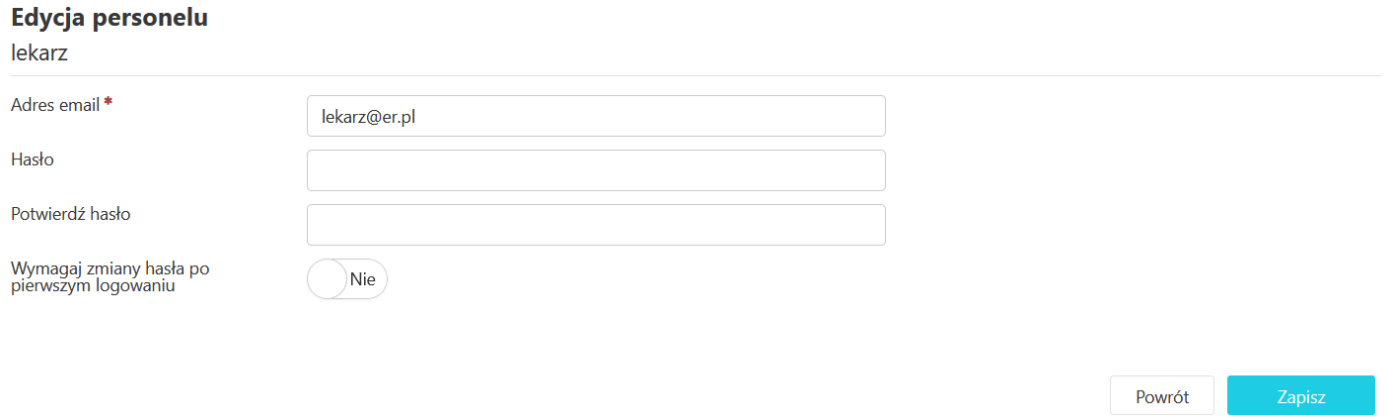
Rysunek 102: Dodawanie administratora

Dane administratora można zmienić zaznaczając w tabeli konto administratora oraz klikając przycisk „Edytuj”, który znajduje się na górnym pasku menu. Hasło nie będzie zmienione, jeśli pola „Hasło” i „Potwierdź hasło zostaną pozostawione puste. Jeśli pola odpowiedzialne za zmianę hasła zostaną uzupełnione to za pomocą „Wymagaj zmiany hasła po pierwszy logowaniu” można wymusić zmianę hasła użytkownika po pierwszym zalogowaniu (ustawione hasło przez administratora ma wtedy charakter tymczasowego).



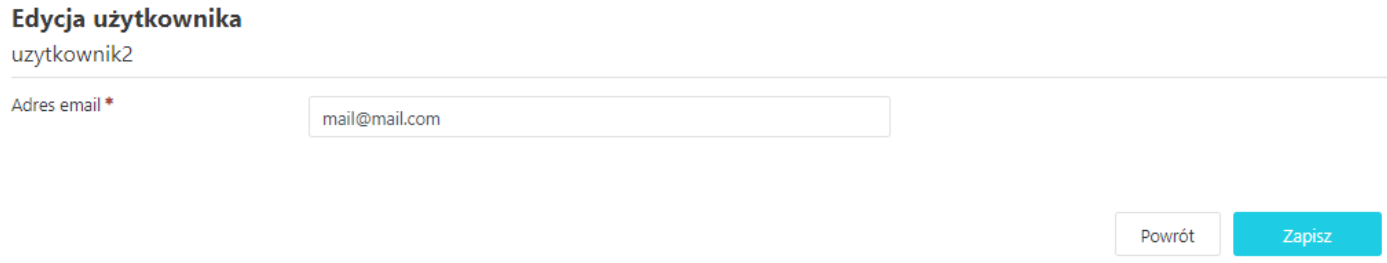
Rysunek 103: Edycja danych administratora

Dane konta personelu również mogą zostać zmienione za pomocą opcji „Edytuj”. Funkcjonalność pozwala na zmianę adresu email oraz hasła. Zmiana hasła odbywa się na identycznych zasadach jak zmiana hasła dla konta administratora.

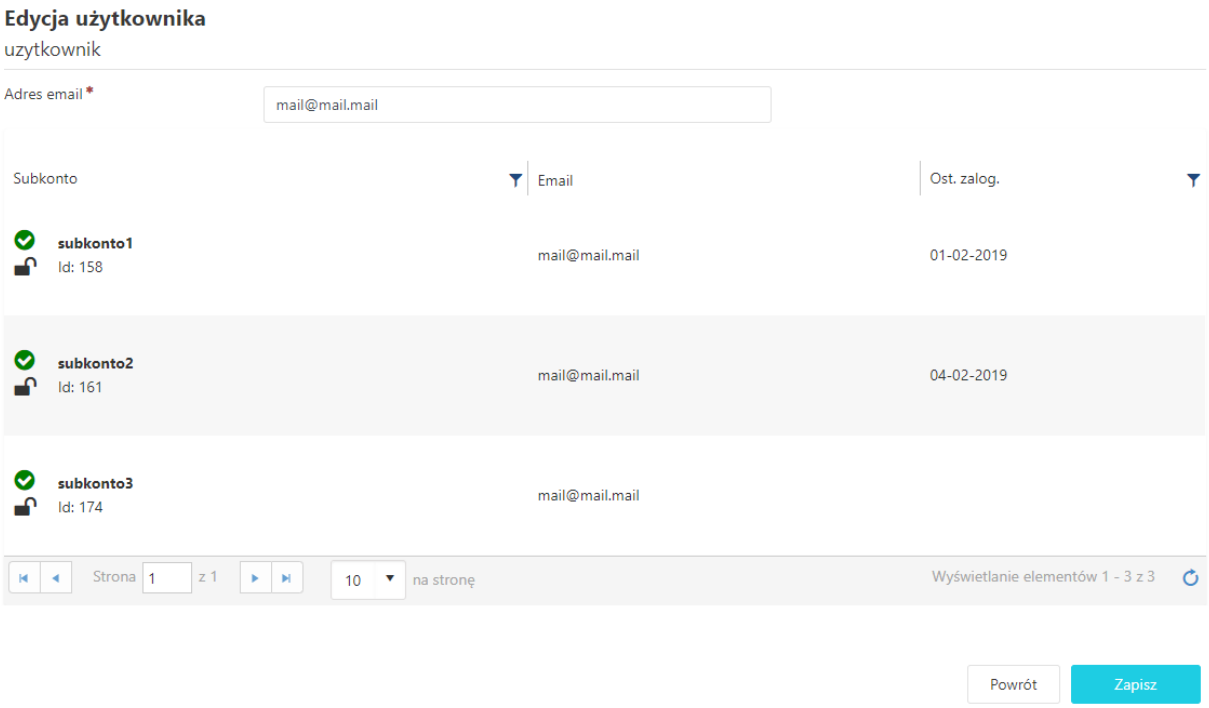


Rysunek 104: Edycja konta personelu

Formatka użytkowników umożliwia również zmianę adresu email użytkowników Portalu. Edycji można dokonać po zaznaczeniu konta użytkownika i naciśnięciu przycisku „Edytuj”.

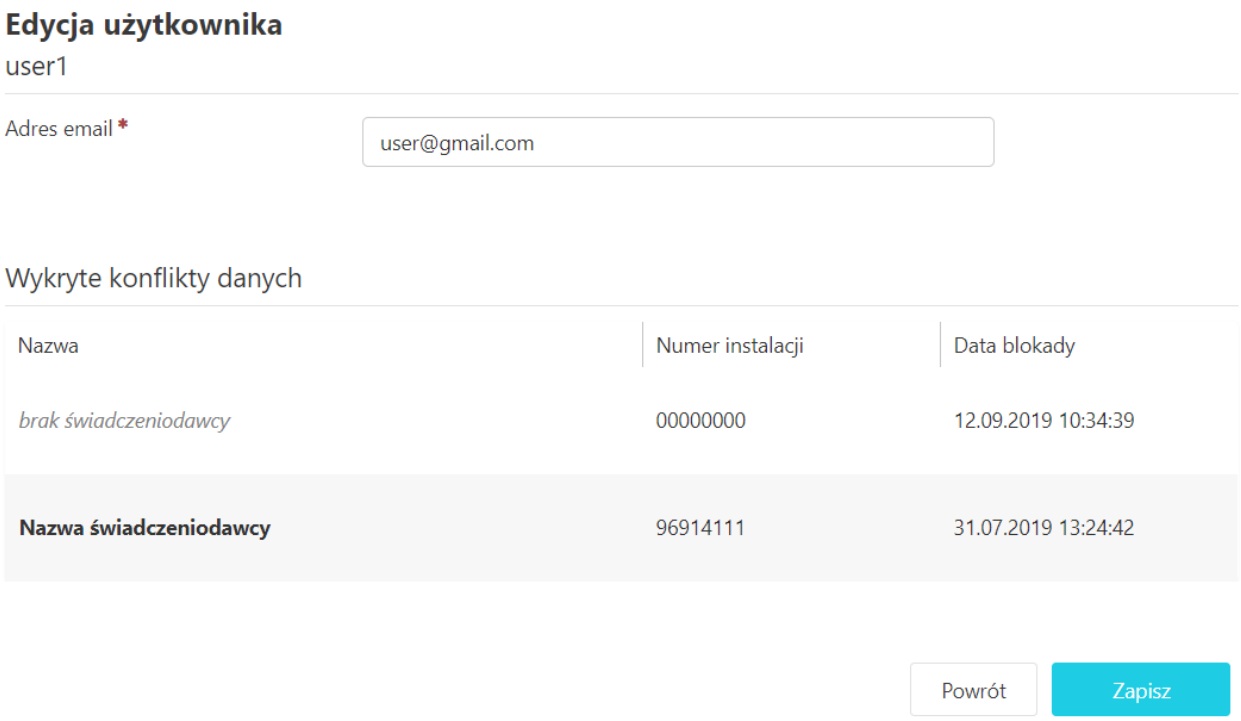


Rysunek 105: Edycja danych użytkownika



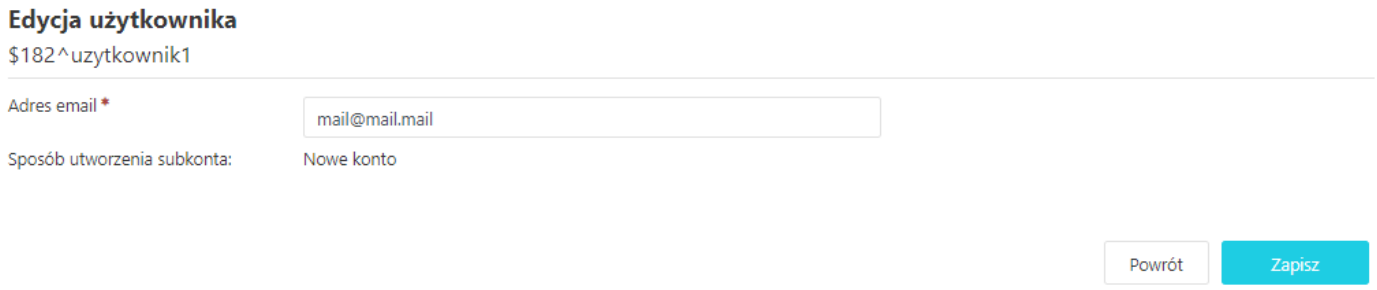
Rysunek 106: Edycja danych użytkownika z przypiętymi subkontami

Jeżeli użytkownik posiada konflikt danych (te same loginy w bazie eR i mM, ale inne dane osobowe) z co najmniej jednym świadczeniodawcą, na formatce edycji użytkownika wyświetla się również lista świadczeniodawców, z którymi wystąpił konflikt. Podany jest ich numer instalacji, data blokady oraz - jeśli dane świadczeniodawcy znajdują się w bazie eRejestracji – jego nazwa.

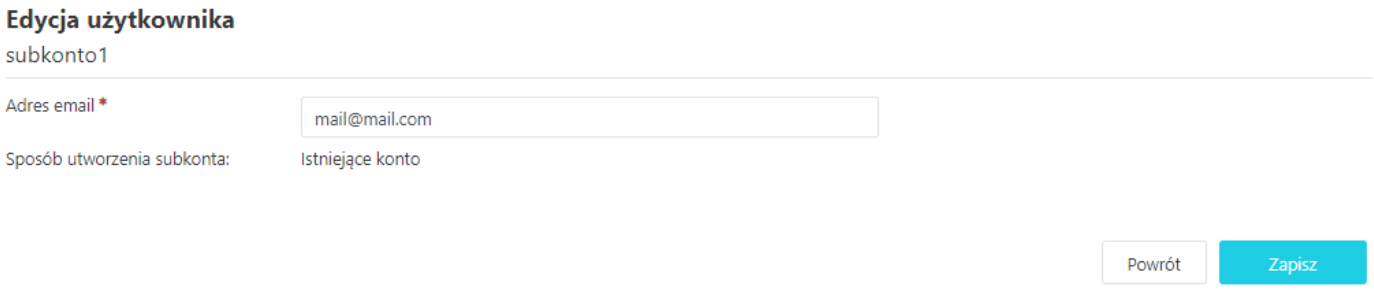


Rysunek 107: Edycja danych użytkownika z listą skonfliktowanych świadczeniodawców

Możliwa jest również edycja subkont. Dodatkowo w oknie edycji subkonta zamieszczona jest informacja o sposobie utworzenia subkonta: „Nowe konto” lub „Istniejące konto”.



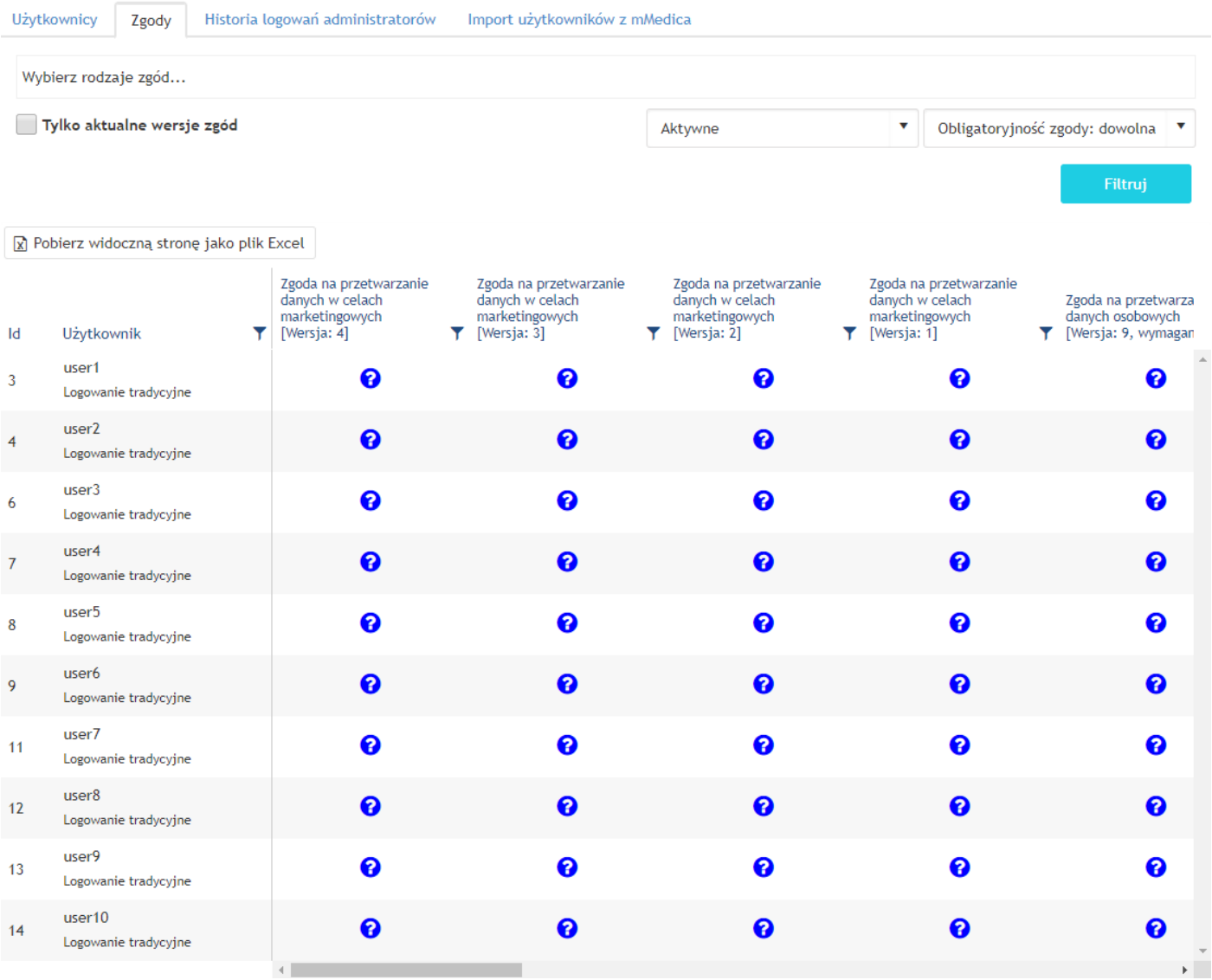
Rysunek 108: Edycja danych subkonta - Nowe konto



Rysunek 109: Edycja danych subkonta - Istniejące konto

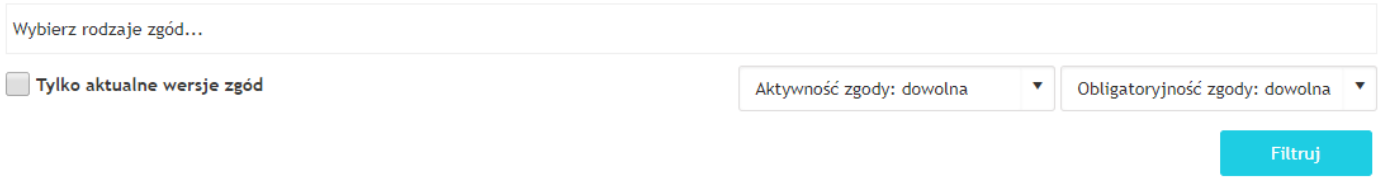
8.3.3.2. Zgody

Obok zakładki „Użytkownicy” znajduje się zakładka „Zgody”. Zawiera ona tabelę wszystkich użytkowników wraz z informacjami jakie zgody zostały przez nich: zaakceptowane, niezaakceptowane lub czy nie podjęli jeszcze decyzji odnośnie zgody.



Rysunek 110: Tabela zgód

Tabelę zgód można filtrować za pomocą filtrów znajdujących się nad tabelą.



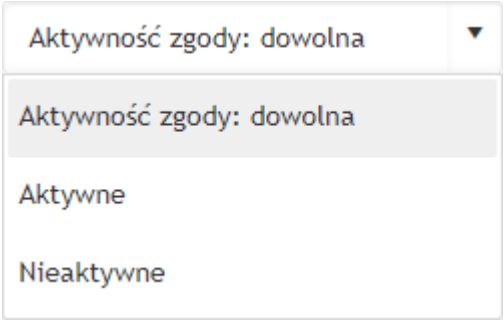
Rysunek 111: Filtry zgód

Po kliknięciu w pole z napisem „Wybierz rodzaj zgód” rozsuwa się lista zgód dodanych w portalu. Lista jest wielokrotnego wyboru.

Zaznaczenie checkboksa „Tylko aktualne wersje zgód” powoduje automatyczne ustawienie pola „Aktywność zgody” na „Aktywne” oraz uniemożliwia edycję tego pola.

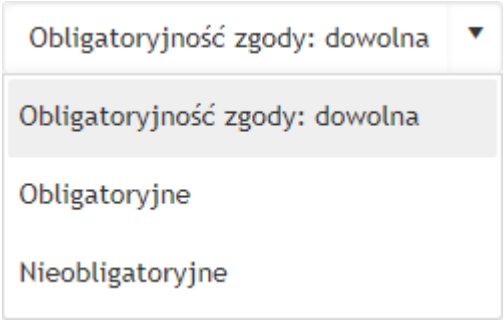
Rysunek 112: Filtry zgód - zaznaczony checkbox "Tylko aktualne wersje zgód"

Jeśli checkbox nie jest zaznaczony, pole „Aktywność zgody” jest aktywne. Kliknięcie w pole powoduje wysunięcie się listy ze statusem aktywności zgody do wyboru: „Aktywność zgody: dowolna” (wybranie tej opcji spowoduje wyświetlenie się zgód niezależnie od ich statusu aktywności), „Aktywne”, „Nieaktywne”.



Rysunek 113: Filtry zgód - Aktywność zgody

Pole Obligatoryjność zgody filtruje listę po statusie obligatoryjności. Możliwe do wyboru są opcje: „Obligatoryjność zgody: dowolna” (wybranie tej opcji spowoduje wyświetlenie się zgód niezależnie od ich statusu obligatoryjności), „Obligatoryjne”, „Nieobligatoryjne”.

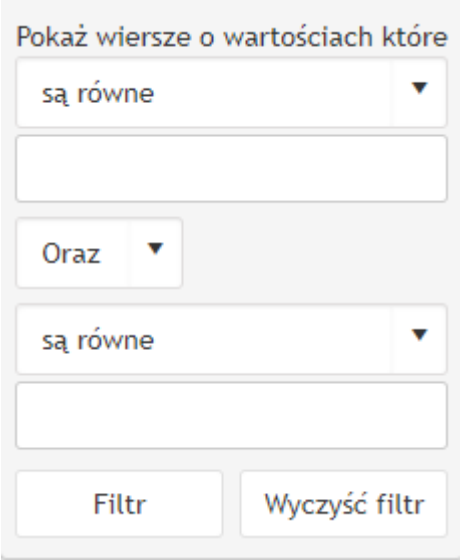


Rysunek 114: Filtry zgód - Obligatoryjność zgody

Filtry zadziałają dopiero po kliknięciu przycisku „Filtruj” znajdującego się pod filtrami.

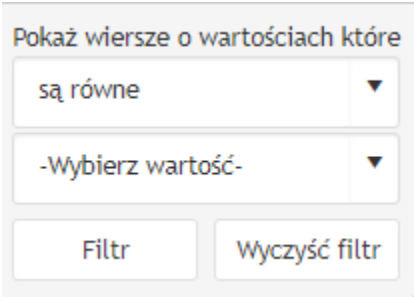
Oprócz głównych filtrów w tabeli znajdują się też filtry dla poszczególnych kolumn. Filtry otwiera się poprzez kliknięcie ikony znajdującej się po prawej stronie obok nazwy kolumny. Oprócz tego możliwe jest sortowanie kolumn „Id” oraz „Użytkownik” poprzez kliknięcie w nagłówek. Pierwsze kliknięcie sortuje ro-snąco (Id)/ alfabetycznie (Użytkownik). Drugie kliknięcie sortuje malejąco (Id)/ od końca alfabetu do początku (Użytkownik). Trzecie kliknięcie wyłącza sortowanie.

Klikając ikonę w kolumnie „Użytkownik” rozwijamy filtr dla tej kolumny. W pierwszym polu należy wybrać z listy rozwijanej jeden z warunków wyszukiwania. Do wyboru: „są równe”, „są inne niż”, zaczynają się od”, „kończą się na”, „zawierają”, „nie zawierają”. Następnie w polu poniżej należy wpisać wartość po jakiej będzie filtrowana kolumna. Jeśli chcemy dodać kolejny warunek, należy kliknąć w trzecie pole i wybrać którąś z opcji: „Oraz”/”lub”. Następnie rozwinąć filtr warunku i wybrać odpowiedni, a w polu poniżej wpisać wartość. Aby filtry zadziałały należy kliknąć przycisk „Filtr”. Jeśli chcemy, by w kolumnie znów wyświetlali się wszyscy użytkownicy, należy kliknąć przycisk „Wyczyść filtr”.



Rysunek 115: Filtry zgód - kolumna „Użytkownik”

Klikając ikonę w kolumnie z konkretną zgodą rozwijamy filtr dla tej kolumny. W pierwszym polu należy wybrać z listy rozwijanej jeden z warunków wyszukiwania. Do wyboru: „są równe”, „są inne niż”. Następnie z pola poniżej należy wybrać którąś z opcji: „Brak decyzji”, „Zgoda”, „Brak zgody”. Aby filtry zadziałały należy kliknąć przycisk „Filtr”. Jeśli chcemy, by w kolumnie znów wyświetlały się wszystkie odpowiedzi, należy kliknąć przycisk „Wyczyść filtr”.

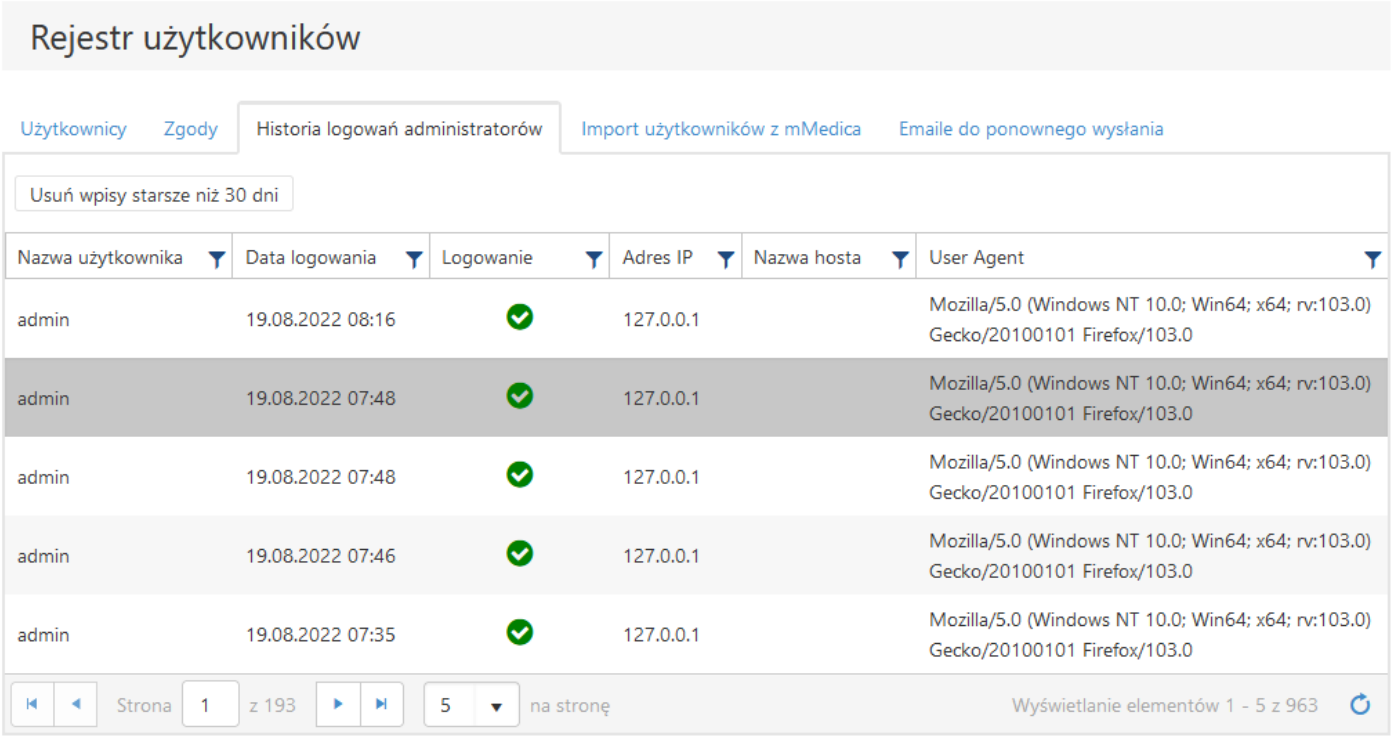


Rysunek 116: Filtry zgód – kolumna zgody

Powyżej tabeli znajduje się przycisk „Pobierz widoczną stronę jako plik Excel”. Kliknięcie tego przycisku generuje plik Excel z tabelą użytkowników i zgód, widoczną aktualnie po zastosowaniu filtrów.

8.3.3.3. Historia logowań administratorów

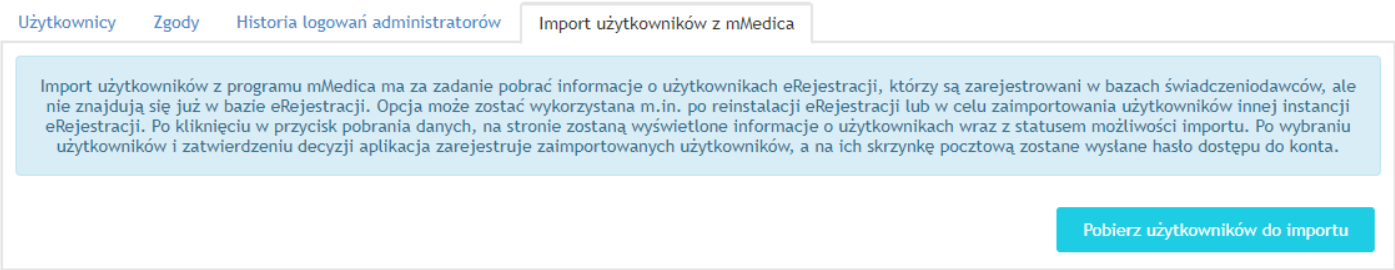
Kolejną po „Użytkownikach” zakładką jest „Historia logowań administratorów” zawierająca archiwum logowań wszystkich administratorów. Przy każdej próbie logowania widnieje data czy logowanie było pomyślne, adres IP z którego się logowano oraz User Agent czyli przeglądarka, której użyto.



Rysunek 117: Historia logowań administratorów

8.3.3.4. Import użytkowników z mMedica

Podczas funkcjonowania portalu eRejestracji może zaistnieć sytuacja, w której konta użytkowników zostaną utracone. Taka sytuacja może zdarzyć się w przypadku reinstalacji programu. We wspomnianym przypadku istnieje możliwość przywrócenia kont wraz z danymi osobowymi na podstawie informacji pobranych z aplikacji mMedica.

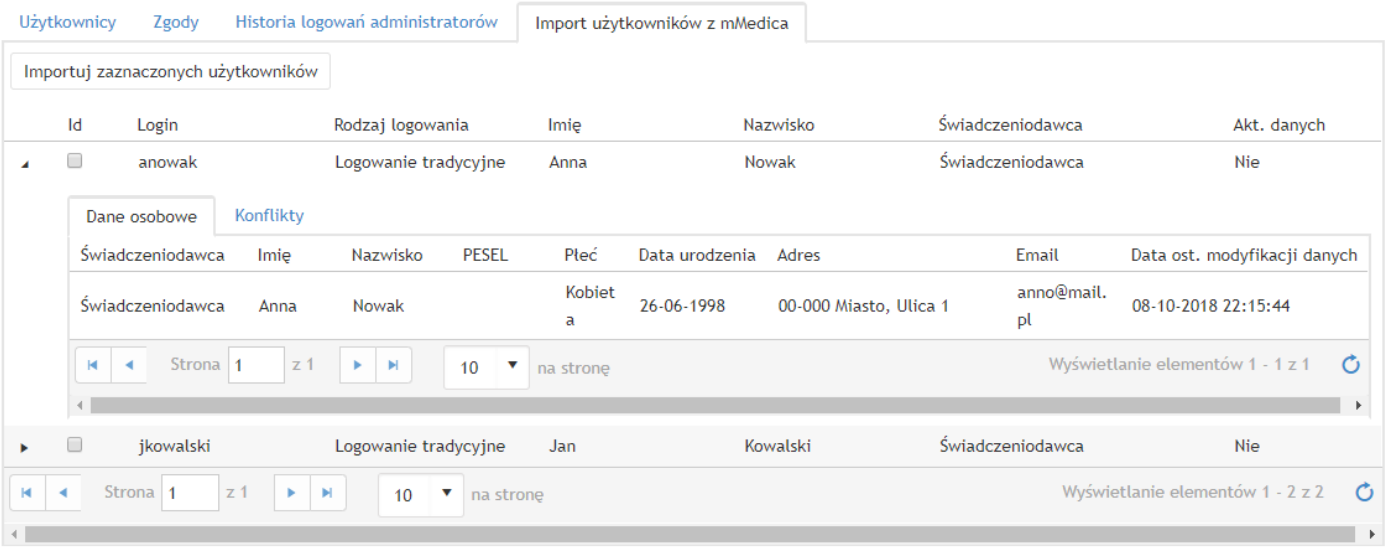


Rysunek 118: Import użytkowników z programu mMedica

Po otwarciu zakładki konfiguracyjnej o nazwie „Import użytkowników z mMedica” na stronie wyświetli się komunikat wyjaśniający szczegółowo sposób działania importu. Znajdujący się w górnej części przycisk „Importuj zaznaczonych użytkowników” służy do pobrania ze słowników świadczeniodawców informacji o użytkownikach, którzy zostali zarejestrowani w mMedica poprzez eRejestracja. Sytuacja ta dotyczy jednak jedynie użytkowników, których konta w danej chwili nie istnieją już w eRejestracji. Gdy dane zostaną pobrane, na stronie ukaże się tabela wyświetlająca dane użytkowników możliwych do zaimportowania.

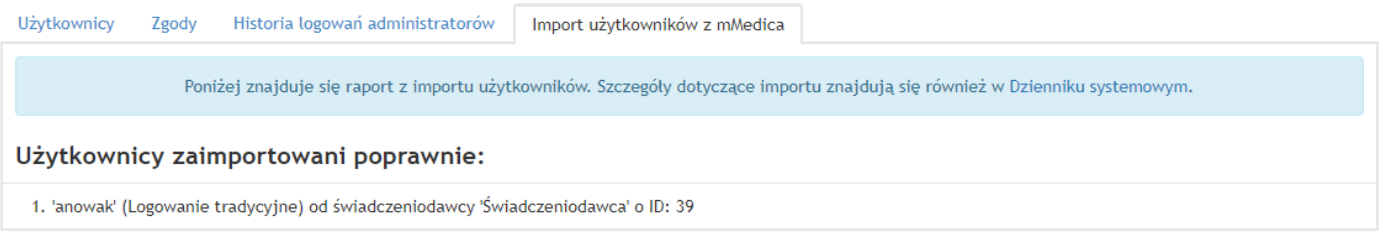
Rysunek 119: Lista danych użytkowników możliwych do zaimportowania

Na tym etapie można zaobserwować, którzy użytkownicy portalu eRejestracji zostali utraceni. Szczegółowe informacje odnośnie określonego konta można wyświetlić poprzez naciśnięcie ikony strzałki znajdującej się z lewej strony tabeli. Jeśli po rozwinięciu dane w zakładce „Dane osobowe” są zaznaczone na zielono, a pole „Akt. danych” posiada zawartość „Tak”, to dane użytkownika zostały scalone. Taka sytuacja zachodzi w przypadku, gdy istnieją konta o tym samym loginie. W takiej sytuacji zostają pobrane najnowsze dane.



Rysunek 120: Import użytkowników – informacje szczegółowe

W celu zaimportowania kont należy zaznaczyć pole wyboru ☑ znajdujące się przed loginem dla każdego użytkownika z osobna, a następnie kliknąć na przycisk „Importuj zaznaczonych użytkowników”. Po zakończeniu przenoszenia danych zostanie wyświetlony raport informujący, czy konta zostały zaimportowane z sukcesem, czy też wystąpiły problemy. Szczegóły zostaną zapisane również w dzienniku systemowym. Użytkownicy, którym przywrócono konto, otrzymają email z informacją o odzyskanym dostępie do portalu eRejestracja, wraz loginem oraz nowym, automatycznie wygenerowanym hasłem.



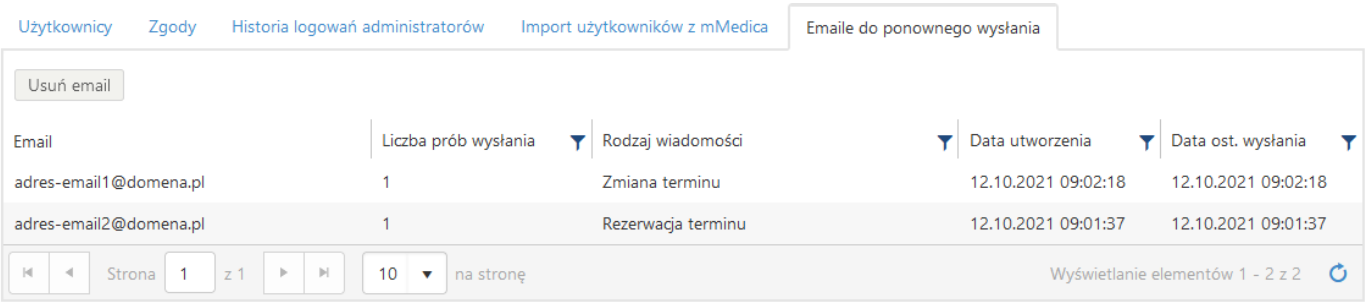
Rysunek 121: Raport z importu użytkowników z aplikacji mMedica

Jeśli zaimportowane konto było subkontem (jego login rozpoczynał się od znaku „$”) to po zalogowaniu użytkownik zostanie poproszony o przymusową zmianę nazwy użytkownika. Takie konto może zostać ponownie podłączone jako subkonto do innego konta.

Jeśli z Portalem eRejestracja nie jest powiązany żaden świadczeniodawca (mógł nie zostać jeszcze dodany lub mógł zostać usunięty jedyny powiązany świadczeniodawca), wówczas zakładka „Import użytkowników z mMedica” jest niedostępna. Dokładny opis dodawania świadczeniodawcy poprzez formularz znajduje się w rozdziale *8.3.1 Świadczeniodawcy*.

8.3.3.5. Emaile do ponownego wysłania

W zakładce „Emaile do ponownego wysłania” znajduje się lista wiadomości e-mail, które nie zostały wysłane np. na skutek błędnego konfiguracji SMTP lub błędnego adresu odbiorcy wiadomości. Jeśli adres odbiorcy jest niepoprawny to istnieje możliwość usunięcia wiadomości przez zaznaczenie pozycji i wybranie przycisku „Usuń email”.



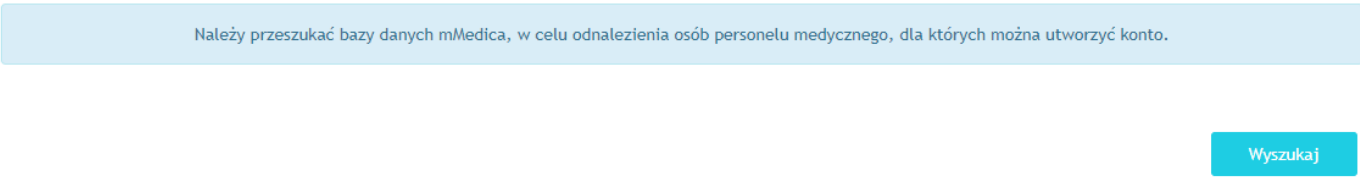
Rysunek 122: Lista wiadomości e-mail do ponownego wysłania

8.3.4. Personel medyczny

Formatka ta służy do utworzenia kont personelu medycznego w Portalu eRejestracja.

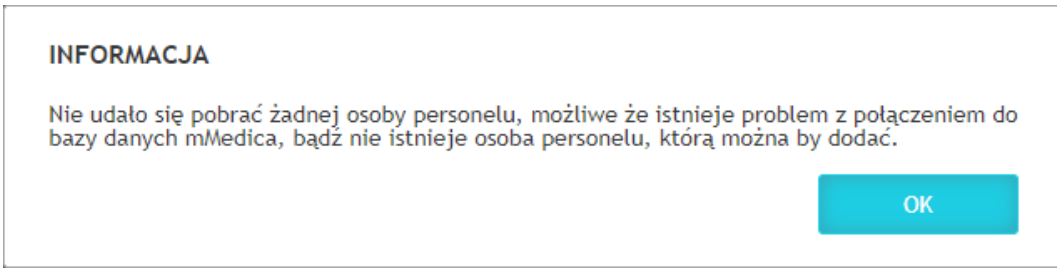
Uwaga: Opcja dostępna jest jedynie w module eRejestracja+.

Konta można założyć tylko osobom będącym jednocześnie personelem i użytkownikiem systemu mMedica. Aby pobrać listę takich użytkowników z systemu mMedica, należy kliknąć przycisk „Wyszukaj”.



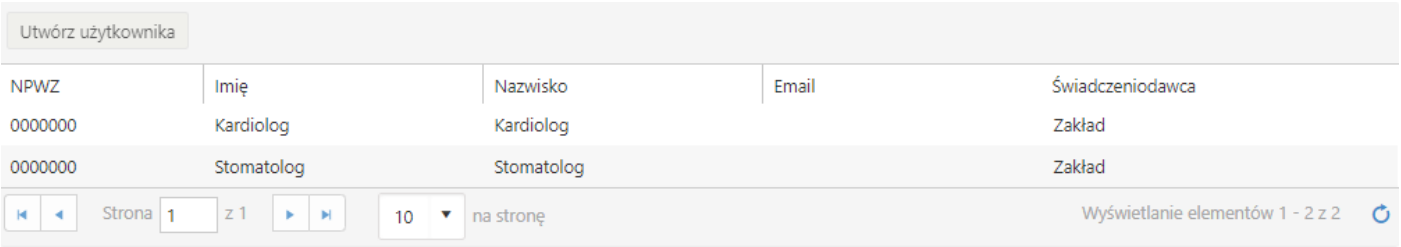
Rysunek 123: Wyszukiwanie personelu medycznego

Jeśli nie istnieją osoby personelu, dla których można utworzyć konto lub jeśli występują problemy z połączeniem do bazy danych systemu mMedica, pojawi się komunikat zawiadamiający o tym.



Rysunek 124: Informacja o braku osób personelu i możliwości problemów z połączeniem do bazy danych mMedica

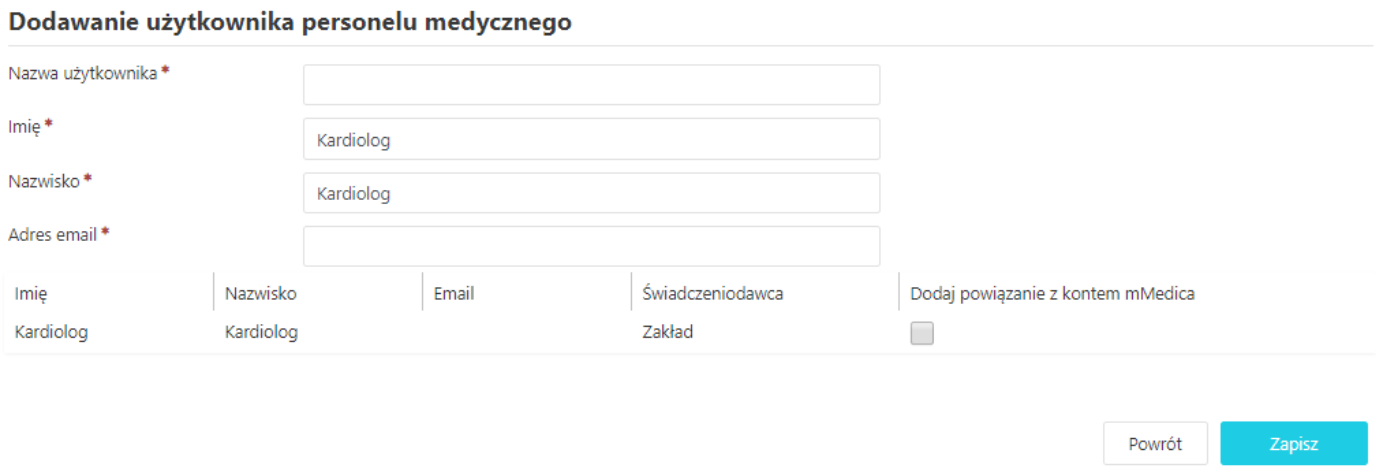
Jeśli istnieją osoby personelu, dla których można utworzyć konto, pojawi się tabela z listą tych użytkowników. W pierwszej kolumnie znajdują się Numery Prawa Wykonywania Zawodu (NPWZ), następnie imię, nazwisko, email personelu, a w ostatniej kolumnie nazwa świadczeniodawcy. Z listy należy wybrać osobę, dla której chce się utworzyć konto w Portalu i kliknąć przycisk „Utwórz użytkownika", znajdujący się powyżej tabeli.



Rysunek 125: Lista personelu medycznego, dla którego można utworzyć konta w Portalu eRejestracja

Następnie pojawi się formularz rejestracyjny dla nowego personelu domyślnie uzupełniona o imię, nazwisko i adres email (jeśli został podany w systemie mMedica). Należy uzupełnić pole „Nazwa użytkownika" oraz w tabeli poniżej formularza zaznaczyć checkbox znajdujący się w ostatniej kolumnie w celu dodania powiązania rejestrowanego konta z kontem mMedica. Aby zatwierdzić wprowadzone dane należy kliknąć przycisk „Zapisz".

Uwaga: Nazwa użytkownika (login), który został podany w formularzu należy przekazać zarejestrowanej osobie personelu! Login nie zostanie przesłany wraz z hasłem w mailu!

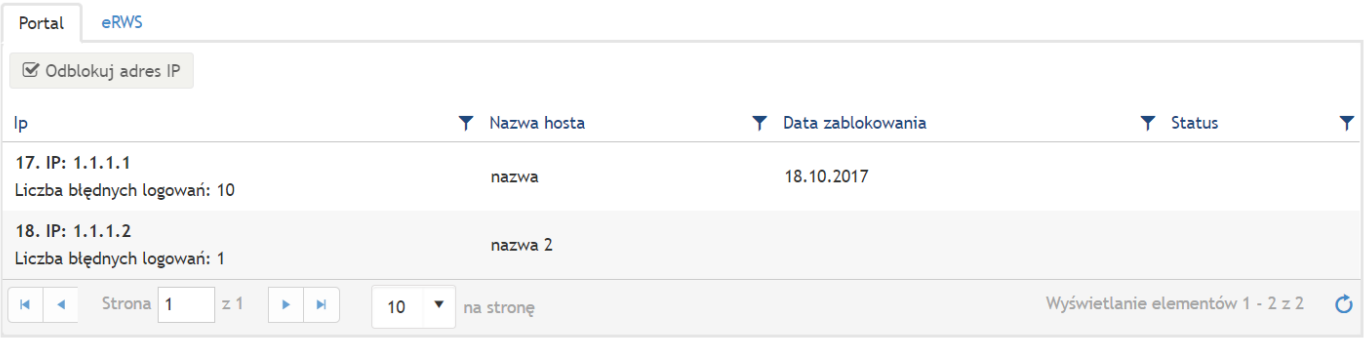


Rysunek 126: Dodawanie użytkownika personelu medycznego

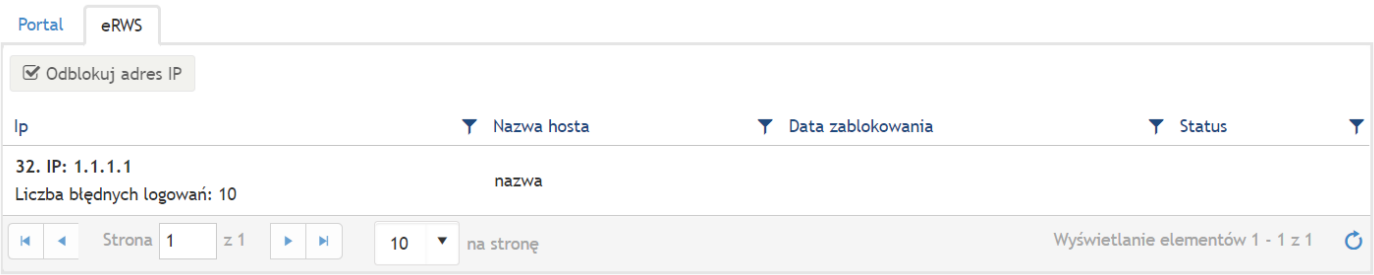
Jeśli z Portalem eRejestracja nie jest powiązany żaden świadczeniodawca (mógł nie zostać jeszcze dodany lub mógł zostać usunięty jedyny powiązany świadczeniodawca), wówczas strona „Personel medyczny" jest niedostępna. Dokładny opis dodawania świadczeniodawcy poprzez formularz znajduje się w rozdziale *8.3.1 Świadczeniodawcy*.

8.3.5. Rejestr zablokowanych IP

Lista zablokowanych adresów IP ukazuje się po wybraniu w konfiguracji opcji „Rejestr zablokowanych adresów IP". Rejestr podzielony jest na dwie zakładki: Portal oraz eRWS. Jeżeli w tabeli znajduje się jakikolwiek wpis, oznacza to, że użytkownik przekroczył liczbę błędnych logowań. W przypadku listy zablokowanych adresów IP dla Portalu, błędne logowanie oznacza próbę zalogowania się na nieistniejące konto, a dla usługi eRWS - podanie nieprawidłowego hasła usług sieciowych. Od tego momentu każdy użytkownik o tym samym adresie IP nie będzie mógł się zalogować na to konto. Adres IP można odblokować poprzez zaznaczenie użytkownika i naciśnięcie przycisku „Odblokuj adres IP".



Rysunek 127: Lista zablokowanych adresów IP w Portalu

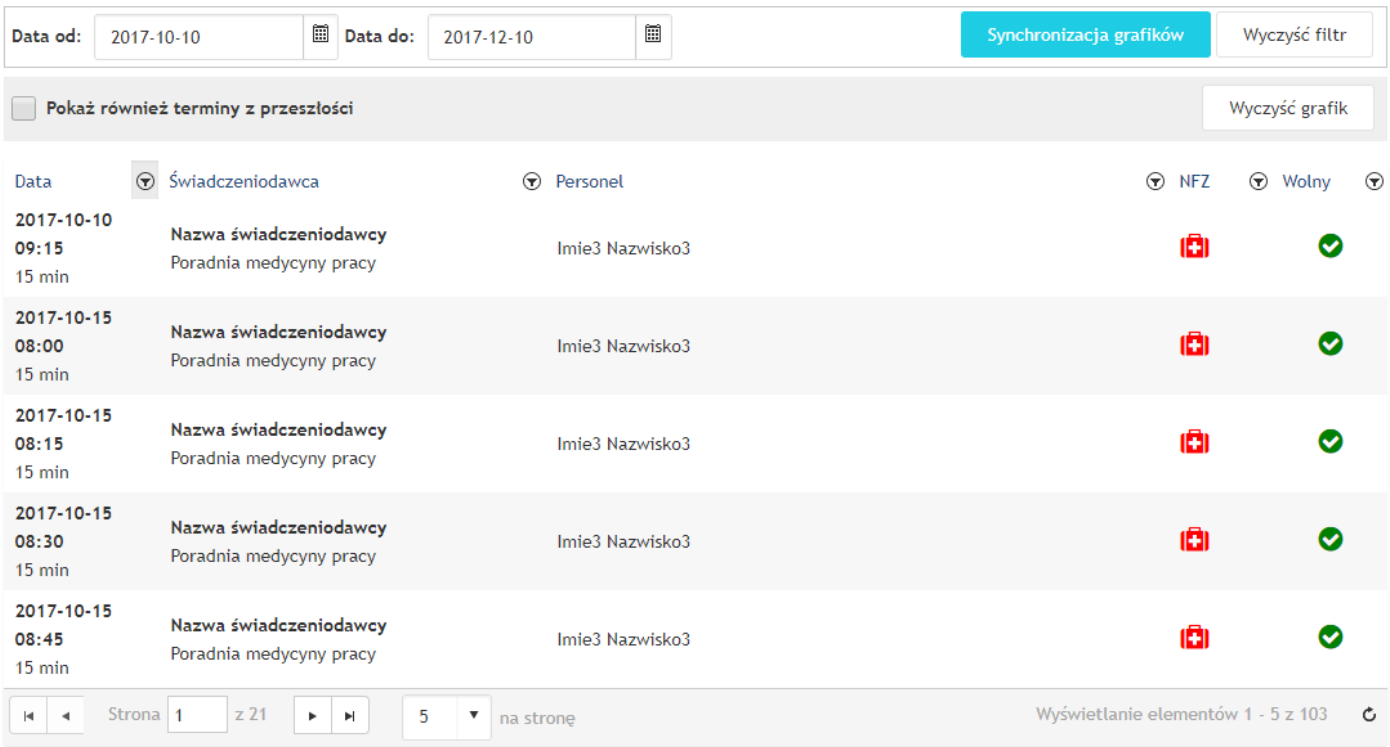


Rysunek 128: Lista zablokowanych adresów IP w usłudze eRWS

8.3.6. Grafik dla trybu offline

Grafik dla trybu offline umożliwia synchronizację grafików w trybie online, co sprawia, że w czasie braku połączenia z bazą danych mMedica, rezerwowanie terminów przez eRejestracja dalej będzie możliwe. W celu synchronizacji grafików należy wybrać zakres czasowy terminów, które chce się udostępnić eRejestracji w razie odłączenia od słownika świadczeniodawców, następnie nacisnąć przycisk „Synchronizacja grafików". Po dokonaniu tej czynności w tabeli ukażą się zsynchronizowane terminy.

Uwaga: W grafiku offline pobierane są do bazy eRejestracji wyłącznie terminy, które w terminarzu mMedica dostępne są dla Portalu eRejestracji i niedostępne dla mMedica.



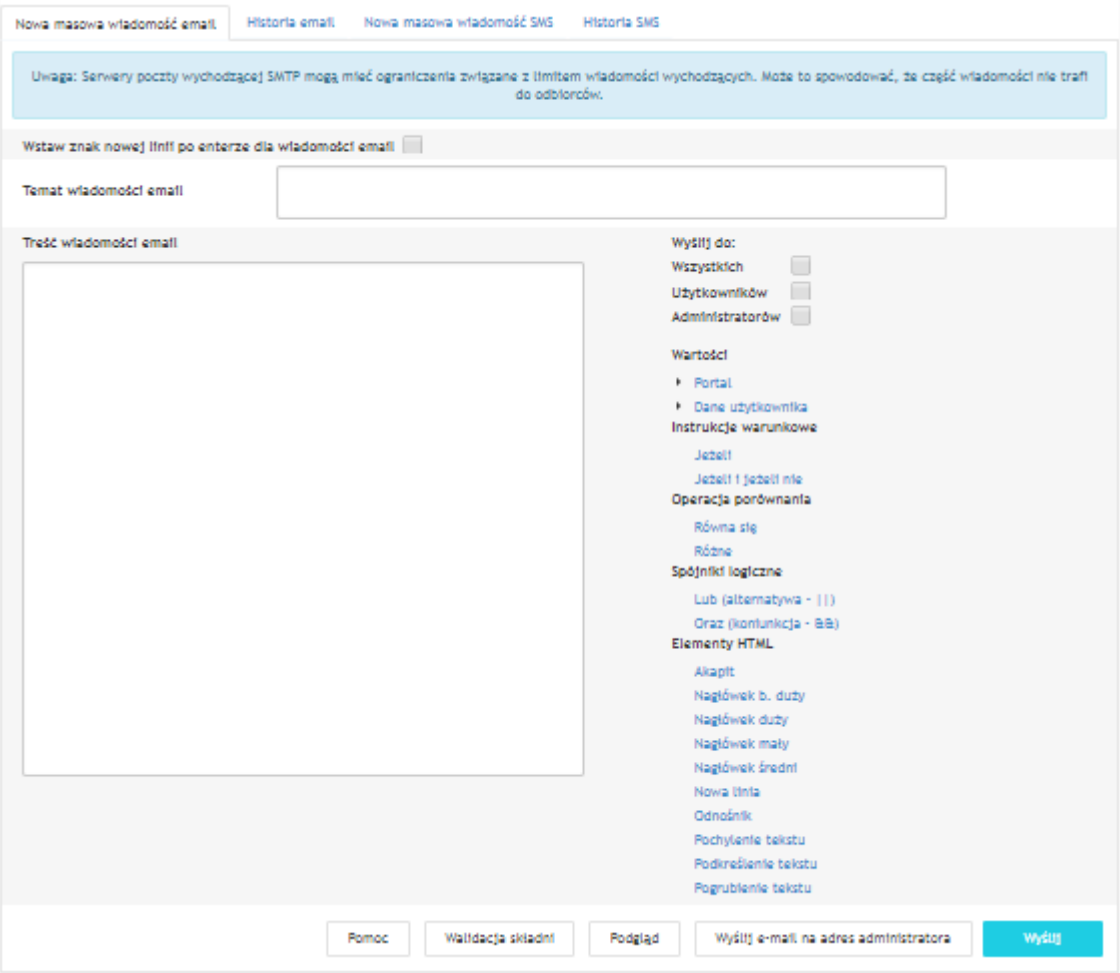
Rysunek 129: Grafik offline

Jeśli z Portalem eRejestracja nie jest powiązany żaden świadczeniodawca (mógł nie zostać jeszcze dodany lub mógł zostać usunięty jedyny powiązany świadczeniodawca), wówczas zakładka „Grafik dla trybu offline” jest niedostępna. Dokładny opis dodawania świadczeniodawcy poprzez formularz znajduje się w rozdziale *8.3.1 Świadczeniodawcy*.

8.3.7. Masowe wiadomości

Portal eRejestracja posiada funkcjonalność konfigurowania oraz wysyłania automatycznych wiadomości email oraz SMS do użytkowników. Istnieje również możliwość utworzenia jednej wiadomości oraz wysłania jej do wszystkich użytkowników portalu.

Uwaga: Funkcjonalność wysyłania masowych wiadomości przeznaczona jest do informowania pacjentów o problemach/przerwach technicznych w funkcjonowaniu Portalu eRejestracji. Wiadomości o charakterze marketingowym należy wysyłać bezpośrednio z aplikacji mMedica, przy wykorzystaniu funkcji "Wyślij powiadomienie"/"Wyślij przypomnienie".



Rysunek 130: Masowe wiadomości

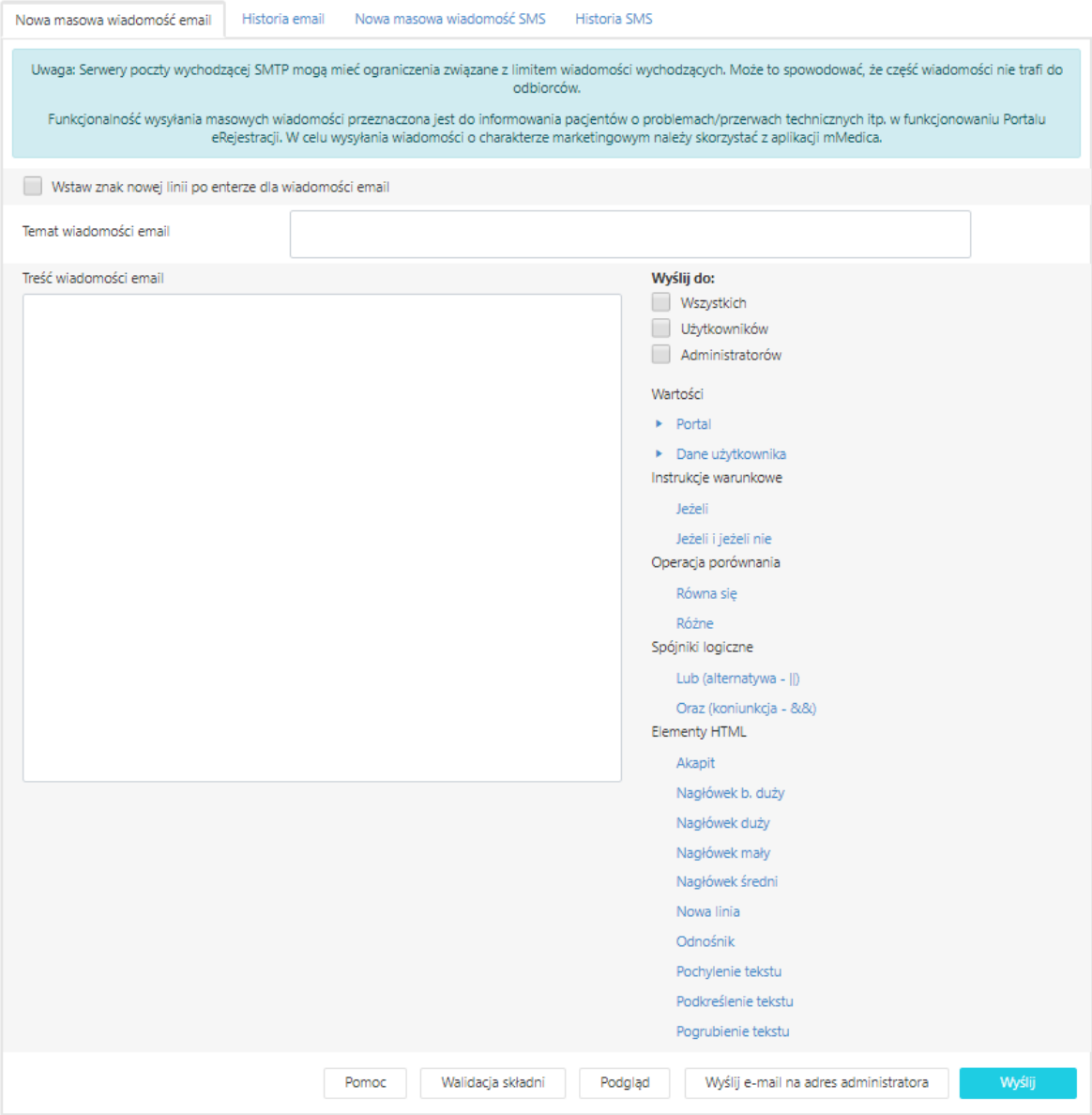
Tworzenie masowej wiadomości email dostępne jest z poziomu konta administratora. Wewnątrz menu „Konfiguracja” należy otworzyć stronę „Masowe wiadomości”.

8.3.7.1. Nowa masowa wiadomość email

Podczas tworzenia nowej wiadomości masowej, administrator musi podać tytuł wiadomości wraz z jej treścią. Za pomocą zaznaczenia odpowiednich pól znajdujących się po lewej stronie określenia tematu, powinien również wskazać, którzy użytkownicy mają otrzymać wysyłaną wiadomość. Dostępne są następujące opcje:

- Wyślij do wszystkich – wiadomość zostanie wysłana do użytkowników i administratorów,
- Wyślij do użytkowników – wiadomość zostanie wysłana jedynie na emaile zwykłych użytkowników,
- Wyślij do administratorów – wiadomość zostanie wysłana jedynie do administratorów portalu eRejestracja.

Treść wiadomości można dostosować do konkretnego użytkownika poprzez konkretne wartości i znaczniki. Istnieje również opcja formatowania wyświetlanego tekstu. Funkcjonalność ta została opisana dokładnie w podrozdziale *8.3.9.3. Szablony wiadomości*.



Rysunek 131: Tworzenie masowej wiadomości email

8.3.7.2. Historia email

Widok tworzenia masowych wiadomości posiada zakładkę „Historia email” zawierającą archiwum wysłanych poprzednio emaili. Każdej wysłanej wiadomości przypisana została unikalna wartość ID, data utworzenia, data wysłania oraz temat wiadomości email. Określeni zostali również adresaci z rozróżnieniem na administratora oraz użytkownika.

Nowa masowa wiadomość email | Historia email | Nowa masowa wiadomość SMS | Historia SMS

Id	Data utworzenia	Data ost. wysłania	Do admin.	Do użytk.	Temat wiadomości email	
28	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
27	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
26	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
25	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
24	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
23	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
22	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
21	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
20	2017-05-25 12:54:43	2017-05-25 12:54:43	✓	✗	fdsf	Użyj
19	2017-05-25 12:54:43	2017-05-25 12:54:43	✓	✗	fdsf	Użyj

Strona 1 z 3 | 10 na stronę | Wyświetlanie elementów 1 - 10 z 27

Rysunek 132: Historia wysłanych masowych wiadomości email

Przy każdym wpisie na początku tabeli umieszczona jest strzałka ▸, która po naciśnięciu rozwinie dany wiersz wyświetlając treść wysłanej wiadomości. Ostatnia kolumna tabeli zawiera przycisk „Użyj”. Kliknięcie tego przycisku wywoła przeniesienie do zakładki „Nowa masowa wiadomość email” wraz z uzupełnioną treścią oraz tematem emaila zgodnymi z zawartością wskazanej w historii wiadomości.

Nowa masowa wiadomość email | Historia email | Nowa masowa wiadomość SMS | Historia SMS

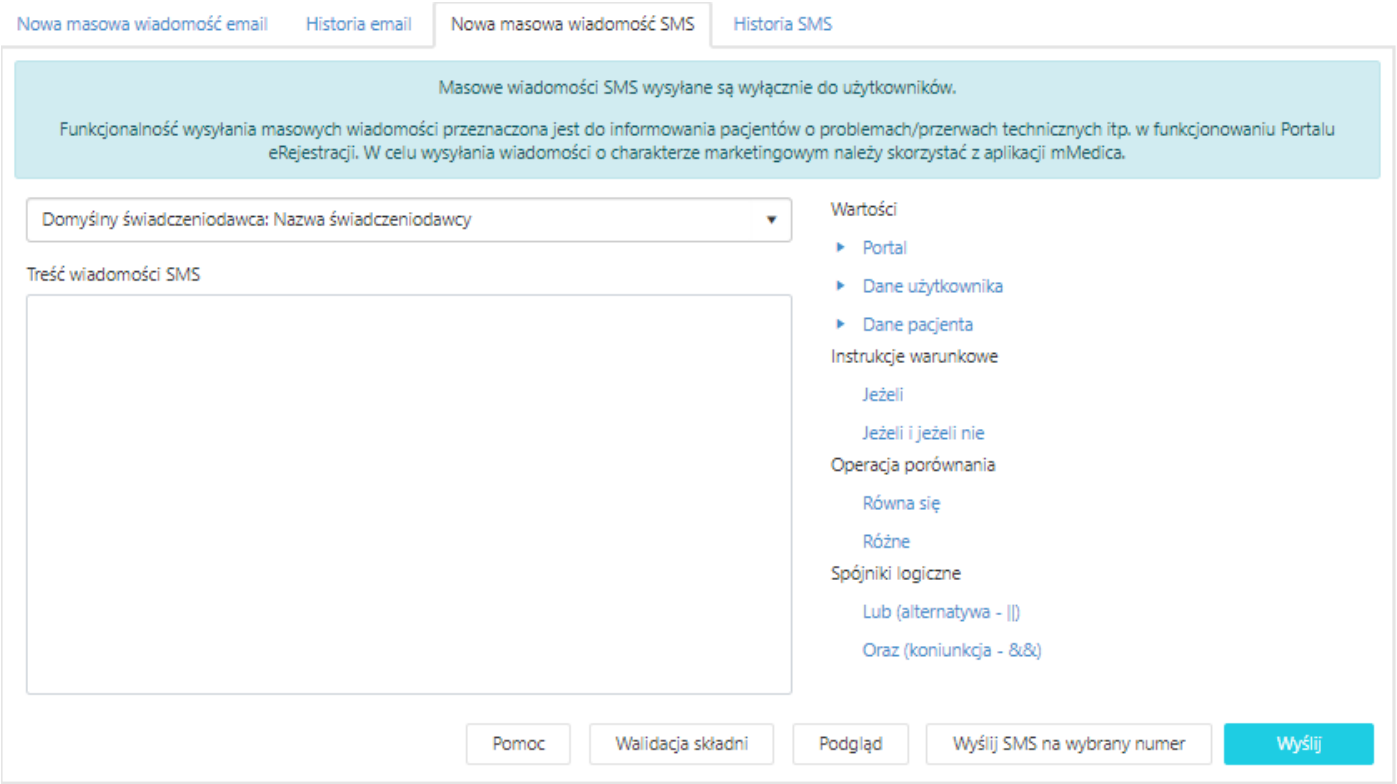
Id	Data utworzenia	Data ost. wysłania	Do admin.	Do użytk.	Temat wiadomości email	
28	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
fdsf						
27	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
26	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
25	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
24	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
23	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
22	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
21	2017-05-25 12:54:44	2017-05-25 12:54:44	✓	✗	fdsf	Użyj
20	2017-05-25 12:54:43	2017-05-25 12:54:43	✓	✗	fdsf	Użyj
19	2017-05-25 12:54:43	2017-05-25 12:54:43	✓	✗	fdsf	Użyj

Strona 1 z 3 | 10 na stronę | Wyświetlanie elementów 1 - 10 z 27

Rysunek 133: Historia wysłanych masowych wiadomości email – zawartość

8.3.7.3. Nowa masowa wiadomość SMS

Kreator tworzenia i wysyłania masowej wiadomości SMS pozwala na wysłanie identycznej wiadomości do wszystkich użytkowników portalu eRejestracja, którzy podali swój numer telefonu.



Rysunek 134: Tworzenie masowej wiadomości SMS

Treść wiadomości można dostosować do konkretnego użytkownika poprzez określone wartości i znaczniki. Funkcjonalność ta została opisana dokładnie w podrozdziale *8.3.9.3. Szablony wiadomości*.

8.3.7.4. Historia SMS

Zakładka „Historia SMS”, dostępna w konfiguracji wiadomości masowych, zawiera archiwum wysłanych masowo wiadomości SMS. Każdej wysłanej wiadomości przypisana została unikalna wartość ID, data utworzenia oraz data wysłania. Przy każdym wpisie na początku tabeli umieszczona jest strzałka ▸, która po naciśnięciu rozwinie dany wiersz, wyświetlając treść wiadomości. Ostatnia kolumna tabeli zawiera przycisk „Użyj”. Kliknięcie tego przycisku wywoła przeniesienie do zakładki „Nowa masowa wiadomość SMS” wraz z uzupełnioną treścią oraz tematem emaila zgodnymi z zawartością wskazanej w historii wiadomości.

Nowa masowa wiadomość email | Historia email | Nowa masowa wiadomość SMS | Historia SMS

Id	Data utworzenia	Data ost. wysłania	Treść wiadomości SMS	
1	2017-05-24 11:05:58	2017-05-24 11:05:58	aaa	Użyj

Strona 1 z 1 | 10 na stronę | Wyświetlanie elementów 1 - 1 z 1

Rysunek 135: Historia wysłanych masowo wiadomości SMS

8.3.8. Kopie zapasowe bazy danych

8.3.8.1. Historia kopii zapasowych

Historia kopii zapasowych zawiera tabelę utworzonych wcześniej automatycznych kopii zapasowych. Tabela zawiera: status, datę utworzenia automatycznej kopii zapasowej, nazwę pliku, numer wersji programu, nazwę użytkownika, który dodał automatyczną kopię zapasową oraz informację czy kopia została zaplanowana, czy utworzona ręcznie.

Historia kopii zapasowych | Automatyczna kopia zapasowa

Status	Data utworzenia	Nazwa pliku	Wersja	Użytkownik	Zaplanowano
✓	23.07.2018 12:48:03	D:\Backups_er\2018-07-23-1248-ERMMEDICA(a).zip	5.12.5	admin	✓
✓	23.07.2018 12:32:04	D:\Backups_er\2018-07-23-1232-ERMMEDICA(a).zip	5.12.5	admin	✓
✓	23.07.2018 11:28:26	D:\Backups_er\2018-07-23-1128-ERMMEDICA(b).zip	5.12.5	admin	✗
✓	23.07.2018 11:18:48	D:\Backups_er\2018-07-23-1118-ERMMEDICA(b).zip	5.12.5	admin	✗

Strona 1 z 1 | 10 na stronę | Wyświetlanie elementów 1 - 4 z 4

Rysunek 136: Historia kopii zapasowych

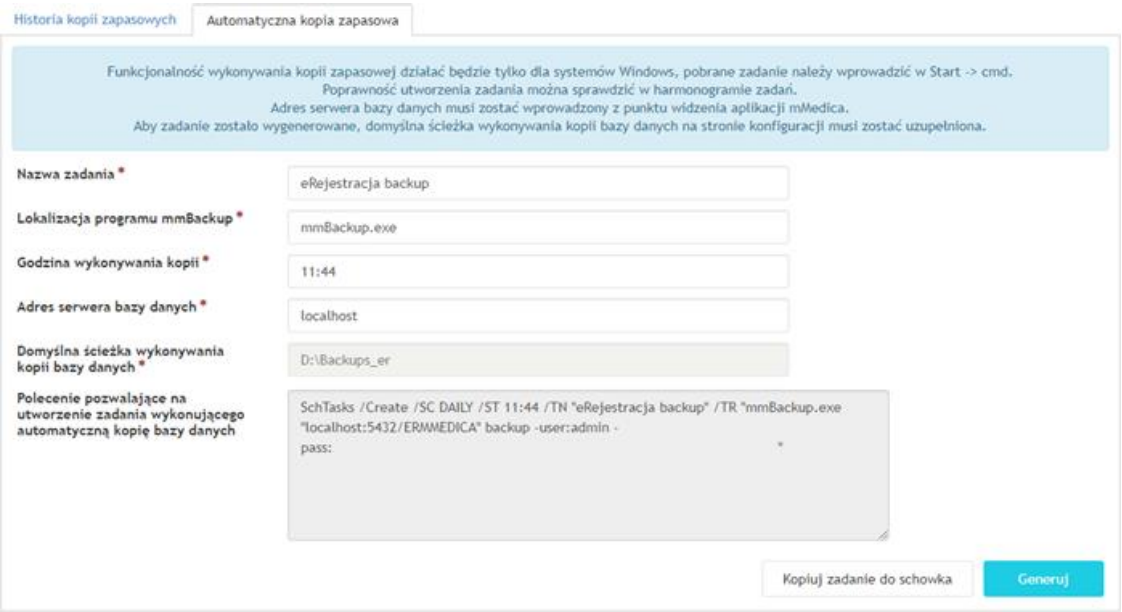
8.3.8.2. Automatyczna kopia zapasowa

Zakładka ta umożliwia zaplanowanie przez administratora wykonywania się automatycznych kopii zapasowych. Aby zaplanować automatyczną kopię, należy wypełnić pola:

- Nazwa zadania,
- Lokalizacja programu mmBackup (należy wpisać pełną ścieżkę dostępu do pliku mmBackup.exe),
- Godzina wykonywania kopii (należy wpisać godzinę, o której codziennie będzie wykonywać się kopia zapasowa),
- Adres serwera bazy danych.

Pole „Domyślna ścieżka wykonywania kopii bazy danych” uzupełniona jest wartością zapisaną w zakładce Konfiguracja -> Podstawowa -> Ogólna w polu „Domyślna ścieżka wykonywania kopii bazy danych” i tylko tam możliwa jest jej edycja.

Po uzupełnieniu pól należy kliknąć przycisk „Generuj”, który utworzy odpowiednie polecenie (w polu „Polecenie pozwalające na utworzenie zadania wykonującego automatyczną kopię bazy danych”). Dane polecenie należy skopiować ręcznie lub poprzez kliknięcie przycisku „Kopiuj zadanie do schowka”. Następnie należy otworzyć na komputerze wiersz poleceń i wkleić do niego skopiowane polecenie, oraz zatwierdzić je naciskając klawisz „Enter”.



Rysunek 137: Automatyczna kopia zapasowa

Uwaga: Za każdym razem, gdy zmieni się hasło użytkownika generującego automatyczną kopię zapasową, należy wygenerować na nowo wszystkie utworzone zadania wykonujące automatyczne kopie bazy danych.

8.3.9. Konfiguracja

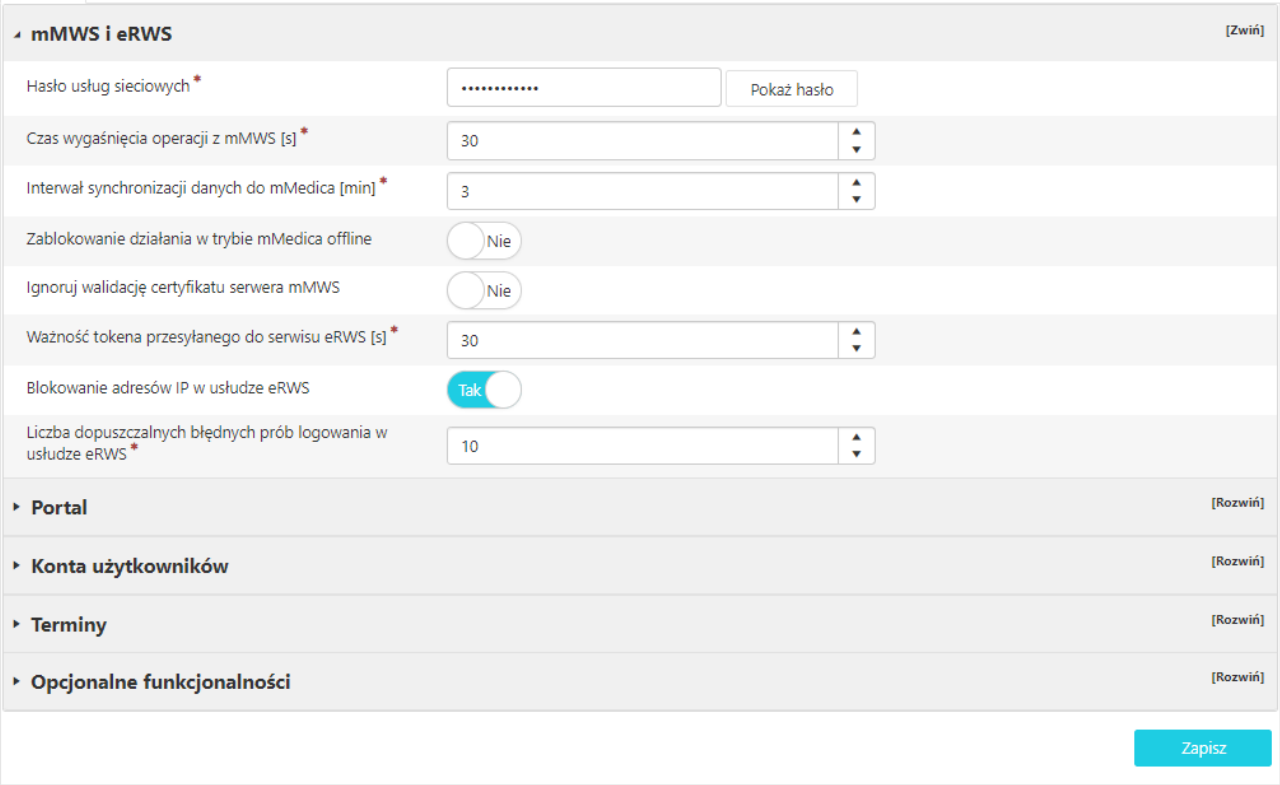
8.3.9.1. Konfiguracja podstawowa

W celu przejścia do ustawień konfiguracyjnych w podstronie „Konfiguracja” należy wybrać opcję „Podstawowa”. Wyświetlona w tym miejscu tabela zawiera wszystkie parametry konfiguracyjne dostępne w portalu eRejestracja.

Aby ułatwić konfigurowanie portalu eRejestracja, ustawienia rozdzielono pomiędzy zakładki: „Ogólna”, „ePUAP”, „SMTP”, „Bramka SMS, „Chmura dla zdrowia” oraz „Informacje Medyczne”. Każda zakładka zawiera w sobie parametry konfiguracyjne ustawień konkretnych usług.

8.3.9.1.1. Konfiguracja ogólna

Zakładka „Ogólna” dotyczy w głównej mierze ustawień wyglądu portalu oraz jego ogólnej funkcjonalności. Pod nimi zawarte są ustawienia dotyczące ogólnych funkcjonalności eRejestracji.

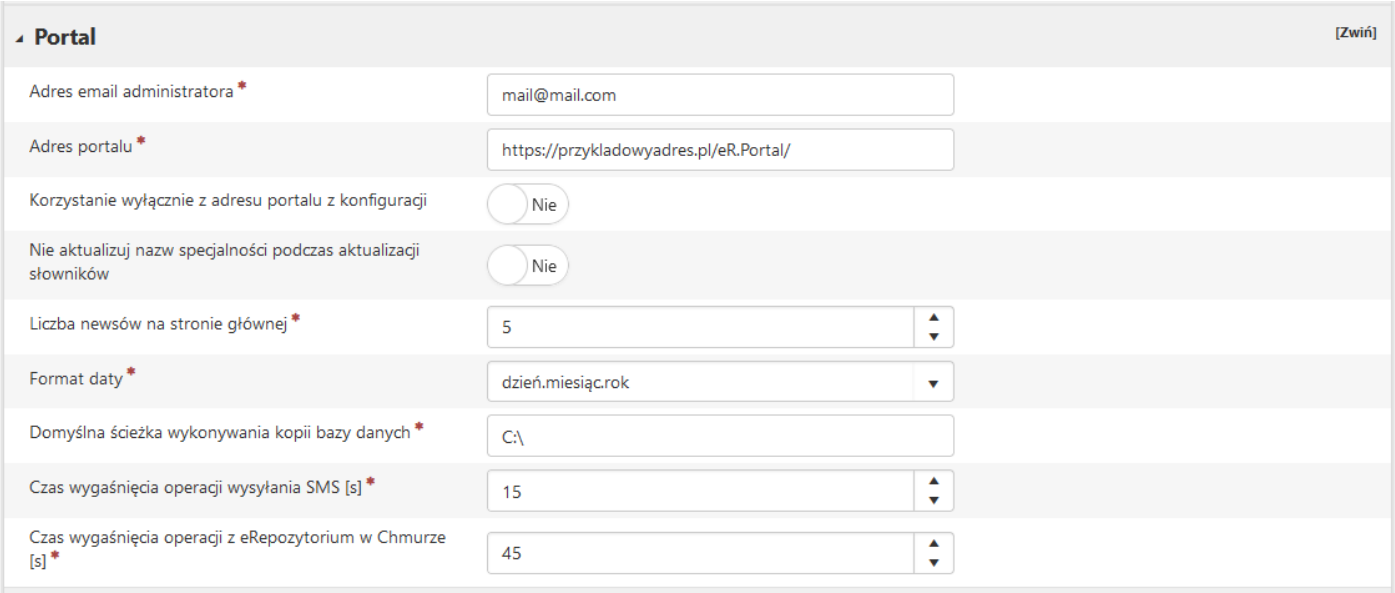


Rysunek 138: Konfiguracja podstawowa – zakładka „Ogólna” – konfiguracja mMWS i eRWS

Poniżej wymieniono każdą z opcji dostępnej do konfiguracji mMWS i eRWS wraz z krótkim opisem:

- Hasło usług sieciowych – hasło dostępu do usług sieciowych programu mMedica. Zmiana parametru powoduje również zmianę hasła usług sieciowych w podłączonych bazach danych mMedica przez skojarzone usługi mMWS. Obok pola na wpisanie hasła znajduje się przycisk „Pokaż hasło”. Po jego kliknięciu zakropkowane hasło stanie się widoczne, a obok niego pojawi się przycisk „Ukryj hasło”, umożliwiający ponowne zakropkowanie hasła.
- Czas wygaśnięcia operacji z mMWS [s] – maksymalny dopuszczalny czas operacji z mMWS (timeout) wyrażony w sekundach.

- Interwał synchronizacji danych do mMedica [min] – czas, po jakim uruchomi się automatyczny proces synchronizacji danych z eRejestracji do programu mMedica, po przywróceniu połączenia pomiędzy eRejestracja a mMedica.
- Zablokowanie działania w trybie offline – w przypadku, gdy z portalem nie będzie połączony żaden aktywny słownik świadczeniodawców, użytkownicy nie będą mogli tworzyć, przeglądać oraz rezerwować wizyt. Zablokowana będzie również funkcjonalność tworzenia nowych kont.
- Ignoruj walidację certyfikatu serwera mMWS – musi być włączona dla certyfikatów samopodpisanych.
- Ważność tokena przesyłanego do serwisu eRWS [s] – okres ważności hasła wygenerowanego do serwisu eRWS wyrażony w sekundach. Zmiana czasu skutkuje zmianą wartości czasu ważności tokena w podłączonych bazach danych mMedica za pośrednictwem usług mMWS.
- Blokowanie adresów IP w usłudze eRWS – określa, czy mechanizm blokowania adresów IP w usłudze eRWS jest włączony. Domyślnie ta opcja jest wyłączona.
- Liczba dopuszczalnych błędnych prób logowania w usłudze eRWS – parametr konfiguracyjny dostępny w przypadku, gdy blokowanie adresów IP w usłudze eRWS jest włączone. W przypadku przekroczenia ustawionej liczby logowań, adres IP zostanie zablokowany.



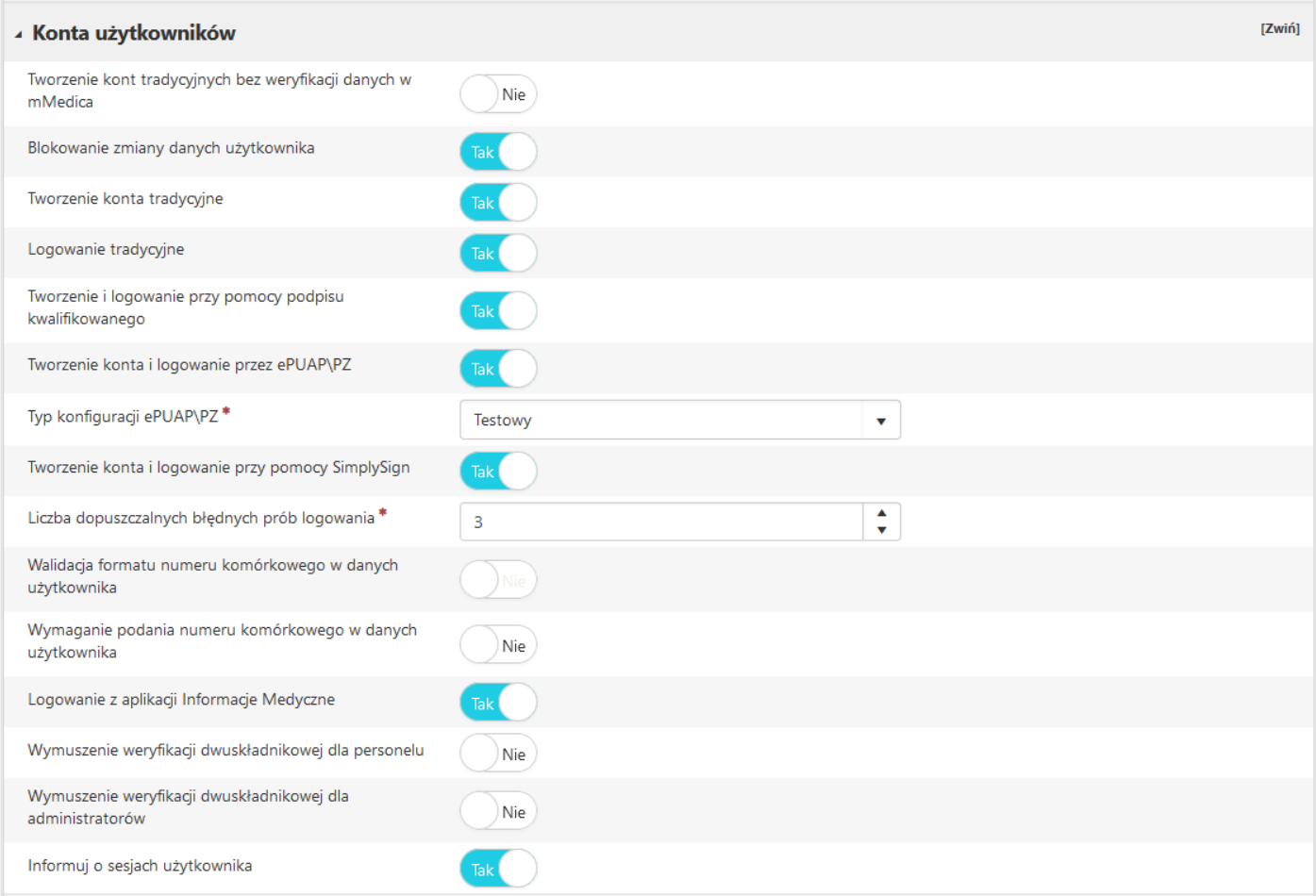
Rysunek 139: Konfiguracja podstawowa – zakładka „Ogólna" - portal

Poniżej wymieniono każdą z opcji dostępnej do konfiguracji Portalu wraz z krótkim opisem:

- Adres email administratora – adres email wyświetlany w stopce strony.
- Adres portalu – adres głównej strony portalu eRejestracja.

- Korzystanie wyłącznie z adresu portalu z konfiguracji – wymusza pobieranie adresu portalu z konfiguracji zamiast z żądania do serwera podczas m.in. tworzenia linków aktywacyjnych lub resetowania hasła. Opcja powinna zostać włączona podczas korzystania z przekierowywania portów na routerach lub w przypadku wykorzystywania protokołu HTTPS na Linux.
- Nie aktualizuj nazw specjalności podczas aktualizacji słowników – określa, czy możliwość zmiany nazwy specjalności podczas wykonywania aktualizacji słowników ma być zablokowana.
- Liczba newsów na stronie głównej – w przypadku przekroczenia liczby newsów o podaną wartość, na stronie przestaną być wyświetlane te z najstarszą datą.
- Format daty – rozwijana lista zawierająca różne formaty dat. Ustawienie dotyczy wszystkich dat wyświetlanych na portalu.
- Domyślna ścieżka wykonywania kopii bazy danych – ustawienie domyślnej ścieżki utworzenia kopii bazy danych eRejestracji. Ścieżka powinna być w zwykłym formacie zgodnym z systemami Microsoft Windows, np. „D:\\kopie_zapasowe\” względem programu mMBackup. Ścieżka zostanie wczytana w programie mMBackup podczas tworzenia kopii zapasowej bazy danych eRejestracji.
- Czas wygaśnięcia operacji wysyłania SMS [s] – maksymalny dopuszczalny czas operacji wysyłania wiadomości SMS (timeout) wyrażony w sekundach.
- Czas wygaśnięcia operacji z eRepozytorium w Chmurze [s] – maksymalny dopuszczalny czas operacji wysyłania żądania do eRepozytorium w Chmurze (timeout) wyrażony w sekundach.

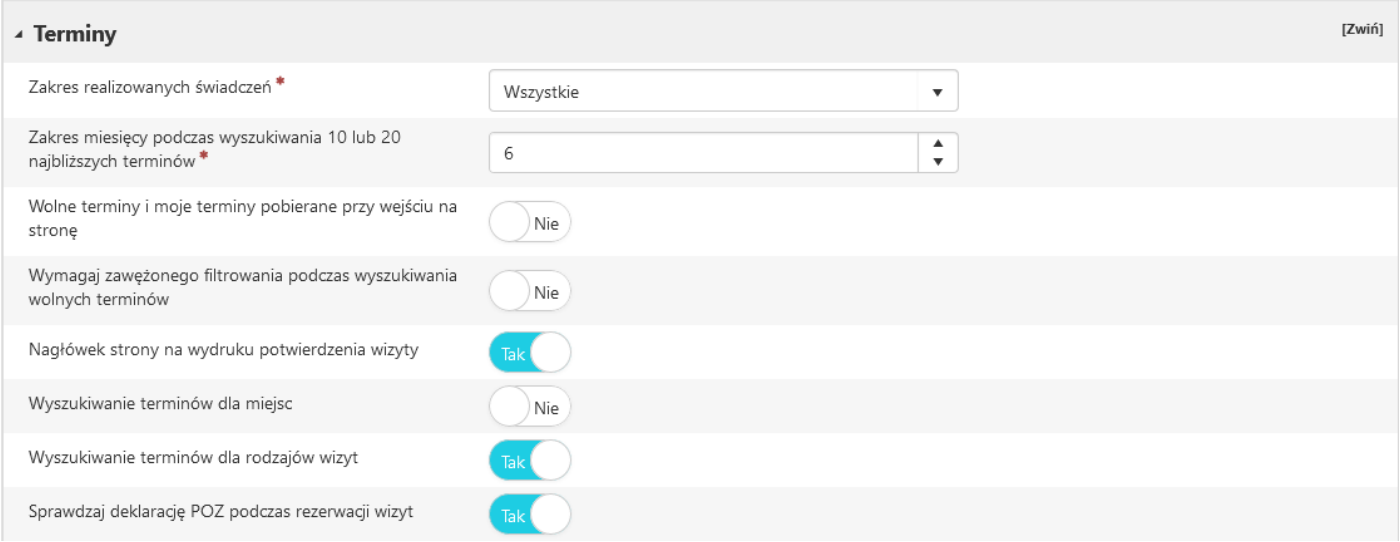
Poniżej wymieniono każdą z opcji dostępnej do konfiguracji kont użytkowników wraz z krótkim opisem:



Rysunek 140: Konfiguracja podstawowa – zakładka „Ogólna”- konta użytkowników

- Tworzenie kont tradycyjnych bez weryfikacji danych w mMedica – włączenie tej funkcjonalności powoduje brak konieczności ręcznej weryfikacji (scalania) kont w mMedica (co jest wymagane w przypadku, kiedy następuje próba utworzenia konta z danymi pacjenta znajdującego się już w bazie mMedica). Włączenie tej opcji związane jest jednak z ryzykiem automatycznego scalenia kont dwóch różnych osób.
- Blokowanie zmiany danych użytkownika – blokuje możliwość zmiany nazwiska oraz danych adresowych użytkownika z poziomu Portalu.
- Tworzenie subkont – definiuje, czy w portalu możliwe jest tworzenie subkont.
- Tworzenie konta tradycyjne – włączenie tej opcji uniemożliwia rejestrację kont na portalu poprzez metodę tradycyjną.
- Logowanie tradycyjne – administrator może zadecydować, które metody logowania będą dostępne dla portalu. W razie wyłączenia opcji logowania tradycyjnego dostępna jest ukryta formatka logowania dla użytkowników posiadających konto o tym typie. Wczytanie formatki nastąpi po dopisaniu do adresu strony końcówki *„/Account/LogOnDefault?forceNormalLogon=true”*

- Tworzenie konta i logowanie przy pomocy podpisu kwalifikowanego – administrator może zadecydować, czy metody logowania i tworzenia konta przy pomocy podpisu kwalifikowanego mogą być dostępne w portalu.
- Tworzenie konta i logowanie przez ePUAP\PZ – administrator może zadecydować, czy metody logowania oraz tworzenia konta przez ePUAP\PZ mają być dostępne w portalu.
- Typ konfiguracji ePUAP\PZ – administrator może zadecydować, czy konfiguracja ma być testowa czy produkcyjna.
- Tworzenie konta i logowanie przy pomocy SimplySign - administrator może zadecydować, czy metody logowania oraz tworzenia konta przy pomocy SimplySign mają być dostępne w portalu.
- Liczba dopuszczalnych błędnych prób logowania – w przypadku przekroczenia ustawionej liczby logowań konto użytkownika zostanie zablokowane.
- Walidacja formatu numeru komórkowego w danych użytkownika – Opcja ta została usunięta. Od wersji 8.3.0 na stałe zostaje nałożony wymóg podawania numeru telefonu w określonym formacie.
- Wymaganie podania numeru komórkowego w danych użytkownika – ustawienie wymogu podania numeru telefonu przez użytkownika przy rejestracji. Dla użytkowników, którzy utworzyli konto bez tego wymogu, zostanie wyświetlona informacja o konieczności podania numeru podczas edytowania danych.
- Logowanie z aplikacji Informacje Medyczne – administrator może zadecydować, czy możliwość logowania z aplikacji Informacje Medyczne ma być dostępna w portalu.
- Wymuszenie weryfikacji dwuskładnikowej dla personelu - aktywacja tej opcji wymusza logowanie dwuskładnikowe przez personel medyczny.
- Wymuszenie weryfikacji dwuskładnikowej dla administratorów – aktywacja tej opcji wymusza logowanie dwuskładnikowe przez administratorów.
- Informuj o sesjach użytkownika – aktywacja tej opcji umożliwia zarządzanie aktywnymi sesjami użytkownika.

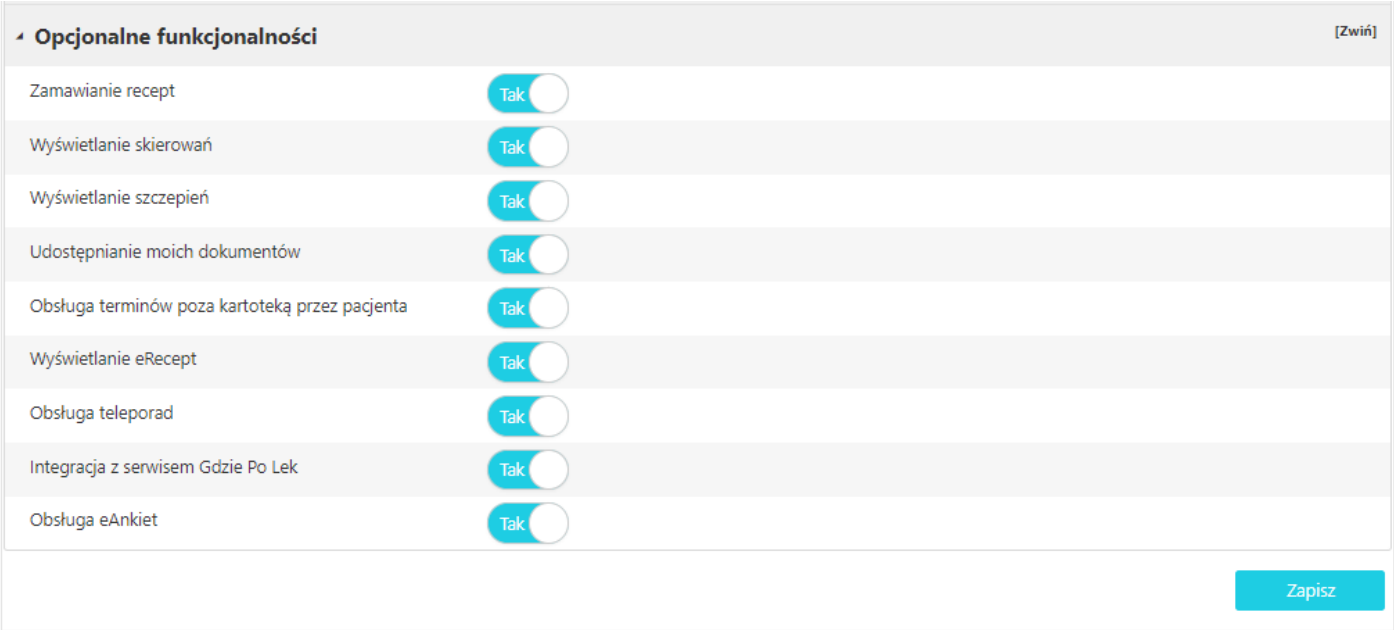


Rysunek 141: Konfiguracja podstawowa – zakładka „Ogólna" - terminy

Poniżej wymieniono każdą z opcji dostępnej do konfiguracji wyszukiwania terminów wraz z krótkim opisem:

- Zakres realizowanych świadczeń – dostępne są do wyboru opcje: wszystkie, NFZ, prywatne. W wolnych terminach będą wyświetlać się wizyty zgodnie z wybranym zakresem realizowanych świadczeń.
- Zakres miesięcy podczas wyszukiwania 10 lub 20 najbliższych terminów – liczba miesięcy jaka jest brana pod uwagę podczas wyszukiwania 10 lub 20 najbliższych terminów.
- Wolne terminy i moje terminy pobierane przy wejściu na stronę – dane w tabelach wolnych terminów i moich terminów mogą być automatycznie wyświetlane przy wchodzeniu na stronę (przy wyłączonej opcji pobierane są dopiero po ustawieniu filtrów wyszukiwania i naciśnięciu „Wyszukaj").
- Wymagaj zawężonego filtrowania podczas wyszukiwania wolnych terminów – wymusza, aby podczas wyszukiwania wolnych terminów wybrać jeden z filtrów dotyczących: specjalności, świadczenia, personelu, rodzaju wizyty lub miejsca.
- Nagłówek strony na wydruku potwierdzenia wizyty – sprawia, że zawartość nagłówka portalu zostaje wydrukowana na potwierdzeniu rezerwacji wizyty użytkownika.
- Wyszukiwanie terminów dla miejsc – w przypadku aktywowania funkcjonalności, pacjenci będą mogli wyszukiwać wolne terminy na wizyty przypisane do miejsc.
- Wyszukiwanie terminów dla rodzajów wizyt - w przypadku aktywowania funkcjonalności, pacjenci będą mogli wyszukiwać wolne terminy ze względu na rodzaj wizyty.

- Sprawdzaj deklarację POZ podczas rezerwacji wizyty - w przypadku aktywowania funkcjonalności, pacjenci będą mogli zarezerwować wizytę POZ (NFZ) tylko jeżeli posiadają w placówce aktywną deklarację. Funkcjonalność weryfikacji deklaracji nie jest sprawdzana dla rezerwacji w trybie offline.



Rysunek 142: Konfiguracja podstawowa – zakładka „Ogólna" – opcjonalne funkcjonalności

Poniżej wymieniono każdą z opcjonalnych funkcjonalności, które można włączyć w Portalu wraz z krótkim opisem:

- Zamawianie recept – w przypadku aktywowania funkcjonalności, pacjenci będą mogli dokonywać rezerwowania wizyt receptowych.

> **Uwaga:** Podczas zamawiania recept zostaną wyświetlone wyłącznie terminy wystawienia, które zostały skonfigurowane w terminarzu mMedica jako przypisane do predefiniowanego miejsca „Wizyta receptowa" (kod „REC").

- Wyświetlanie skierowań – aktywacja tej opcji pozwala pacjentom przeglądać swoje skierowania.
- Wyświetlanie szczepień – aktywacja tej opcji pozwala pacjentom przeglądać historię swoich szczepień oraz zaplanowane szczepienia.
- Udostępnianie moich dokumentów – aktywacja tej opcji umożliwia użytkownikom wyświetlanie i pobieranie dokumentów medycznych (w formacie HL7) udostępnionych przez personel w mMedica. Dokumenty są pobierane z eRepozytorium w Chmurze lub Archiwum (w zależności od licencji na oprogramowanie mMedica).

eRejestracja obsługuje dokumenty medyczne zgodne z Polską Implementacją Krajową HL7 CDA. Dokumenty są wyświetlane za pomocą transformat bazujących na transformatach Centrum Systemów Informacyjnych Ochrony Zdrowia w wersjach 1.2, 1.3.1 oraz 1.3.2. Poniżej przedstawiono obsługiwane rodzaje dokumentów:

Grupa (filtr w eR)	Rodzaj dokumentu	Kod LOINC	Kod KLAS_DOK_P1
Informacje	Zalecenia pielęgniarskie	64295-9	05.50
Informacje	Konsultacja lekarska	11488-4	05.00
Inne	Dokument własny pacjenta	72170-4	00.00
Inne	Protokół operacyjny	11504-8	00.60
Inne	Zlecenie na zaopatrzenie w wyroby medyczne	57829-4	02.81
Inne	Pozostałe dokumenty pielęgniarskie	46208-5	05.70
Inne	Wpis do karty szczepień	34109-9	07.61
Inne	Dokument anulujący	51851-4	08.80
Karty informacyjne	Informacja dla lekarza kierującego	51852-2	08.90
Karty informacyjne	Informacja o odmowie przyjęcia	11488-4	00.65
Karty informacyjne	Karta informacyjna z leczenia szpitalnego	18842-5	00.20
Recepty	Recepta	57833-6	04.01
Skierowania	Skierowanie na badanie lub leczenie	57832-8	02.10
Skierowania	Skierowanie na konsultację	57133-1	02.11
Skierowania	Prośba o objęcie opieką	34140-4	02.12
Wyniki badań	Wyniki badań laboratoryjnych	11502-2	06.10
Wyniki badań	Wyniki badań diagnostycznych	70004-7	06.00

Uwaga: Funkcjonalność wymaga modułu eRejestracja+. Dodatkowo w zależności od źródła podchodzenia dokumentów, funkcjonalność wymaga licencji na Moduł Integracji eRepozytorium w Chmurze lub eArchiwum. Pobierane z Archiwum wymaga poprawnie skonfigurowanego oprogramowania mMedica Archiwum oraz właściwej konfiguracji modułu Archiwum w mMedica. Z kolei z eRepozytorium w Chmurze wymaga pobranej konfiguracji połączenia do Chmury dla zdrowia z mMedica.

- Obsługa terminów poza kartoteką przez pacjenta – aktywacja tej opcji umożliwia pacjentom wykonywanie szybkich rezerwacji. Rezerwacja, zmiana lub odwołanie terminu wizyty następuje przez portal eRejestracji bez potrzeby tworzenia konta (wymaga wysyłki wiadomości SMS).

Uwaga: Funkcjonalność wymaga modułu eRejestracja+, puli SMS oraz dotyczy wyłącznie wizyt komercyjnych.

- Wyświetlanie eRecept – aktywacja tej opcji pozwala pacjentom na przeglądanie wystawionych eRecept (wraz z kodem dostępowym do odbioru eRecept).
- Obsługa teleporad – aktywacja tej opcji pozwala na wykonywanie wizyt za pomocą między innymi następujących kanałów komunikacji: telefon, Skype, WhatsApp, wideorozmowa.

Uwaga: Funkcjonalność wymaga modułu Teleporada. Do obsługi teleporad wymagana jest konfiguracja harmonogramów użyciem predefiniowanego miejsca „Teleporada" (kod „TELE") w mMedica. Grafik trybu offline nie wspiera obsługi teleporad.

- Integracja z serwisem Gdzie Po Lek – aktywacja tej opcji pozwala na wyszukanie dostępności leku za pomocą kodu EAN przez serwis gdziepolek.pl w funkcjonalnościach użytkownika związanych z zamawianiem recept, wystawionymi eReceptami oraz historią zamówionych recept.
- Obsługa eAnkiet – uruchomienie funkcjonalności pozwala na tworzenie eAnkiet dla użytkowników po zalogowaniu lub po rezerwacji terminu na podstawie skonfigurowanych akcji ankietowych. Dodatkowo umożliwia użytkownikom przeglądanie utworzonych eAnkiet.

Uwaga: Funkcjonalność wymaga modułu eAnkiety oraz pobranej konfiguracji połączenia do Chmury dla zdrowia z mMedica.

8.3.9.1.2. Konfiguracja ePUAP\PZ

Zakładka „ePUAP\PZ" pozwala skonfigurować parametry komunikacji z platformą ePUAP. Administrator portalu powinien wprowadzić nazwę SAML, wgrać certyfikat za pomocą przycisku „Wybierz…" oraz uzupełnić pole hasła. Wprowadzone dane muszą być zgodne z danymi rejestracyjnymi w systemie PZ (podsystem ePUAP) i mogą zostać zmienione w dowolnej chwili. Więcej informacji znajduje się w punkcie *8.5. Konfiguracja ePUAP.*

Rysunek 143: Konfiguracja ePUAP

Uwaga: Do poprawnej integracji wymaganie jest skonfigurowanie adresu strony w *8.3.9.1.1 Konfiguracja ogólna* zgodnie z adresami podanymi w formularzu rejestracyjnych w systemie PZ.

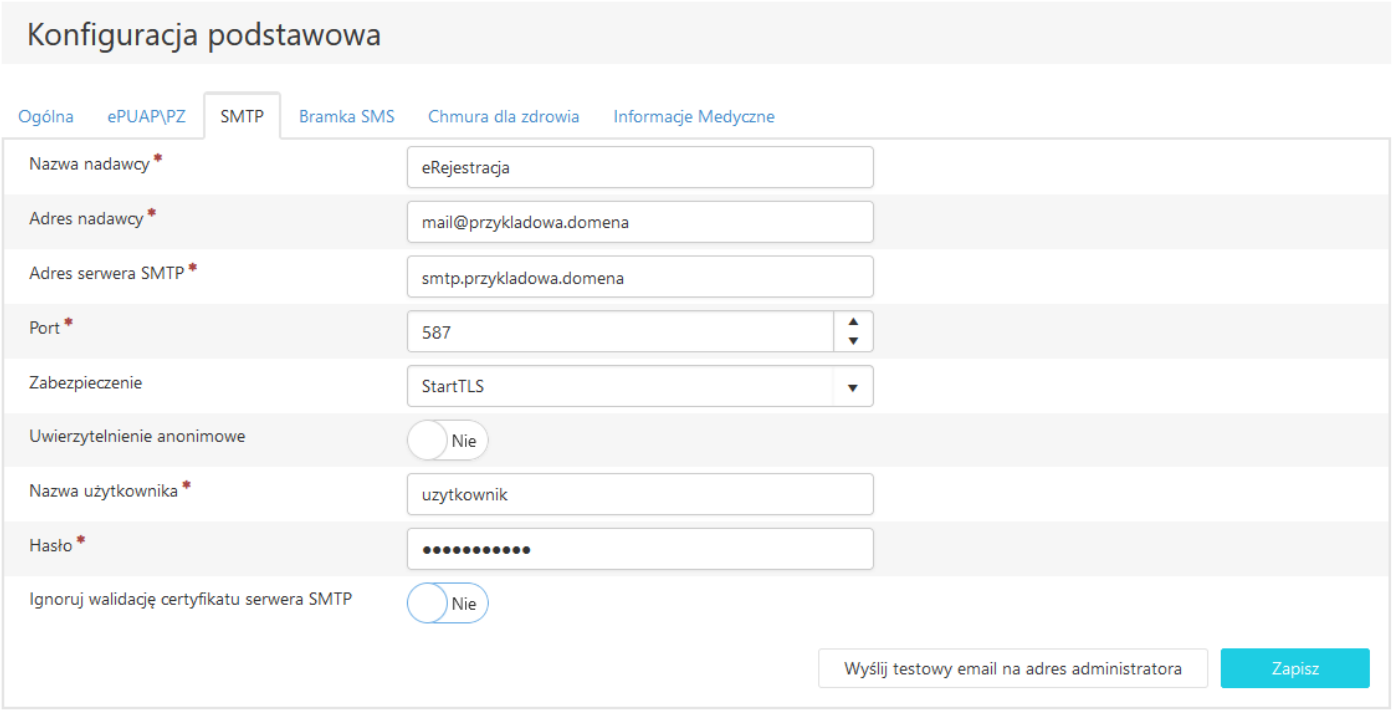
8.3.9.1.3. Konfiguracja SMTP

Konfiguracja SMTP umożliwia skonfigurowanie połączenia z serwerem poczty wychodzącej. W przypadku uwierzytelniania anonimowego, pola podania nazwy użytkownika oraz hasła znikną. Po wprowadzeniu zmian należy wysłać testowy email na adres administratora w celu sprawdzenia poprawności konfiguracji. Email testowy wysyłany jest poprzez naciśnięcie przycisku „Wyślij testowy email na adres administratora".

Ignorowanie walidacji certyfikatu serwera SMTP powinno być zawsze włączone dla certyfikatów samopodpisanych.

W przypadku problemów komunikacyjnych z wysłaniem wiadomości email aplikacja ponawia wysyłkę w momencie ustanowienia poprawnego połączenia do serwera SMTP.

Uwaga: eRejestracja wspiera zarówno komunikacje bez szyfrowania, jak i standard komunikacji szyfrowanej TLS. Konfiguracja dostępu do serwera SMTP zależy od usługodawcy poczty. Jeżeli usługodawca nie podaje portu do komunikacji szyfrowanej TLS, należy wpisać domyślny port tego standardu, czyli 587. Domyślną opcją konfiguracji zabezpieczonej komunikacji jest „StartTLS".

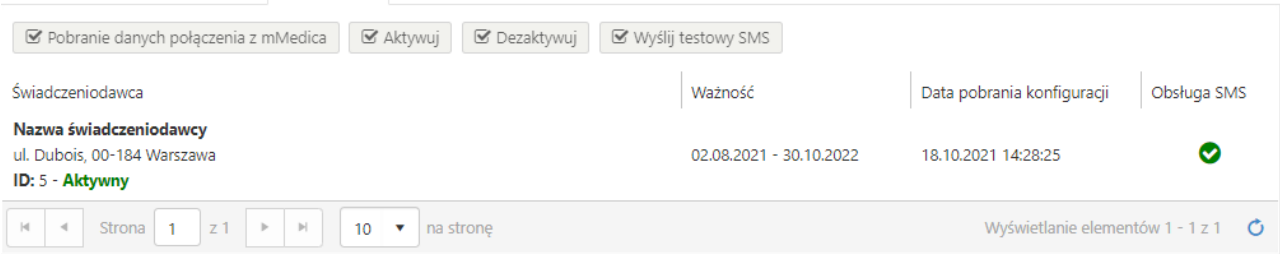


Rysunek 144: Konfiguracja SMTP

8.3.9.1.4. Bramka SMS

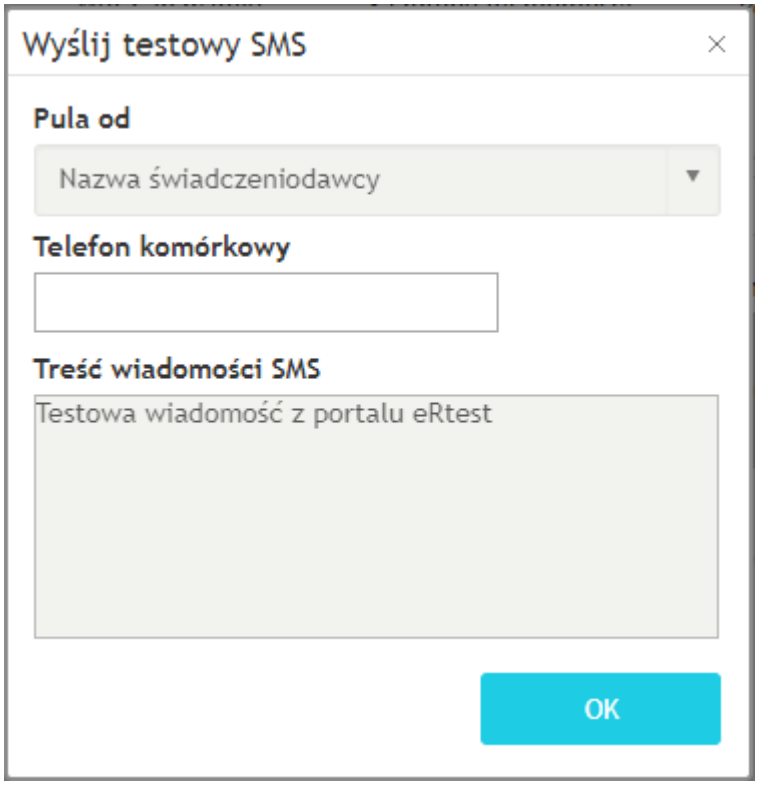
Zakładka umożliwia pobranie konfiguracji dla bramki SMS ze słownika świadczeniodawców połączonego z portalem eRejestracja. Korzystanie z opcji powiadomień SMS na portalu wymaga posiadania w aplikacji mMedica modułu SMS oraz puli wiadomości do wysłania. Dla wybranej bramki świadczeniodawcy dostępne są następujące opcje:

- Pobranie danych połączenia z mMedica,
- Aktywuj,
- Dezaktywuj,
- Wyślij testowy SMS.



Rysunek 145: Konfiguracja Bramki SMS

Pobranie bieżących ustawień konfiguracyjnych następuje po zaznaczeniu wybranego słownika świadczeniodawcy i naciśnięciu przycisku „Pobranie danych połączenia z mMedica”, dostępnego w górnym poziomym menu aplikacji. W celu weryfikacji wykonanych ustawień należy wysłać wiadomość testową za pomocą przycisku „Wyślij testowy SMS”, a następnie w nowo otwartym oknie podać numer telefonu komórkowego. Jeśli konfiguracja została przeprowadzona poprawnie, na podany numer przyjdzie testowa wiadomość SMS.

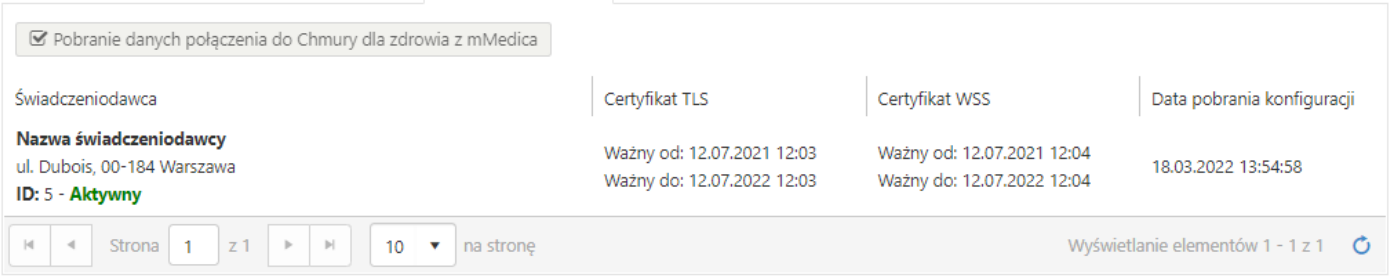


Rysunek 146: Konfiguracja Bramki SMS – wysyłanie wiadomości testowej

Uwaga: Dodatkowe informacje o konfiguracji bramki SMS znajdują się w rozdziale *8.3.11.1. Specjalności*.

8.3.9.1.5. Chmura dla zdrowia

Zakładka wyświetla pobrane z mMedica informacje o danych uwierzytelniających połączenie do Chmury dla zdrowia. Na Chmurę dla zdrowia składa się m.in. eRepozytorium w Chmurze oraz eAnkiety. Dane połączeniowe pobierane są podczas dodawania świadczeniodawcy oraz aktualizacji jego danych.



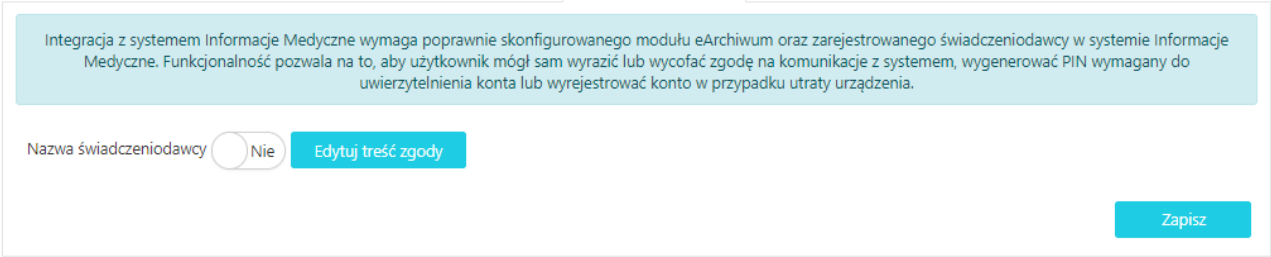
Rysunek 147: Konfiguracja połączenia do Chmury dla zdrowia

Po zaznaczeniu świadczeniodawcy możliwe jest ponowne pobranie danych za pomocą przycisku „Pobranie danych połączenia do Chmury dla zdrowia z mMedica". W przypadku, w którym certyfikat TLS lub WSS utracił ważność wymagane jest ponowne pobranie danych połączeniowych.

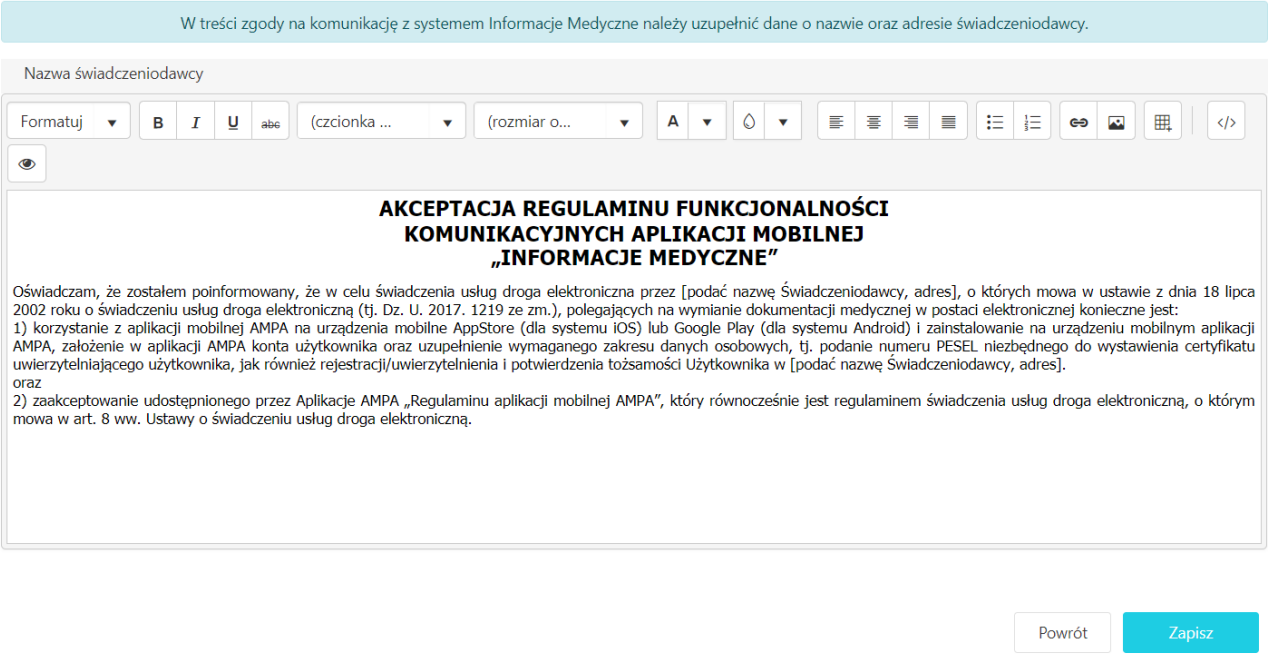
Uwaga: Funkcjonalność wymaga licencji na Moduł Integracji eRepozytorium w Chmurze lub licencji na eAnkiety.

8.3.9.1.6. Informacje Medyczne

Konfiguracja integracji z systemem Informacje Medyczne (IM) składa się z dwóch ustawień dla wszystkich zarejestrowanych w tym systemie świadczeniodawców: włączenie/wyłączenie integracji oraz edycja treści zgody użytkownika na komunikację z systemem IM. Integracja z systemem IM wymaga także poprawnie skonfigurowanego modułu eArchiwum.



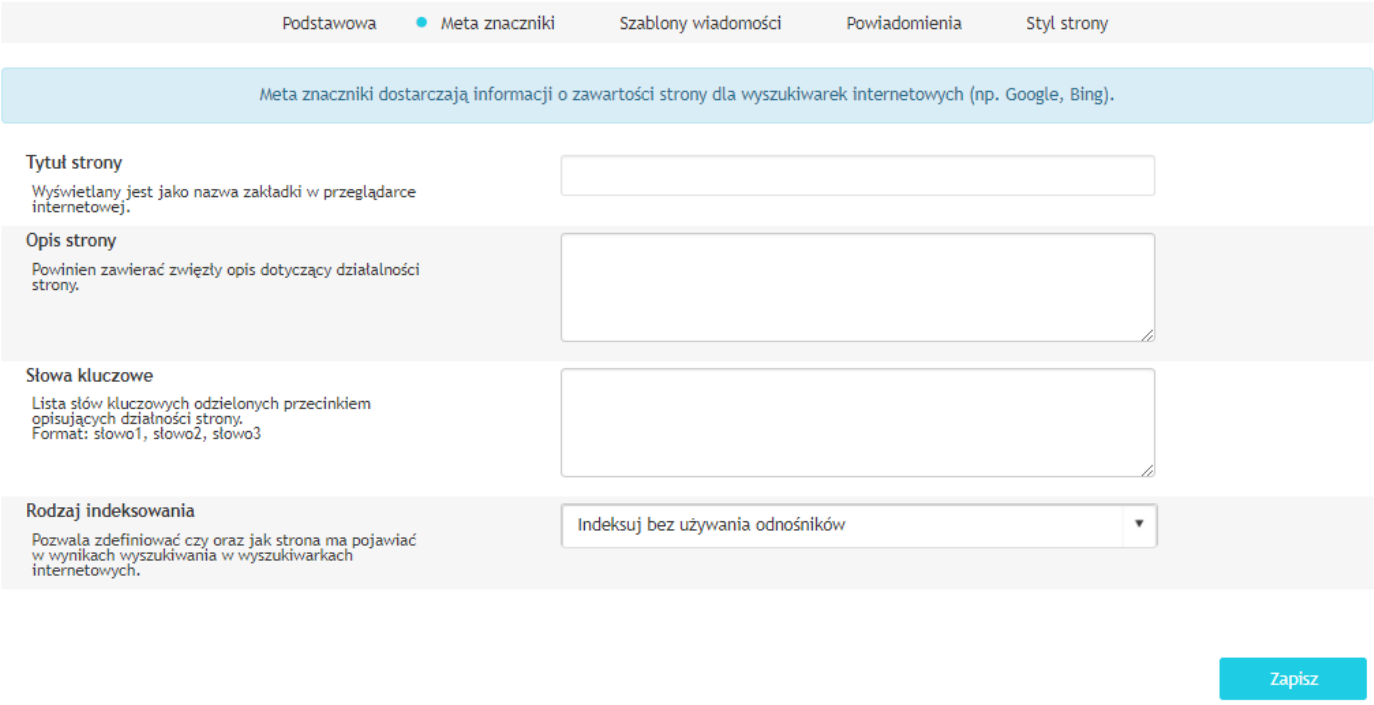
Rysunek 148: Konfiguracja integracji z systemem Informacje Medyczne



Rysunek 149:Edycja treści zgody na komunikację z systemem Informacje Medyczne dla wybranego świadczeniodawcy

8.3.9.2. Meta znaczniki

Meta znaczniki mają za zadanie dostarczyć informacje dla przeglądarki internetowej oraz wyszukiwarek internetowych takich jak np.: Google, Bing, Yahoo. Podstrona pozwala na zdefiniowanie tytułu strony, który będzie wyświetlany m.in. w nazwie zakładki przeglądarce internetowej. Ponadto możliwe jest zdefiniowanie opisu strony oraz słów kluczowych, które są brane pod uwagę w niektórych wyszukiwarkach internetowych. Możliwe jest również ustawienie, czy i jak strona ma zostać wyświetlona (indeksowana) w wyszukiwarkach internetowych.



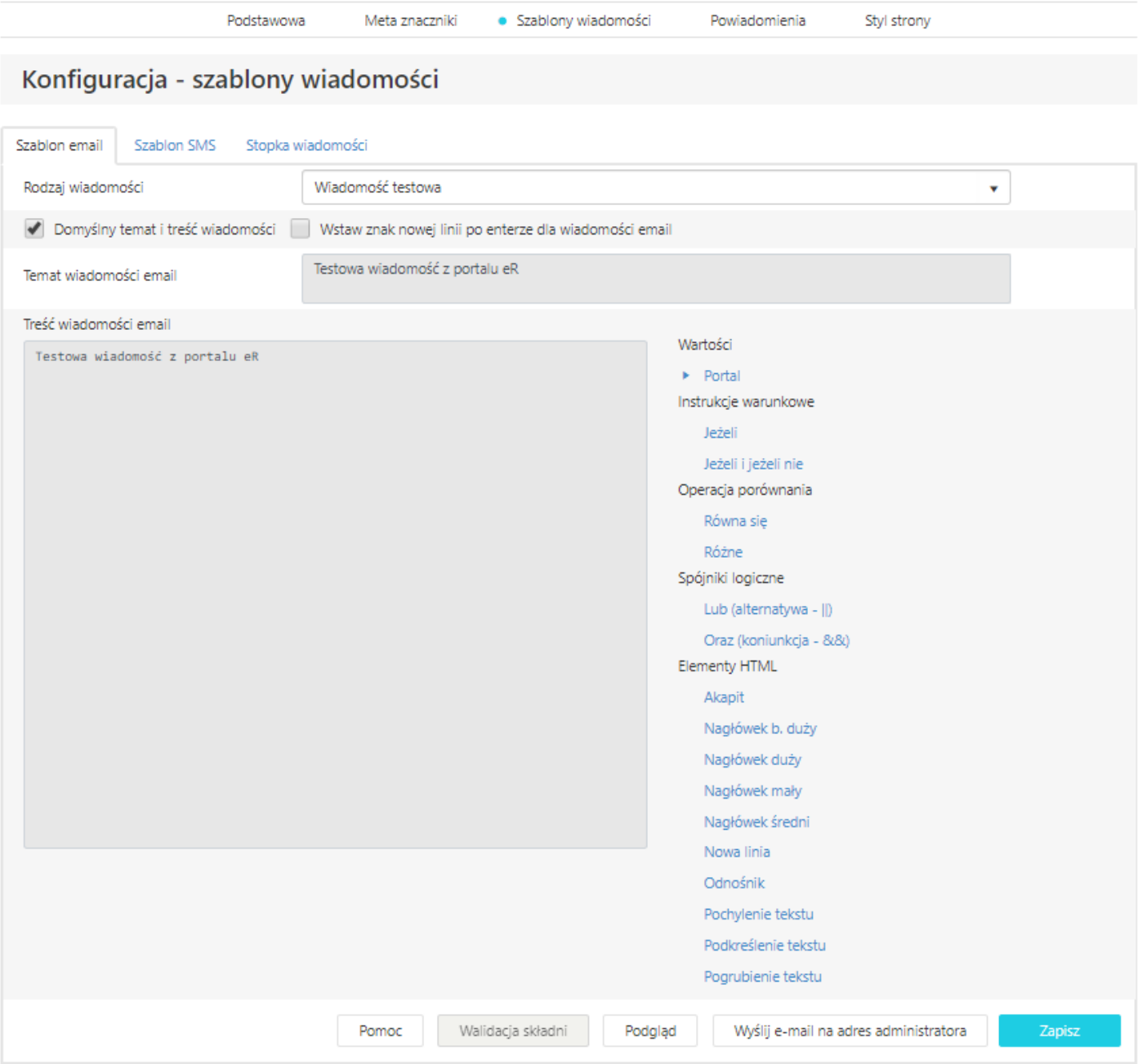
Rysunek 150: Podstrona konfiguracji meta znaczników

8.3.9.3. Szablony wiadomości

Kolejna z zakładek konfiguracji podstawowej umożliwia wprowadzanie zmian w treści wysyłanych do użytkownika wiadomości. Konfiguracja została podzielona w zależności od sposobu wysyłania wiadomości na zakładki „Szablon email” oraz „Szablon SMS”. Istnieje też możliwość zdefiniowania stopki wiadomości w zakładce „Stopka wiadomości”.

Rozwijana lista umieszczona na górze okien konfiguracyjnych szablonów, zawierająca spis wszystkich typów wiadomości wysyłanych przez Portal, daje sposobność wyboru wiadomości, która ma być obecnie edytowana. Odznaczenie opcji „Domyślny temat i treść wiadomości”/„Domyślna treść wiadomości” pozwala na samodzielne skonfigurowanie ich zawartości. Opcja „Wstaw znak nowej linii po enterze”, dostępna wyłącznie w szablonach e-mail, umożliwia automatyczne tworzenie znacznika HTML odpowiedzialnego za przejście tekstu do nowej linii. Należy zwrócić uwagę, że bez znacznika <br> w miejscu, po którym tekst ma znaleźć się w nowym wierszu, pozostanie on w jednej linii (pomimo tego, że na edytorze widoczny jest odstęp).

Dostępne pod polami edycji przyciski otwierają okno pomocy, podglądu wiadomości, umożliwiają zapis wprowadzonych zmian oraz wysłanie wiadomości na adres administratora. Przycisk „Walidacja składni” pozwala zweryfikować poprawność utworzonego szablonu oraz zlokalizować ewentualne błędy.



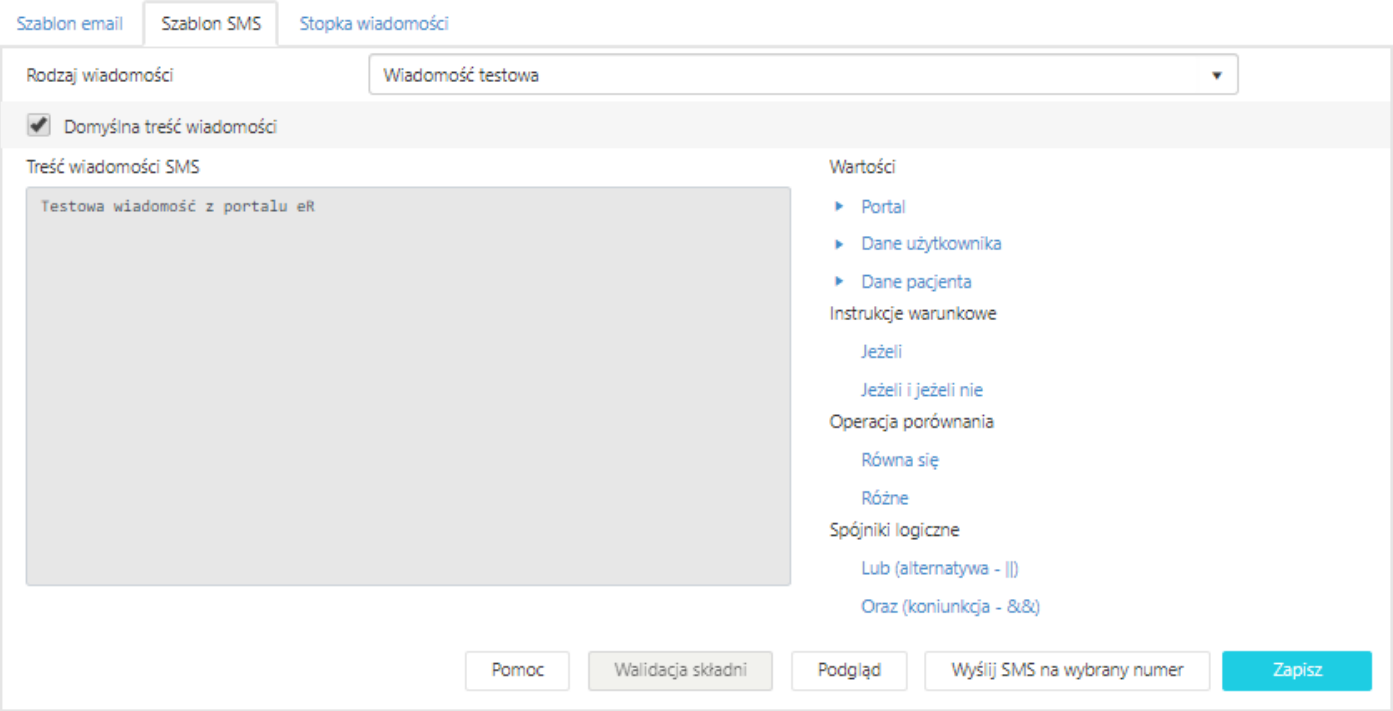
Rysunek 151: Szablon emaili – wiadomość testowa

Zadaniem parametrów umieszczonych po prawej stronie okna konfiguracji jest ułatwienie edycji wiadomości oraz umożliwienie wstawienia danych z eRejestracji. Zakładka „Wartości” daje sposobność wstawienia do treści emaila takich informacji jak adres email portalu, nazwa użytkownika wraz z jego danymi, szczegóły zarezerwowanych wizyt. Instrukcje warunkowe umożliwiają wyświetlenie tekstu w zależności od spełnienia danego warunku. Operacje porównania wstawiane są do wnętrza instrukcji warunkowej. Najprostszym przykładem instrukcji warunkowej jest sytuacja, w której sprawdza się płeć użytkownika i w zależności od niej w wiadomości wyświetla się zwrot „Pan” lub „Pani”. Instrukcje warunkowe mogą być rozbudowane dzięki możliwości zastosowania spójników logicznych „Lub” (alternatywy) i „Oraz” (koniunkcji). Bardziej szczegółowe wyjaśnienia oraz przykłady zawarte są w pomocy widocznej po naciśnięciu przycisku „Pomoc”.

Podczas tworzenia instrukcji warunkowej należy pamiętać, by zawarte w przyrównaniu wartości tekstowe były umieszczone w cudzysłowie. Przed słowem kluczowym *if*, *else* oraz *end* należy zamieścić znak *$*. Poniżej podano przykład ilustrujący te założenia.

```
$if({Nazwa użytkownika} == "Użytkownik")
    instrukcja pierwsza
$else
   instrukcja druga
$end
```

Zakładka „Elementy HTML” zawiera listę znaczników, które można wykorzystać przy konfiguracji szablonów emailowych. Służą one do formatowania tekstu wiadomości. Znacznik po naciśnięciu na jego nazwę zostanie wstawiony w miejscu, które jest zaznaczone kursorem w polu edycji. Istnieje również możliwość zaznaczenia pojedynczego wyrazu, zdania bądź całego bloku tekstu. Znacznik obejmie wtedy zaznaczony fragment.



Rysunek 152: Szablon SMS – wiadomość testowa

Szablon email | Szablon SMS | Stopka wiadomości

Wstaw znak nowej linii po enterze dla wiadomości email

Taka sama stopka email oraz SMS

Treść stopki dla email

```
<p>
Ta wiadomość została wygenerowana automatycznie. Prosimy na nią nie odpowiadać.
</p>
```

Treść stopki dla SMS

```
test
```

Wartości

- Portal

Instrukcje warunkowe

- Jeżeli
- Jeżeli i jeżeli nie

Operacja porównania

- Równa się
- Różne

Spójniki logiczne

- Lub (alternatywa - ||)
- Oraz (koniunkcja - &&)

Elementy HTML

- Akapit
- Nagłówek b. duży
- Nagłówek duży
- Nagłówek mały
- Nagłówek średni
- Nowa linia
- Odnośnik
- Pochylenie tekstu
- Podkreślenie tekstu
- Pogrubienie tekstu

Pomoc | Walidacja składni | Podgląd | Zapisz

Rysunek 153: Ustawienie treści stopki dla wiadomości email i SMS

Szablon email | Szablon SMS | Stopka wiadomości

Wstaw znak nowej linii po enterze dla wiadomości email

☑ Taka sama stopka email oraz SMS

Treść stopki dla email i SMS

Wartości

- Portal

Instrukcje warunkowe

- Jeżeli
- Jeżeli i jeżeli nie

Operacja porównania

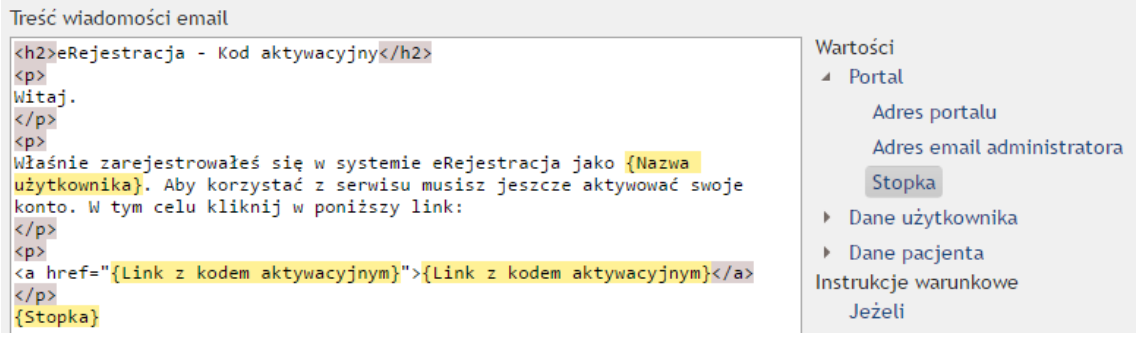
- Równa się
- Różne

Spójniki logiczne

- Lub (alternatywa - ||)
- Oraz (koniunkcja - &&)

Pomoc | Walidacja składni | Podgląd | Zapisz

Rysunek 154: Ustawienie takiej samej treści stopki dla wiadomości email i SMS

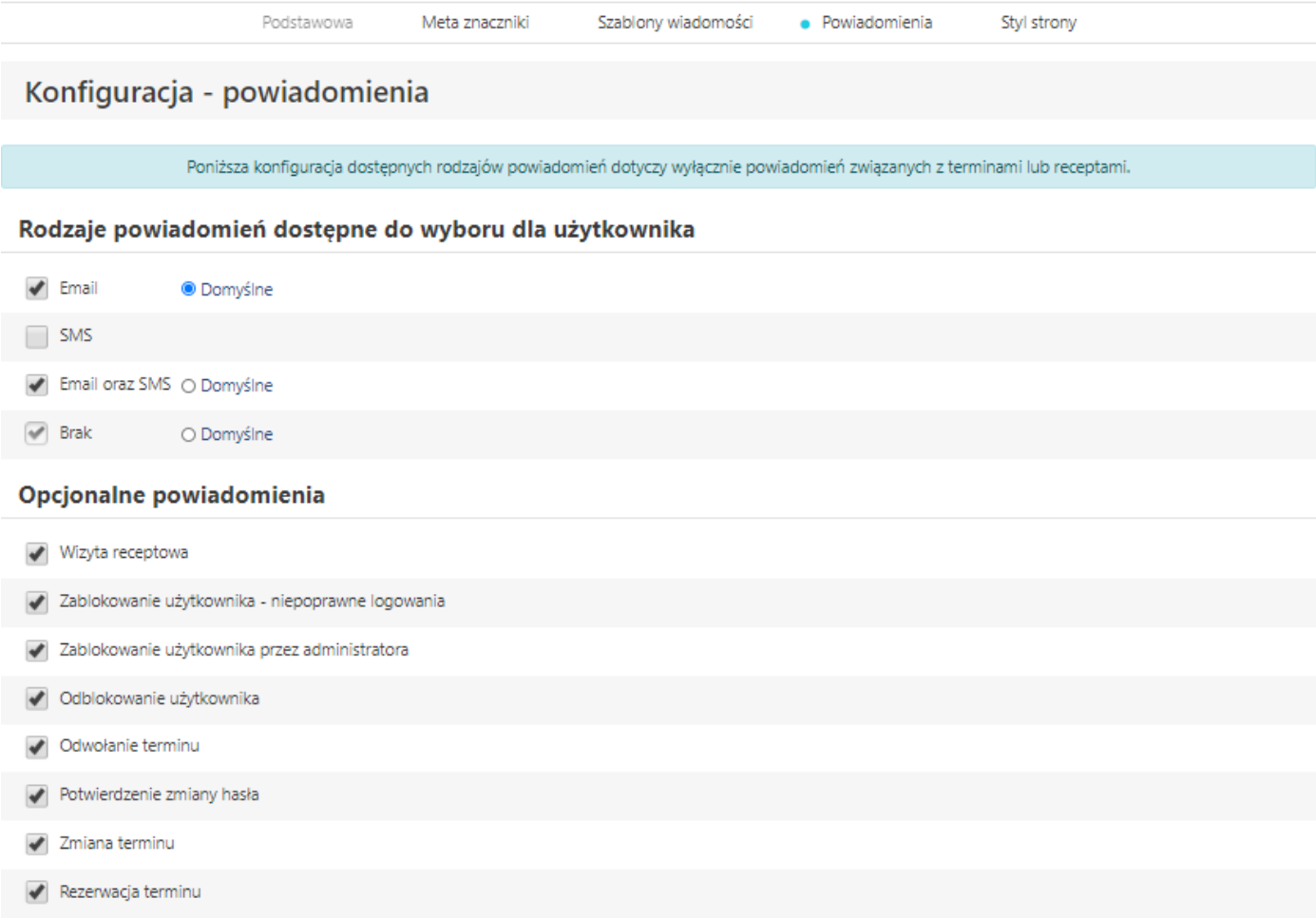


Rysunek 155: Wstawienie zawartości stopki do szablonu wiadomości

8.3.9.4. Powiadomienia

Następna zakładka konfiguracji podstawowej pozwala administratorowi na określenie, które z powiadomień mają być wysyłane do użytkownika.

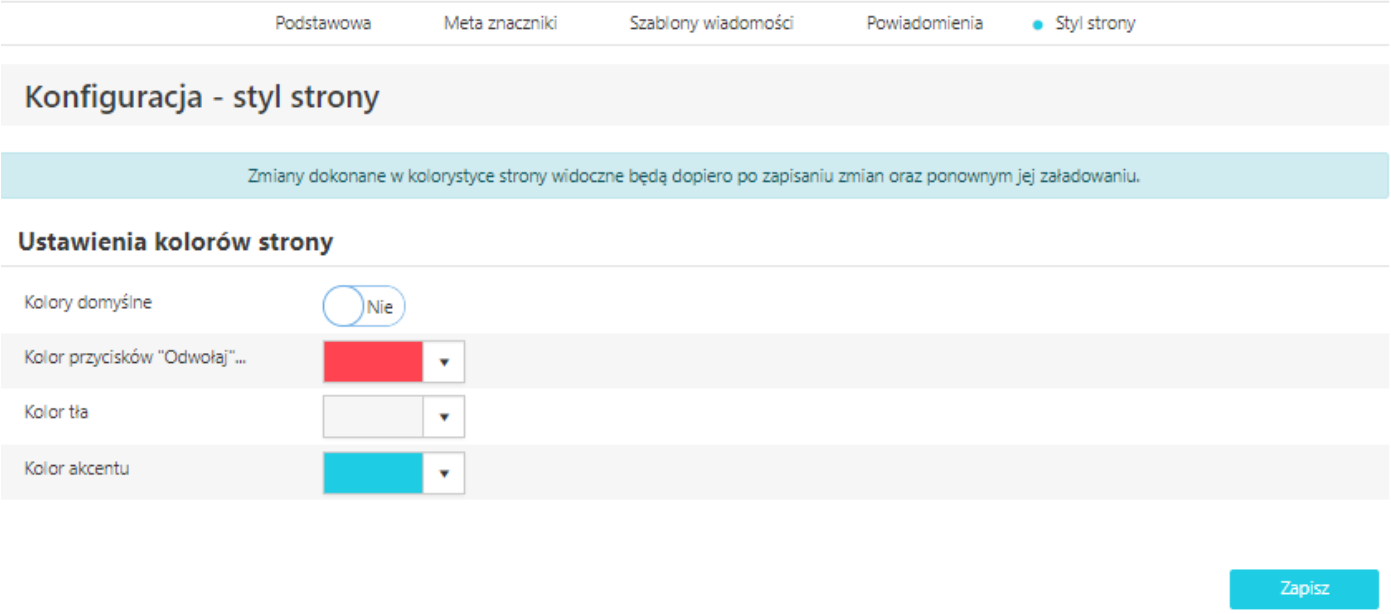
Poprzez ustawienia „Rodzaje powiadomień dostępne do wyboru dla użytkownika” administrator jest w stanie określić, która z metod jest dostępna, oraz wskazać domyślną opcję. Użytkownik dokonuje wyboru sposobu otrzymania wiadomości podczas rejestracji konta, w dalszym etapie może go zmienić poprzez edycję swoich danych. Lista wiadomości wysyłanych automatycznie do użytkownika znajduje się w menu *Konfiguracja -> Podstawowa -> Szablony wiadomości.* Wiadomości które nie są dostępne na liście szablonów SMS, a znajdują się na liście szablonów e-mail, zostaną wysłane pocztą elektroniczną pomimo wybrania opcji SMS.



Rysunek 156: Konfiguracja powiadomień

8.3.9.5. Styl strony

Ostatnia zakładka konfiguracji podstawowej pozwala administratorowi na określenie stylu strony. Standardowo ustawione są kolory domyślne. Można je dowolnie zmienić według upodobań.



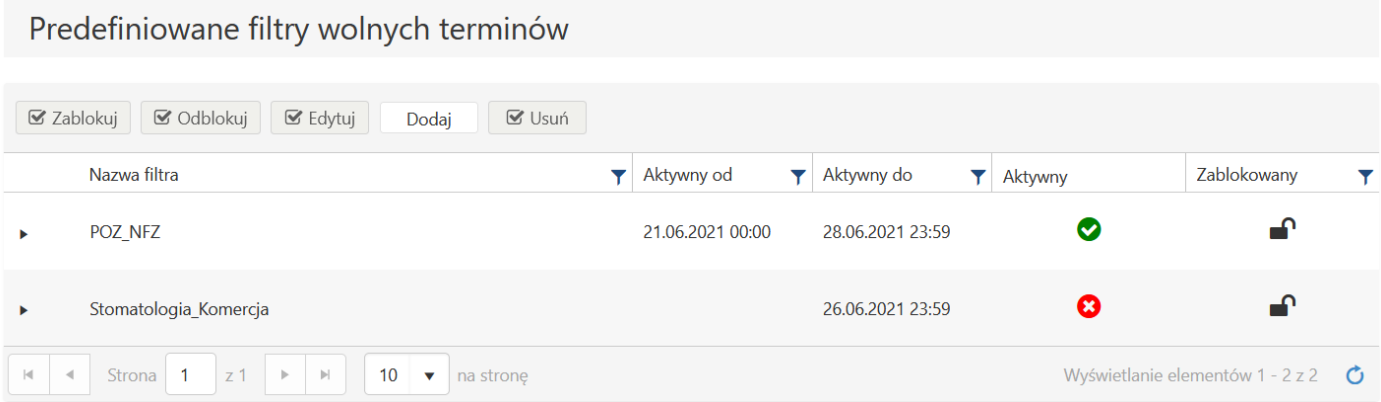
Rysunek 157: Konfiguracja stylu strony

8.3.9.6. Predefiniowane filtry wolnych terminów

Predefiniowane filtry wolnych terminów pozwalają administratorowi na tworzenie gotowych odnośników prowadzących do wolnych terminów z dowolnie skonfigurowanymi filtrami. Funkcjonalność pozwala na wygenerowanie odnośników, które mogą zostać użyte na stronach zewnętrznych np. do kampanii reklamowych. Wejścia na utworzone odnośniki są zliczane do statystyk, które można śledzić w Zarządzanie / Statystyki.

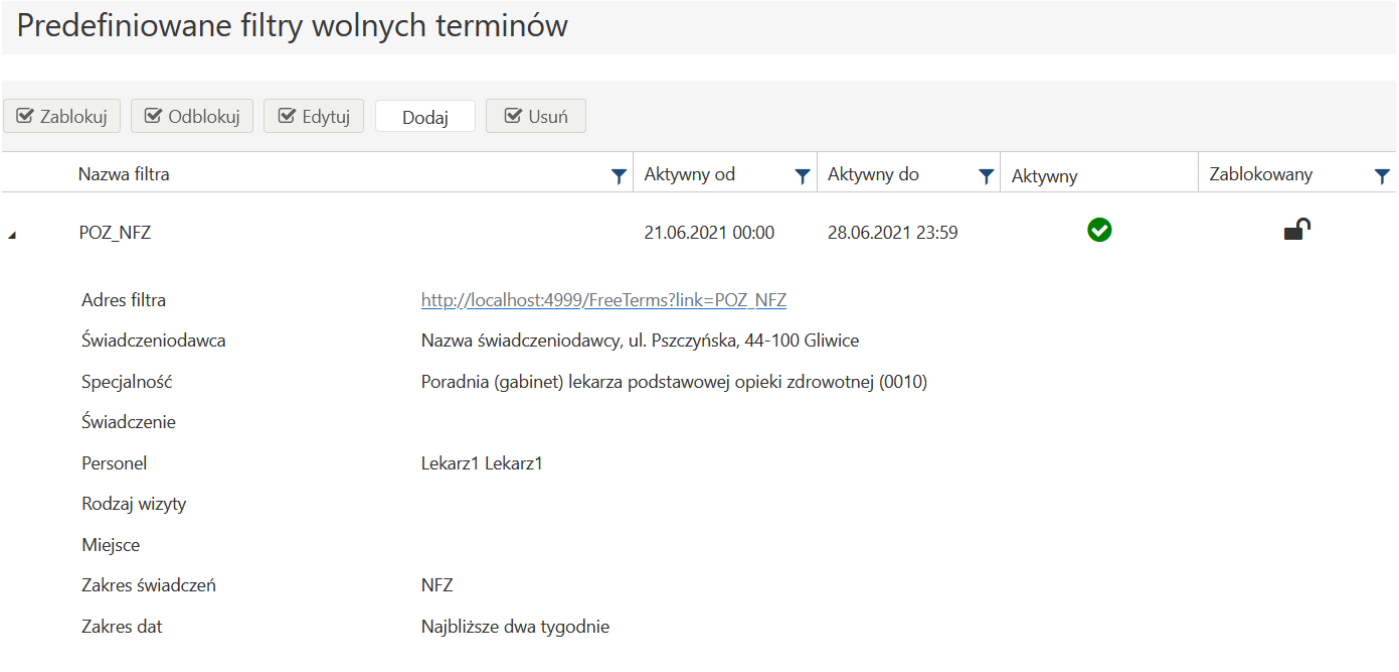
Tabela filtrów wolnych terminów składa się z kolumn:

- Nazwa filtry – unikalna nazwa, która zostanie zawarta w wygenerowanym odnośniku,
- Aktywny od – czas aktywności od kiedy odnośnik jest aktywny,
- Aktywy do – czas aktywności do kiedy odnośnik jest aktywny,
- Aktywny – informacja czy odnośnik jest aktywny na podstawie dat w kolumnach Aktywny od i Aktywny do,
- Zablokowany – informacja czy odnośnik jest zablokowany / odblokowany przez administratora.



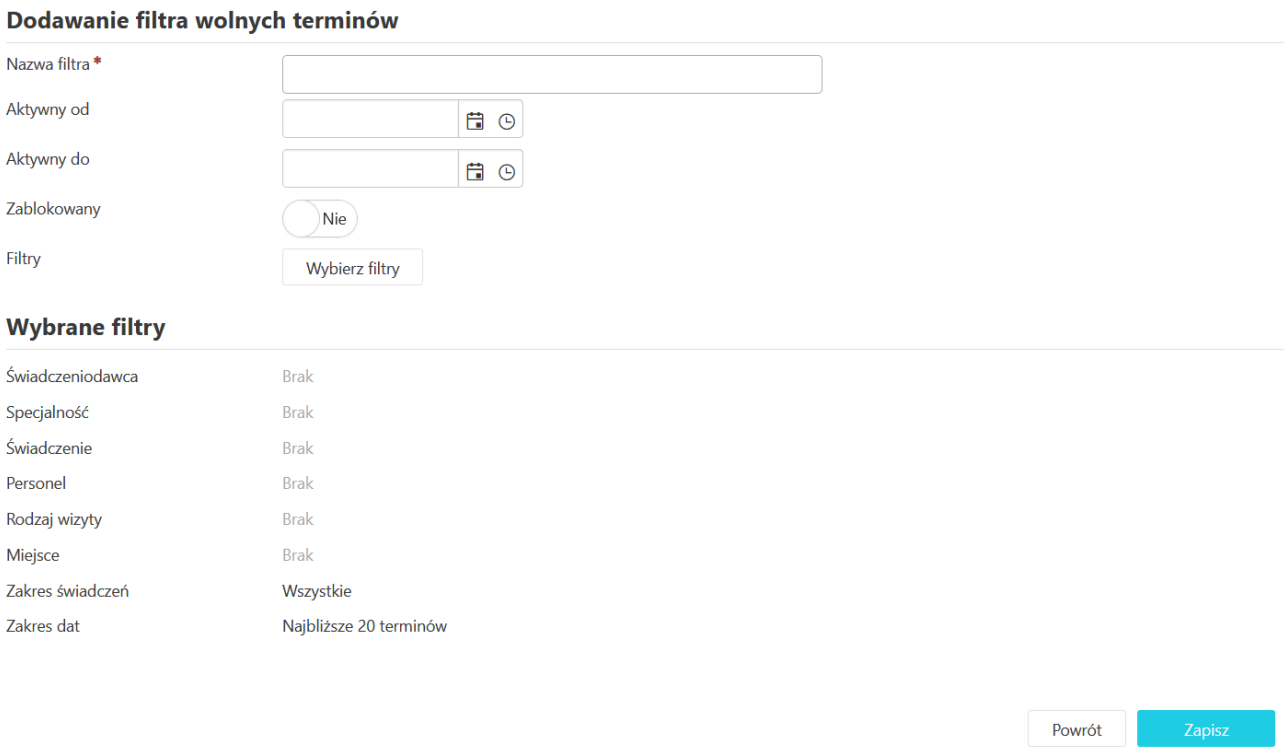
Rysunek 158: Predefiniowane filtry wolnych terminów

Pozycje w tabeli można rozwinąć za pomocą strzałki po lewej stronie nazwy filtra. W rozwiniętym obszarze znajdują się szczegóły ustawień filtrów oraz adres filtra, czyli odnośnik, który przenosi na stronę wolnych terminów z odpowiednio ustawionymi filtrami.



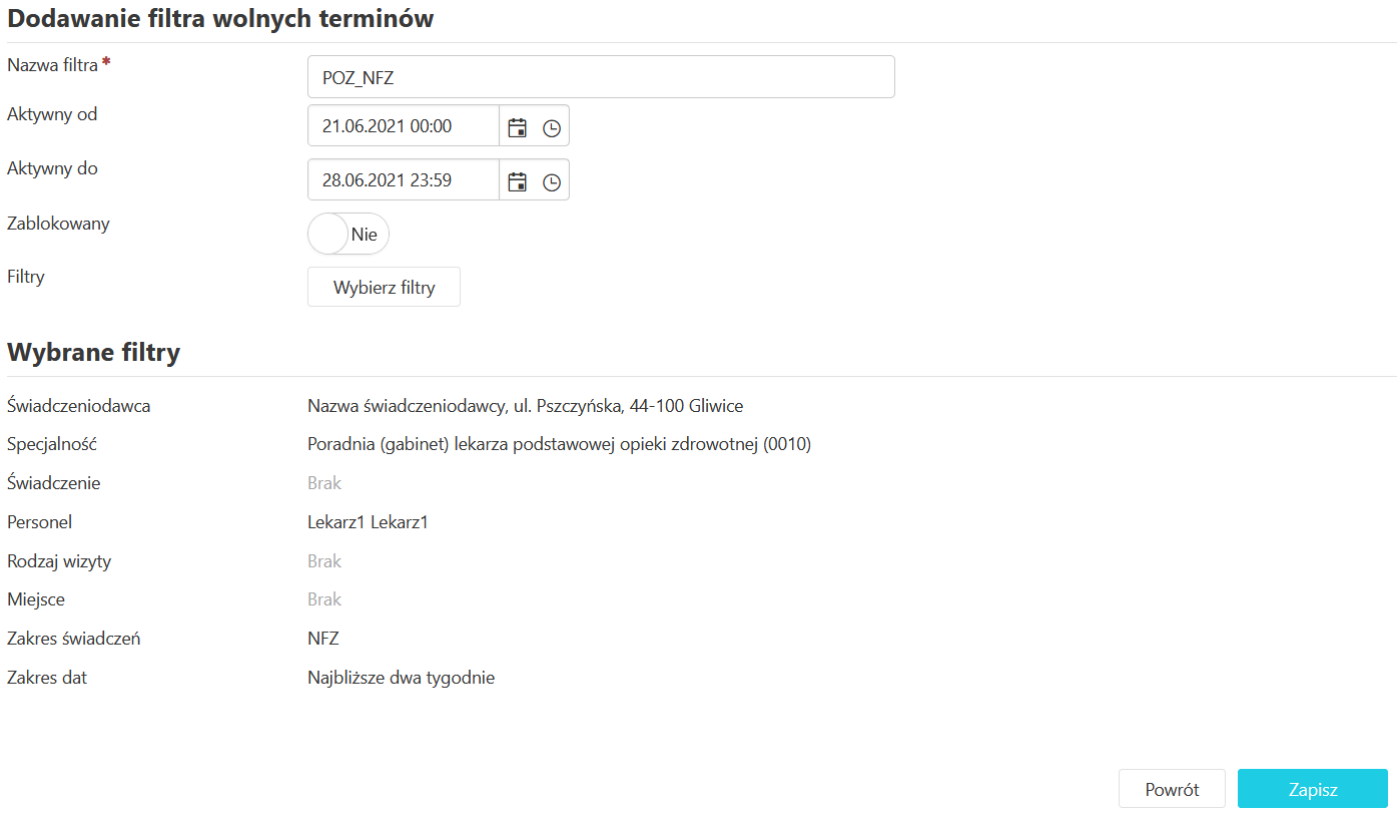
Rysunek 159: Rozwinięty predefiniowany filtr wolnych terminów

Dodanie nowej pozycji odbywa się po wybraniu przycisku „Dodaj”, gdzie administrator nadaje parametry tworzonej pozycji.



Rysunek 160: Dodawanie predefiniowanego filtru wolnych terminów

Ustawienia filtrów są wybierane po wybraniu przycisku „Wybierz filtry”, która przenosi administratora na zmodyfikowaną stronę wolnych terminów, na której może ustawić i sprawdzić filtry, a także zapisać ustawienia.



Rysunek 161: Dodawanie predefiniowanego filtru wolnych terminów – uzupełnione wartości

Administrator po zaznaczeniu dowolnej pozycji w tabeli ma możliwość zablokowania / odblokowania pozycji, a także jej edycji oraz usunięcia. Funkcjonalność edycji jest analogiczna jak dodawanie nowej pozycji.

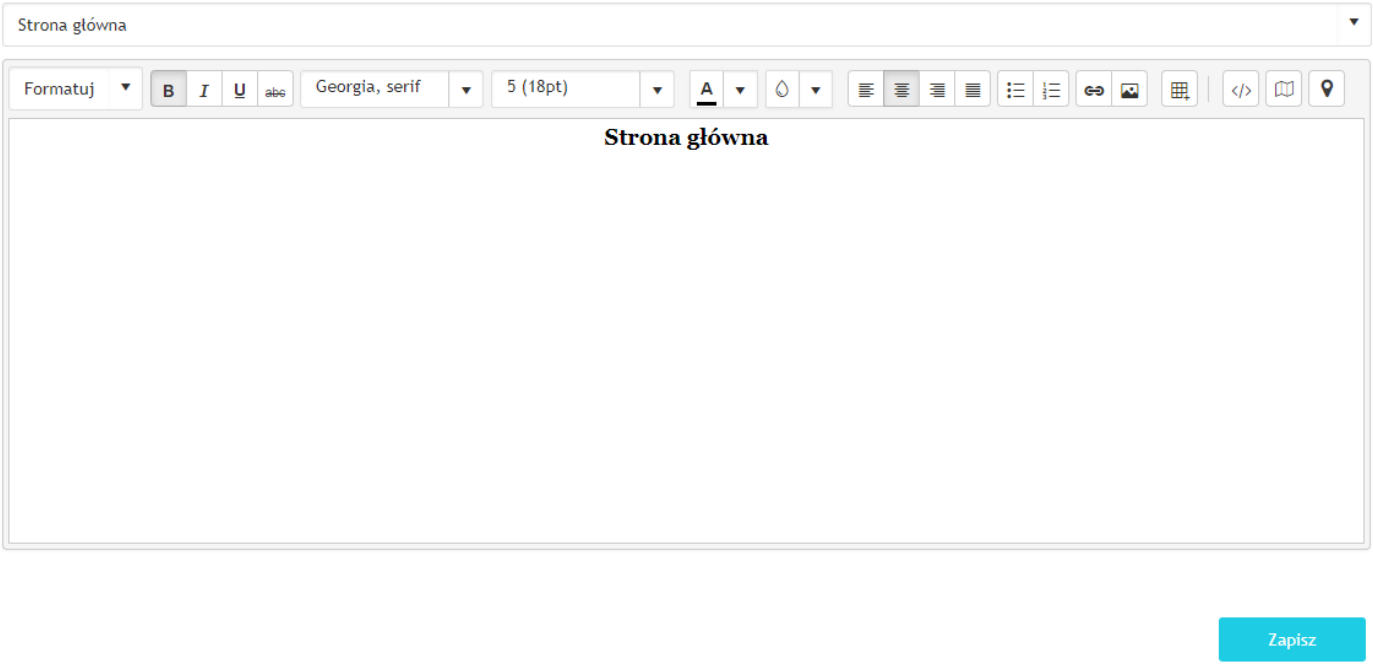
Jeśli użytkownik wejdzie na odnośnik, który jest nieaktywny lub zablokowany to wyświetli mu się komunikat informujący, że nie znaleziono podanej strony.

8.3.10. Zawartość strony

Niektóre treści widoczne na Portalu eRejestracja mogą być konfigurowane przez administratora. Funkcjonalność ta pozwala na dostosowanie strony do indywidualnych potrzeb. Wśród dostępnych opcji znajdują się narzędzia edycji tekstu, stylu, wstawiania obrazów, odnośników oraz tabel.

8.3.10.1. Treści

Treści zawartości strony dotyczą stałych elementów wyświetlanych w Portalu eRejestracja. Dostępne są opcje konfiguracji strony głównej, nagłówka strony, regulaminu strony oraz konfiguracji strony offline. Lista rozwijana widoczna poniżej podmenu aplikacji pozwala na wybór aktualnie edytowanej zawartości.



Rysunek 162: Konfiguracja treści portalu

Dane uzupełniane są poprzez edytor pola tekstowego oraz jego narzędzia. Każdy z przycisków posiada podpowiedź wyjaśniającą, jakie ma on zastosowanie. Jest ona wyświetlana po najechaniu na przycisk kursorem myszy. Wprowadzone zmiany można zobaczyć na podglądzie poprzez naciśnięcie ikony oka, znajdującej

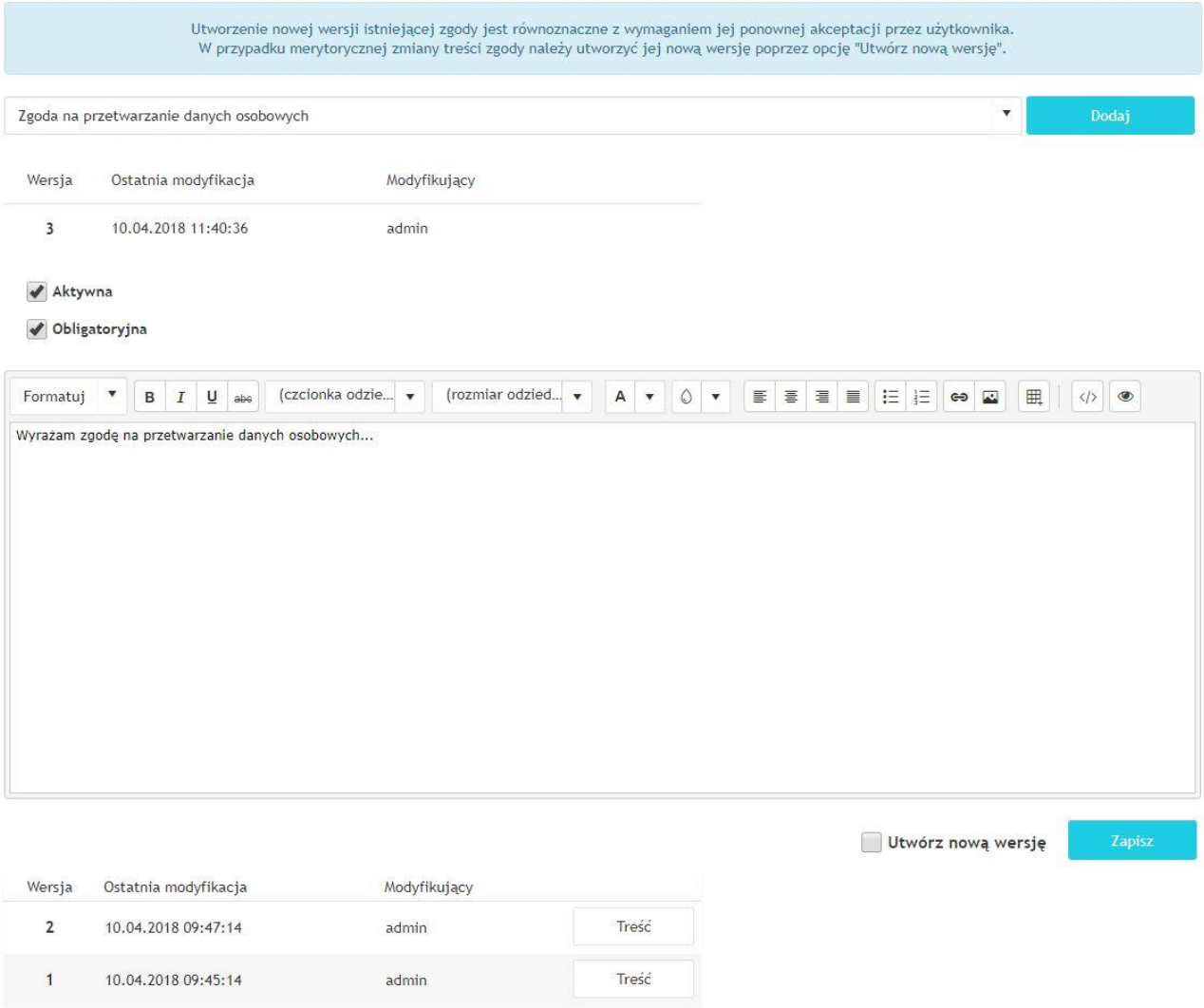
się na pasku narzędzi. Po uzupełnieniu danych należy je zapisać klikając przycisk „Zapisz”. Poniżej opisano każdą z dostępnych do konfiguracji opcji:

- Strona główna – Po poprawnym uzupełnieniu wprowadzone dane powinny pojawić się na stronie głównej Portalu;
- Nagłówek – Może to być logo lub dane adresowe placówki. Istnieje możliwość wygenerowania zawartości nagłówka do druku zarezerwowanej przez pacjenta wizyty. W tym celu należy przejść do ogólnych ustawień konfiguracyjnych (punkt *8.3.9.1.1. Konfiguracja ogólna*);
- Regulamin strony – Portal posiada możliwość stworzenia własnego regulaminu. Jest to dodatkowa funkcjonalność portalu eRejestracja która domyślnie jest wyłączona. W celu jej włączenia należy wprowadzić treść do edytora oraz zapisać zmiany. Dopóki w treści regulaminu będzie znajdował się jakikolwiek tekst, od każdego użytkownika będzie wymagane zaakceptowanie regulaminu podczas rejestracji nowego konta. Jeśli pole tekstowe jest puste, a mimo tego regulamin dalej wyświetla się na stronie rejestracji konta, należy otworzyć narzędzie podglądu HTML oraz usunąć z niego wszystko;
- Strona offline – Strona offline jest uruchamiana w przypadku braku połączenia z bazą danych eRejestracji. Dzieje się tak pod warunkiem, że w pliku appsettings.json, znajdującym się w katalogu Portalu, klucz „ShowOfflinePageWhenERDBIsOffline” ma ustawioną wartość „true”. Możliwe jest również wymuszenie wyświetlenia strony offline niezależnie od stanu połączenia z bazą danych eRejestracji, poprzez ustawienie wartości „true” w kluczu „ShowOfflinePageNow”. Poprawne działanie strony offline wymaga również odpowiedniej konfiguracji serwera WWW.

8.3.10.2. Zgody

Portal eRejestracja umożliwia konfigurację treści zgód, które mogą zostać zaakceptowane przez użytkowników. W bazie danych Portalu na stałe zdefiniowane są dwa rodzaje zgód oraz klauzula informacyjna, z domyślną treścią:

- *Zgoda na przetwarzanie danych osobowych*
- *Zgoda na przetwarzanie danych w celach marketingowych*
- *Klauzula informacyjna*



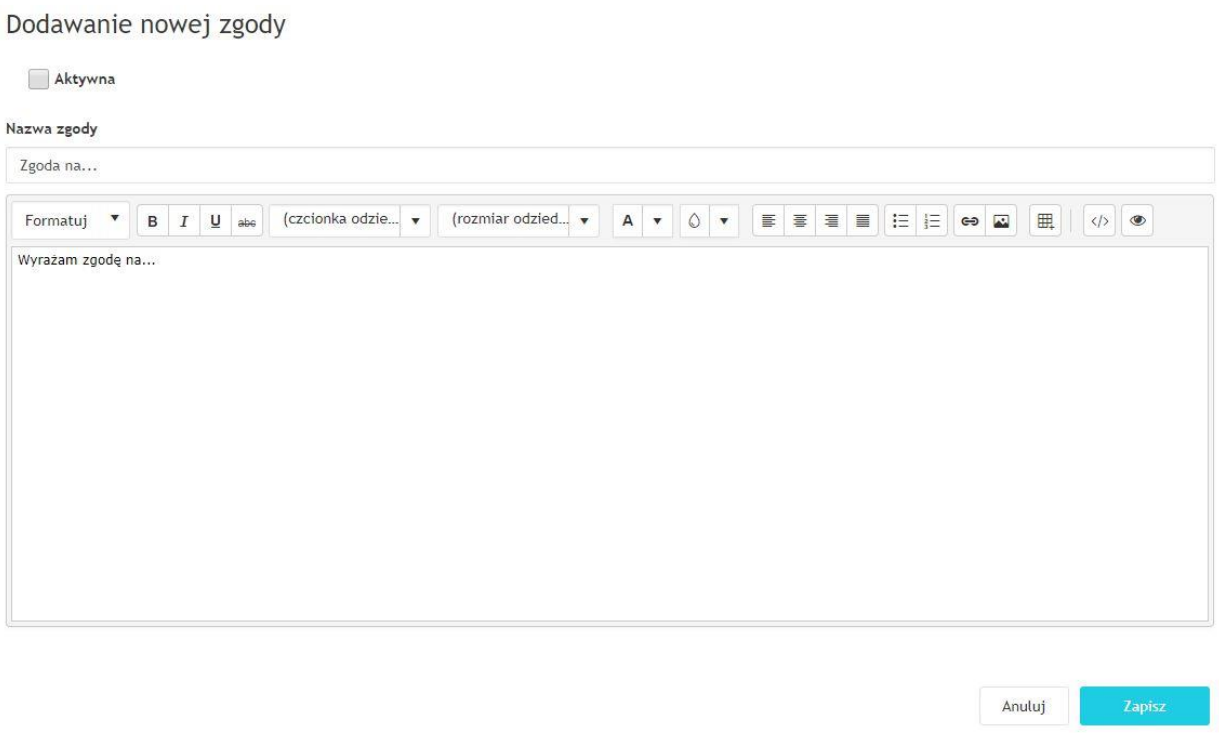
Rysunek 163: Konfiguracja zgód

Administrator ma możliwość edycji treści powyższych zgód oraz ustawienia opcji ich aktywności. Dodatkowo, zgoda na przetwarzanie danych osobowych posiada parametr określający jej obligatoryjność, czyli obowiązek zatwierdzenia przez użytkownika. Zgody, które zostały oznaczone jako aktywne, zostaną wyświetlone na formatce tworzenia konta użytkownika w postaci treści wraz z polem wyboru decydującym o akceptacji danej zgody przez rejestrującego się w Portalu użytkownika. Edycja danego typu zgody następuje po wybraniu odpowiedniej pozycji z listy rozwijanej znajdującej się na górze formatki.

Jeżeli zmiana treści zgody jest merytoryczna, należy przed zapisaniem zmian zaznaczyć opcję „Utwórz nową wersję”. Utworzenie nowej wersji istniejącej zgody jest równoznaczne z wymaganiem jej ponownej akceptacji przez użytkownika. Informacja o aktualnej wersji zgody umieszczona jest pod listą rozwijaną istniejących zgód. Oprócz numeru wersji wyświetlane są także data ostatniej modyfikacji oraz nazwa użytkownika administratora, który jako ostatni dokonał modyfikacji danej zgody. Lista wcześniejszych wersji treści edytowanej zgody jest wyświetlana pod edytorem tekstu.

Klauzula informacyjna działa podobnie do zgód z pewnym wyjątkiem jakim jest brak możliwości wyrażanie na nią zgody przez użytkowników. Służy ona jedynie do informowania użytkowników m.in. o swoich danych kontaktowych, celu przetwarzania, odbiorcach danych osobowych itd. na podstronie tworzenia konta. Podobnie jak zgody jest ona wersjonowana.

W Portalu eRejestracja możliwe jest także definiowanie własnych zgód. Kliknięcie przycisku „Dodaj”, znajdującego się obok listy rozwijanej istniejących zgód, wyświetla formatkę tworzenia nowej zgody.

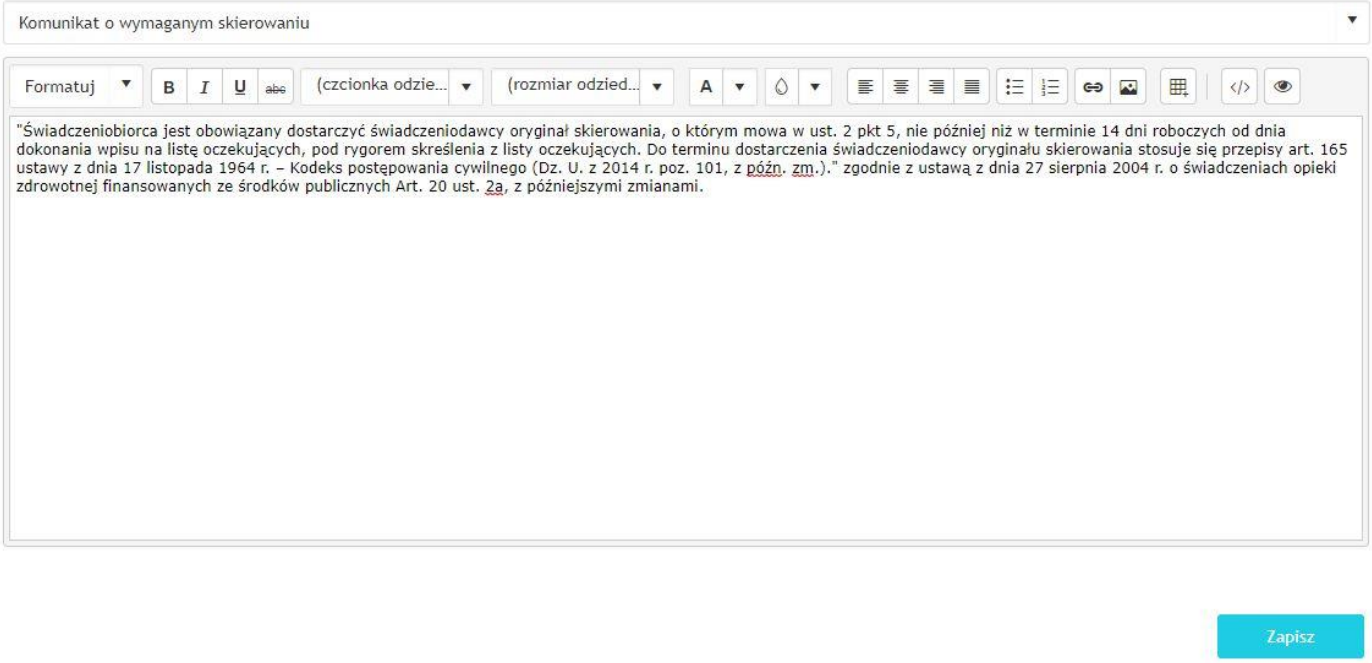


Rysunek 164: Dodawanie nowej zgody

Uwaga: Domyślne treści zdefiniowanych zgód są jedynie propozycją. Obowiązkiem administratora danych osobowych jest samodzielne sformułowanie treści zgód zgodnie z wymogami RODO - w sposób prosty, zrozumiały, ze wskazaniem potencjalnego ryzyka oraz określeniem celów, dla których dane są zbierane.

8.3.10.3. Komunikaty

Niektóre komunikaty, które wyświetlane są dla użytkownika Portalu eRejestracja, mogą być konfigurowane przed administratora. Zakres edycji tekstu określają dostępne nad polem tekstowym narzędzia. Wprowadzone zmiany można zobaczyć na podglądzie poprzez naciśnięcie ikony oka znajdującej się na pasku narzędzi. Po uzupełnieniu danych należy je zapisać klikając przycisk „Zapisz”.



Rysunek 165: Konfiguracja komunikatów

Dostępne do edycji komunikaty znajdują się na rozwijanej liście widocznej poniżej podmenu aplikacji. Poniżej opisano każdy z nich wraz z informacją, w którym momencie są one wyświetlane użytkownikowi:

- Komunikat o wymaganym skierowaniu – komunikat wyświetlany podczas rezerwacji wizyty wymagającej skierowania. Tekst opisuje pole zaznaczenia dotyczące zaświadczenia o posiadaniu przez pacjenta skierowania dla danej specjalności;
- Komunikat o wymaganym skierowaniu (offline) – komunikat wyświetlany podczas rezerwacji wizyty wymagającej skierowania w trybie offline. Tekst opisuje pole zaznaczenia dotyczące zaświadczenia o posiadaniu przez pacjenta skierowania dla danej specjalności;
- Komunikat o specjalności przeznaczonej dla dorosłych – komunikat wyświetlany podczas rezerwacji wizyty dla przypadku, gdy osoba niepełnoletnia próbuje zarezerwować wizytę w specjalności przeznaczonej dla dorosłych;
- Komunikat o specjalności przeznaczonej dla dzieci – komunikat wyświetlany podczas rezerwacji wizyty dla przypadku, gdy osoba pełnoletnia próbuje zarezerwować wizytę w specjalności przeznaczonej dla dzieci.

8.3.10.4. Newsy

Newsy są wiadomościami wyświetlanymi na stronie głównej portalu. Funkcjonalność pozwala na zarządzanie kategoriami, czasem wyświetlania, wyglądem oraz istotnością zamieszczonych informacji. Konfiguracja dostępna jest po wybraniu z menu opcji Zawartość strony/Newsy.

Rysunek 166: Domyślna strona konfiguracji newsów

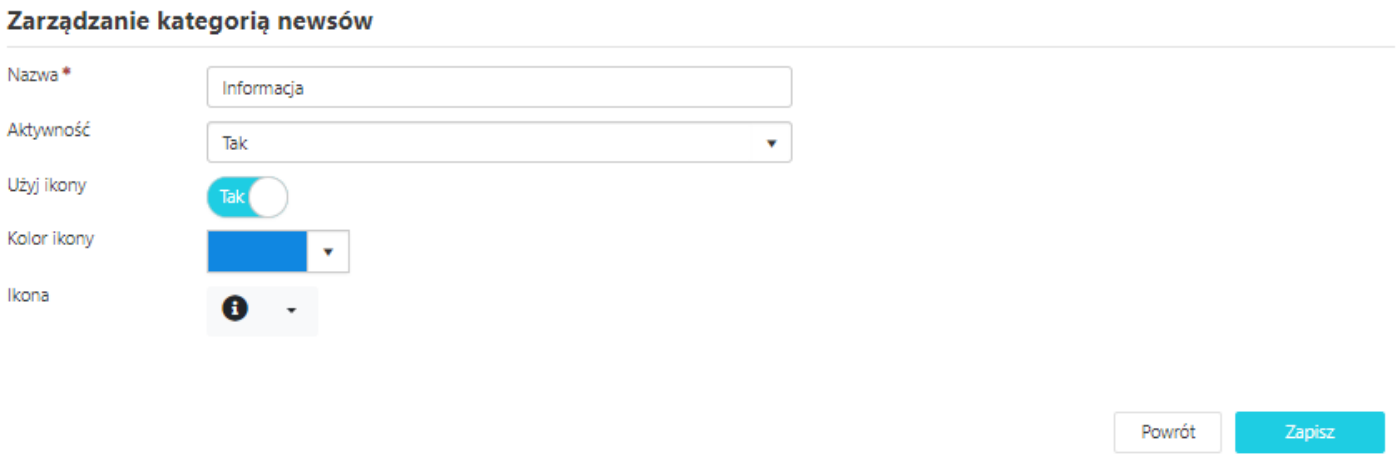
Strona tworzenia newsów posiada trzy przyciski umożliwiające zarządzanie wiadomościami. Poniżej opisano każdy z nich:

- Edytuj - pozwala edytować utworzony news,
- Usuń - pozwala usunąć zaznaczony news,
- Dodaj - pozwala utworzyć nowy news.

Dodatkowo jest również zakładka „Kategorie newsów”. Kategorie newsów pomagają usystematyzować wiadomości oraz określić ich stopień ważności. Utworzenie nowej kategorii należy rozpocząć od wejścia w „Kategorie newsów”, a następnie nacisnąć ikonę dodawania nowej kategorii „Dodaj”.

Rysunek 167: Kategorie newsów

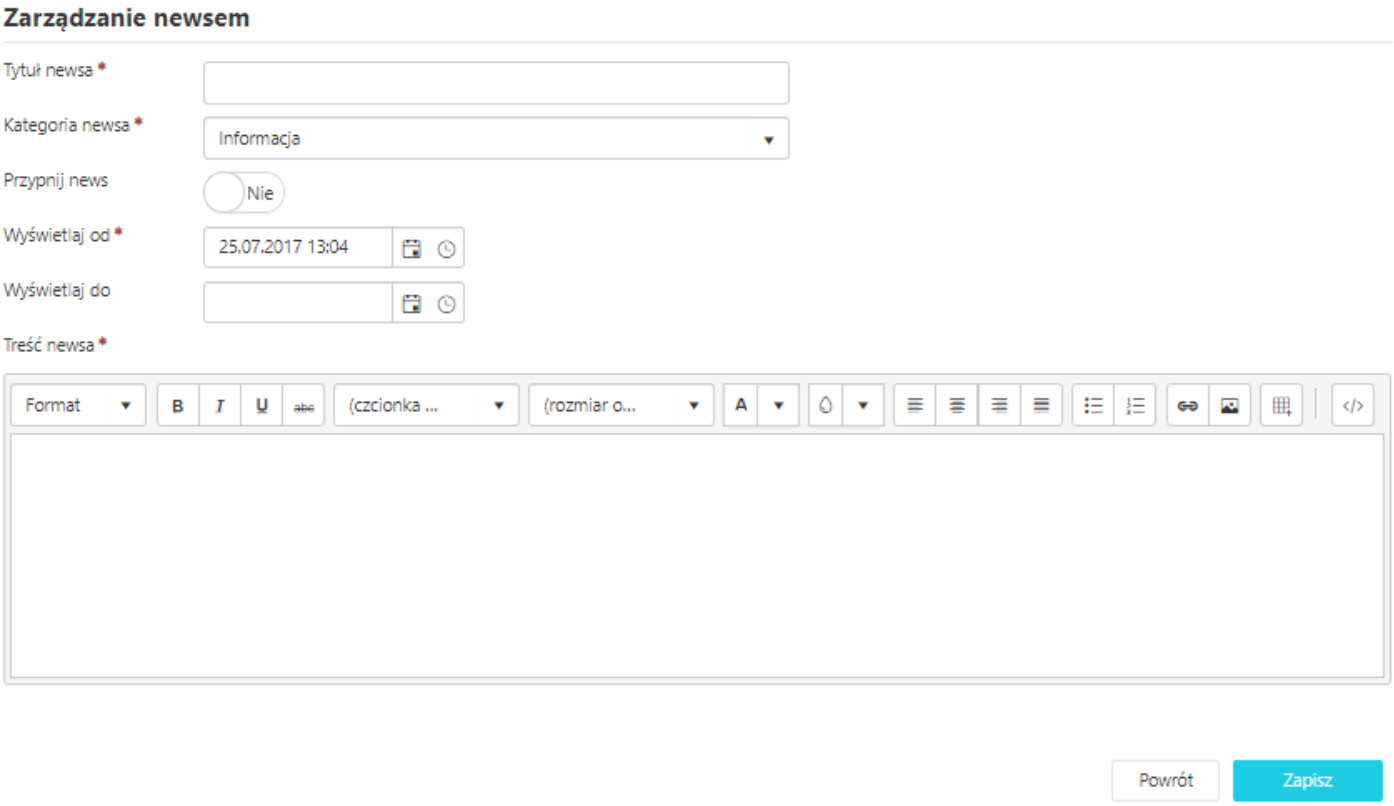
Strona tworzenia nowej kategorii wymaga podania nazwy oraz koloru ikony, jeśli występuje. Lista „Aktywność” pozwala określić, czy wiadomości danej kategorii będą wyświetlane. W przypadku dezaktywacji, wszystkie newsy należące do danej kategorii przestaną być wyświetlane na stronie głównej portalu. Istnieje możliwość wgrania własnej ikony lub skorzystania z gotowych wzorów. Ikony mogą pomóc w przyciągnięciu uwagi użytkownika, bądź określić stopień ważności zamieszczonych informacji.



Rysunek 168: Tworzenie nowej kategorii newsów

Edycja kategorii newsów może być dokonana po zaznaczeniu zmienianej kategorii oraz naciśnięciu ikony edycji. Strona edycji wygląda tak samo jak strona tworzenia nowej grupy wiadomości. Usunięcia niechcianej kategorii dokonuje się za pomocą przycisku „Usuń”.

Po utworzeniu przynajmniej jednej kategorii newsów można tworzyć nowe wiadomości. W celu dodania newsa należy nacisnąć przycisk „Dodaj”. Po dokonaniu tej czynności wyświetli się strona tworzenia wiadomości. Osoba tworząca news powinna wybrać jego kategorię, datę wyświetlania, tytuł oraz treść. Zawartość tekstu może być formatowana w dowolny sposób dzięki możliwości wykorzystania edytora HTML . Edytor tekstowy umożliwia również prostą edycję tekstu za pomocą odpowiednio opisanych kontrolek oraz list. Włączenie opcji przypięcia newsa powoduje umiejscowienie wiadomości na samej górze bez względu na czas jej powstania. W ten sposób można dodatkowo wyróżnić istotne informacje lub ogłoszenia.



Rysunek 169: Tworzenie newsa

8.3.10.5. Elementy menu

Poza domyślnymi elementami menu dostępnymi na portalu, możliwe jest utworzenie własnych elementów. Mogą być to dodatkowe strony portalu (zawierające na przykład informacje odnośnie godzin otwarcia placówki, mapy dojazdu czy innych uzupełniających informacji) lub odnośniki do zewnętrznych stron internetowych. Zarządzanie elementami menu dostępne jest w: Zawartość strony/Elementy menu.

Tabela zawiera utworzone przez administratora elementy wraz z informacją o kolejności wyświetlania, typie, nazwie, widoczności dla różnych typów użytkowników, miejsca wyświetlania oraz dacie ostatniej aktualizacji. Edycja utworzonego elementu możliwa jest poprzez kliknięcie na wybrany wiersz tabeli i naciśnięcie przycisku „Edytuj”, usunięcie za pomocą „Usuń”, natomiast kolejność wyświetlania linków zmieniana jest poprzez przyciski „Zmień kolejność do góry” i „Zmień kolejność w dół”.

Edytuj | Usuń | Zmień kolejność do góry | Zmień kolejność w dół | Dodaj

Kolejność	Typ	Nazwa	Widoczna dla	Wyświetl	Aktualizacja
1	Strona	Kontakt	Wszyscy	W górnym menu, pod stopką strony	26.07.2017 08:26
2	Odnośnik	Odnośnik	Zalogowani	W górnym menu, pod stopką strony	26.07.2017 08:54
3	Strona	Komunikaty	Wszyscy	W górnym menu, pod stopką strony	26.07.2017 11:34
4	Strona	Info	Wszyscy	W górnym menu, pod stopką strony	26.07.2017 11:34

Strona 1 z 1 | 5 na stronę | Wyświetlanie elementów 1 - 4 z 4

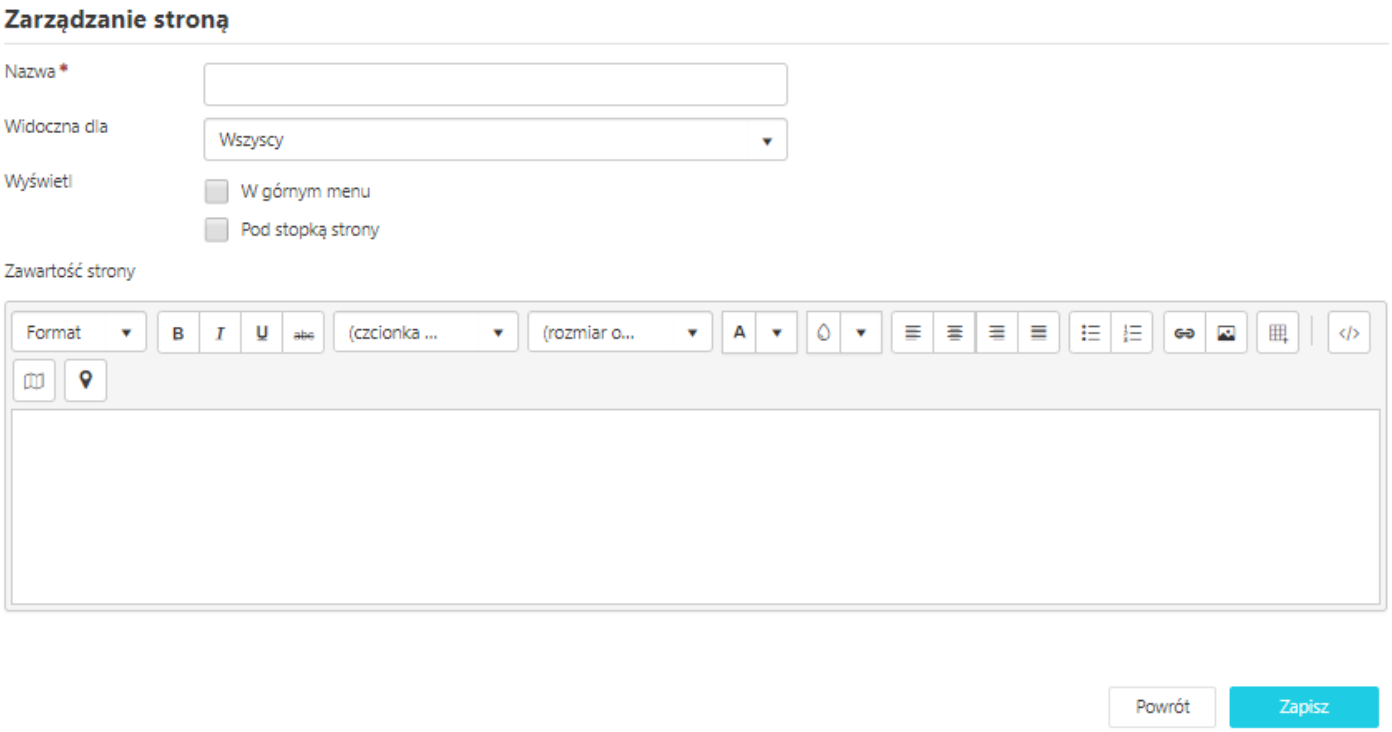
Rysunek 170: Zarządzanie elementami menu

Utworzenie nowego elementu menu następuje po naciśnięciu przycisku „Dodaj” dostępnego w górnym poziomym menu portalu. Należy uzupełnić wyświetlony formularz oraz ustawić poszczególne opcje zgodnie z wymaganiami. Nowy element może być wyświetlony dla każdego użytkownika, istnieje jednak możliwość wprowadzenia ograniczeń. Pewne z nich mogą być na przykład dostępne jedynie dla administratorów albo użytkowników zalogowanych.

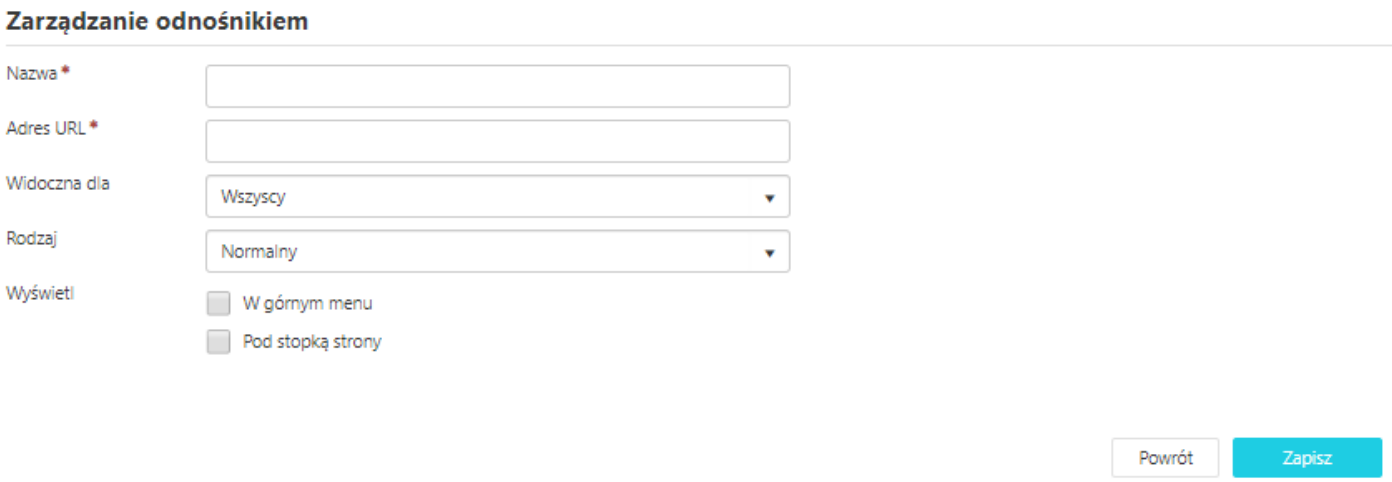
Dostępne są dwa typy elementów menu: strony oraz odnośniki do zewnętrznych witryn internetowych. W zawartości strony mogą znajdować się bloki tekstowe, obrazki oraz linki do różnych witryn. Odnośniki do zewnętrznych stron mogą być wyświetlane na trzy sposoby: na tej samej karcie („Normalny”), na nowej karcie lub w ramce (wewnątrz portalu).

Parametr „Wyświetl” wymaga określenia, gdzie utworzone elementy menu mają być widoczne. Wśród nich dostępne są następujące opcje:

- W górnym menu – linki zostaną wyświetlone w poziomym menu (pod menu głównym) znajdującym się w górnej części portalu,
- Pod stopką strony – linki zostaną wyświetlone poziomo pod stopką strony.



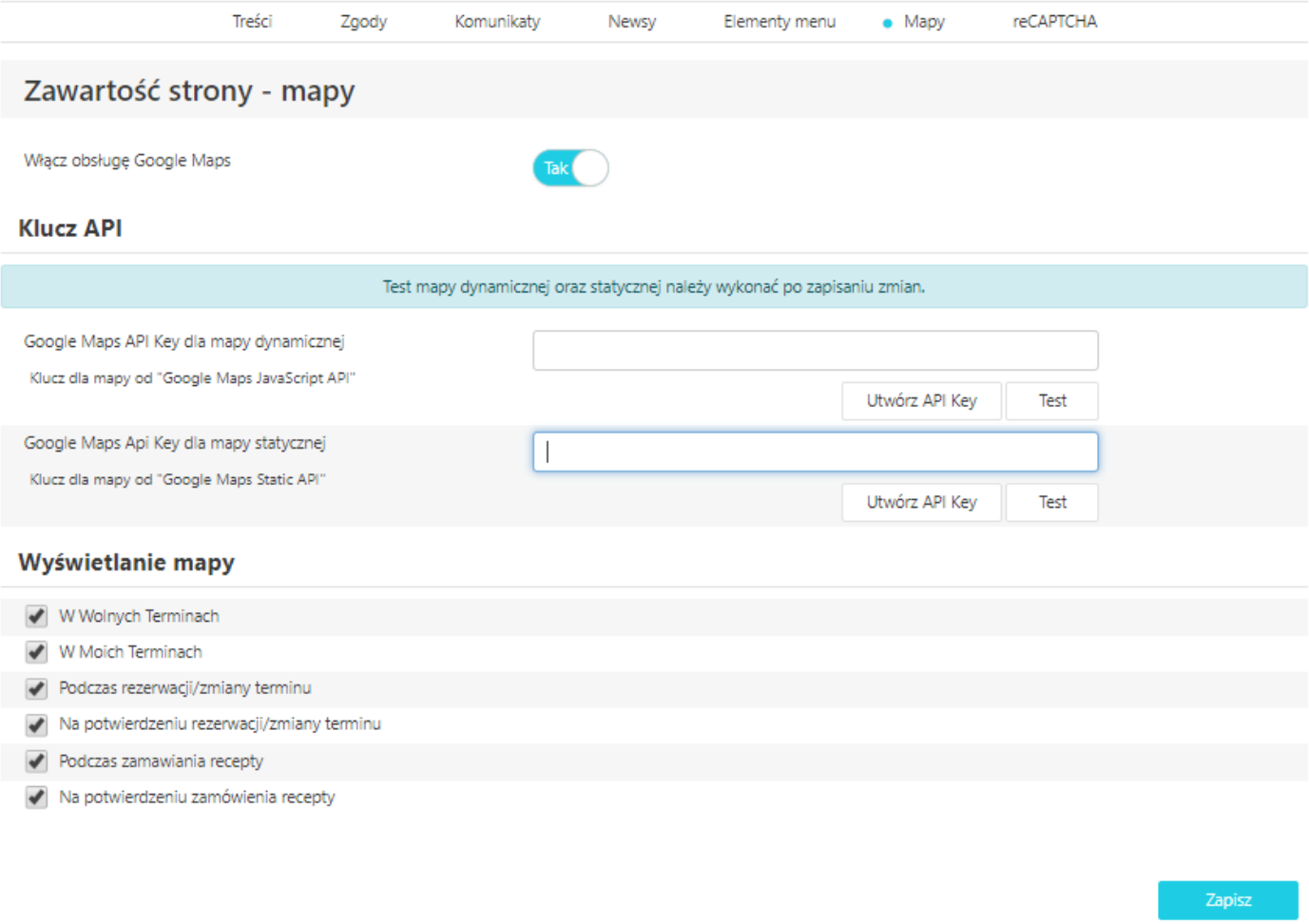
Rysunek 171: Tworzenie nowego elementu menu – strona



Rysunek 172: Tworzenie nowego elementu menu – odnośnik

8.3.10.6. Mapy

Konfiguracja map pozwala na włączenie/wyłączenie obsługi map w portalu. Przy włączonej obsłudze map istnieje możliwość wygenerowania nowych kluczy dla Google API, podgląd map oraz wskazanie, w których miejscach portalu mają zostać wyświetlone mapy.



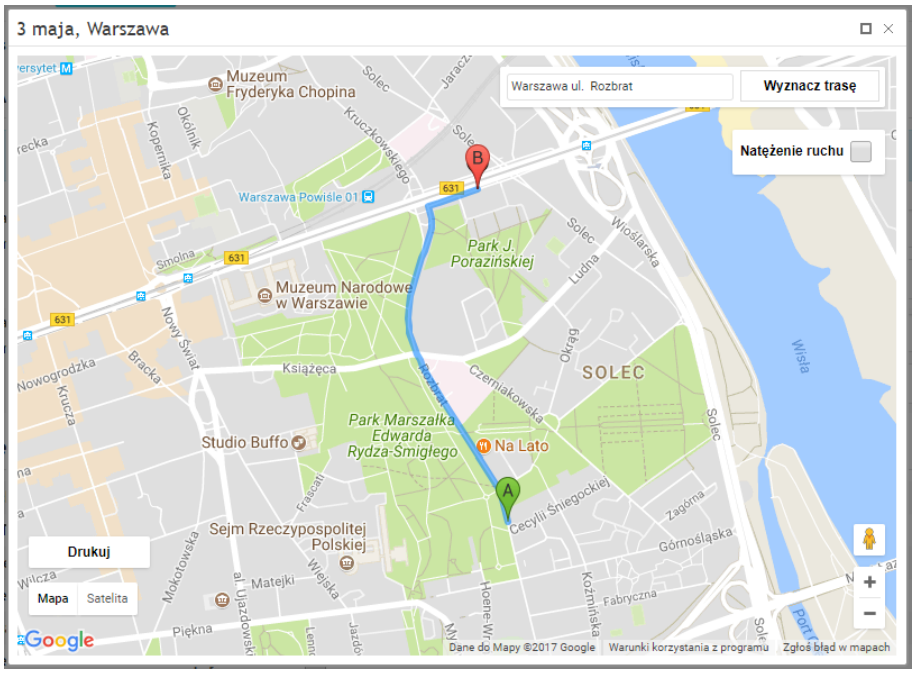
Rysunek 173: Konfiguracja map

Portal eRejestracja posiada gotowe klucze dla Google Maps JavaScript API (mapy dynamiczne) oraz Google Maps Static API (mapy statyczne). Istnieje jednak możliwość samodzielnego wygenerowania kluczy. Po naciśnięciu przycisku „Utwórz API Key” otworzona zostanie strona tworzenia kluczy. Należy upewnić, się, że utworzony projekt, dla którego wygenerowany został klucz API mapy dynamicznej, posiada włączone usługi: *Maps JavaScript API, Geocoding API* oraz *Directions API*. Po wprowadzeniu zmian przez firmę Google do sposobu korzystania z usługi wyświetlania map, możliwe jest także użycie tego samego klucza API dla map statycznych, po włączeniu usługi *Maps Static API*. Włączenie wybranych usług możliwe jest na stronie https://console.developers.google.com po zalogowaniu się na konto Google.

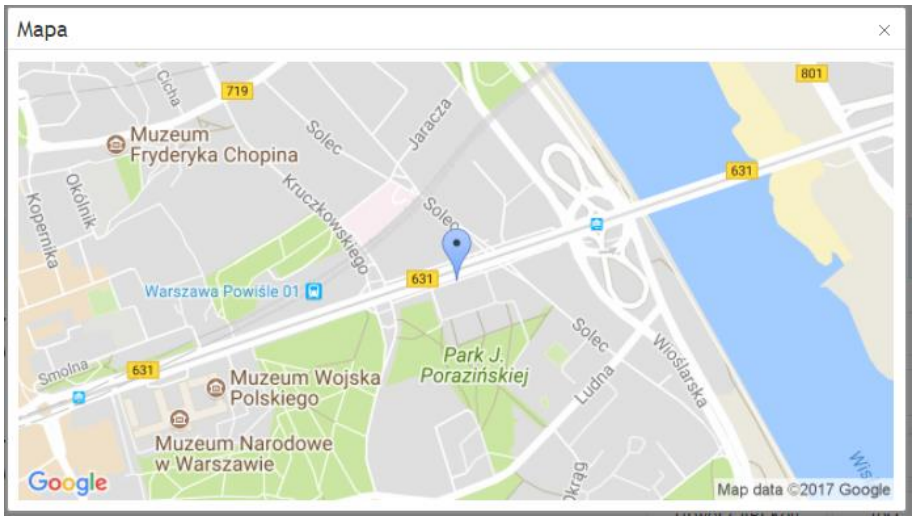
Przycisk „Test” pozwala na wyświetlenie okna zawierającego mapę dynamiczną i statyczną. Mapa dynamiczna pozwala na wyznaczanie trasy pomiędzy punktem A i B, przy czym jednym z punktów jest adres placówki. Mapa statyczna zaznacza tylko lokalizację placówki.

Sekcja „Wyświetlanie mapy” pozwala na wybór miejsc na portalu, w których wyświetlone mają zostać przyciski otwierające okno mapy.

Uwaga: Widoczność przycisku otwierającego okno mapy zależna jest także od ustawień w edycji specjalności (*8.3.11.1. Specjalności*). Dla wybranej specjalności można całkowicie włączyć lub wyłączyć opcję wyświetlania mapy.



Rysunek 174: Konfiguracja map – podgląd wyznaczania trasy (mapa dynamiczna)



Rysunek 175: Konfiguracja map – podgląd zaznaczenia lokalizacji (mapa statyczna)

Nazwa świadczeniodawcy, 02-495 Warszawa 1 Maja | Oddział kardiologiczny | NFZ

Świadczenie: dowolne | Personel: dowolny | Najbliższe 20 terminów

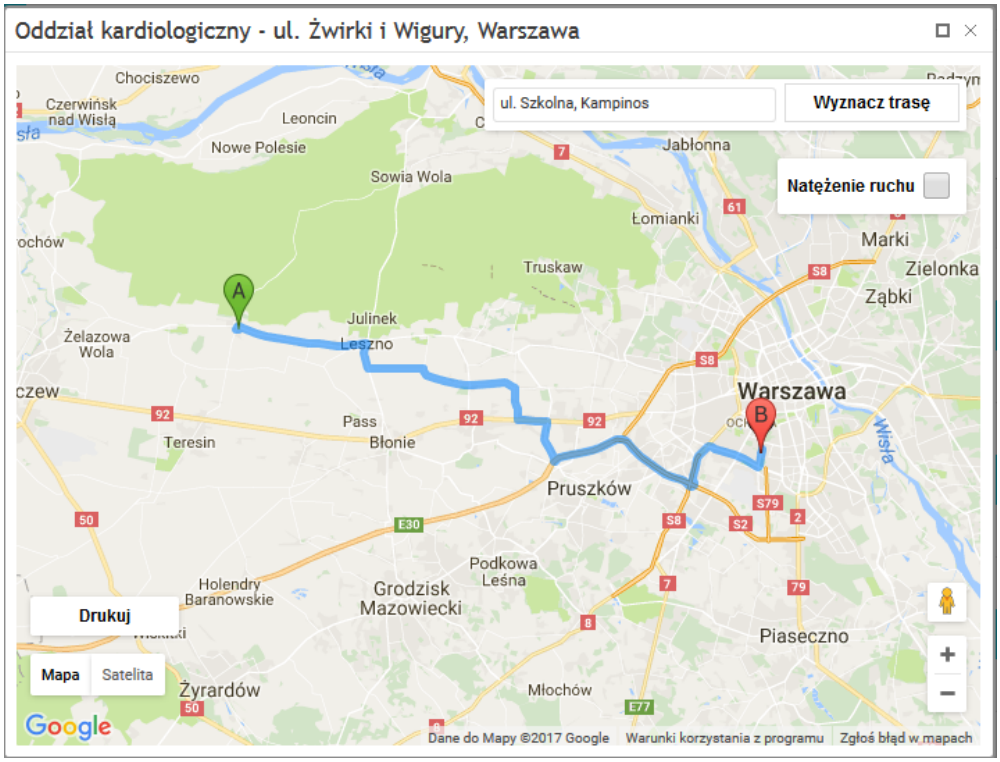
Wyszukaj

Wolne terminy

25.10.2017 (środa) [Zwiń]

16:00	Nazwisko1 Imie1 Oddział kardiologiczny ul. Żwirki i Wigury, Warszawa Nazwa świadczeniodawcy	NFZ	Rezerwuj
16:15	Nazwisko1 Imie1 Oddział kardiologiczny ul. Żwirki i Wigury, Warszawa Nazwa świadczeniodawcy	NFZ	Rezerwuj
16:30	Nazwisko1 Imie1 Oddział kardiologiczny ul. Żwirki i Wigury, Warszawa Nazwa świadczeniodawcy	NFZ	Rezerwuj
16:45	Nazwisko1 Imie1 Oddział kardiologiczny ul. Żwirki i Wigury, Warszawa Nazwa świadczeniodawcy	NFZ	Rezerwuj

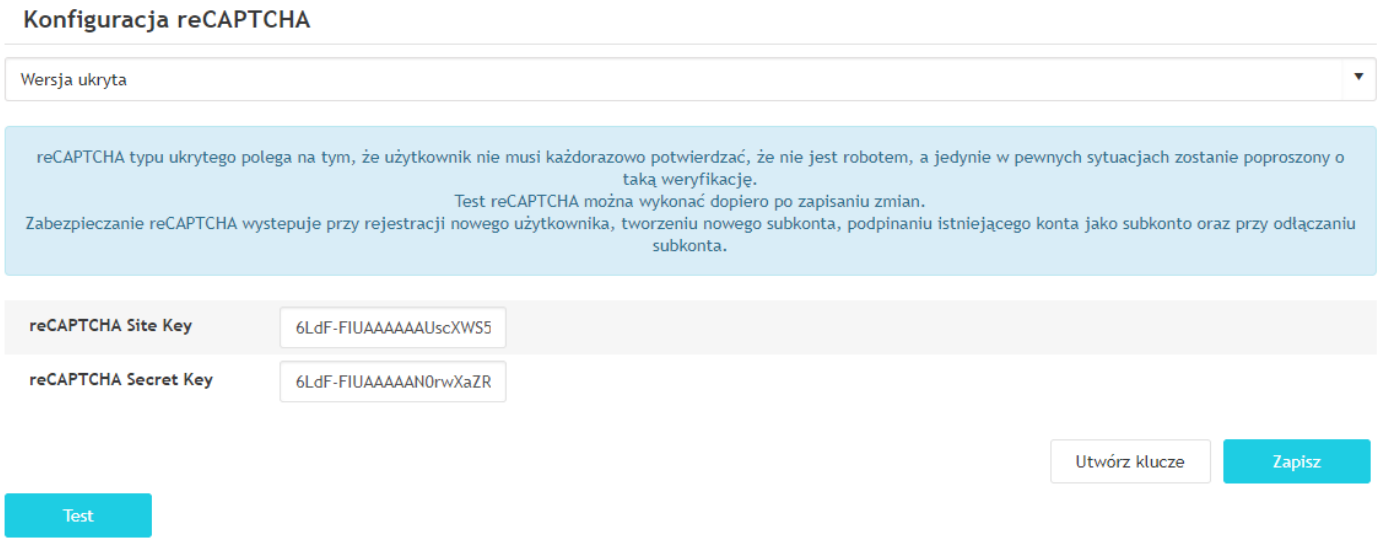
Rysunek 176: Wyświetlanie map w wolnych terminach



Rysunek 177: Wyznaczenie trasy pomiędzy placówką a wskazanym adresem

8.3.10.7. reCAPTCHA

Konfiguracja reCAPTCHA pozwala na włączenie jednego z trzech trybów pracy (opis tych trybów znajduje się poniżej) lub pełne wyłączenie jej. Strona ta pozwala na wygenerowanie nowych kluczy dla reCAPTCHA.



Rysunek 178: Konfiguracja reCAPTCHA

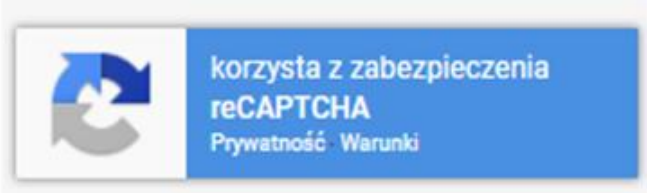
Na portalu dostępne są do wyboru trzy wersje reCAPTCHA:

- Wersja V2 podstawowa - wymagająca od użytkownika zaznaczenia checkboxa, tzw. reCAPTCHA v2;
- Wersja V2 ukryta - niewymagająca zaznaczenia checkboxa, tzw. Invisible reCAPTCHA;
- Wersja V3 - działająca w podobny sposób do wersji V2 ukrytej, dodatkowo pozwala ona ustalić na formatce konfiguracji, minimalny poziom wiarygodności użytkowników.

Niezależnie od wersji reCAPTCHA, wymaga ona posiadania kluczy, które można wygenerować rejestrując portal na stronie Google, dostępnych po kliknięciu przycisku „Utwórz klucze”.

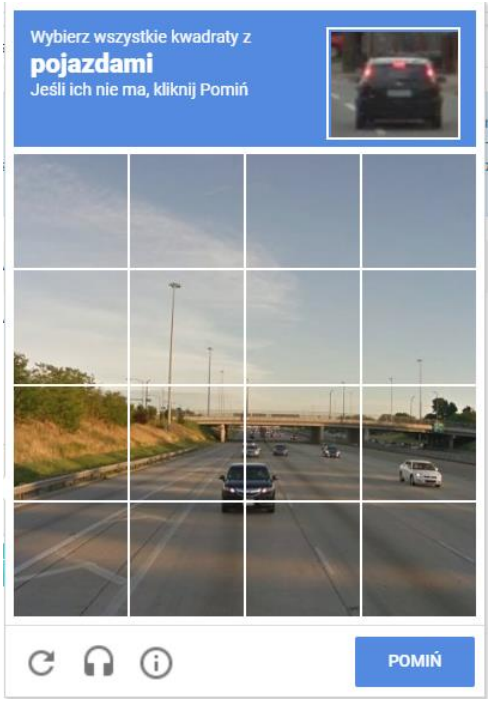
Po zapisaniu konfiguracji, udostępniona zostaje możliwość przetestowania reCAPTCHA.

Jeżeli strona została prawidłowo zarejestrowana, efektem będzie pojawienie się zabezpieczenia na formatkach: rejestracji konta metodą nazwy użytkownika oraz hasła, tworzenia nowego subkonta, podpinania istniejącego konta jako subkonto oraz odpinania subkonta. Na rysunku poniżej, przedstawiono odpowiednio w kolejności - wersję V2 podstawową i V2 ukrytą/V3.



Rysunek 179. Działanie reCAPTCHA

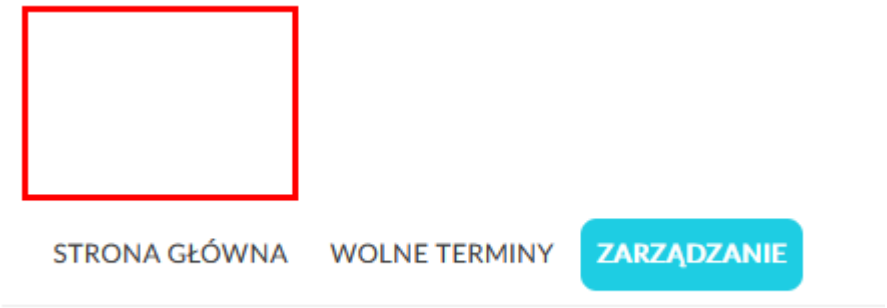
Niezależnie od wybranej wersji reCAPTCHA, użytkownik może zostać poproszony o dodatkową weryfikację, w celu określenia czy jest człowiekiem.



Rysunek 180: Dodatkowa weryfikacja reCAPTCHA

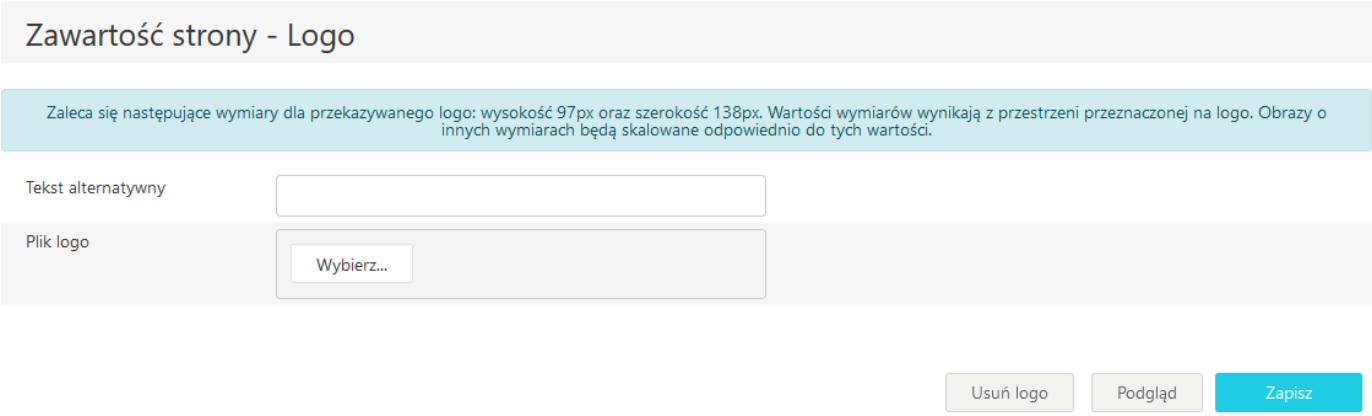
8.3.10.8. Logo

Funkcjonalność pozwala na konifgurowanie własnego logo, które będzie wyświetlane w górnej lewej górnej części strony.



Rysunek 181: Obszar wyświetlania konfigurowalnego logo

Logo może zostać załadowane jako plik z dysku komputera (przez przycisk „Wybierz…). Funkcjonalność obsługuje popularne formaty graficzne takie jak: png, jpg, jpeg, svg, gif, a maksymalny rozmiar pliku wynosi 200 kB. Jeśli z jakiś powodów nie uda się wyświetlić skonfigurowanego logo zostanie wyświetlony tekst z pola „Tekst alternatywny”. Po załadowaniu pliku można testowo go podejrzeć za pomocą przycisku „Podgląd”. Z kolei przycisk „Usuń logo” resetuje ustawienia.



Rysunek 182: Konifguracja logo

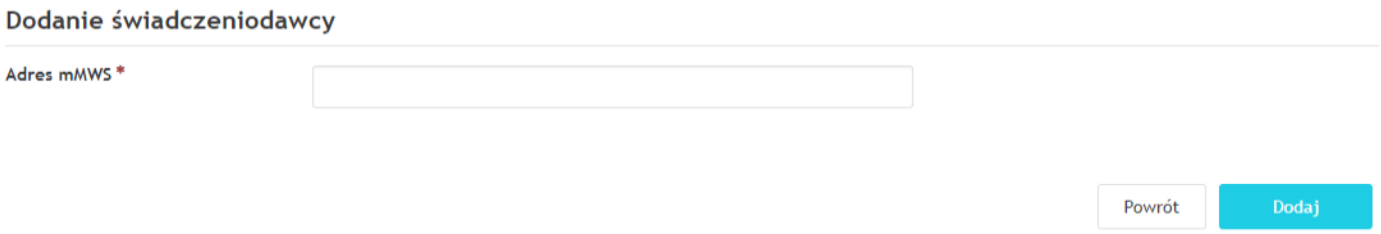
Rozmiar logo jest automatycznie dopasywowany do mniejszego rozmiaru okna, w tym do widoku mobilnego. Jeśli logo nie zostanie zdefiniowane to w widoku mobilnym zostanie wyświetlona ikona, która jest jednocześnie odnośnikiem do strony głównej.

8.3.11. Zarządzanie podmiotami

W celu przejścia do konfiguracji słowników świadczeniodawcy należy wybrać w menu „Konfiguracja” opcję „Zarządzanie podmiotami”.

Rysunek 183: Strona słowników świadczeniodawcy w sytuacji, gdzie nie jest dodany żaden słownik

Jeżeli zawartość strony nie różni się od powyższego zrzutu ekranu, oznacza to, że do Portalu nie został przypisany żaden słownik. W celu dodania słownika świadczeniodawcy należy nacisnąć przycisk „Dodaj świadczeniodawcę".

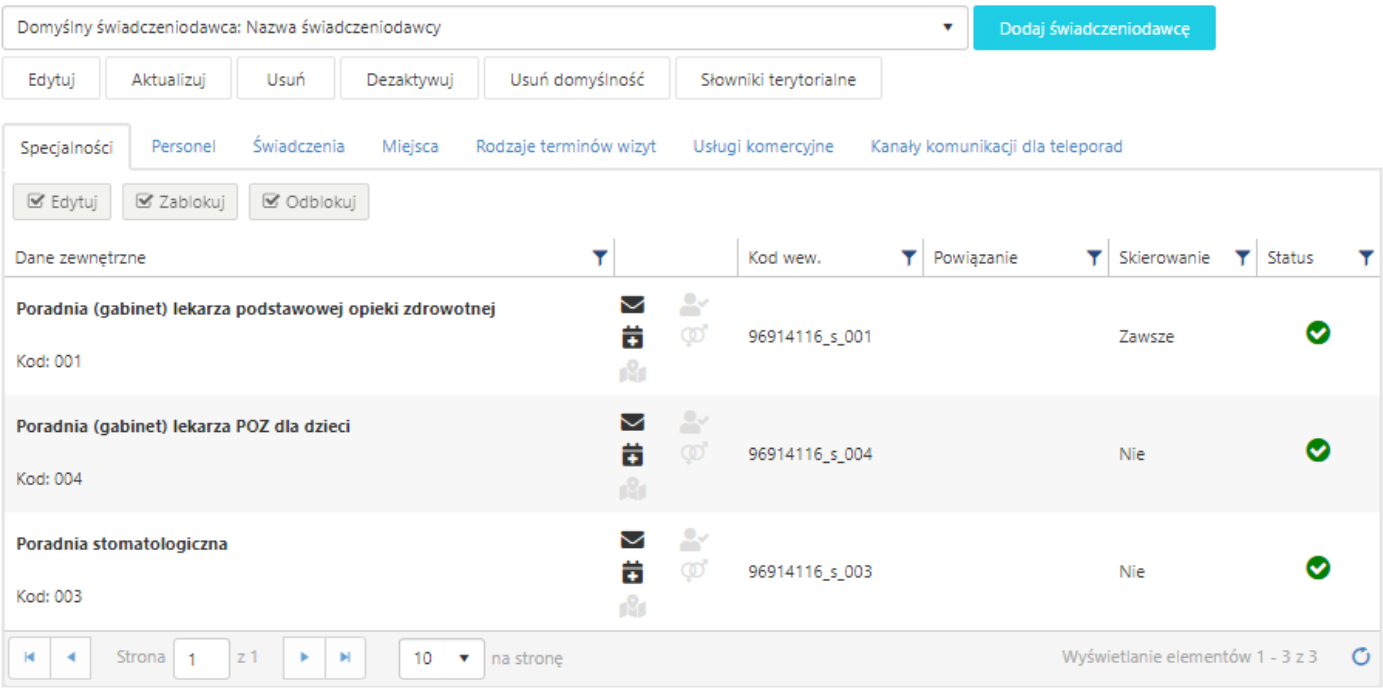


Rysunek 184: Dodawanie świadczeniodawcy

Po otwarciu okienka dodawania świadczeniodawcy należy wpisać adres mMWS oraz nacisnąć przycisk „Dodaj".

Uwaga: Adres mMWS powinien rozpoczynać się od typu protokołu tj. „http" lub „https" oraz kończyć frazą „mMWS" lub „mMWS_nazwa". Adres mMWS to http.*adres-mMDAB*/mMWS.

Nastąpi integracja słowników z systemem eRejestracja. Integracja słowników przebiegła pomyślnie, jeżeli w „Słownikach" istnieje możliwość wyboru z listy któregoś ze świadczeniodawców. Jeśli dodano tylko jeden słownik, zostanie on wczytany domyślnie. Wgranie słownika świadczeniodawcy skutkuje możliwością zarządzania nim na portalu eRejestracja.



Rysunek 185: Słowniki świadczeniodawcy

Słowniki świadczeniodawcy zawierają menu podręczne, składające się z następujących przycisków: „Edytuj”, „Aktualizuj”, „Usuń”, „Dezaktywuj”, „Ustaw jako domyślny” i „Słowniki terytorialne”.

Edycja danych świadczeniodawcy, umożliwia uzupełnienie lub zmianę pól, takich jak: nazwa, adres mMWS, kod pocztowy, miasto, ulica, a także podgląd danych: kod izby oraz kod resortowy części I. Dane te wyświetlane są przy terminach rezerwacji świadczeniodawcy oraz na potwierdzeniu wizyty.

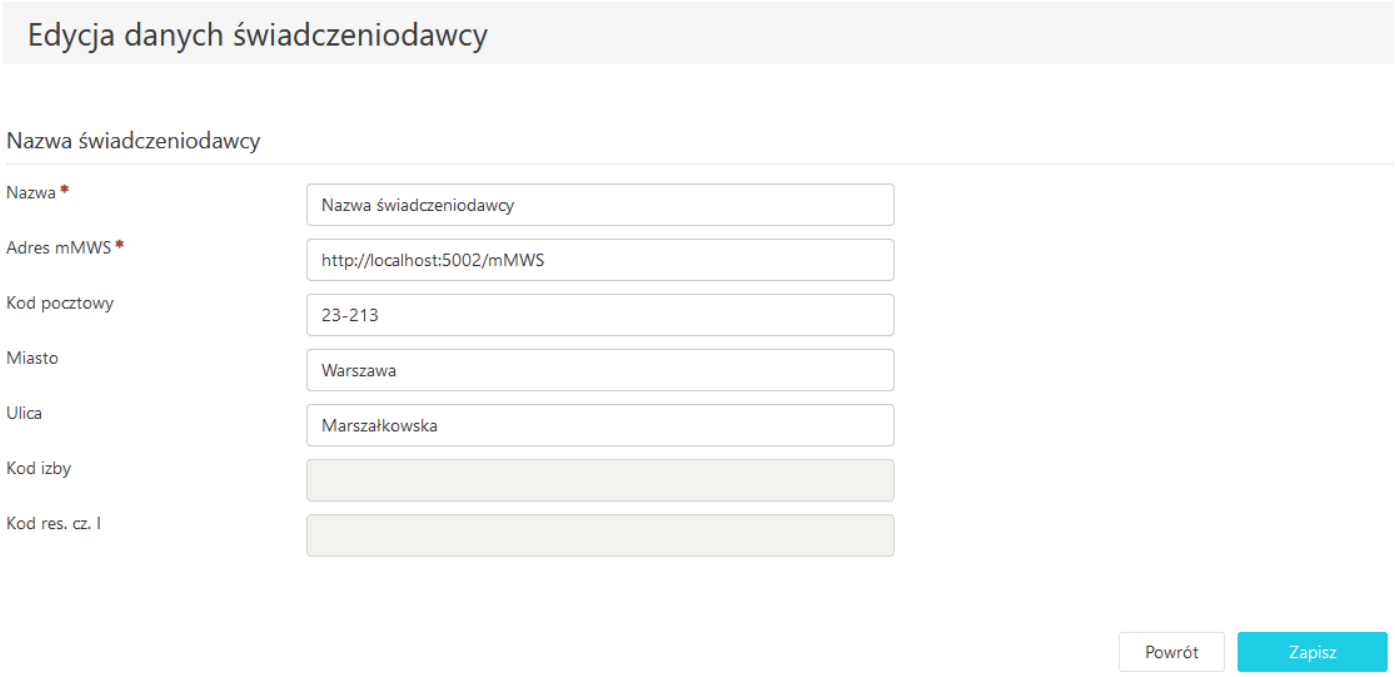
Przycisk „Aktualizuj” pobiera najnowsze dane dotyczące: specjalności, personelu, miejsc, usług komercyjnych oraz pozwala na ściągnięcie nowej wersji słowników terytorialnych.

Kliknięciu przycisku „Usuń”, powoduje usunięcie świadczeniodawcy.

Dezaktywacja słownika sprawia, że wizyty świadczeniodawcy nie są wyświetlane w wolnych terminach, a personel i świadczenia nie widnieją w listach wyszukiwania.

Zaznaczenie opcji „Ustaw jako domyślny”, skutkuje załadowaniem wizyt wybranego świadczeniodawcy, jeśli inny nie został wskazany przez użytkownika. Tylko jeden ze słowników na portalu może być domyślny. Jeśli żaden ze świadczeniodawców nie został oznaczony jako domyślny, wczytane zostaną wizyty od pierwszego w kolejności pobierania świadczeniodawcy.

Słowniki terytorialne wyświetlają listę wszystkich miejscowości w Polsce według podziału terytorialnego: województwa, powiaty, gminy i miasta. Każda z jednostek terytorialnych posiada swój unikalny kod.



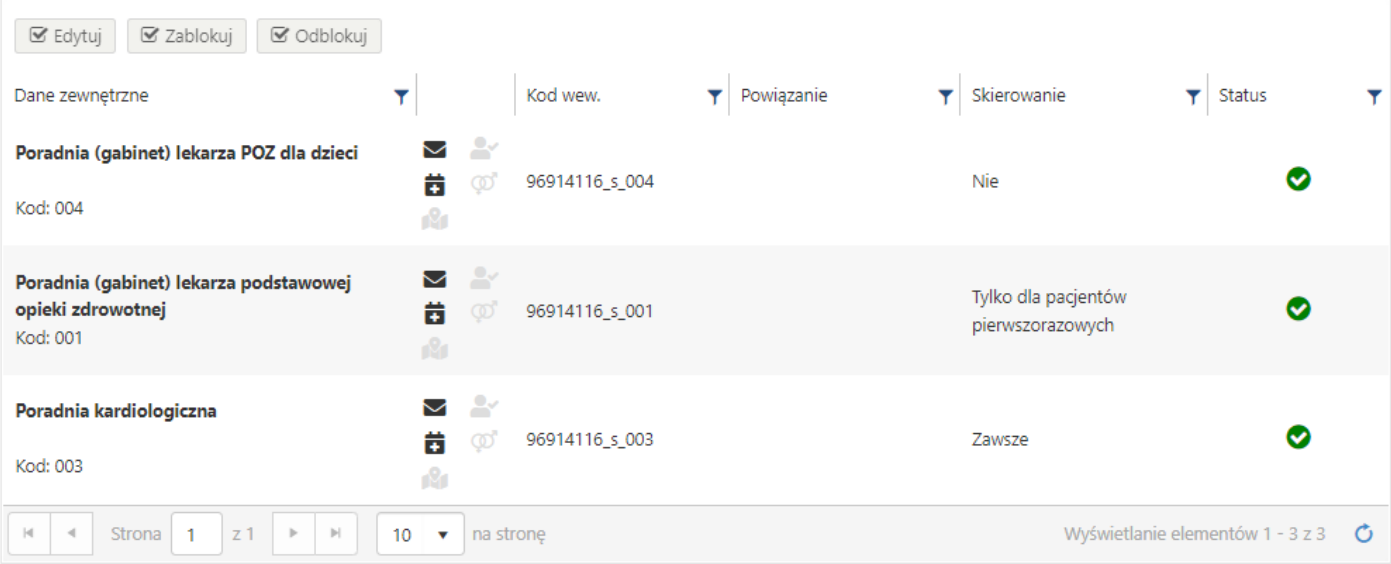
Rysunek 186: Edycja danych świadczeniodawcy

Słownik zawiera ponadto przyciski służące do edycji wpisów specjalności, personelu oraz świadczeń. Niektóre z przycisków mogą być niedostępne w ramach wybranej zakładki, przykładowo z poziomu eRejestracji nie można dodać nowej specjalności ani personelu, jednak możliwe jest to dla świadczeń. Poniżej opisano dostępne przyciski dostępne na górnym pasku menu:

- Edytuj - pozwala edytować dane specjalności, personelu lub świadczenia,
- Zablokuj - pozwala zablokować wybraną specjalność, personel lub świadczenie,
- Odblokuj - pozwala odblokować wybraną specjalność, personel lub świadczenie,
- Usuń - pozwala usunąć wybrane świadczenie w zakładce „Świadczenia”,
- Dodaj - pozwala utworzyć nowe świadczenie w zakładce „Świadczenia”.

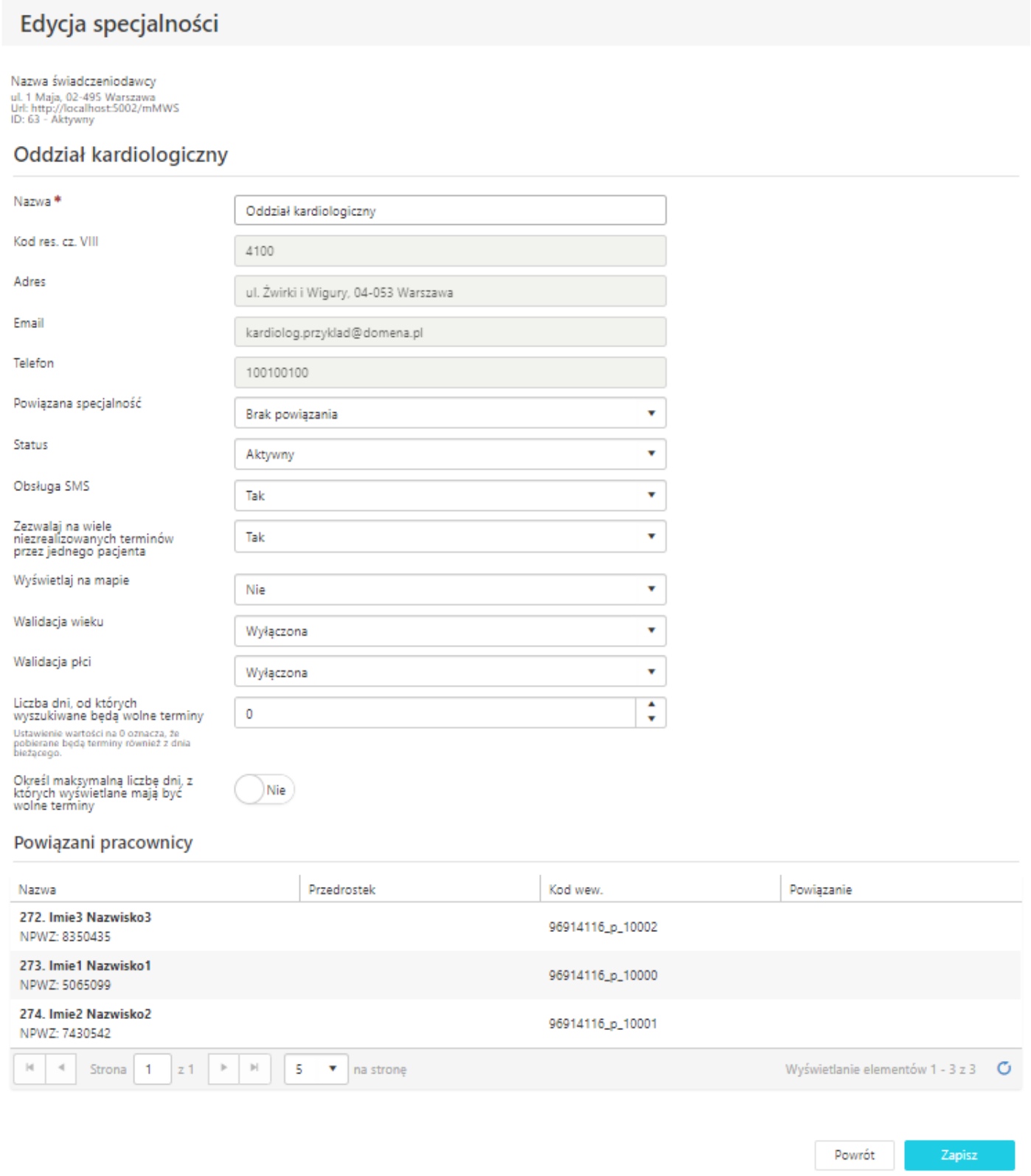
8.3.11.1. Specjalności

Zakładka „Specjalności” wyświetlana jest domyślnie po otwarciu strony zarządzania podmiotami. Zawiera listę wszystkich specjalności wybranego świadczeniodawcy.



Rysunek 187: Słownik specjalności

Edycja danych specjalności umożliwia zmianę nazwy, statusu oraz ustawienie powiązania specjalności. Wyświetlany jest także kod resortowy cz. VIII oraz dane kontaktowe. W razie chęci utworzenia powiązania należy rozwinąć listę „Powiązana specjalność”, wybrać żądaną wartość oraz zapisać zmiany. Jeżeli powiązanie zakończyło się pomyślnie, specjalność przyjmie nazwę specjalności skojarzonej, natomiast w polu „Powiązanie” zostanie wpisany jej kod wewnętrzny.

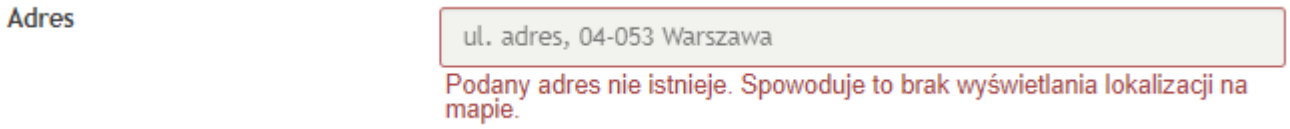


Rysunek 188: Edycja danych specjalności

Portal eRejestracja posiada możliwość wyświetlenia lokalizacji specjalności z poziomu moich terminów, zarezerwowanych terminów oraz potwierdzeń rezerwacji wizyt. Do wyświetlenia przycisku mapy potrzebny jest adres placówki, włączenie widoczności map dla danej specjalności oraz wskazanie, w których miejscach

mają być wyświetlane. W przypadku adresu, który nie może zostać namierzony, wyświetlany jest komunikat „Podany adres nie istnieje. Spowoduje to brak wyświetlenia lokalizacji na mapie”. Rozwijana lista „Wyświetlaj na mapie” pozwala na włączenie lub wyłączenie opcji wyświetlenia mapy dla obecnie edytowanej specjalności.

Uwaga! W konfiguracji map (*8.3.10.6. Mapy*) należy zaznaczyć miejsca wyświetlania przycisków otwierających okno mapy.



Rysunek 189: Adres specjalności niemożliwy do wyświetlenia na mapie

Rozwijana lista „Obsługa SMS" pozwala na włączenie lub wyłączenie wysyłania wiadomości SMS dotyczących danej specjalności. Należy jednak zauważyć, że nadrzędnymi ustawieniami są ustawienia bramki świadczeniodawcy (więcej informacji w rozdziale *8.3.9.1.4. Bramka* SMS). Ustawienie dezaktywacji lub aktywacji SMS dla specjalności będą obowiązywać dopiero wówczas, gdy bramka SMS świadczeniodawcy będzie aktywna.

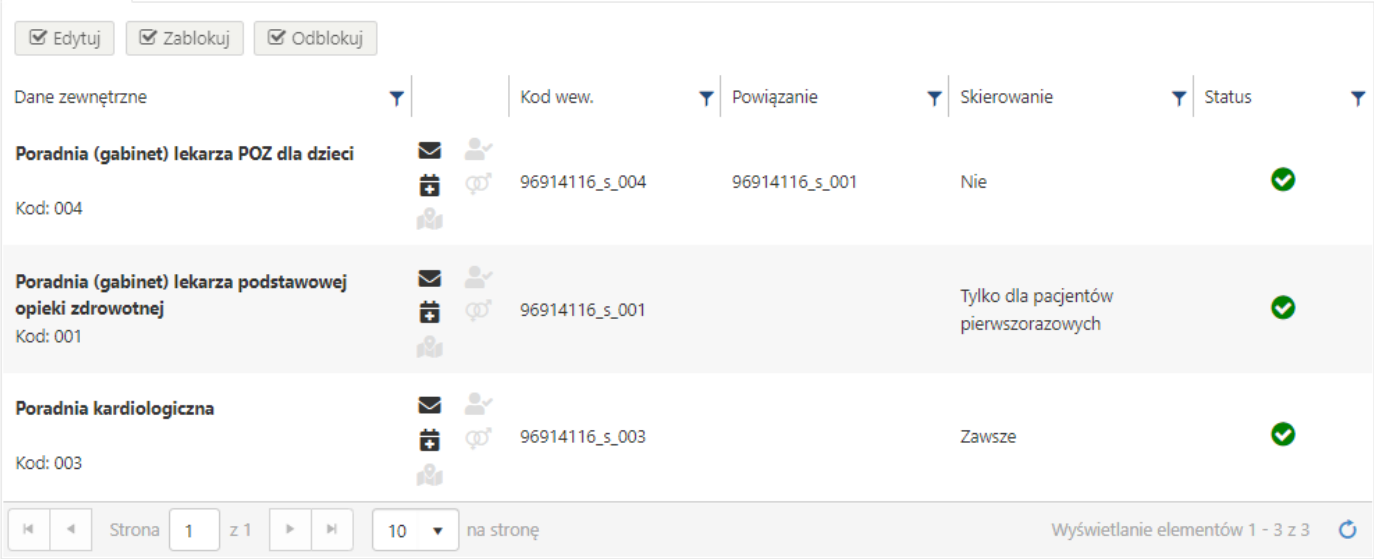
Podczas edycji specjalności możliwa jest konfiguracja ustawień dostępności rezerwacji wizyt w jej obrębie w zależności od wieku użytkownika. Dostępne są następujące opcje:

- Wyłączona – wizyty z danej specjalności mogą być rezerwowane niezależnie od wieku pacjenta,
- Dzieci – wizyty z danej specjalności mogą być rezerwowane wyłącznie dla pacjentów poniżej 18 roku życia,
- Dorośli – wizyty z danej specjalności mogą być rezerwowane tylko przez osoby, które ukończyły 18 rok życia.

Możliwa jest również konfiguracja ustawień dostępności rezerwacji wizyt w jej obrębie w zależności od płci użytkownika. Dostępne są następujące opcje:

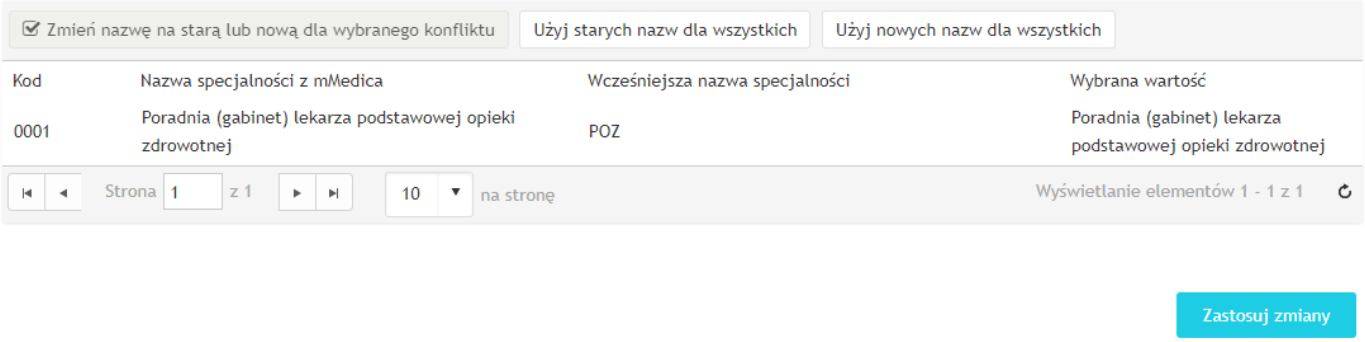
- Wyłączona – wizyty z danej specjalności mogą być rezerwowane niezależnie od płci pacjenta,
- Mężczyźni – Wizyty z danej specjalności mogą być rezerwowane wyłącznie dla pacjentów płci męskiej,
- Kobiety – Wizyty z danej specjalności mogą być rezerwowane wyłącznie dla pacjentów płci żeńskiej.

Możliwe jest również określenie liczby dni, od których maja być wyszukiwane wolne terminy jak i maksymalną liczbę dni z kórych mogą być wyświetlane wolne terminy. Druga opcja spowoduje to, że nawet jeśli użytkownik wybierze wyświetlanie terminów z dłuższego okresu, wyszukiwanie zostanie zawężone jedynie do liczby dni ustawionej w konfiguracji. Opcja ta jest aktywna po zaznaczeniu pola „Określ maksymalną liczbę dni…". Łącząc działanie obu parametrów można stworzyć okna czasowe, z których wyświetlane będą wolne terminy, np. ustawiając liczbę dni, od którch wyświetlane mają być wolne terminy na 2 oraz maxymalną liczbę dni, z których wyświetlane mają być wolne terminy na 3 i przyjmując że aktualny dzień to 22.05 to wyświetlane użytkwonikowi wolne terminy będą z dni od 24.05 do 27.05.



Rysunek 190: Powiązana specjalność ze świadczeniodawcą

Podczas odświeżania słowników świadczeniodawcy może wystąpić konflikt nazw specjalności. Portal eRejestracja umożliwia zmianę nazw danych specjalności na własne, jednak w momencie odświeżania słowników świadczeniodawców pobierane są dane oryginalne z aplikacji mMedica. Aby uniknąć problemu ciągłej konieczności zmiany nazw, eRejestracja posiada mechanizm pozwalający zadecydować administratorowi, których z nich chce używać.

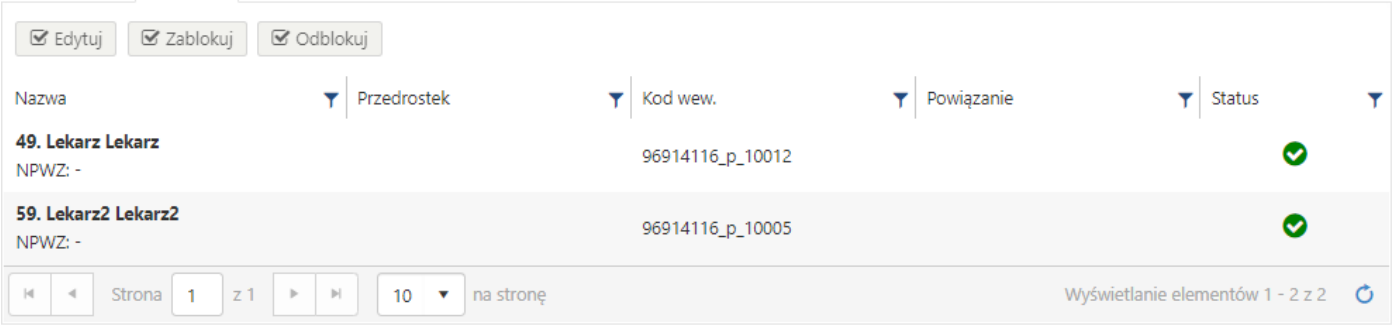


Rysunek 191: Rozwiązywanie konfliktów nazw specjalności

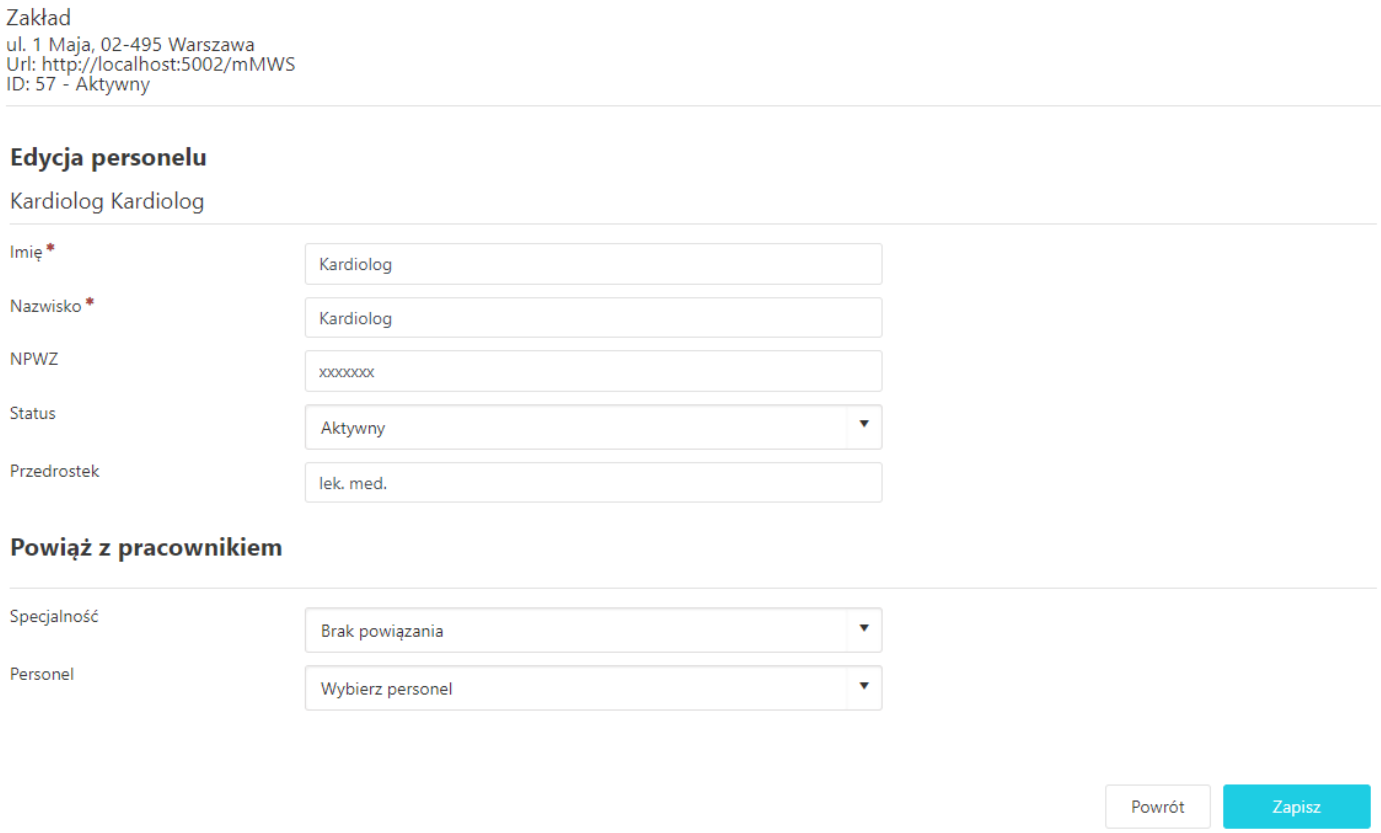
W przypadku wspomnianym powyżej, po zaktualizowaniu słownika świadczeniodawcy zostanie wyświetlona tabela z nazwami specjalności użytymi przed dokonaniem aktualizacji oraz obecnymi z mMedica. Naciśnięcie przycisku „Użyj starych nazw dla wszystkich” sprawi, że w portalu zostaną ustawione nazwy sprzed aktualizacji. Kliknięcie przycisku „Użyj nowych nazw dla wszystkich” wymusza użycie nowych nazw pobranych po aktualizacji. Można również dokonać wyboru dla pojedynczych specjalizacji za pomocą przycisku „Zmień nazwę na starą lub nową dla wybranego konfliktu”. Wybrana nazwa dla danej specjalności wyświetlana jest w tabeli w kolumnie „Wybrana wartość”. Ustawienia należy zapisać poprzez użycie przycisku „Zastosuj zmiany”. Do momentu, w którym nie zatwierdzi się zmian, używane są nazwy pobrane z aplikacji mMedica.

8.3.11.2. Personel

Tabela zawiera dane personelu, który jest przypisany do określonego świadczeniodawcy. Każda osoba posiada przypisany kod wewnętrzny, NPWZ, kod ewentualnego powiązania oraz status aktywności na portalu. W celu powiązania osoby z pracownikiem należy zaznaczyć daną osobę i kliknąć przycisk „Edycja”. Nowo otwarta strona wyświetli formularz umożliwiający zmianę imienia, nazwiska, NPWZ oraz statusu. Poniżej znajduje się panel „Powiąż z pracownikiem”, który zawiera rozwijane listy pozwalające na dokonanie przypisania. Należy wybrać żądane wartości oraz zapisać wprowadzone zmiany przyciskiem „Zapisz”. Osoba, z którą powiązano innego pracownika przyjmie jego imię i nazwisko.



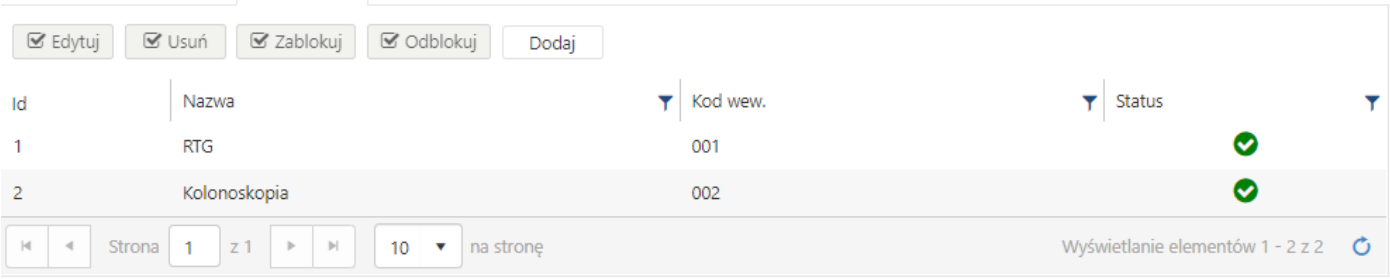
Rysunek 192: Dane personelu



Rysunek 193: Powiązanie osoby personelu z pracownikiem

8.3.11.3. Świadczenia

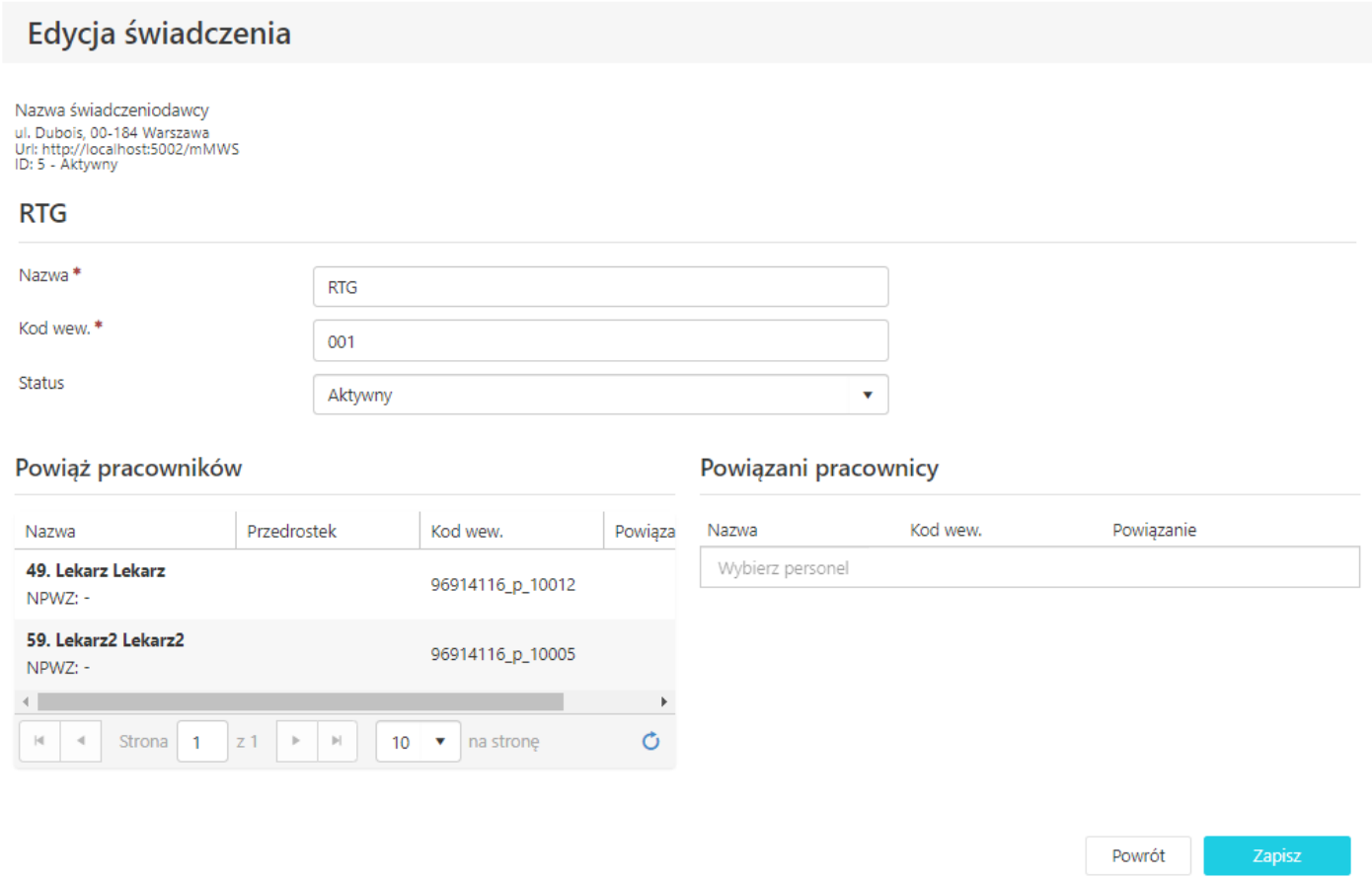
Zakładka zawiera świadczenia przypisane do określonego świadczeniodawcy oraz umożliwia przypisanie do niego osoby z personelu.



Rysunek 194: Świadczenia

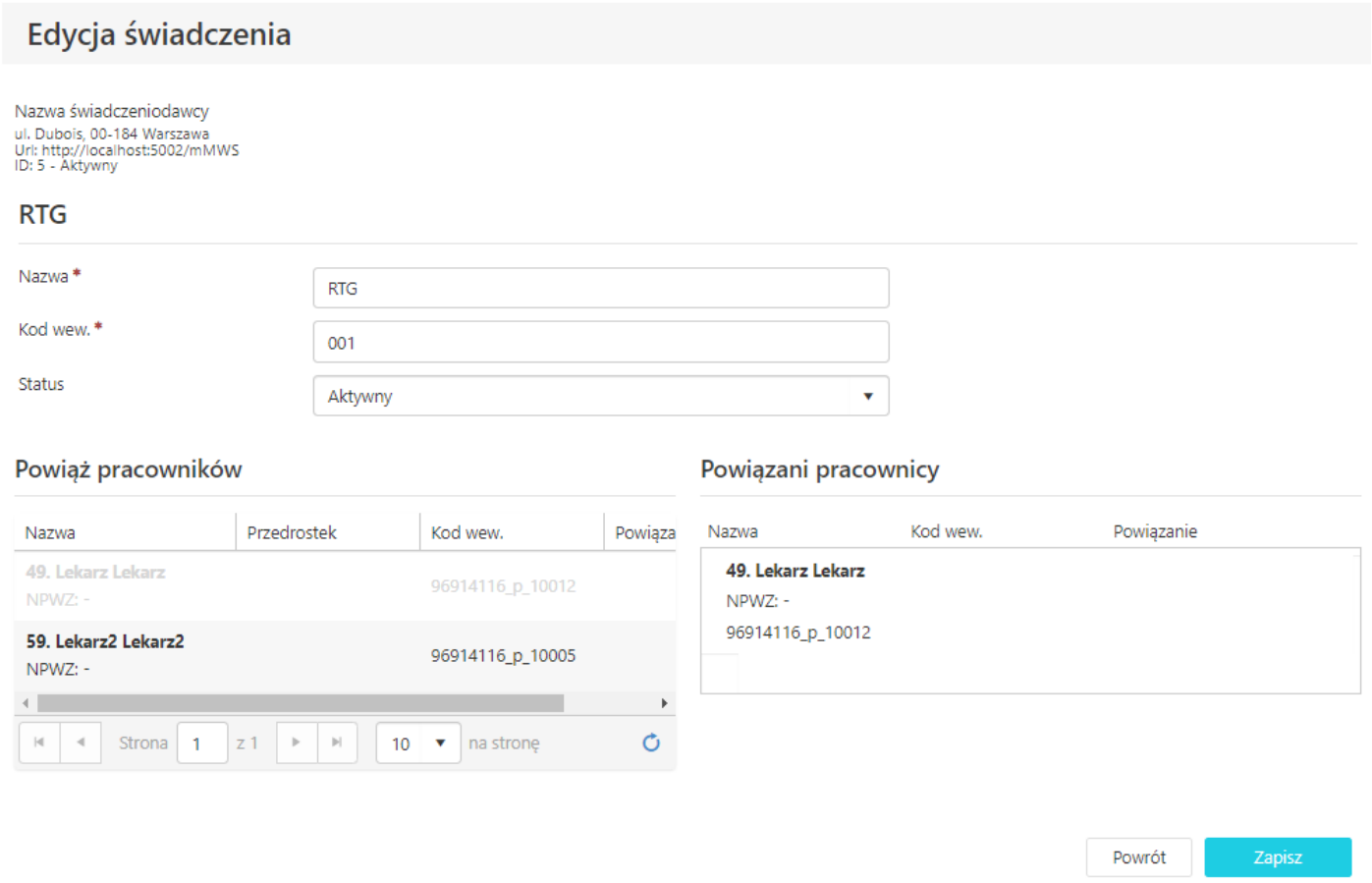
W tabeli wyświetlane są wszystkie świadczenia wybranego z listy słownika świadczeniodawcy. Proces dodania nowego świadczenia należy zacząć od naciśnięcia przycisku „Dodaj” dostępnej w górnym menu aplikacji. Po dokonaniu tej czynności otworzy się nowa strona zawierająca listę osób personelu oraz możliwość ich dodawania poprzez kliknięcie na danego pracownika. Pracownik zostanie usunięty z listy świadczenia, jeśli naciśnie się jego pozycję a następnie znak krzyżyka po prawej.

Istnieje również możliwość edycji świadczenia. W tym celu należy zaznaczyć świadczenie oraz nacisnąć przycisk „Edycja” znajdujący się w górnym menu portalu.



Rysunek 195: Okno dodawania oraz edycji świadczenia

Zablokowanie świadczenia odbywa się poprzez naciśnięcie przycisku „Zablokuj”. Działanie to wywoła zmianę statusu świadczenia na nieaktywny , co oznacza, że wizyty personelu przypisanych do danego świadczenia oraz świadczenie nie będą dostępne w wyszukiwarce wolnych terminów. Odblokowanie świadczenia następuje poprzez ponowne naciśnięcie przycisku „Odblokuj”. Utworzone świadczenia mogą zostać usunięte z portalu eRejestracja za pomocą przycisku „Usuń”.

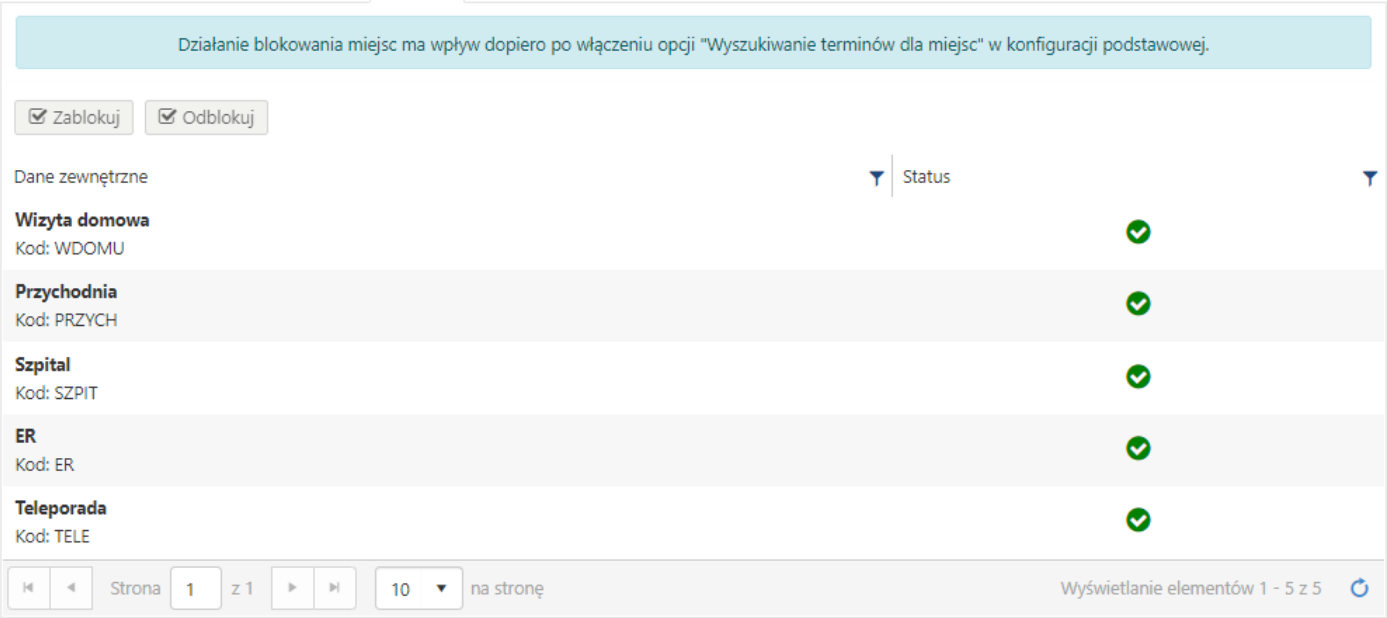


Rysunek 196: Powiązywanie pracowników personelu z świadczeniami

8.3.11.4. Miejsca

Zakładka przedstawia miejsca, dla których możliwa jest rejestracja wizyt w Portalu eRejestracja. W tabeli widoczne są: nazwa miejsca, kod oraz status.

Administrator ma możliwość zablokowania/odblokowania miejsca. Wówczas zmienia się status danego miejsca na „Nieaktywny”/”Aktywny”. Aby to zrobić należy wybrać miejsce, które chcemy zablokować/odblokować, a następnie kliknąć jeden z przycisków znajdujących się nad tabelą: „Zablokuj”/”Odblokuj”. Należy jednak pamiętać, że działania blokowania miejsc mają wpływ dopiero, gdy w zakładce „Konfiguracje”, dalej „Podstawowe”, włączona jest opcja „Wyszukiwanie terminów dla miejsc”.

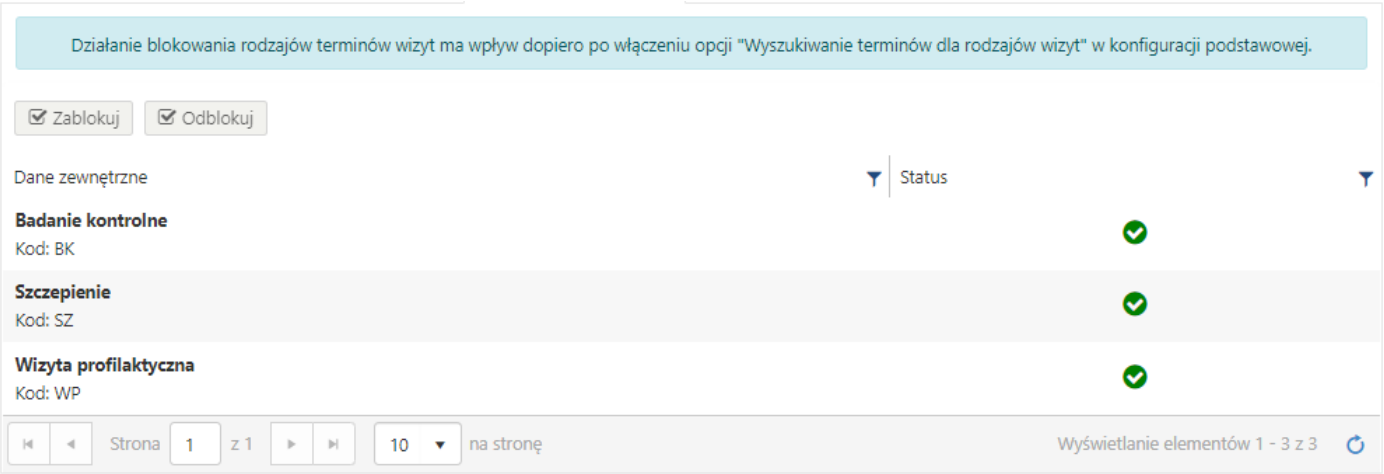


Rysunek 197: Miejsca

8.3.11.5. Rodzaje terminów wizyt

W zakładce znajduje się lista rodzajów terminów wizyt, dla których możliwa jest rejestracja wizyt w Portalu eRejestracja. W tabeli widoczne są: nazwa rodzaju terminu wizyty, kod oraz status.

Administrator ma możliwość zablokowania/odblokowania rodzaju terminu wizyty. Wówczas zmienia się status danego miejsca na „Nieaktywny”/”Aktywny”. Aby to zrobić należy wybrać rodzaj, który chcemy zablokować/odblokować, a następnie kliknąć jeden z przycisków znajdujących się nad tabelą: „Zablokuj”/”Odblokuj”. Należy jednak pamiętać, że działania blokowania rodzajów terminów wizyt mają wpływ dopiero, gdy w zakładce „Konfiguracje”, dalej „Podstawowe”, włączona jest opcja „Wyszukiwanie terminów dla rodzajów wizyt”.



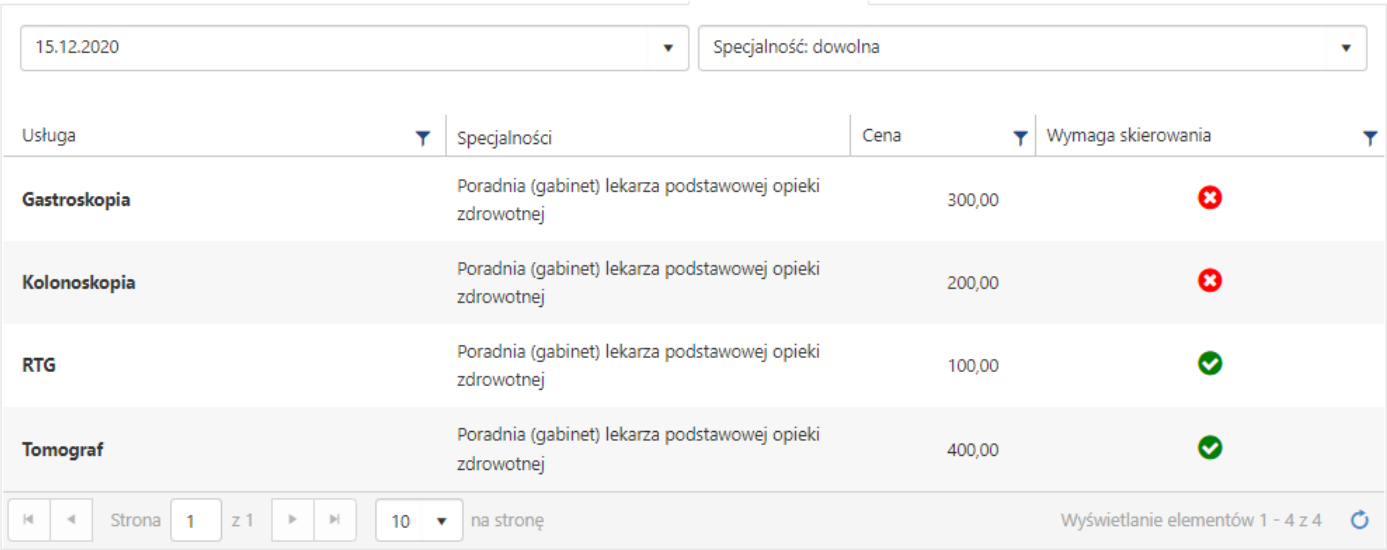
Rysunek 198: Rodzaje terminów wizyt

8.3.11.6. Usługi komercyjne

Zakładka zawiera tabelę usług komercyjnych zdefiniowanych w programie mMedica. Na górze zakładki znajdują się dwie rozwijane listy. W pierwszej można wybrać cennik po zakresie dat jego obowiązywania, a w drugiej specjalność, po których można filtrować tabelę.

W tabeli wyświetlają się: nazwa danej usługi, specjalności, dla których możliwe jest zamówienie danej usługi, cena usługi oraz informacja czy dana usługa wymaga skierowania.

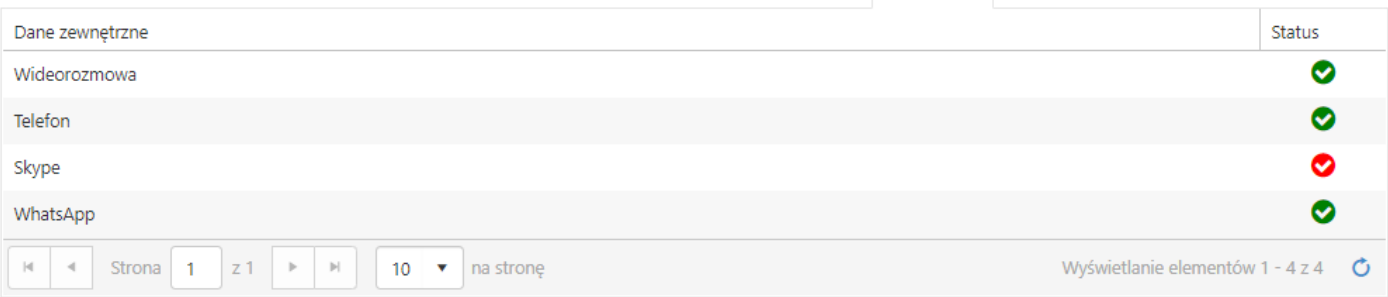
Usługi komercyjne są dostępne jedynie dla wizyt prywatnych.



Rysunek 199: Usługi komercyjne

8.3.11.7. Teleporady

Zakładka zawiera listę kanałów komunikacji dla teleporad. Konfiguracja aktywności poszczególnych kanałów odbywa się w mMedica. Po zmianie aktywności kanałów należy zaktualizować słowniki świadczeniodawcy w Portalu eRejestracja.

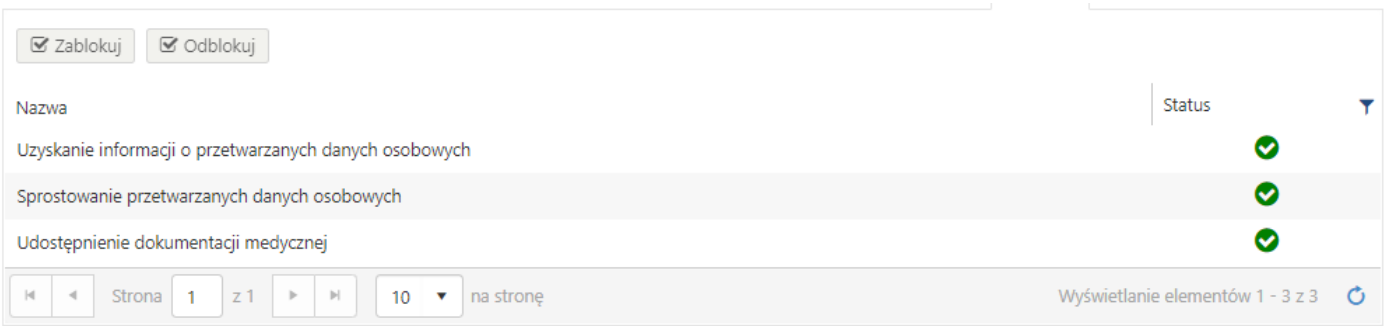


Rysunek 200: Kanały komunikacji dla teleporad

8.3.11.8. Wnioski

Zakładka pozwala na konfigurowanie, które rodzaje wniosków są możliwe do wysłania przez zalogowanego pacjenta dla wybranego świadczeniodawcy. W tabeli widoczne są: nazwa rodzaju wniosku oraz status. Administrator ma możliwość zablokowania/odblokowania zaznaczonego rodzaju wniosku.

Zalogowany pacjent nie będzie mógł wysłać nowego wniosku, którego rodzaj został zablokowany, ale w poglądzie wysłanych wniosków będzie widzieć wszystkie rodzaje wniosków (nienależenie od statusu).

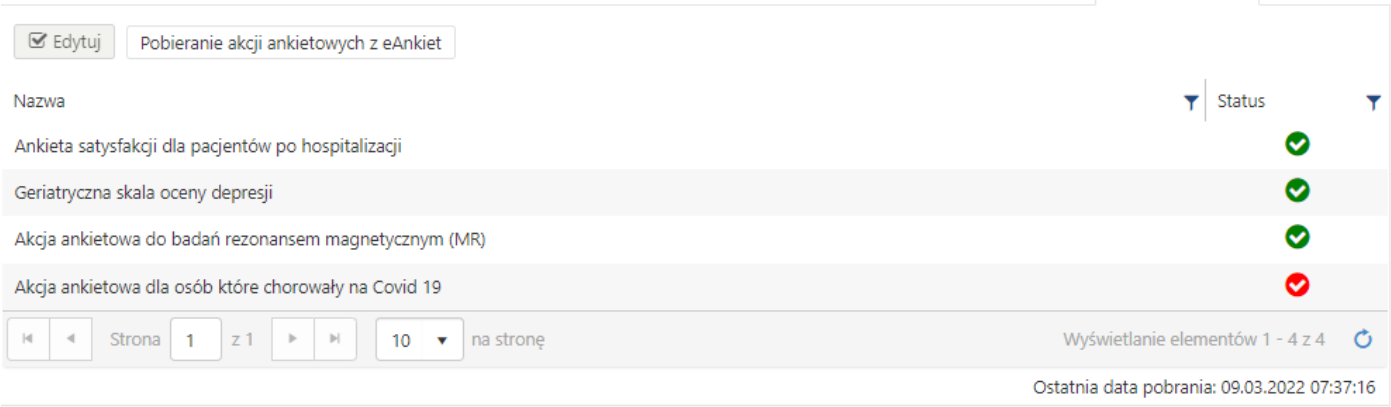


Rysunek 201: Obsługa wniosków

8.3.11.9. Akcje ankietowe

Uwaga: Funkcjonalność wymaga uzupełnienia nr PESEL przez administratora na stronie Moje konto/Zmień dane.

Na zakładce administrator może pobrać wcześniej skonfigurowane akcje ankietowe z systemu eAnkiet (przycisk „Pobierz akcje ankietowej z eAnkiet”). Akcje ankietowe pozwalają na tworzenie eAnkiet dla użytkownika po jego zalogowaniu lub po wykonaniu rezerwacji terminu. Status akcji ankietowych oznacza, czy dana akcja jest aktywna w systemie eAnkiet (status jest nieedytowalny z poziomu eR). Tworzenie eAnkiet możliwe jest wyłącznie, gdy akcja ankietowa jest aktywna.

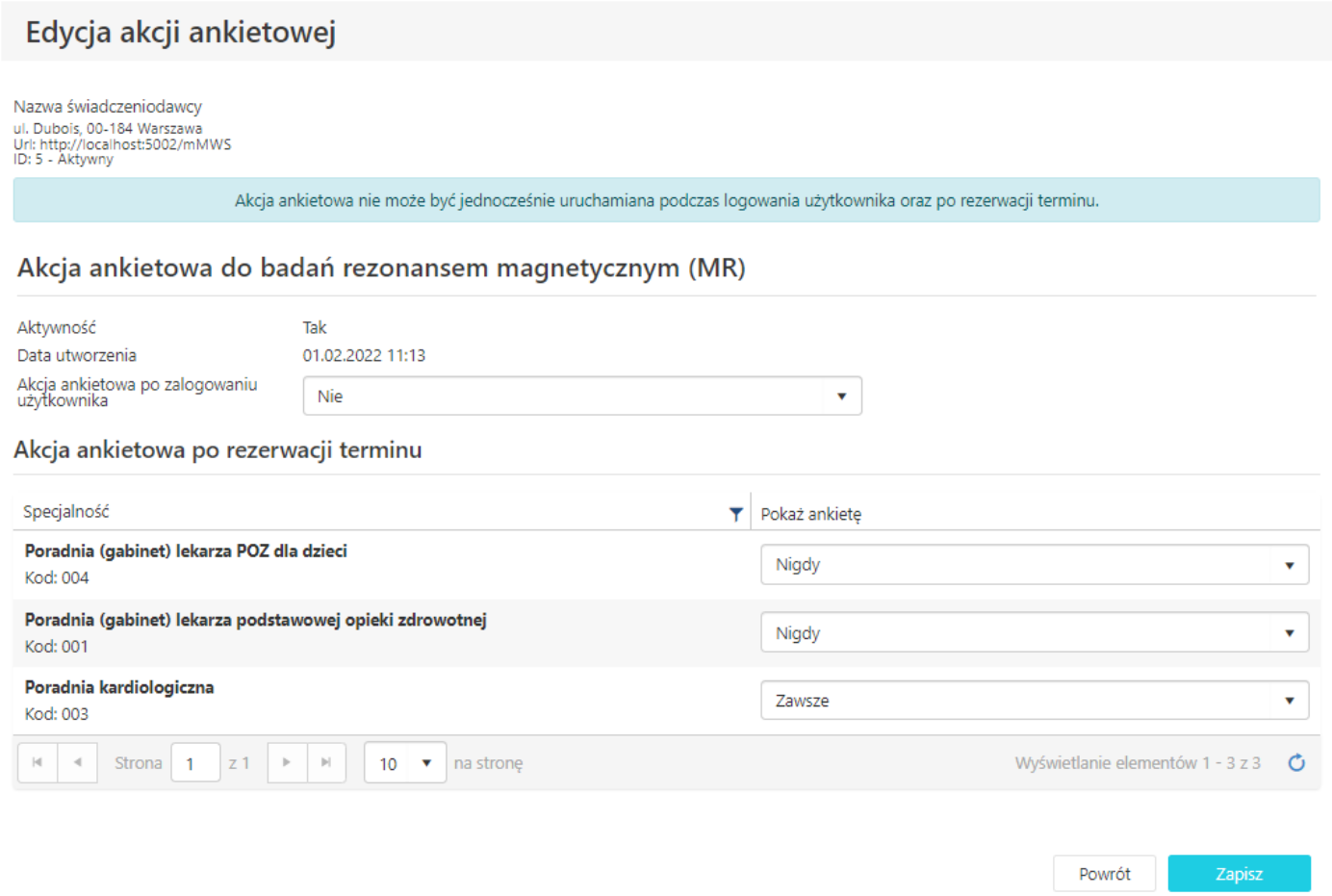


Rysunek 202: Akcje ankietowe pobrane z eAnkiet

Pod tabelą akcji ankietowych znajduje się informacja o ostatniej dacie pobrania akcji z systemu eAnkiet.

Po zaznaczeniu akcji ankietowej możliwa jest jej edycja za pomocą przycisku „Edytuj”. Edycja akcji ankietowej pozwala na tworzenie eAnkiet po pierwszym zalogowaniu użytkownika, a także po wykonaniu rezerwacji (przez zalogowanego użytkownika lub zalogowany personel medyczny). W przypadku rezerwacji, tworzenie eAnkiety definiuje się poprzez wybór specjalności oraz jednego z rodzajów wyświetlania ankiet:

- Nigdy – ustawienie domyślne, eAnkiety nie są tworzone,
- Tylko dla pierwszorazowych – eAnkieta jest tworzono wyłącznie, gdy pacjent wykonał pierwszą od dwóch lat rezerwację (dla komercji i NFZ),
- Zawsze – eAnkieta jest tworzono każdorazowo po wykonaniu rezerwacji.



Rysunek 203: Edycja akcji ankietowej

Nie jest możliwe włączenie dla jednej akcji ankietowej tworzenia eAnkiet po zalogowaniu oraz po rezerwacji. Z kolei istnieje możliwość skonfigurowania wielu akcji ankietowych po zalogowaniu lub rezerwacji terminu.

Jeśli użytkownik nie uzupełni eAnkiet po zalogowaniu to istnieje możliwość jej uzupełnienia z poziomu Panelu Pacjenta (zakładka „Ankiety”).

8.3.12. Statystyki

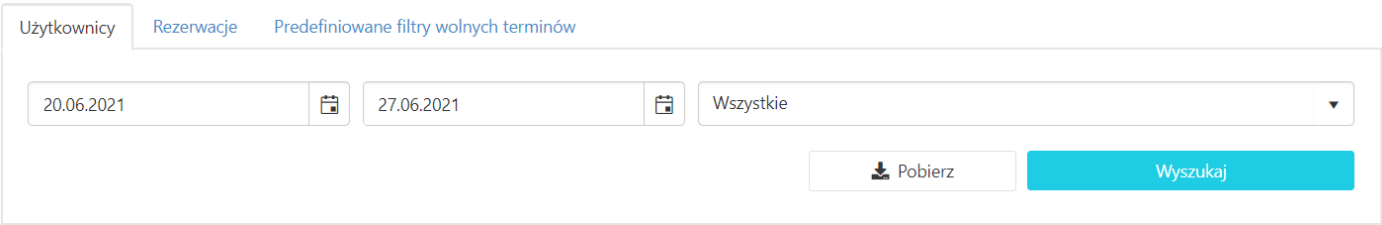
Funkcjonalność statystyk w Portalu eRejestracja umożliwia administratorowi podgląd liczby różnych działań wykonywanych przez użytkowników.

8.3.12.1. Użytkownicy

Z dostępnych na górze strony filtrów można wybrać rodzaj statystyk do wyświetlenia. Dostępne są:

- Rejestracje,
- Utworzone subkonta,
- Blokady,
- Logowania,
- Wszystkie.

Dodatkowo można wybrać zakres dat, dla których mają wyświetlać się wybrane statystyki. Po ustawieniu filtrów należy kliknąć „Wyszukaj”. Przycisk „Pobierz” służy do pobrania statystyk w formacie csv.



Rysunek 204: Statystyki użytkowników

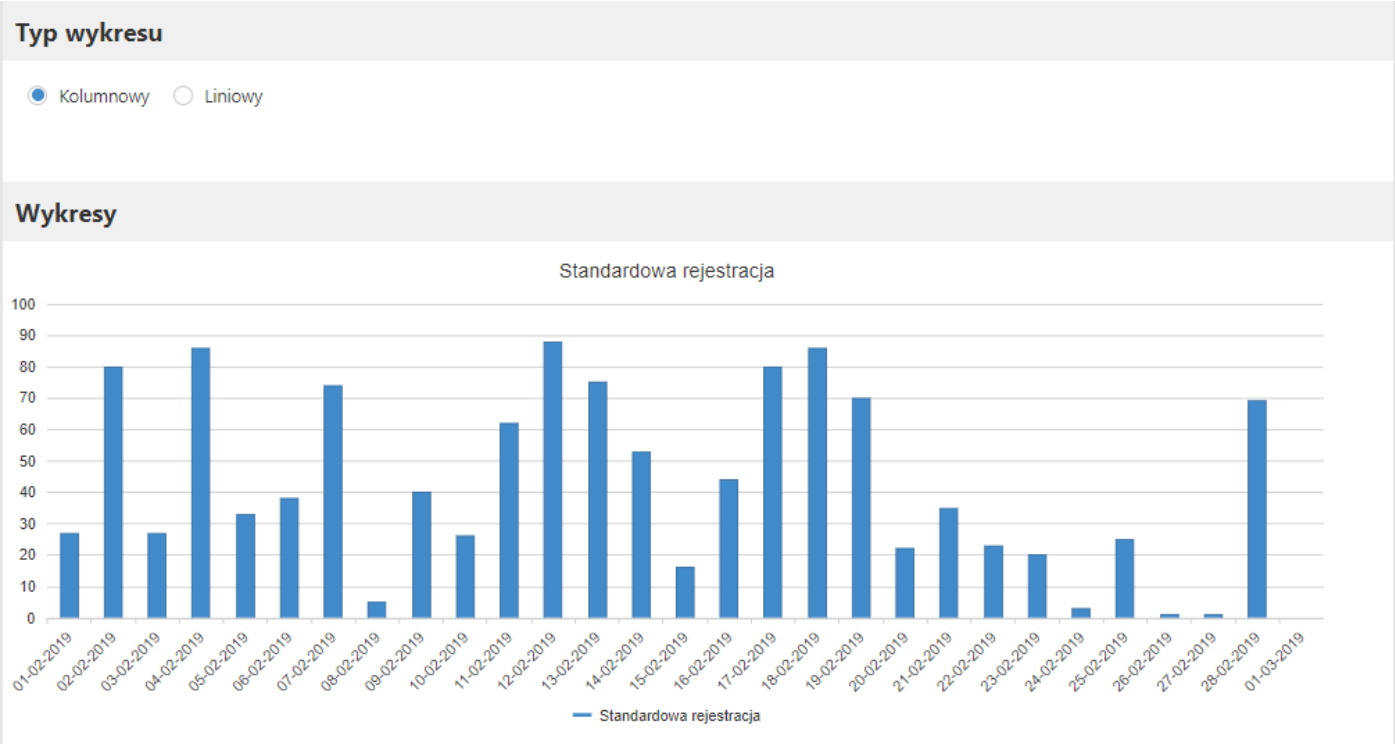
8.3.12.1.1. Statystyki użytkowników – Rejestracje

Statystyki rejestracji zawierają informacje o tym ilu użytkowników zarejestrowało się do Portalu eRejestracja i w jaki sposób:

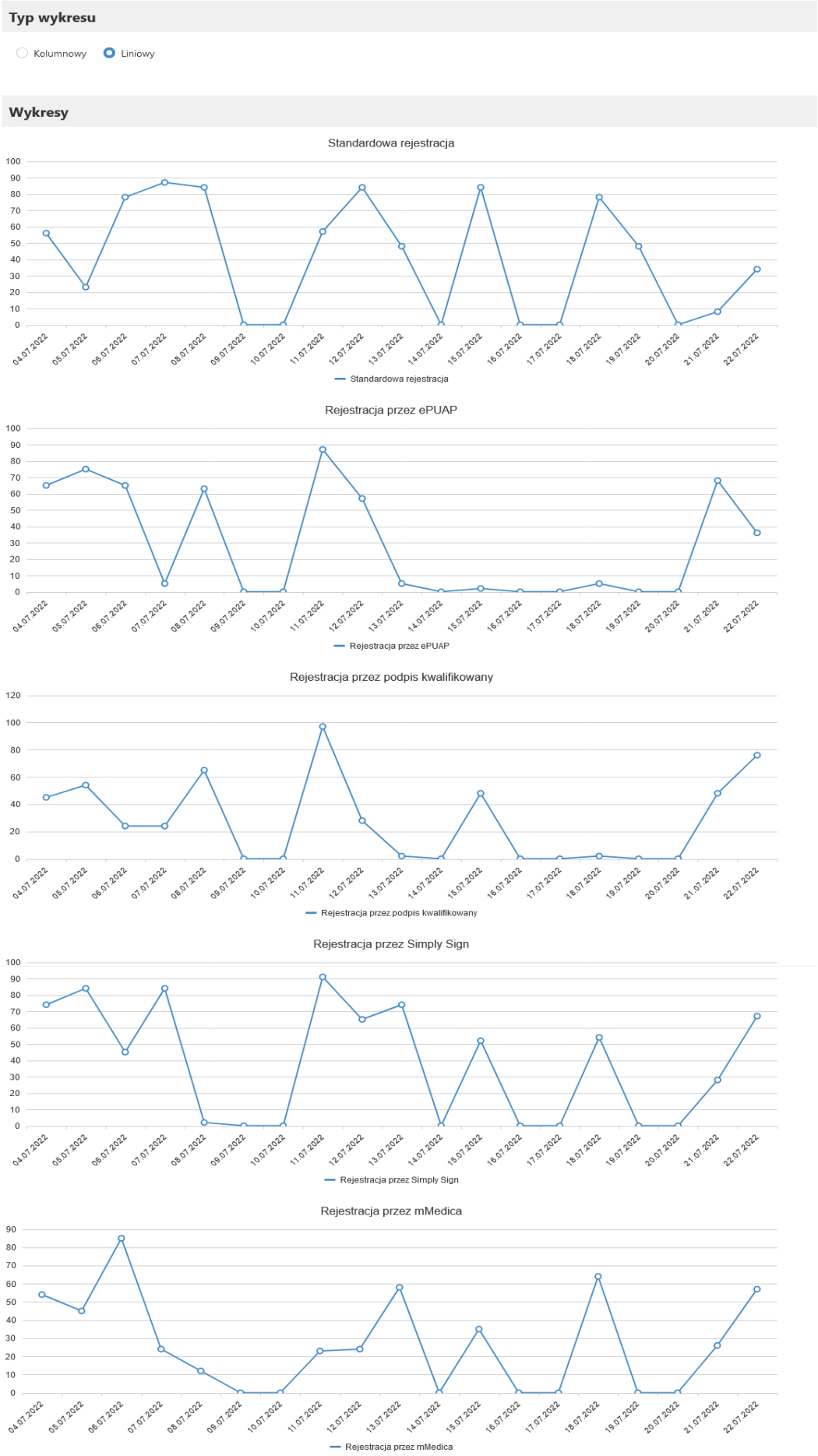
- Standardowa rejestracja (poprzez login i hasło),
- Rejestracja przez ePUAP,
- Rejestracja przez podpis kwalifikowany,
- Rejestracja przez SimplySign,

- Rejestracja przez mMedica.

Wykresy przedstawiają liczbę rejestracji w ciągu poszczególnych dni. Mogą mieć postać kolumnową lub liniową. Aby zmienić rodzaj wykresu należy zaznaczyć odpowiedni znacznik w polu „Typ wykresu”. Znajduje się on na górze strony, bezpośrednio nad wykresami.



Rysunek 205: Statystyki użytkowników - standardowa rejestracja (wykres kolumnowy)



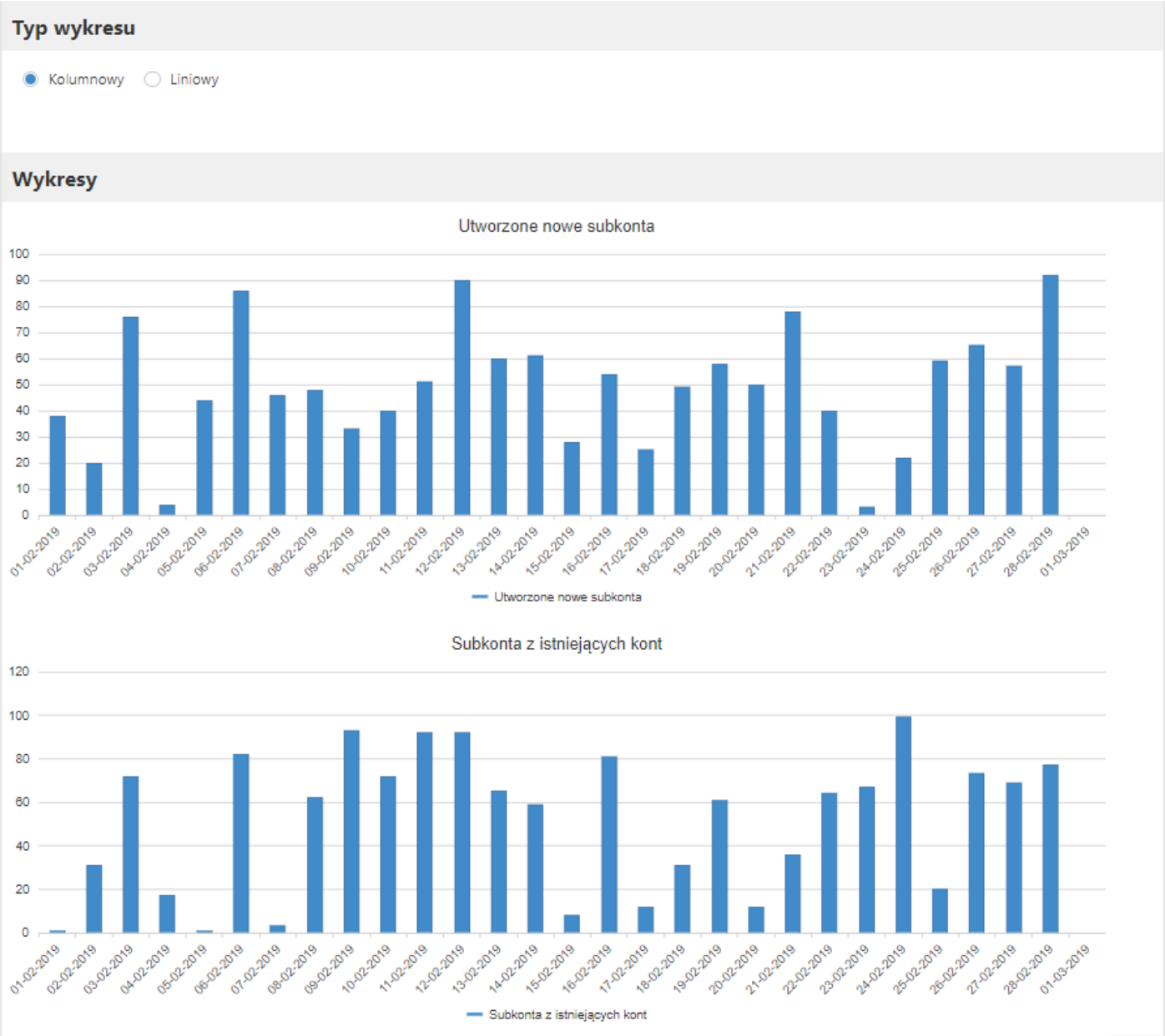
Rysunek 206: Statystyki użytkowników - wykresy liniowe

8.3.12.1.2. Statystyki użytkowników - Utworzone subkonta

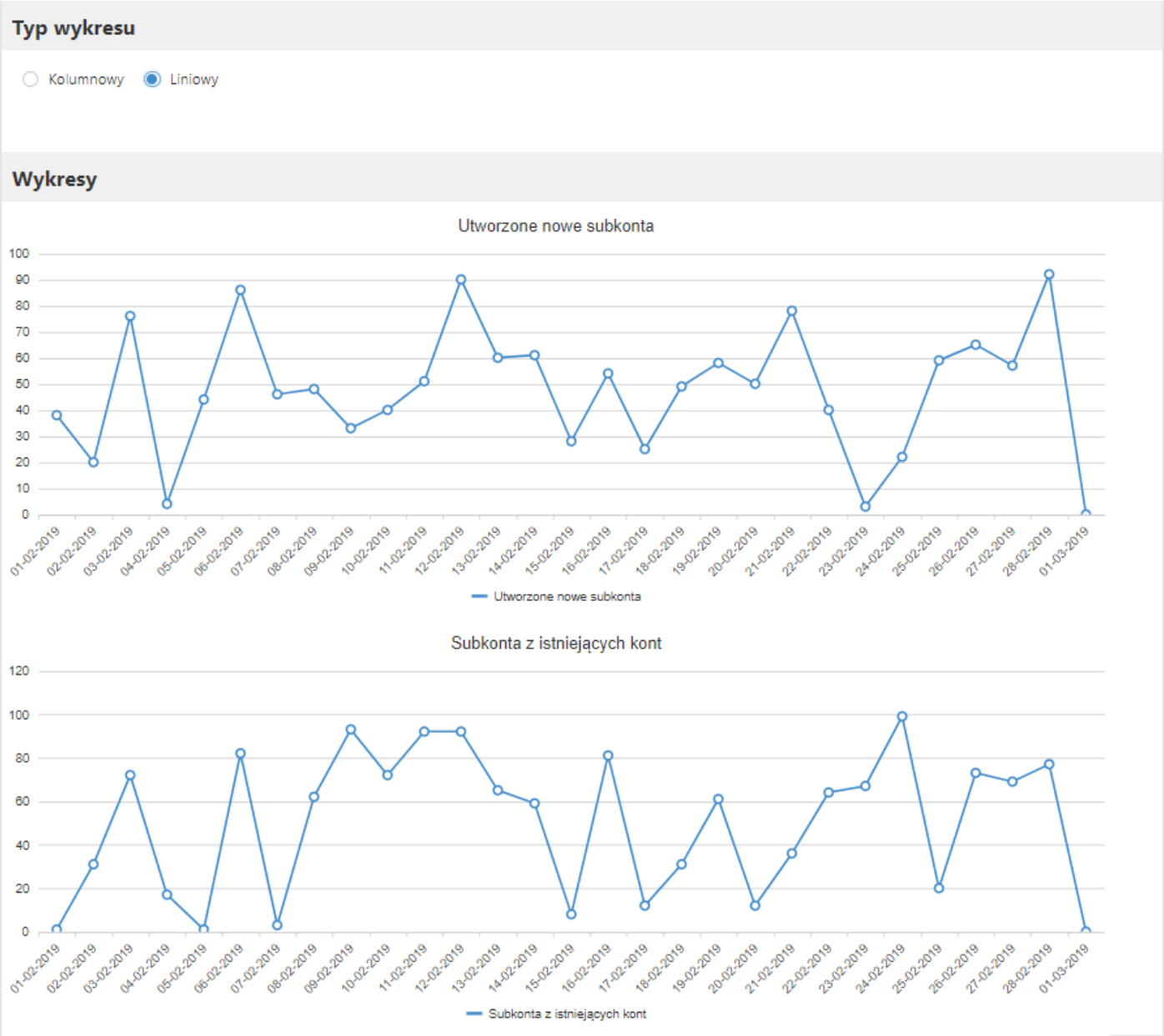
Statystyki utworzonych subkont zawierają informacje o tym, ile subkont zostało utworzonych w Portalu eRejestracja i w jaki sposób:

- Utworzone nowe subkonta – konta utworzone bezpośrednio na profilu rodzica/opiekuna,
- Subkonta z istniejących kont – przypięcie istniejącego niezależnie konta do profilu rodzica/opiekuna.

Wykresy przedstawiają liczbę utworzonych subkont w ciągu poszczególnych dni. Mogą mieć postać kolumnową lub liniową. Aby zmienić rodzaj wykresu należy znaczyć odpowiedni znacznik w polu „Typ wykresu". Znajduje się on na górze strony, bezpośrednio nad wykresami.



Rysunek 207: Statystyki użytkowników - dodane subkonta (wykres kolumnowy)



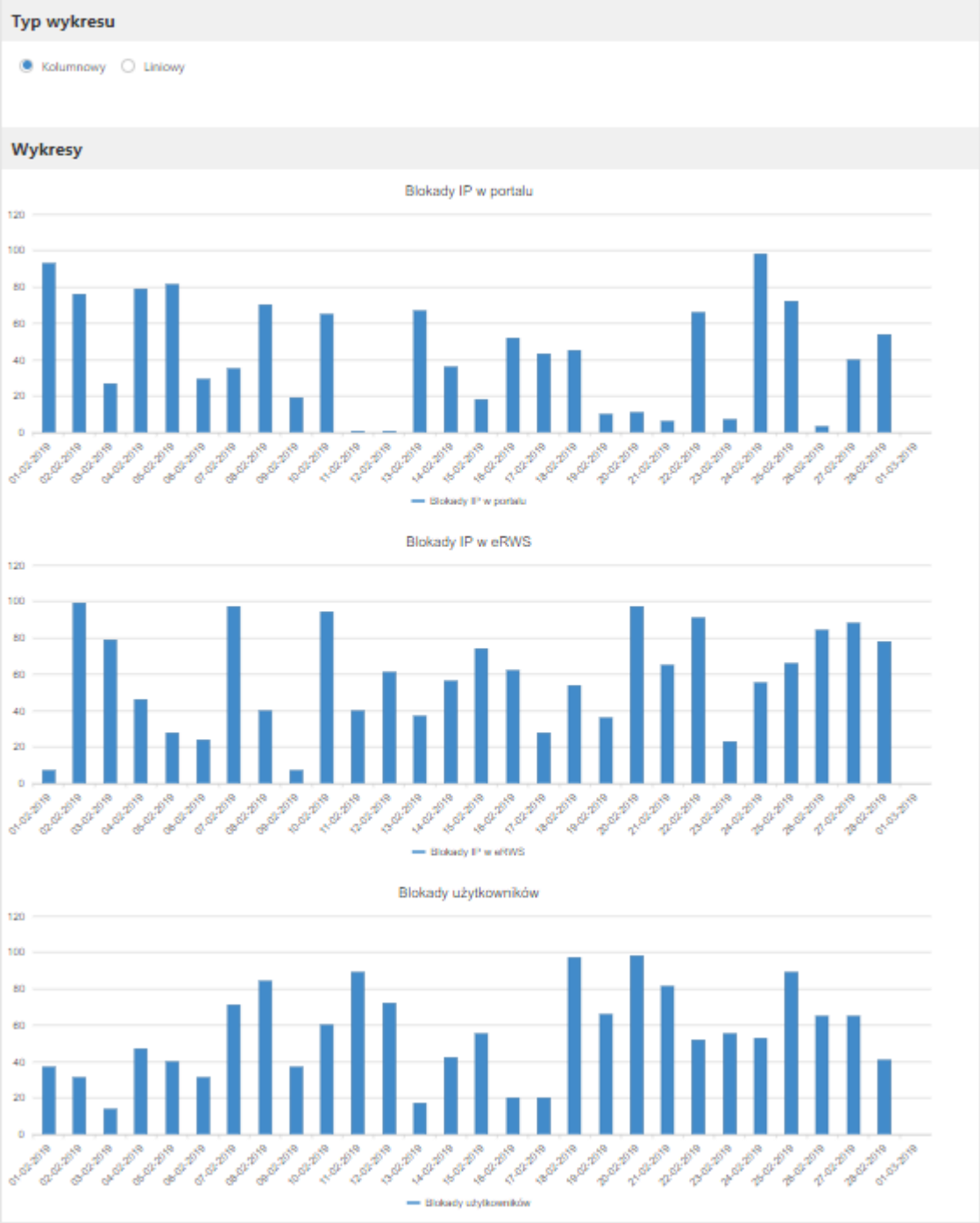
Rysunek 208: Statystyki użytkowników - dodane subkonta (wykres liniowy)

8.3.12.1.3. Statystyki użytkowników – Blokady

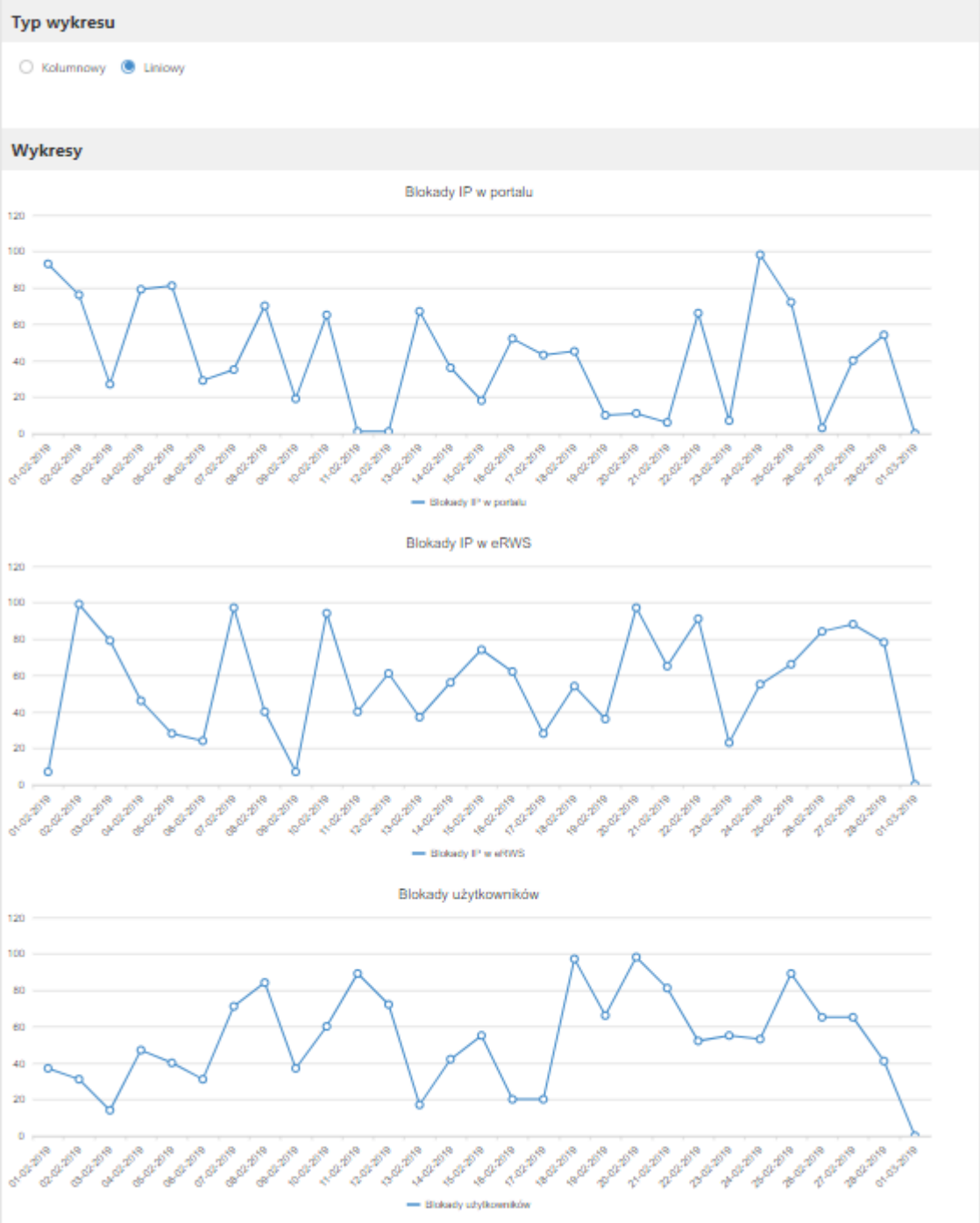
Statystyki blokad zawierają informacje o tym, ile kont i adresów IP zostało zablokowanych i w jaki sposób:

- Blokady IP w portalu – spowodowane zbyt dużą liczbą logowań na nieistniejące w Portalu konto,
- Blokady IP w eRWS – spowodowane zbyt dużą liczbą prób połączenia się z mMWS błędnym tokenem,
- Blokady użytkowników – spowodowane zbyt dużą liczbą błędnych logowań na istniejące konto w Portalu lub ręcznym zablokowaniem konta przez administratora Portalu.

Wykresy przedstawiają liczbę zablokowanych kont/adresów IP w ciągu poszczególnych dni. Mogą mieć postać kolumnową lub liniową. Aby zmienić rodzaj wykresu należy znaczyć odpowiedni znacznik w polu „Typ wykresu”. Znajduje się on na górze strony, bezpośrednio nad wykresami.



Rysunek 209: Statystyki użytkowników - blokady (wykres kolumnowy)



Rysunek 210: Statystyki użytkowników - blokady (wykres liniowy)

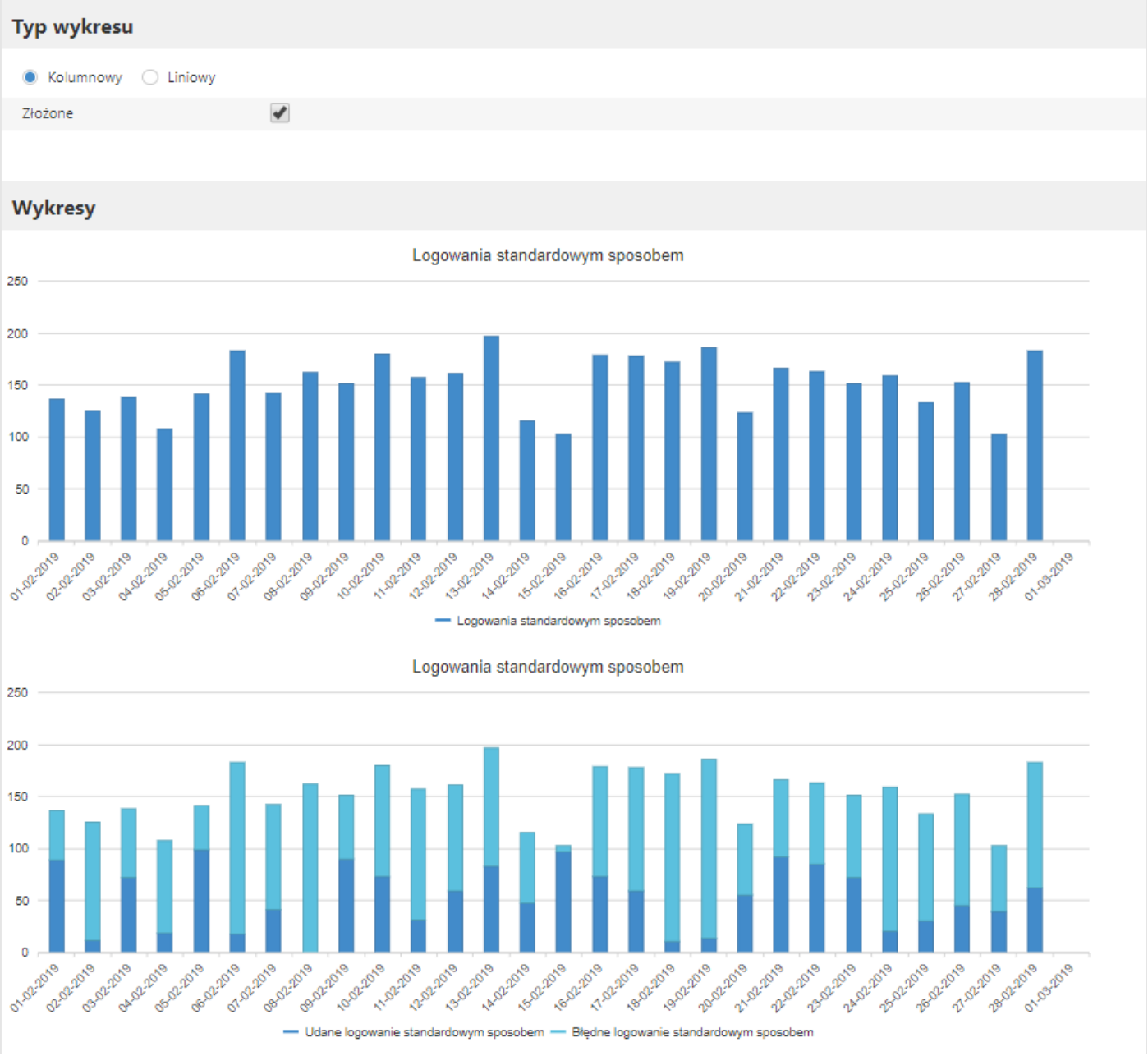
8.3.12.1.4. Statystyki użytkowników – Logowania

Statystyki logowania zawierają informacje o tym ilu użytkowników zalogowało się do Portalu eRejestracja, ilu użytkownikom nie udało się zalogować do Portalu i w jaki sposób się logowali:

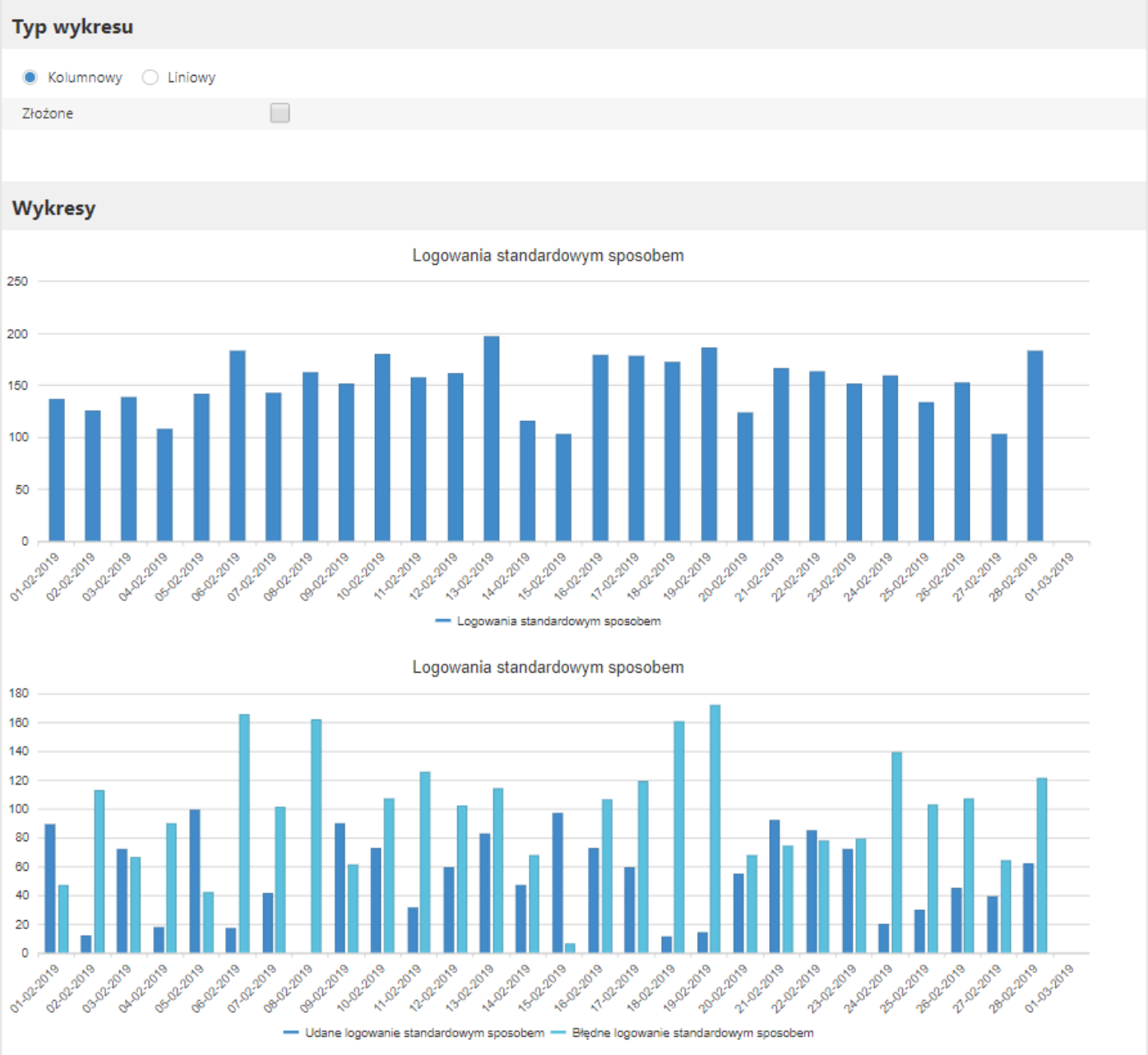
- Logowania standardowym sposobem (poprzez login i hasło),
- Logowania poprzez ePUAP,
- Logowania poprzez podpis kwalifikowany,

- Logowania poprzez SimplySign,
- Logowania poprzez Informacje Medyczne (poprzez aplikację mobilną).

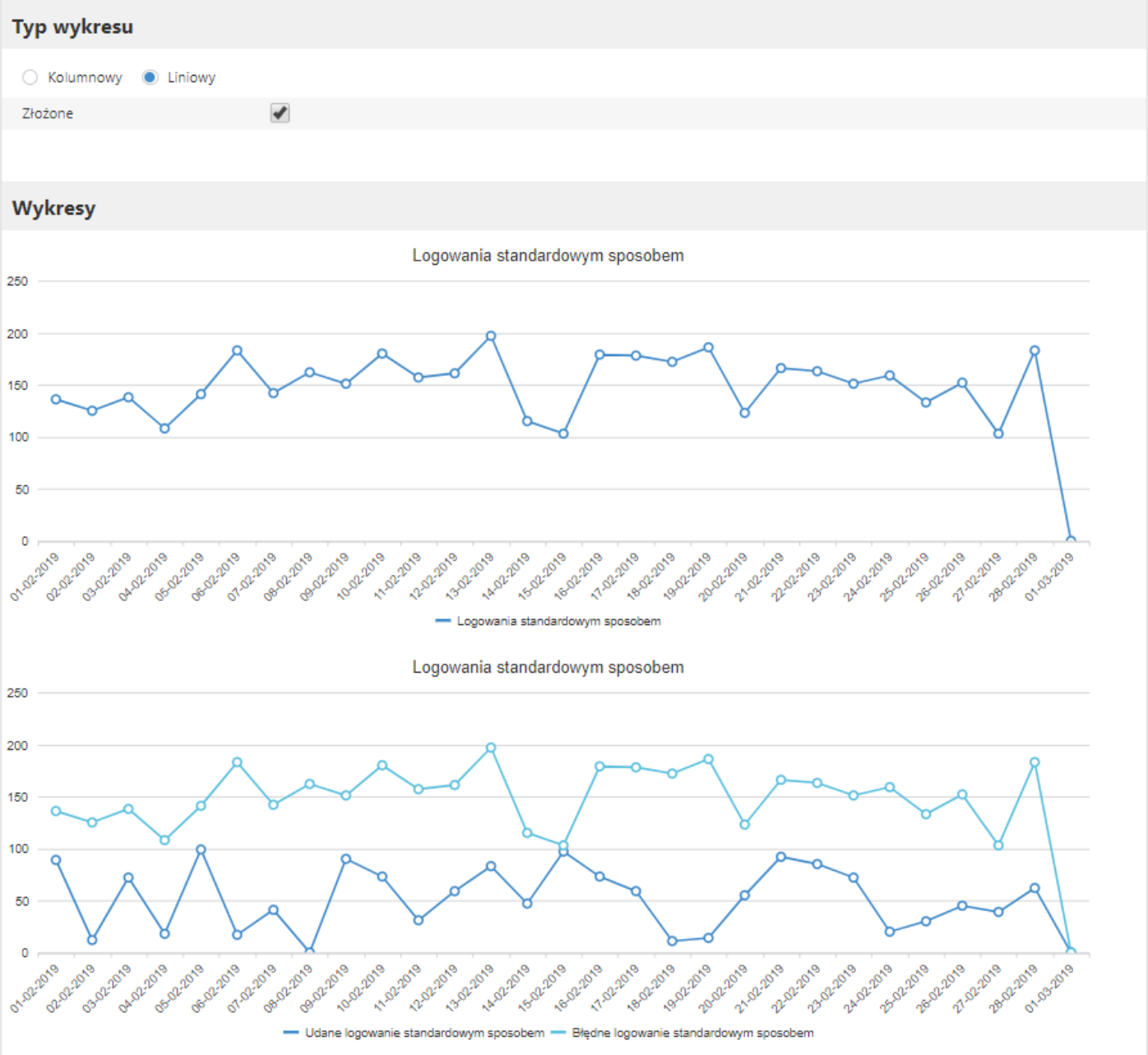
Wykresy przedstawiają liczbę logowań w ciągu poszczególnych dni. Mogą mieć postać kolumnową lub liniową. Aby zmienić rodzaj wykresu należy zaznaczyć odpowiedni znacznik w polu „Typ wykresu". Dodatkowo wykresy poprawnych i błędnych logowań mogą być złożone razem lub przedstawione oddzielnie. Aby wykresy były pokazywane oddzielnie należy odznaczyć pole „Złożone". Ustawienia wykresów znajdują się na górze strony, bezpośrednio nad wykresami.



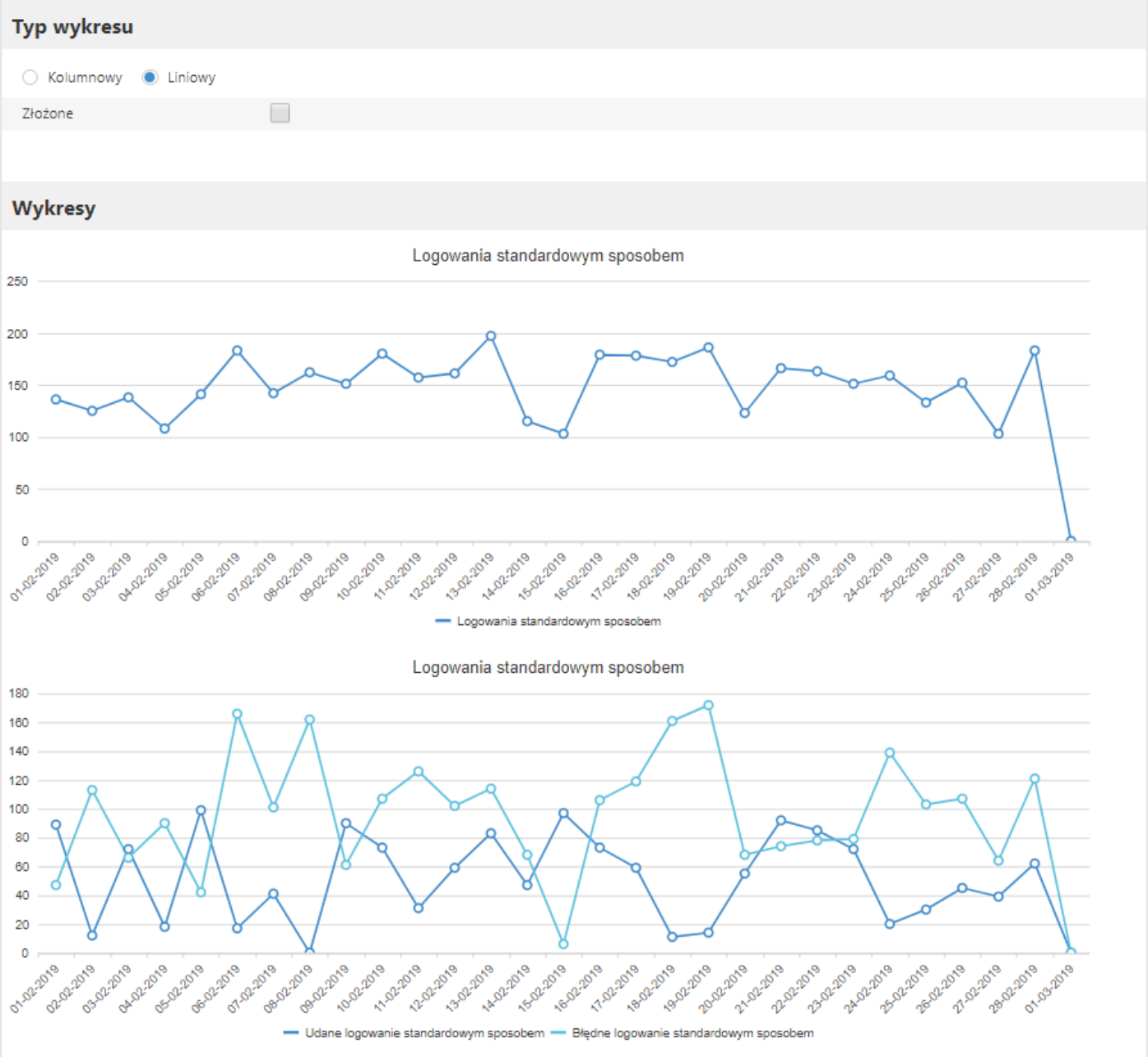
Rysunek 211: Statystyki użytkowników - logowania standardowym sposobem (wykres kolumnowy złożony)



Rysunek 212: Statystyki użytkowników - logowanie standardowym sposobem (wykres kolumnowy)

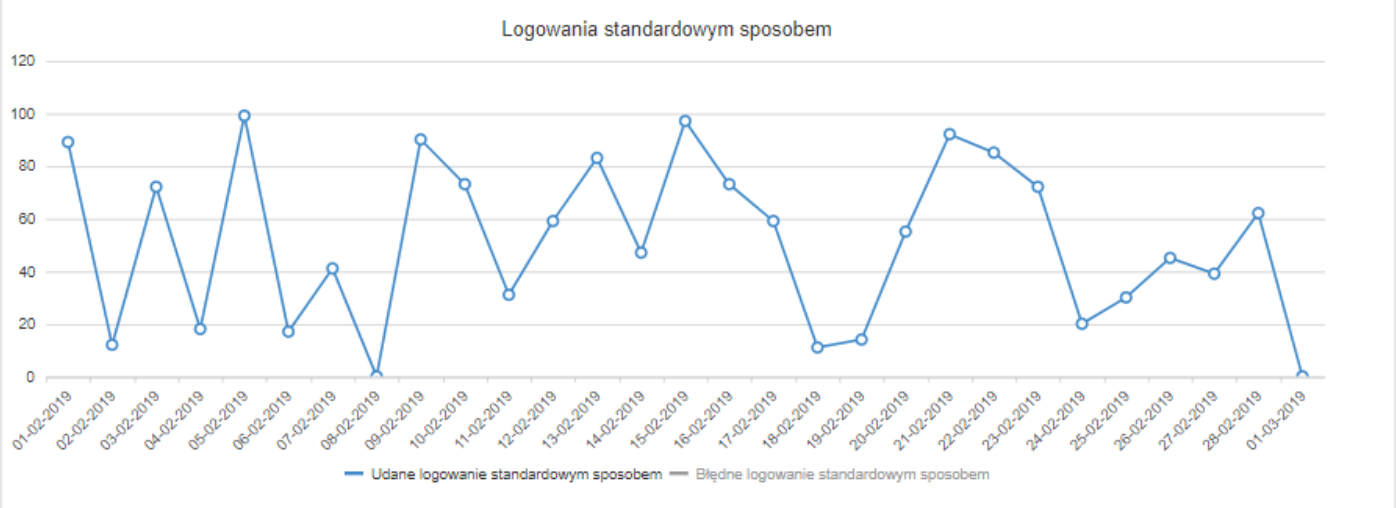


Rysunek 213: Statystyki użytkowników - logowania standardowym sposobem (wykres liniowy złożony)



Rysunek 214: Statystyki użytkowników - logowania standardowym sposobem (wykres liniowy)

Istnieje możliwość ukrywania wykresów. Aby to zrobić należy kliknąć na podpis danego wykresu w legendzie.



Rysunek 215: Wykres logowania standardowym sposobem - wyłączony wykres błędnych logowań

8.3.12.1.5. Statystyki użytkowników – Wszystkie

Statystyki wszystkie zawierają zebrane w jednym miejscu wszystkie informacje dotyczące użytkowników. Wykresy i tabelki podzielone są na cztery główne kategorie:

- Statystyki logowań,
- Statystyki rejestracji,
- Statystyki tworzenia subkont,
- Statystyki blokad.

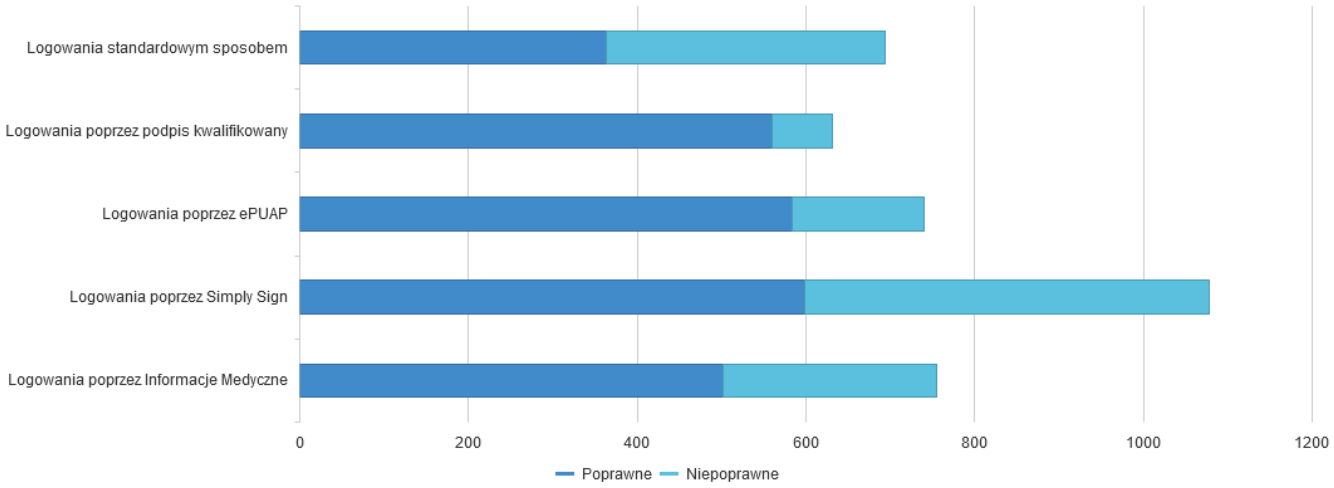
Dane przedstawione są w formie tabel oraz poziomych wykresów kolumnowych. Wykresy statystyk logowań i statystyk rejestracji mogą być złożone razem lub przedstawione oddzielnie. Aby wykresy były pokazywane oddzielnie należy odznaczyć pole „Złożone”. Ustawienia wykresów znajdują się na górze strony, bezpośrednio nad wykresami.

Typ wykresu

☑ Złożone

Statystyki logowań

	Wszystkie	Poprawne	Niepoprawne
Logowania standardowym sposobem	693	363	330
Logowania poprzez podpis kwalifikowany	631	560	71
Logowania poprzez ePUAP	739	583	156
Logowania poprzez Simply Sign	1077	598	479
Logowania poprzez Informacje Medyczne	754	501	253
Sumarycznie	3894	2605	1289



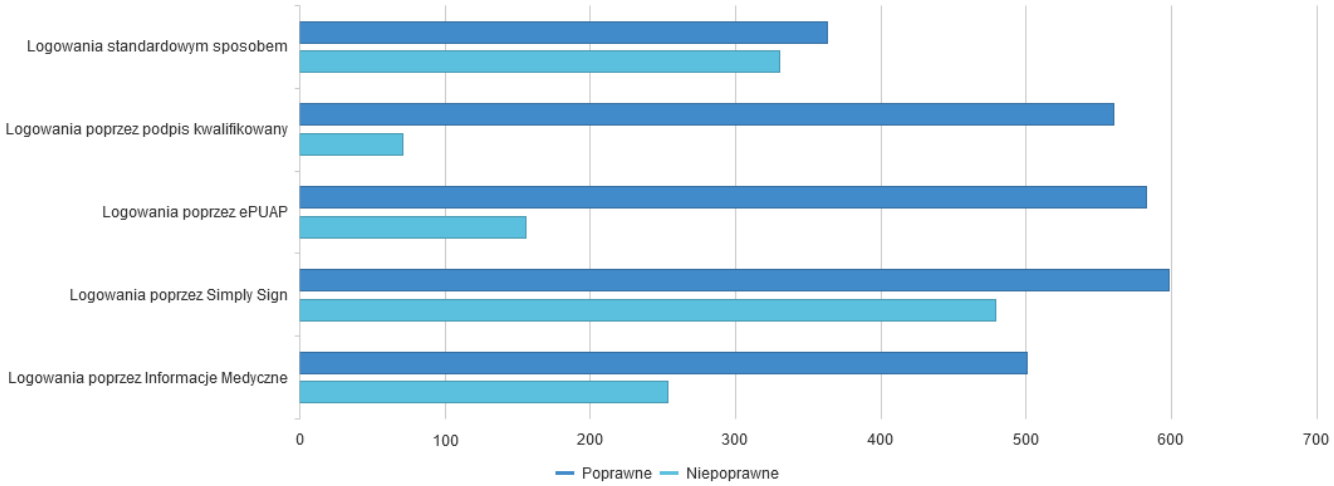
Rysunek 216: Statystyki użytkowników – wszystkie: logowania (wykres poziomy kolumnowy złożony)

Typ wykresu

☐ Złożone

Statystyki logowań

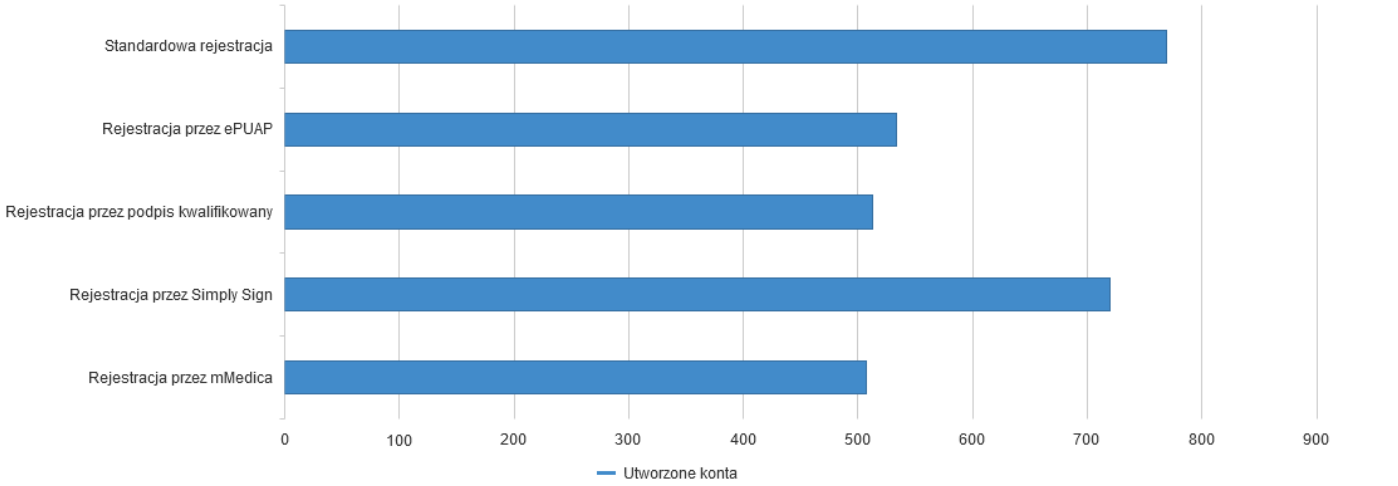
	Wszystkie	Poprawne	Niepoprawne
Logowania standardowym sposobem	693	363	330
Logowania poprzez podpis kwalifikowany	631	560	71
Logowania poprzez ePUAP	739	583	156
Logowania poprzez Simply Sign	1077	598	479
Logowania poprzez Informacje Medyczne	754	501	253
Sumarycznie	3894	2605	1289



Rysunek 217: Statystyki użytkowników – wszystkie: logowania (wykres poziomy kolumnowy)

Statystyki rejestracji

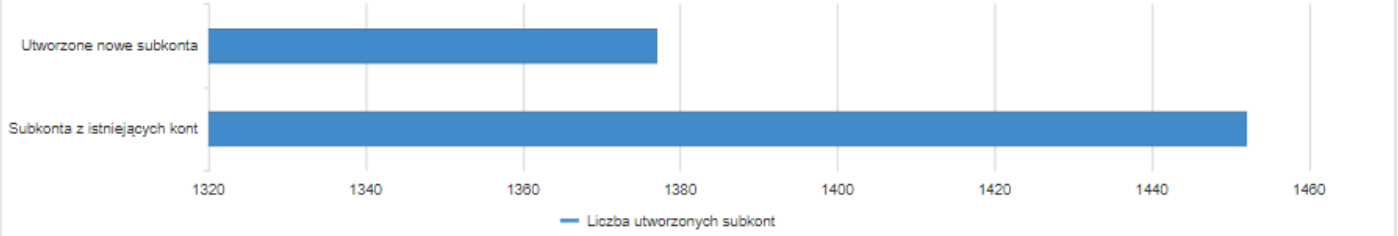
Standardowa rejestracja	769
Rejestracja przez podpis kwalifikowany	513
Rejestracja przez ePUAP	533
Rejestracja przez Simply Sign	720
Rejestracja przez mMedica	507
Sumarycznie	3042



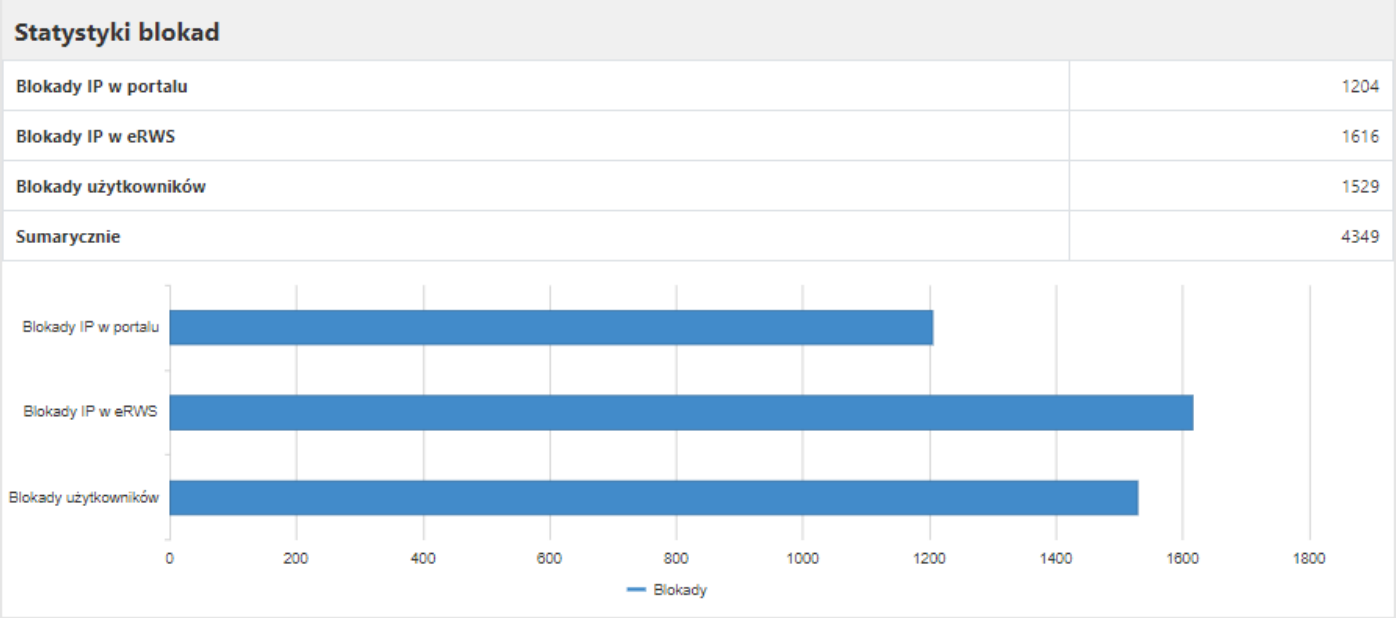
Rysunek 218: Statystyki użytkowników – wszystkie: rejestracje (wykres poziomy kolumnowy złożony)

Statystyki tworzenia subkont

Utworzone nowe subkonta	1377
Subkonta z istniejących kont	1452
Sumarycznie	2829



Rysunek 219: Statystyki użytkowników – wszystkie: utworzone subkonta (wykres poziomy kolumnowy)



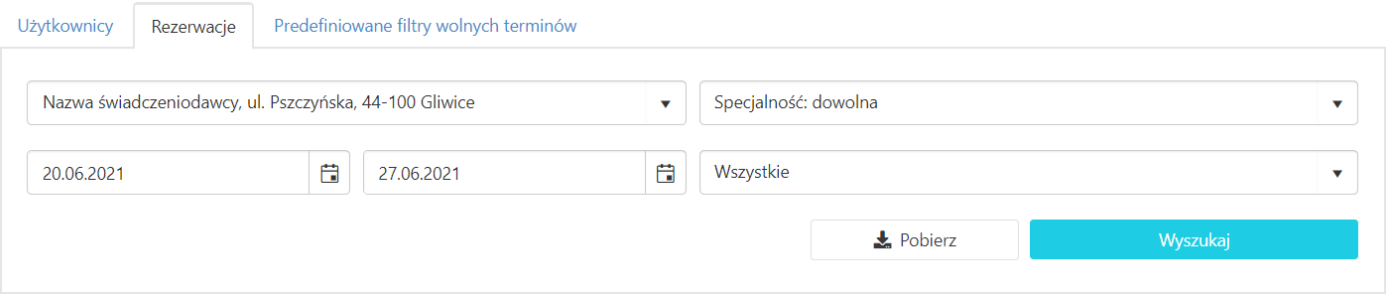
Rysunek 220: Statystyki użytkowników – wszystkie: blokady (wykres poziomy kolumnowy)

8.3.12.2. Rezerwacje

Z dostępnych na górze strony filtrów można wybrać rodzaj statystyk do wyświetlenia. Dostępne są:

- Wolne terminy,
- Wizyty receptowe,
- Wszystkie.

Dodatkowo można wybrać zakres dat oraz specjalność, dla których mają wyświetlać się wybrane statystyki. Po ustawieniu filtrów należy kliknąć „Wyszukaj”. Przycisk „Pobierz” służy do pobrania statystyk w formacie csv.



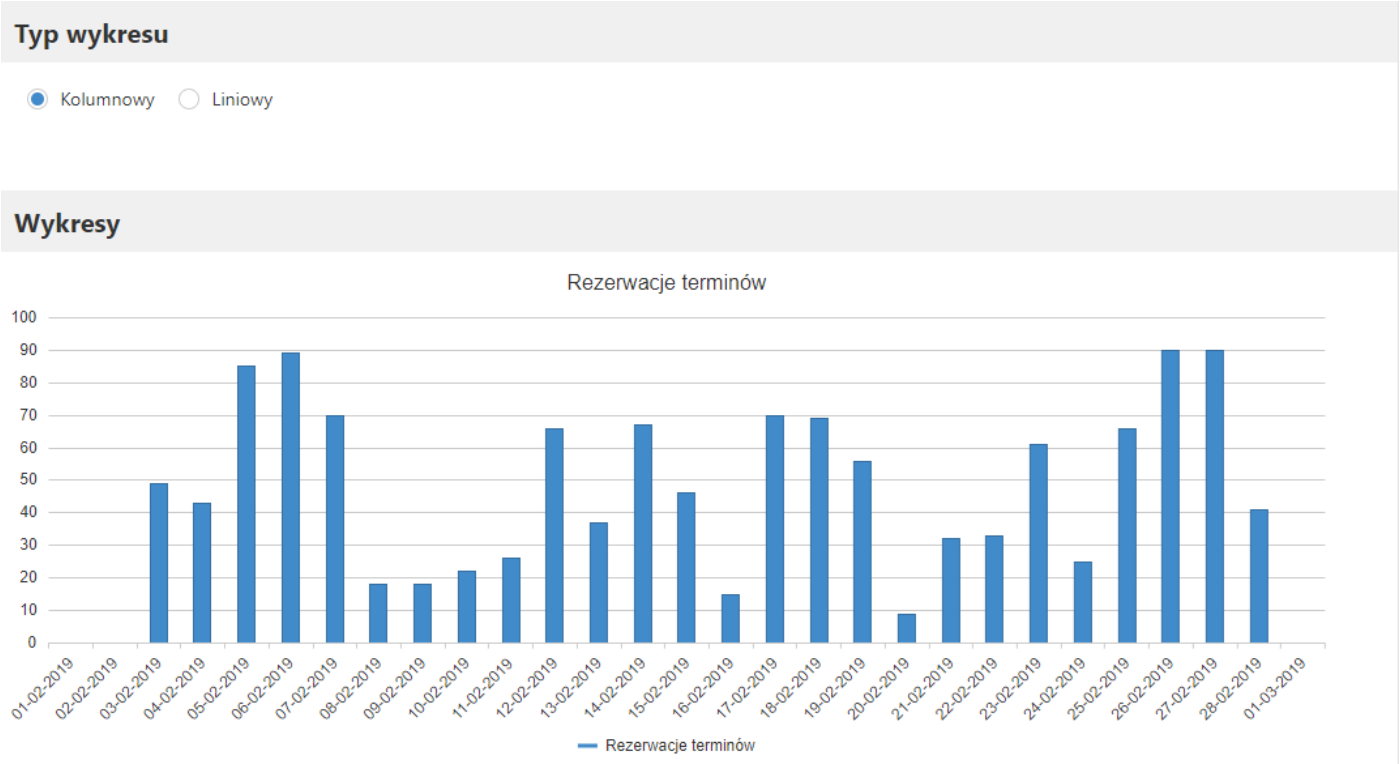
Rysunek 221: Statystyki rezerwacji

8.3.12.2.1. Statystyki rezerwacji - Wolne terminy

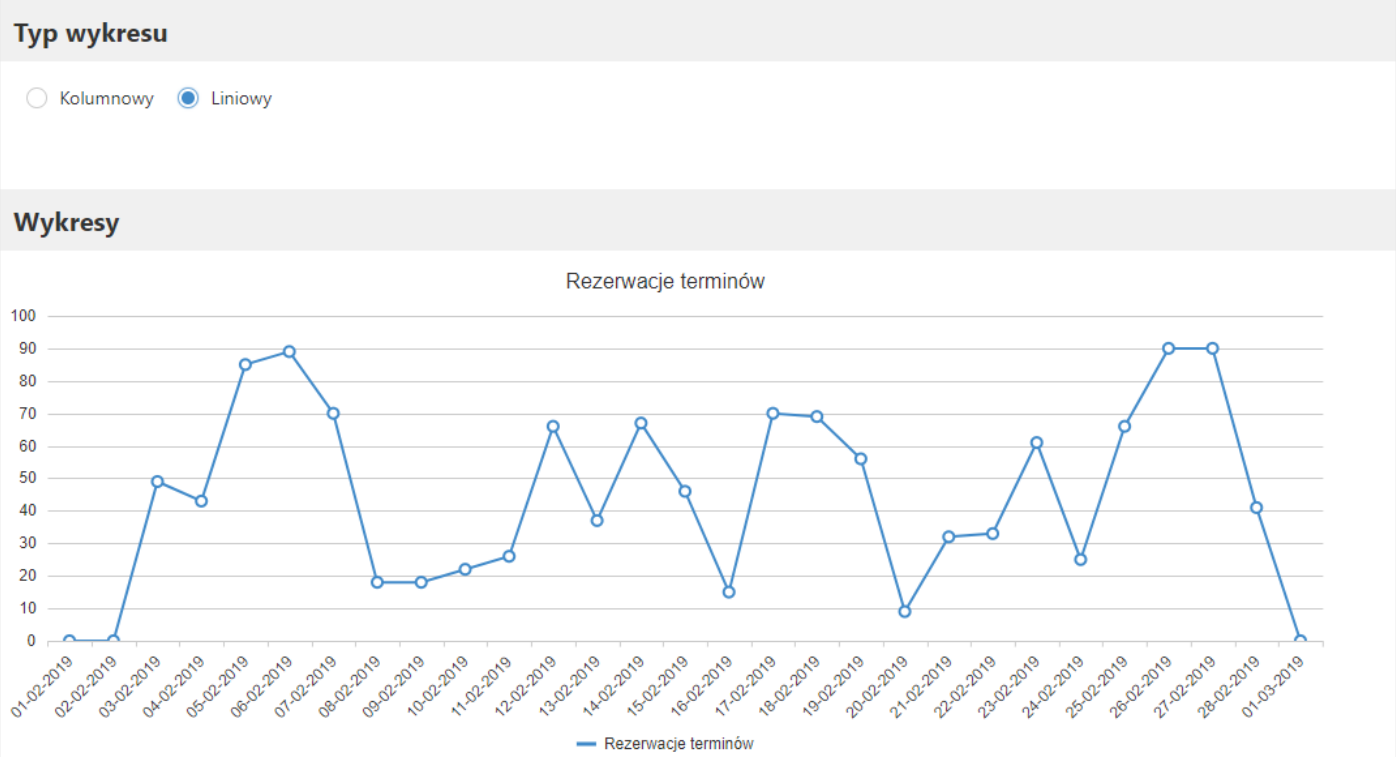
Statystyki wolnych terminów zawierają informacje o tym, ile wizyt dla danych specjalizacji zostało zarezerwowanych, zmienianych i odwołanych:

- Rezerwacje terminów – rezerwacje wizyt przez użytkowników,
- Zmiany terminów – zmiany terminów wizyt przez użytkowników,
- Anulowane terminy – anulowania wizyt przez użytkowników,
- Rezerwacje wizyt przez personel.

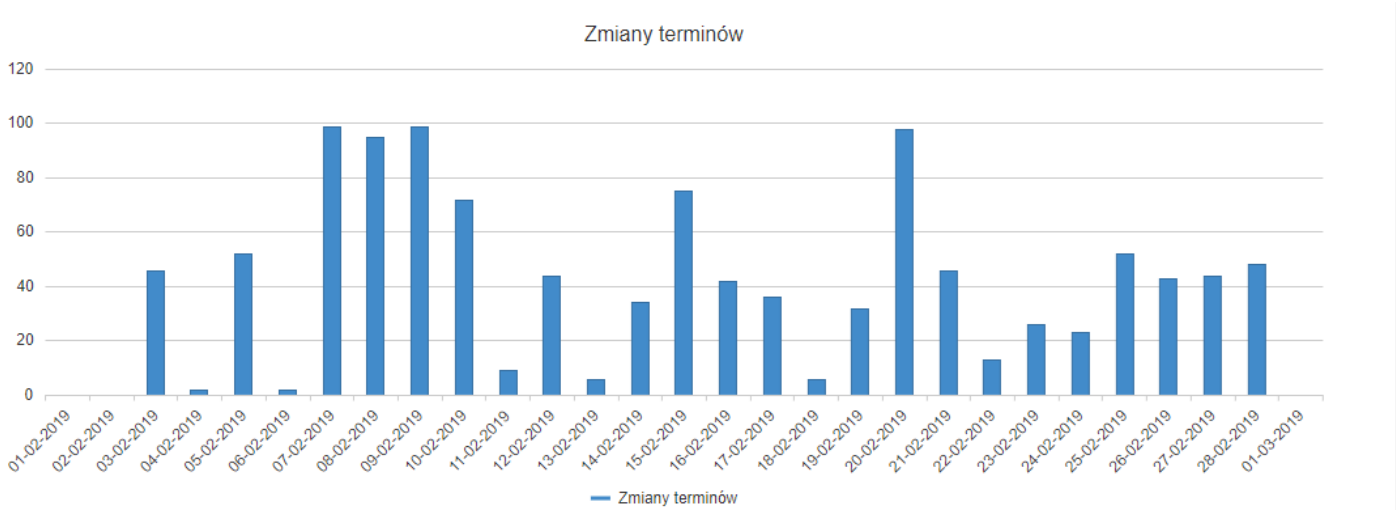
Wykresy przedstawiają liczbę zarezerwowanych/zmienionych/odwołanych terminów wizyt w ciągu poszczególnych dni. Mogą mieć postać kolumnową lub liniową. Aby zmienić rodzaj wykresu należy zaznaczyć odpowiedni znacznik w polu „Typ wykresu". Znajduje się on na górze strony, bezpośrednio nad wykresami.



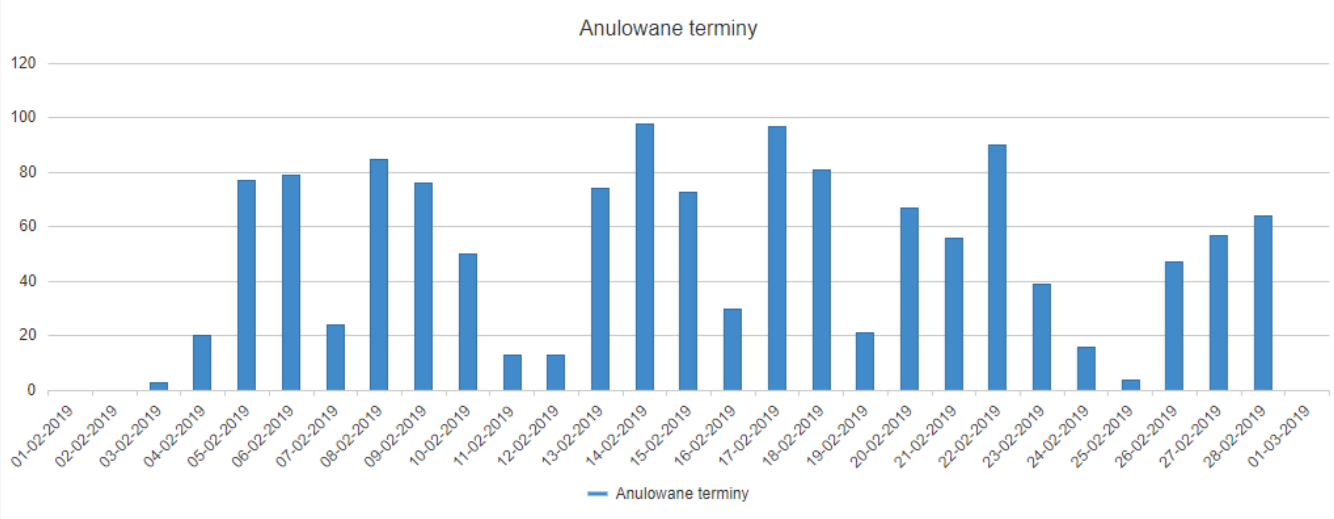
Rysunek 222: Statystyki rezerwacji - rezerwacje terminów (wykres kolumnowy)



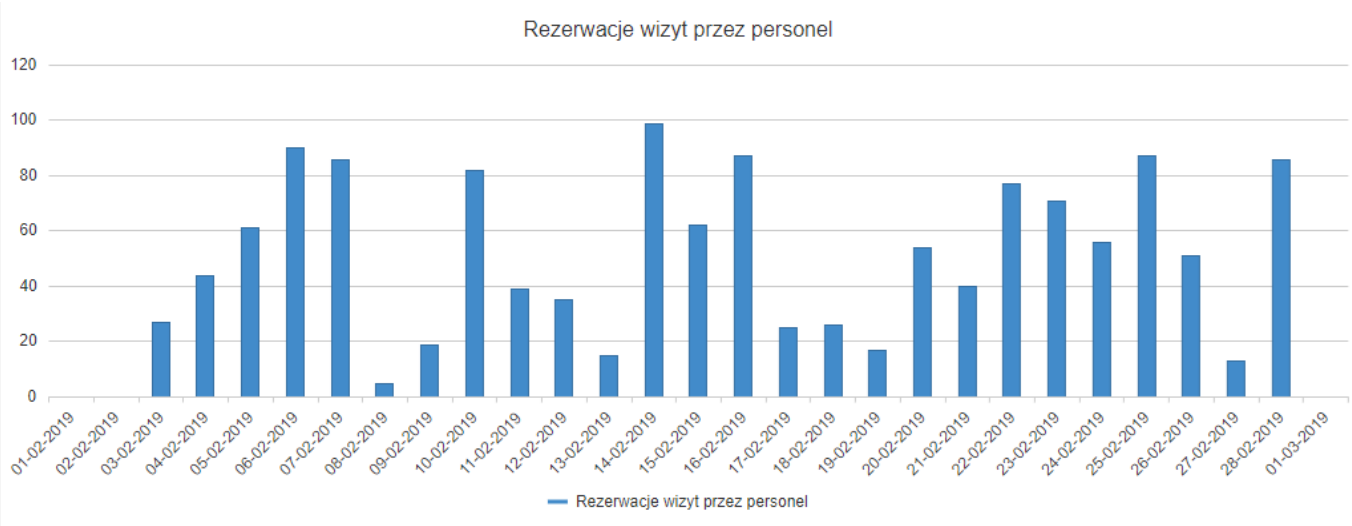
Rysunek 223: Statystyki rezerwacji - rezerwacje terminów (wykres liniowy)



Rysunek 224: Statystyki rezerwacji - zmiany terminów (wykres kolumnowy)



Rysunek 225: Statystyki rezerwacji – anulowane terminy (wykres kolumnowy)



Rysunek 226: Statystyki rezerwacji - rezerwacje wizyt przez personel (wykres kolumnowy)

8.3.12.2.2. Statystyki rezerwacji - Wizyty receptowe

Statystyki wizyt receptowych zawierają informacje o tym, ile recept dla danych specjalizacji zostało zamówionych, a z ilu zrezygnowano:

- Zamówione wizyty receptowe,
- Anulowane wizyty receptowe.

Wykresy przedstawiają liczbę zamówionych/anulowanych recept w ciągu poszczególnych dni. Mogą mieć postać kolumnową lub liniową. Aby zmienić rodzaj wykresu należy znaczyć odpowiedni znacznik w polu „Typ wykresu”. Znajduje się on na górze strony, bezpośrednio nad wykresami.

Typ wykresu

Kolumnowy Liniowy

Wykresy

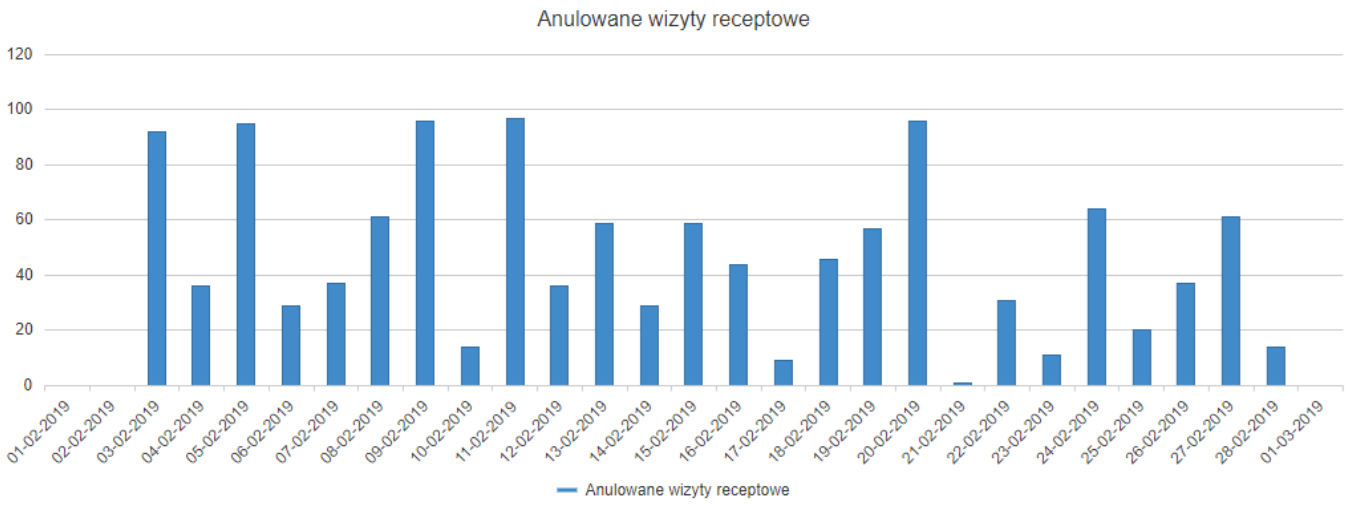
Rysunek 227: Statystyki rezerwacji – zamówione wizyty receptowe (wykres kolumnowy)

Typ wykresu

Kolumnowy Liniowy

Wykresy

Rysunek 228: Statystyki rezerwacji – zamówione wizyty receptowe (wykres liniowy)



Rysunek 229: Statystyki rezerwacji – anulowane wizyty receptowe (wykres kolumnowy)

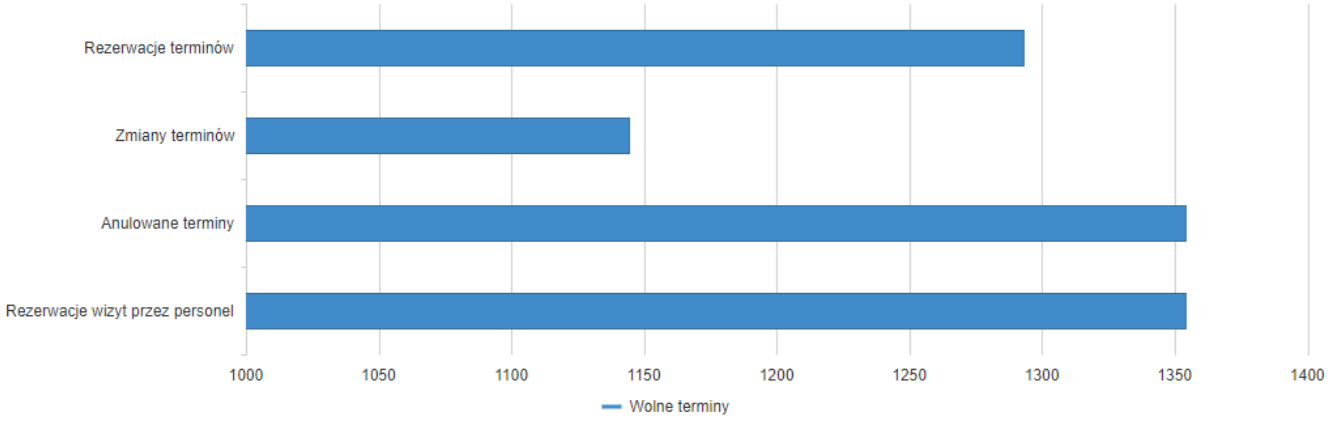
8.3.12.2.3. Statystyki rezerwacji – Wszystkie

Statystyki wszystkie zawierają zebrane w jednym miejscu wszystkie informacje dotyczące rezerwacji wizyt. Wykresy i tabelki podzielone są na dwie kategorie:

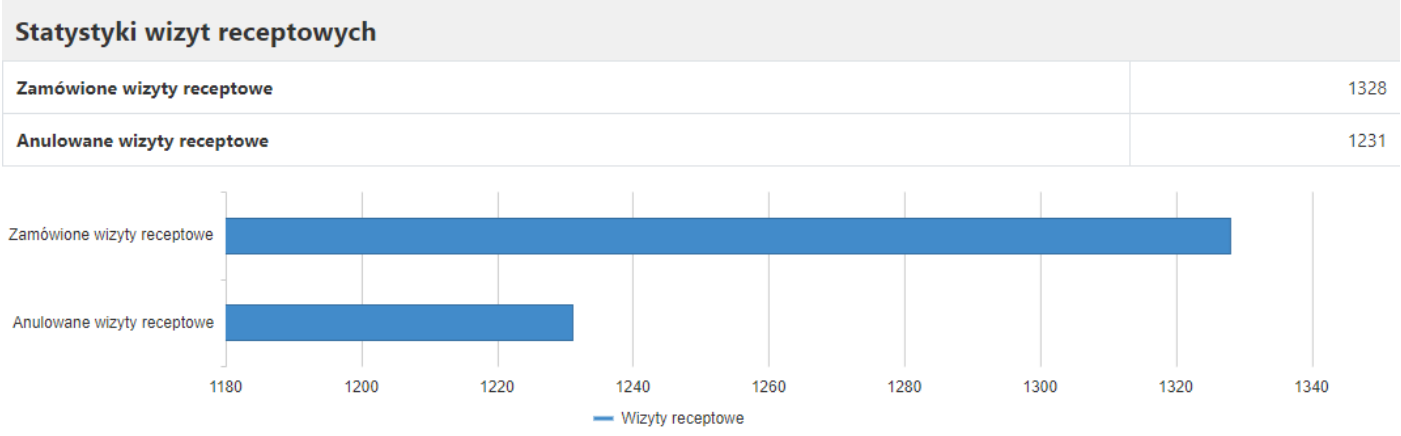
- Statystyki wolnych terminów,
- Statystyki wizyt receptowych.

Dane przedstawione są w formie tabel oraz poziomych wykresów kolumnowych.

Statystyki wolnych terminów	
Rezerwacje terminów	1293
Zmiany terminów	1144
Anulowane terminy	1354
Rezerwacje wizyt przez personel	1354



Rysunek 230: Statystyki rezerwacji – wszystkie: wolne terminy (wykres poziomy kolumnowy)

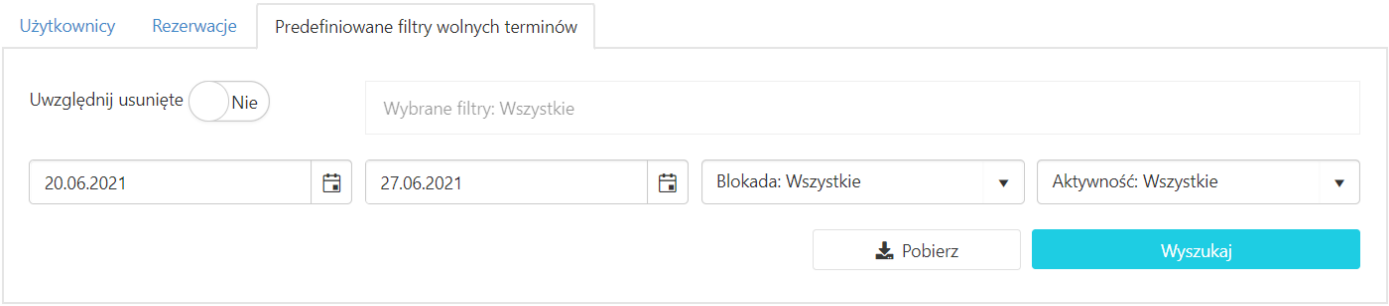


Rysunek 231: Statystyki rezerwacji – wszystkie: wizyty receptowe (wykres poziomy kolumnowy)

8.3.12.3. Predefiniowane filtry wolnych terminów

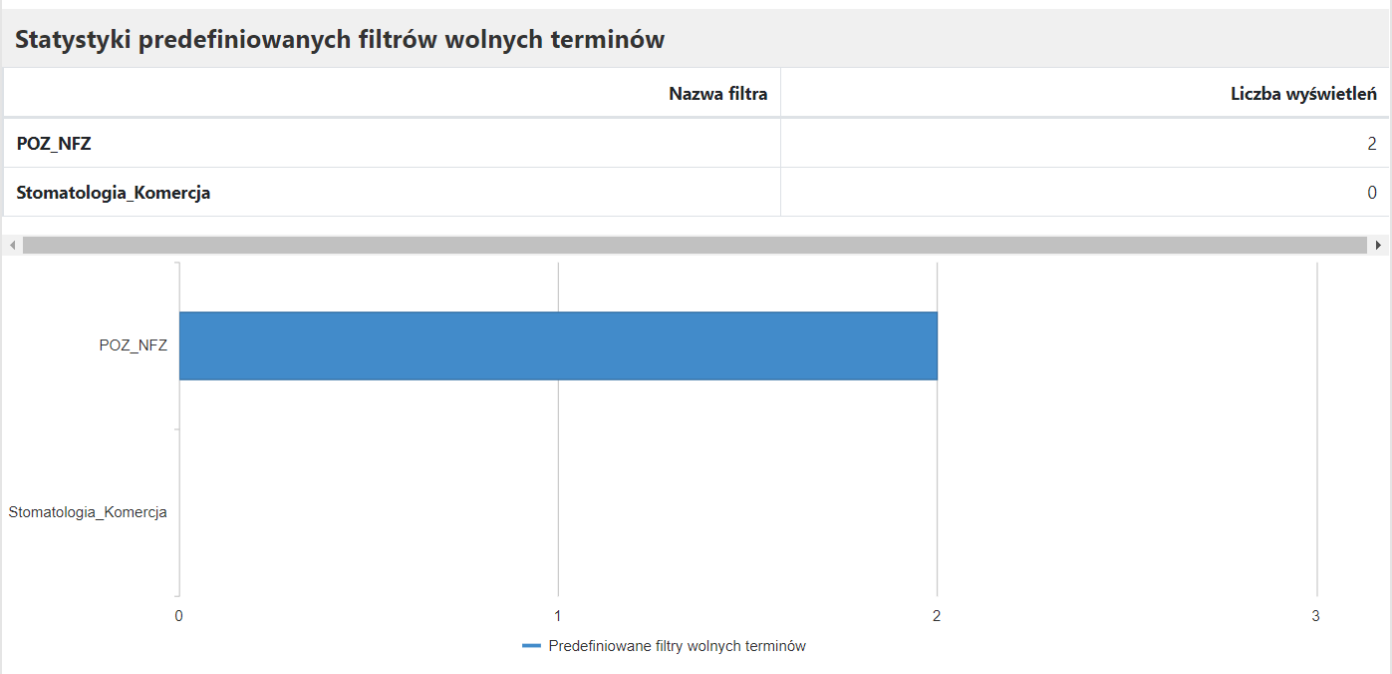
Statystyki predefiniowanych filtrów wolnych terminów zawierają informacje o liczbie wejść na utworzone przez administratora odnośniki predefiniowanych filtrów wolnych terminów.

Zestaw filtrów na górze strony pozwala wybrać predefiniowane nazwy filtrów, które mają zostać uwzględnione oraz ich stan (usunięte, blokada oraz aktywności). Dodatkowo można wybrać zakres dla których mają wyświetlać się wybrane statystyki.



Rysunek 232: Statystyki predefiniowanych filtrów wolnych terminów

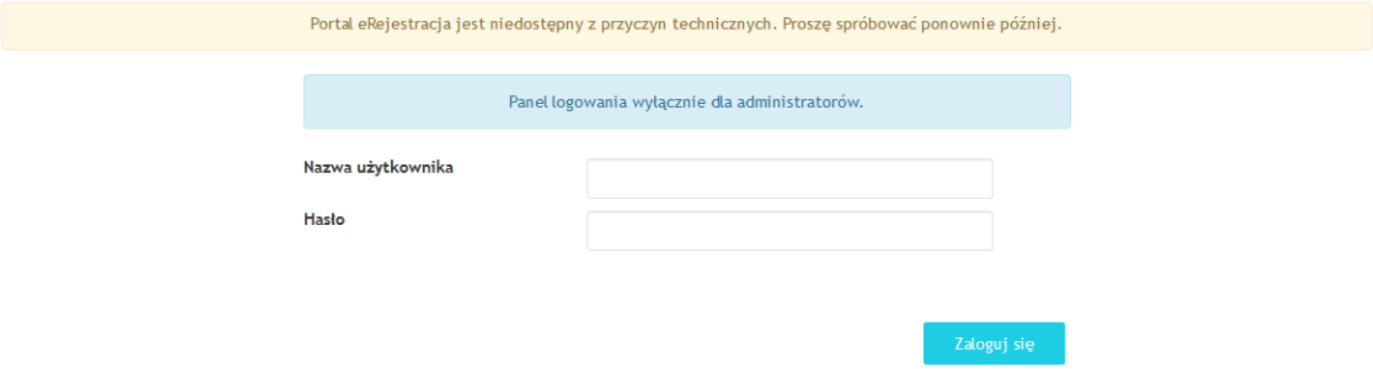
Po ustawieniu filtrów należy kliknąć „Wyszukaj”. Przycisk „Pobierz” służy do pobrania statystyk w formacie csv.



Rysunek 233: Wykres statystyk predefiniowanych filtrów wolnych terminów

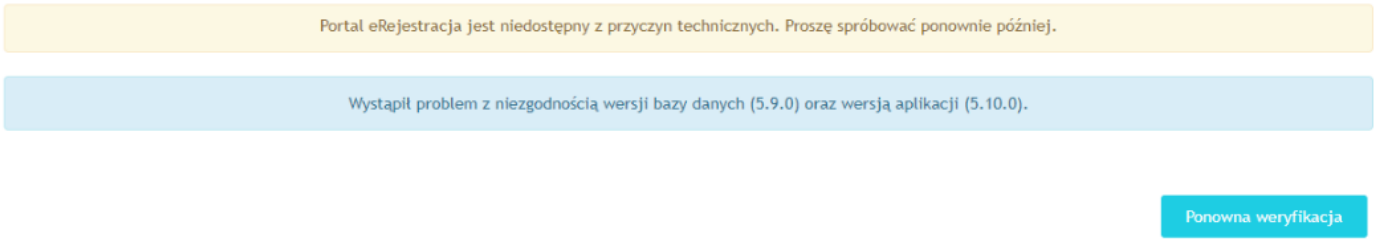
8.4. Niezgodność wersji bazy danych z wersją aplikacji

W celu uniknięcia powstawania błędów oraz konfliktów w eRejestracji został dodany mechanizm sprawdzający, czy wersja bazy danych eRejestracji oraz jej wersja aplikacji jest są takie same. Dopóki istnieje ich zgodność, portal może być normalnie użytkowany, w przeciwnym wypadku zostaje on w całości zablokowany.



Rysunek 234: Niezgodność wersji aplikacji z bazą danych – konto administratora

Niezgodność wersji powinna zostać rozwiązana poprzez zainstalowanie najnowszej wersji programu eRejestracja oraz odpowiadającej jej wersji bazy danych. Po dokonaniu tej czynności należy w Portalu eR użyć opcji „Ponowna weryfikacja”. Jeśli problem został rozwiązany, portal zostanie odblokowany.



Rysunek 235: Niezgodność wersji aplikacji z bazą danych – użytkownik niezalogowany

8.5. Konfiguracja ePUAP\PZ

Moduł eRejestracja może być skonfigurowany do połączenia z portalem ePUAP\PZ. Umożliwia to powiązanie konta eR z kontem ePUAP\PZ, logowanie i zakładanie konta w Portalu eR za pomocą ePUAP\PZ. Oznacza to, że moduł eR będzie miał uprawnienia pobierania danych osobowych z zatwierdzonych urzędowo profili zaufanych użytkowników. PZ, czyli Profil Zaufany, to wydzielona część platformy ePUAP, służąca do logowania użytkowników oraz wykonywania operacji podpisu elektronicznego.

Moduł eR można skonfigurować tak, aby łączył się ze środowiskiem produkcyjnym (bazującym na prawdziwych danych) lub testowym ePUAP\PZ. Docelowo powinno zostać wybrane środowisko produkcyjne. Wybór środowiska dokonuje się w konfiguracji ogólnej za pomocą parametru „Typ konfiguracji ePUAP\PZ" (patrz: *8.3.9.1.1. Konfiguracja ogólna*). Adresy portali:

a) Środowisko produkcyjne:
   - Portal ePUAP: https://epuap.gov.pl
   - Portal PZ: https://pz.gov.pl

b) Środowisko testowe (integracyjne):
   - Portal ePUAP: https://int.epuap.gov.pl
   - Portal PZ: https://int.pz.gov.pl

Pozostałe parametry konfiguracyjne zostały opisane w . *Obsługa teleporad* – aktywacja tej opcji pozwala na wykonywanie wizyt za pomocą między innymi następujących kanałów komunikacji: telefon, Skype, WhatsApp, wideorozmowa.

> **Uwaga:** Funkcjonalność wymaga modułu Teleporada. Do obsługi teleporad wymagana jest konfiguracja harmonogramów użyciem predefiniowanego miejsca „Teleporada" (kod „TELE") w mMedica. Grafik trybu offline nie wspiera obsługi teleporad.

Integracja z serwisem Gdzie Po Lek – aktywacja tej opcji pozwala na wyszukanie dostępności leku za pomocą kodu EAN przez serwis gdziepolek.pl w funkcjonalnościach użytkownika związanych z zamawianiem recept, wystawionymi eReceptami oraz historią zamówionych recept.

Obsługa eAnkiet – uruchomienie funkcjonalności pozwala na tworzenie eAnkiet dla użytkowników po zalogowaniu lub po rezerwacji terminu na podstawie skonfigurowanych akcji ankietowych. Dodatkowo umożliwia użytkownikom przeglądanie utworzonych eAnkiet.

Uwaga: Funkcjonalność wymaga modułu eAnkiety oraz pobranej konfiguracji połączenia do Chmury dla zdrowia z mMedica.

Konfiguracja ePUAP\PZ.

Przed przystąpieniem do konfiguracji należy zapoznać się z *8.5.1. Podmiot publiczny ePUAP oraz uprawnienia dla środowiska produkcyjnego*, *8.5.2. Konfiguracja w Portalu eRejestracja.*

8.5.1. Podmiot publiczny ePUAP oraz uprawnienia dla środowiska produkcyjnego

Proces utworzenia konta Podmiotu Publicznego oraz uzyskania wymaganych uprawnień wygląda następująco:

1. Założenie konta Podmiotu Publicznego zgodnie z instrukcją na stronie epuap.gov.pl: STREFA URZĘDNIKA\POMOC\Instrukcje i podręczniki\Zakładanie konta o uprawnieniach instytucji publicznej.
2. Wygenerowanie żądania certyfikatu do komunikacji zgodnie z instrukcją na stronie epuap.gov.pl: STREFA URZĘDNIKA\POMOC\Dla integratorów\Instrukcja generowania żądania certyfikatu do komunikacji z ePUAP oraz PZ (punkty 1-2).
3. Wystąpienie o wydanie certyfikatu na stronie epuap.gov.pl: STREFA URZĘDNIKA\Udostępnianie usług\Wydanie certyfikatu dla systemu teleinformatycznego służącemu zapewnieniu bezpieczeństwa wymiany informacji ePUAP (w polu CSR należy podać CSR wygenerowany w kroku nr 2).
4. Scalenie certyfikatu do komunikacji do pliku p12 zgodnie z instrukcją na stronie epuap.gov.pl: STREFA URZĘDNIKA\POMOC\Dla integratorów\Instrukcja generowania żądania certyfikatu do komunikacji z ePUAP oraz PZ (punkt 3).
5. Wystąpienie e-mailowe o nadanie uprawnień pod adres epuap-pomoc@coi.gov.pl, w korespondencji należy zamieścić:
   a) ID podmiotu ePUAP
   b) Dane, które posłużyły do generacji certyfikatu
   c) Zakres uprawnień: tpUserInfo, logowanie SSO
   d) Issuer (nazwa SAML) – adres domenowy eR lub publiczny, stały adres IP
   e) Adresy zwrotne dla usługi SSO: *http://przykładowa.domena.er.pl/*Account/PZ
   f) Adres zwrotny dla usługi SLO: *http://przykładowa.domena.er.pl/*Account/PZLogout

Przy podawaniu adresów usług SSO, SLO oraz wartości Issuer należy wykorzystać adres domenowy lub publiczny, stały adres IP portalu eR (ustawienie musi być zgodne z adresem strony w *8.3.9.1.1. Konfiguracja ogólna*, wielkość liter ma znaczenie).

Uwaga: Konta użytkowników, profile firm oraz instytucji, certyfikaty oraz uprawnienia są zawsze dedykowane na konkretne środowisko (produkcyjne lub testowe). W przypadku konfiguracji obu środowisk należy przejść pełen proces dwukrotnie.

Uwaga: Certyfikat posiada okres ważności 2 lata. Aby zachować ciągłość dostępu do usług należy wystąpić o jego przedłużenie co najmniej 30 dni przed końcem ważności aktualnego certyfikatu.

8.5.2. Konfiguracja w Portalu eRejestracja

1. Zalogować się do Portalu jako administrator.
2. Wejść do Konfiguracji ePUAP\PZ (patrz: . *Obsługa teleporad* – aktywacja tej opcji pozwala na wykonywanie wizyt za pomocą między innymi następujących kanałów komunikacji: telefon, Skype, WhatsApp, wideorozmowa.

   Uwaga: Funkcjonalność wymaga modułu Teleporada. Do obsługi teleporad wymagana jest konfiguracja harmonogramów użyciem predefiniowanego miejsca „Teleporada" (kod „TELE") w mMedica. Grafik trybu offline nie wspiera obsługi teleporad.
3. Integracja z serwisem Gdzie Po Lek – aktywacja tej opcji pozwala na wyszukanie dostępności leku za pomocą kodu EAN przez serwis gdziepolek.pl w funkcjonalnościach użytkownika związanych z zamawianiem recept, wystawionymi eReceptami oraz historią zamówionych recept.
4. Obsługa eAnkiet – uruchomienie funkcjonalności pozwala na tworzenie eAnkiet dla użytkowników po zalogowaniu lub po rezerwacji terminu na podstawie skonfigurowanych akcji ankietowych. Dodatkowo umożliwia użytkownikom przeglądanie utworzonych eAnkiet.
5. Uwaga: Funkcjonalność wymaga modułu eAnkiety oraz pobranej konfiguracji połączenia do Chmury dla zdrowia z mMedica.
6. Konfiguracja ePUAP\PZ), wprowadzić parametry konfiguracyjne zgodnie z formularzem z *8.5.1. Podmiot publiczny ePUAP oraz uprawnienia dla środowiska* produkcyjnego.
7. Od tej pory w Portalu eRejestracja można logować się za pomocą ePUAP oraz tworzyć powiązania kont z ePUAP\PZ.

9. Personel

Z Portalu eRejestracja korzystać może również personel medyczny. Ma on możliwość rezerwacji wizyty dla pacjenta. Aby móc korzystać z Portalu eRejestracja jako personel medyczny, należy być użytkownikiem systemu mMedica i być w nim równocześnie zarejestrowanym jako personel medyczny.

Uwaga: Opcje związane z kontem personelu są dostępne w module eRejestracja+.

9.1. Dodanie do Portalu i pierwsze logowanie

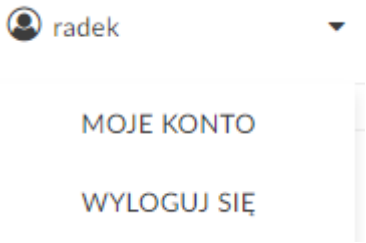
Możliwość dodania personelu do Portalu eRejestracja ma wyłącznie administrator Portalu. Podczas zakładania konta nadaje on nazwę użytkownika (login), który następnie przekazuje osobie personelu, dla której tworzone było konto.

Po utworzeniu konta użytkownik (personel) otrzyma wiadomość e-mail, w której znajdować się będzie hasło do profilu. Od tego momentu może się zalogować.

Podczas pierwszego logowania zalecana jest zmiana hasła. Jak to zrobić można przeczytać w rozdziale *8.2.1. Zmiana hasła.*

9.2. Moje konto

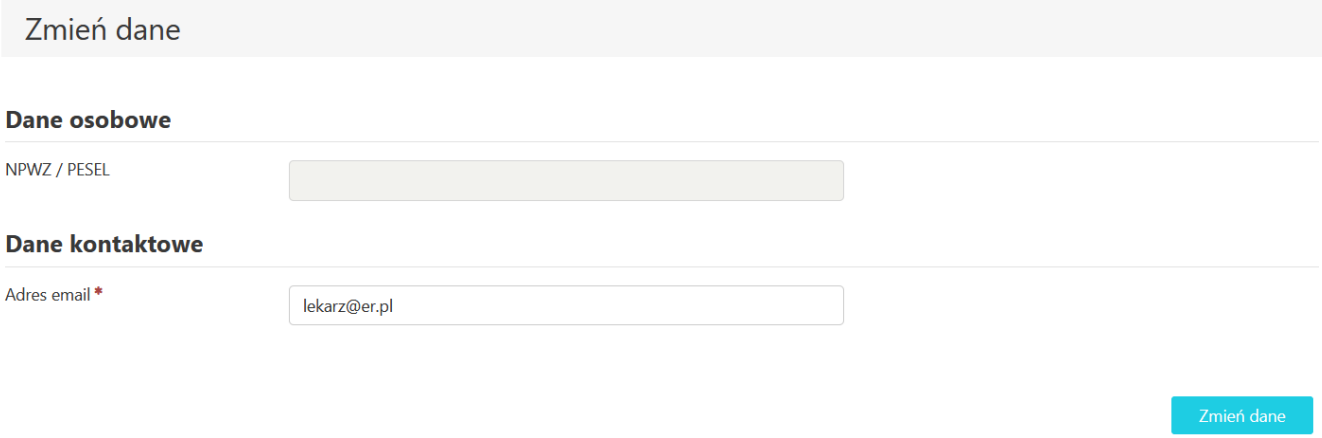
Po zalogowaniu się personelu do Portalu, w rozwijanym menu po prawej stronie aplikacji zostanie wyświetlony przycisk „Moje konto”. Przycisk ten otwiera stronę zarządzania kontem personelu medycznego.



Rysunek 236: Menu rozwijane personelu medycznego

9.2.1. Zmień dane

Funkcjonalność umożliwia personelowi zmianę adres email oraz wyświetlenie identyfikatora konta w formie NPWZ lub PESEL.



Rysunek 237: Edycja konta przez personel

9.2.2. Zmień hasło

Zakładka ta umożliwia personelowi medycznemu zmianę hasła do konta na Portalu eRejestracja. Opcja ta jest opisana w rozdziale *8.2.1 Zmiana hasła.*

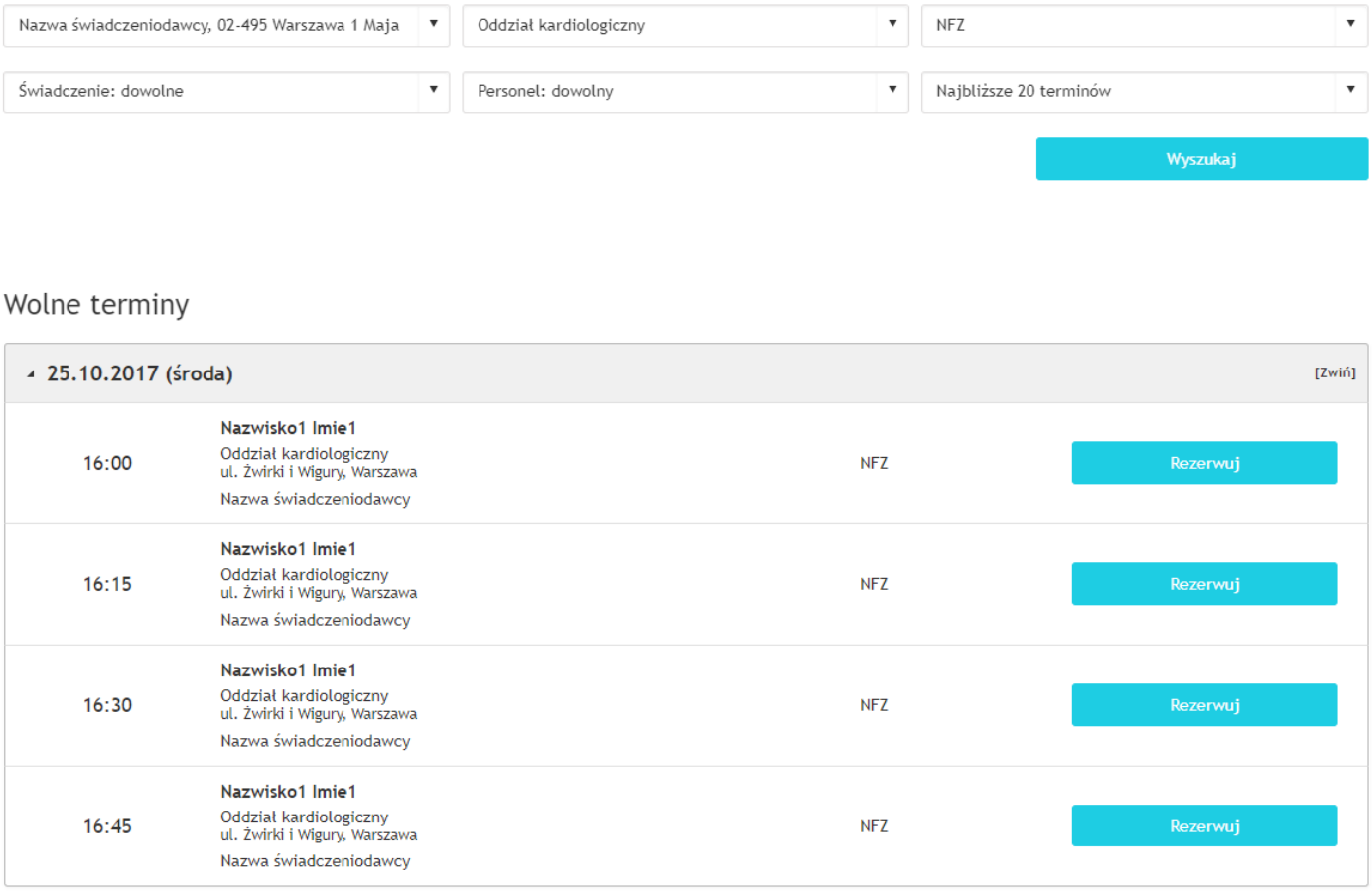
9.2.3. Weryfikacja dwuskładnikowa

Weryfikacja dwuskładnikowa jest dodatkową formą zabezpieczenia podczas logowania się na konto. Dokładny opis działania tej funkcji znajduje się w rozdziale *8.2.3 Weryfikacja dwuskładnikowa.*

9.3. Wolne terminy

Zakładka „Wolne terminy” służy do wyszukiwania wolnych terminów wizyt oraz wykonywanie rezerwacji dla pacjenta.

W celu zarezerwowania terminu należy wybrać z głównego menu przycisk „Wolne terminy”.



Rysunek 238: Wyszukiwanie wolnych terminów

Określenie parametrów wyszukiwania ułatwia zarezerwowanie terminu. Parametry te pozwalają zawężać wyszukiwane wizyty jedynie do tych, które interesują użytkownika. Personel posiada możliwość wybrania świadczeniodawcy, specjalności, świadczenia, osoby personelu, daty, wizyty oraz typu wizyty (prywatna lub NFZ). Na liście rozwijanej specjalności obok nazwy może zostać wyświetlony 4-znakowy kod resortowy, charakteryzujący specjalność komórki organizacyjnej. Wizyty zgodne z ustawionymi parametrami zostaną wyświetlone po naciśnięciu przycisku „Wyszukaj”.

Rezerwacja terminu odbywa się poprzez użycie przycisku „Rezerwuj”. Następnie w formularzu danych do rezerwacji należy uzupełnić wymagane pola i zatwierdzić rezerwację klikając przycisk „Rezerwuj”.

Rezerwacja wykonywana poza kartoteką.

Dane do rezerwacji

Dane wizyty

Data wizyty:	08-11-2018 08:00
Personel:	Lekarz2 Lekarz2
Miejsce wizyty:	Przychodnia
Rodzaj wizyty:	NFZ

Dane placówki

Specjalność:	Poradnia (gabinet) lekarza POZ dla dzieci
Adres poradni:	ul. Raciborska, Gliwice
Świadczeniodawca:	Świadczeniodawca
Adres świadczeniodawcy:	ul. Sezamkowa 1, Gliwice

Dane pacjenta

Imię *

Nazwisko *

Telefon komórkowy

Powrót Rezerwuj

Rysunek 239: Dane do rezerwacji

W przypadku rezerwacji na teleporadę dostępne są wyłącznie kanały komunikacji: telefon, WhatsApp. Następnie następuje przekierowanie do formatki potwierdzenia rezerwacji.

Potwierdzenie rezerwacji

Dane wizyty

Data wizyty:	19-11-2018 10:15
Personel:	Stomatolog1 Stomatolog1
Miejsce wizyty:	Przychodnia
Rodzaj wizyty:	NFZ

Dane placówki

Specjalność:	Poradnia stomatologiczna
Adres poradni:	ul. Pszczyńska, Gliwice
Świadczeniodawca:	Świadczeniodawca
Adres świadczeniodawcy:	ul. Sezamkowa 1, Gliwice

Dane pacjenta

Imię	imię
Nazwisko	nazwisko
Telefon komórkowy	

Drukuj Powrót

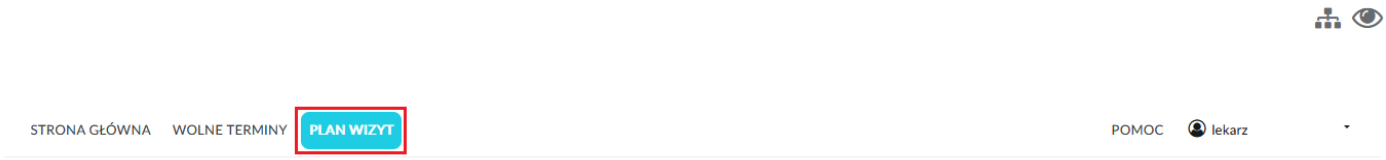
Rysunek 240: Potwierdzenie rezerwacji wizyty dla pacjenta

Istnieje możliwość wydrukowania potwierdzenia rezerwacji wizyty poprzez kliknięcie przycisku „Drukuj”.

9.4. Plan wizyt

Plan wizyt to funkcjonalność przeznaczona dla personelu medycznego, umożliwiająca wygodny i szybki dostęp do wszystkich rezerwacji dla danego użytkownika.

Po zalogowaniu się jako personel medyczny, należy kliknąć przycisk „Plan wizyt”, który znajduje się w menu głównym.



Rysunek 241: Położenie przycisku "Plan wizyt" w głównym menu dla personelu medycznego

Plan wizyt składa się z kilku głównych elementów:

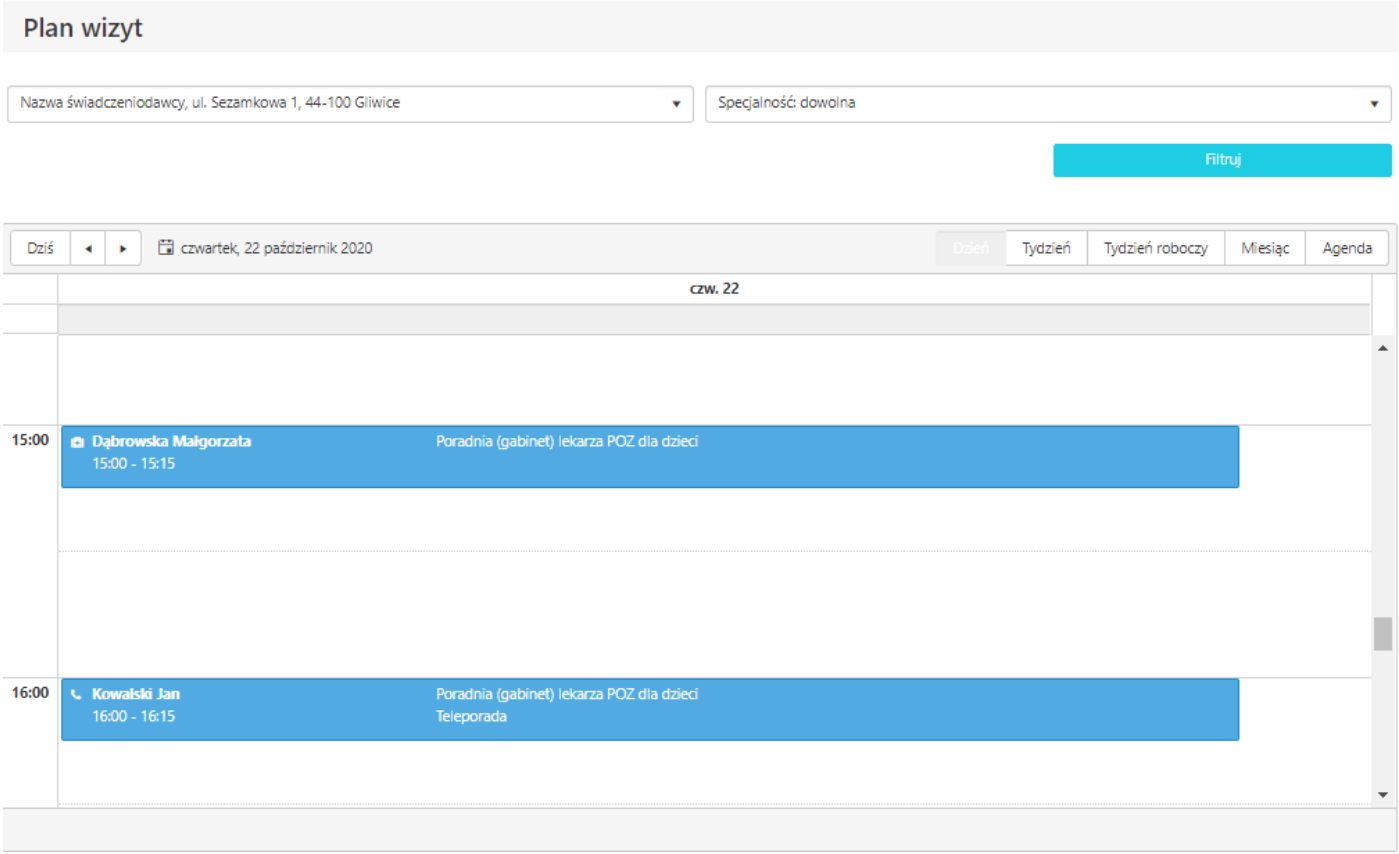
1. Filtrów na świadczeniodawcę oraz na komórkę organizacyjną.
2. Przycisku do filtrowania.
3. Planu wizyt, który jest podzielony na zakładki:
    a. Dzień,
    b. Tydzień,

c. Tydzień roboczy,

d. Miesiąc,

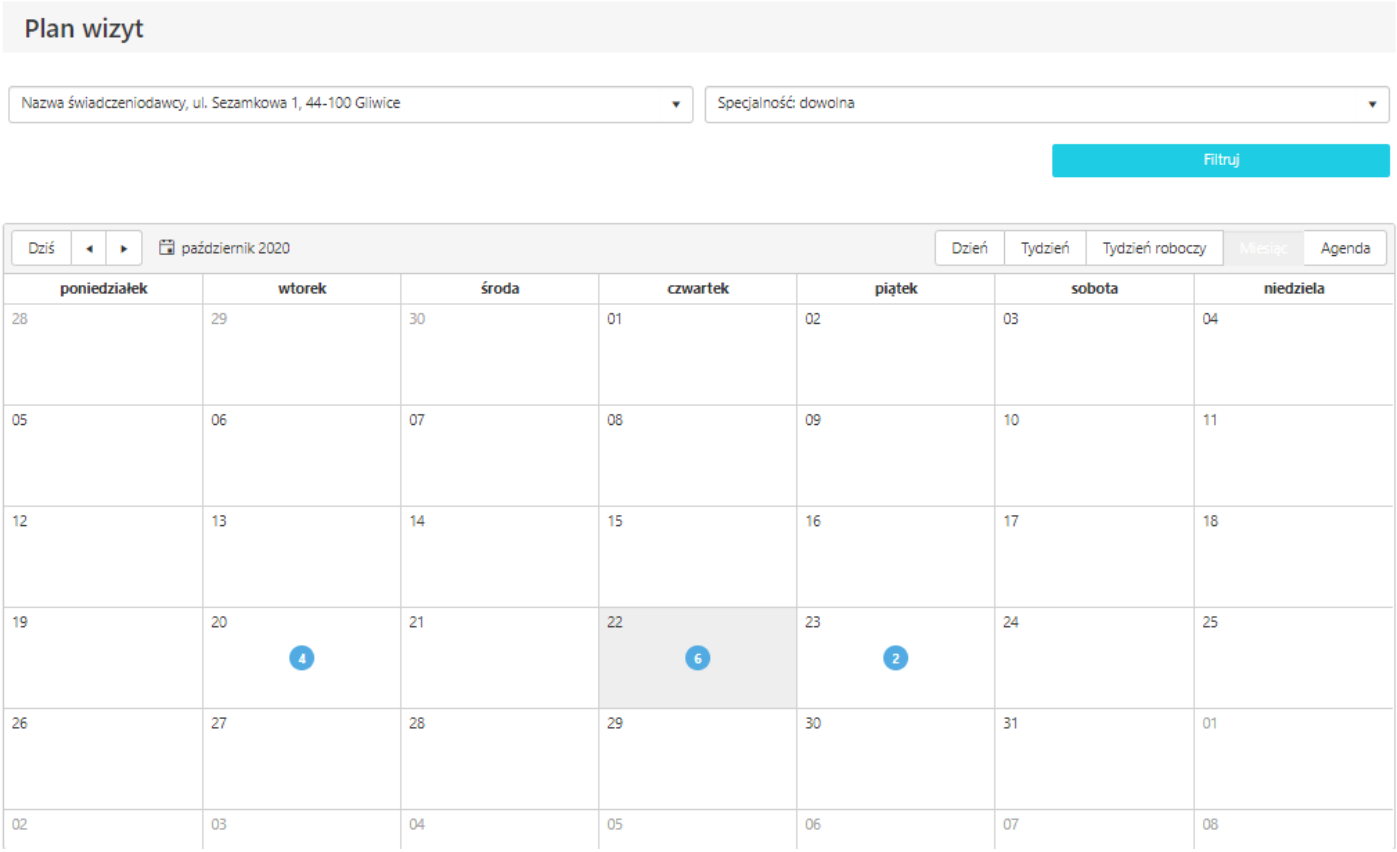
e. Agenda.

Po wybraniu odpowiednich parametrów w filtrach i kliknięciu przycisku „Filtruj”, w planie wizyt wyświetlą się rezerwacje pacjentów do konkretnego personelu medycznego. W przypadku zakładek: „Dzień”, „Tydzień” i „Tydzień roboczy”, wyświetlają się kafelki dla zarezerwowanych wizyt. Po najechaniu kursorem na dany kafelek, pojawi się chmurka z informacjami tj.: imię i nazwisko pacjenta, specjalność, godzina rezerwacji i opcjonalnie miejsce.



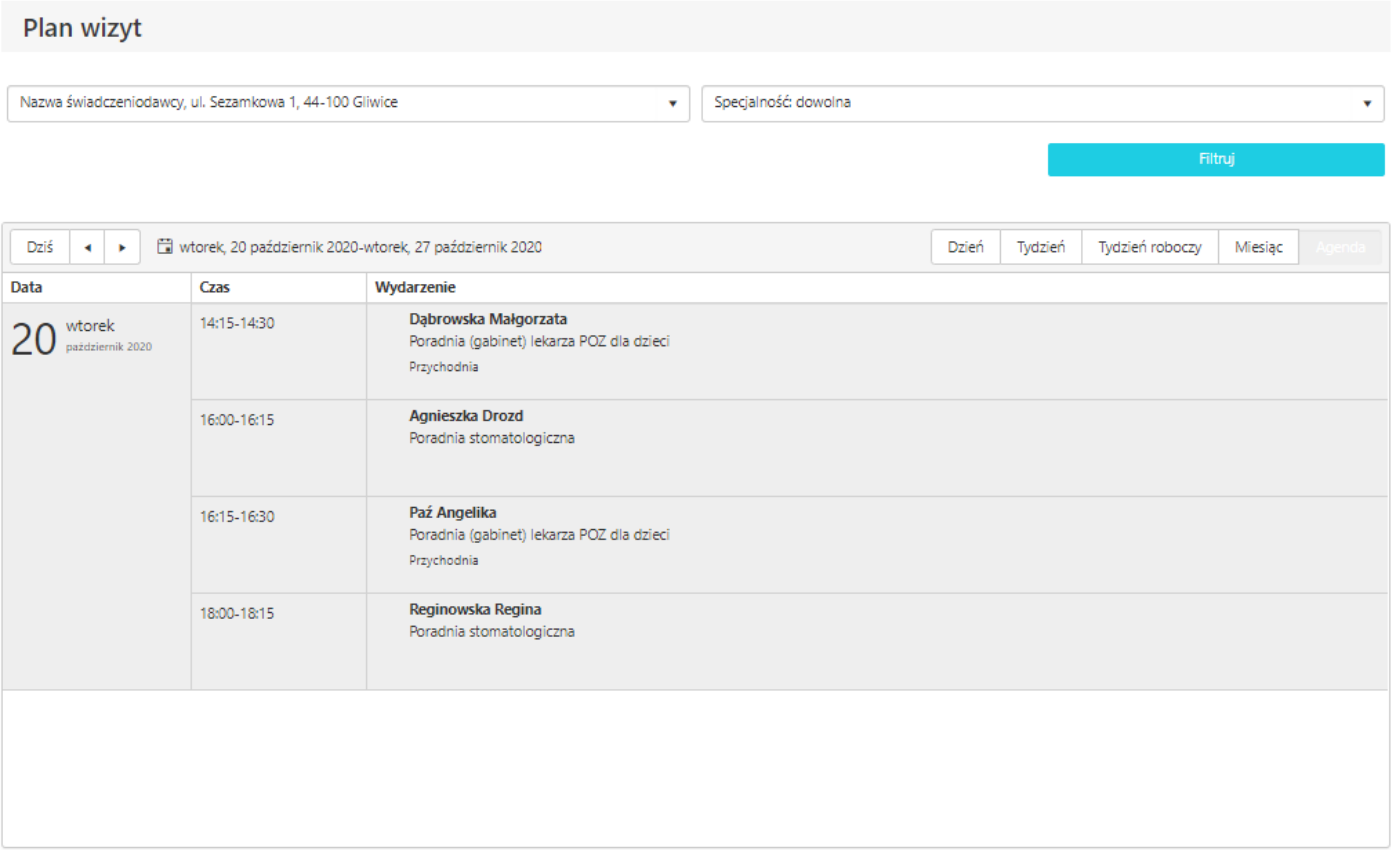
Rysunek 242: Przykładowy widok wyświetlających się rezerwacji dla zakładki „Dzień”

W przypadku zakładki „Miesiąc”, użytkownik ma możliwość sprawdzenia ilości rezerwacji, na wybrany dzień w ciągu danego miesiąca. Po kliknięciu w wybrany dzień, następuje przekierowanie na zakładkę „Dzień”.



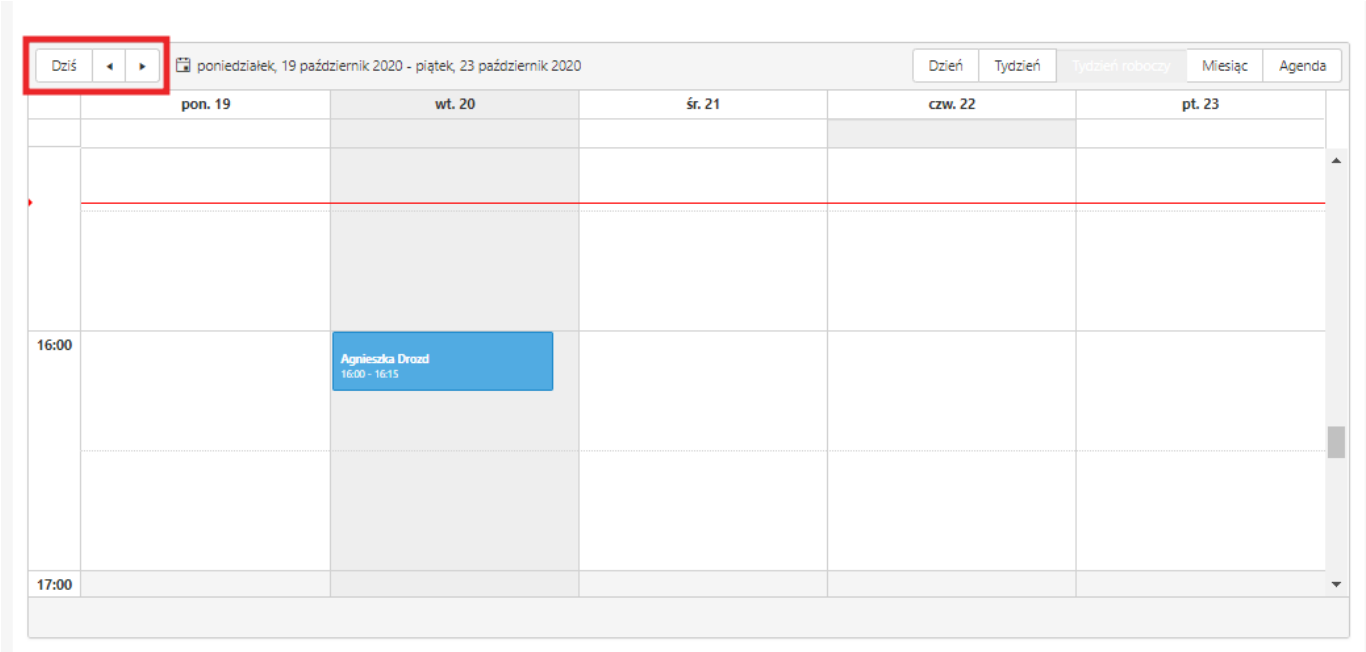
Rysunek 243: Przykładowy widok wyświetlających się rezerwacji dla zakładki „Miesiąc”

Po kliknięciu zakładki „Agenda”, użytkownik może sprawdzić uporządkowany dzienny plan rezerwacji, wskazujący na: datę, czas oraz wydarzenie.

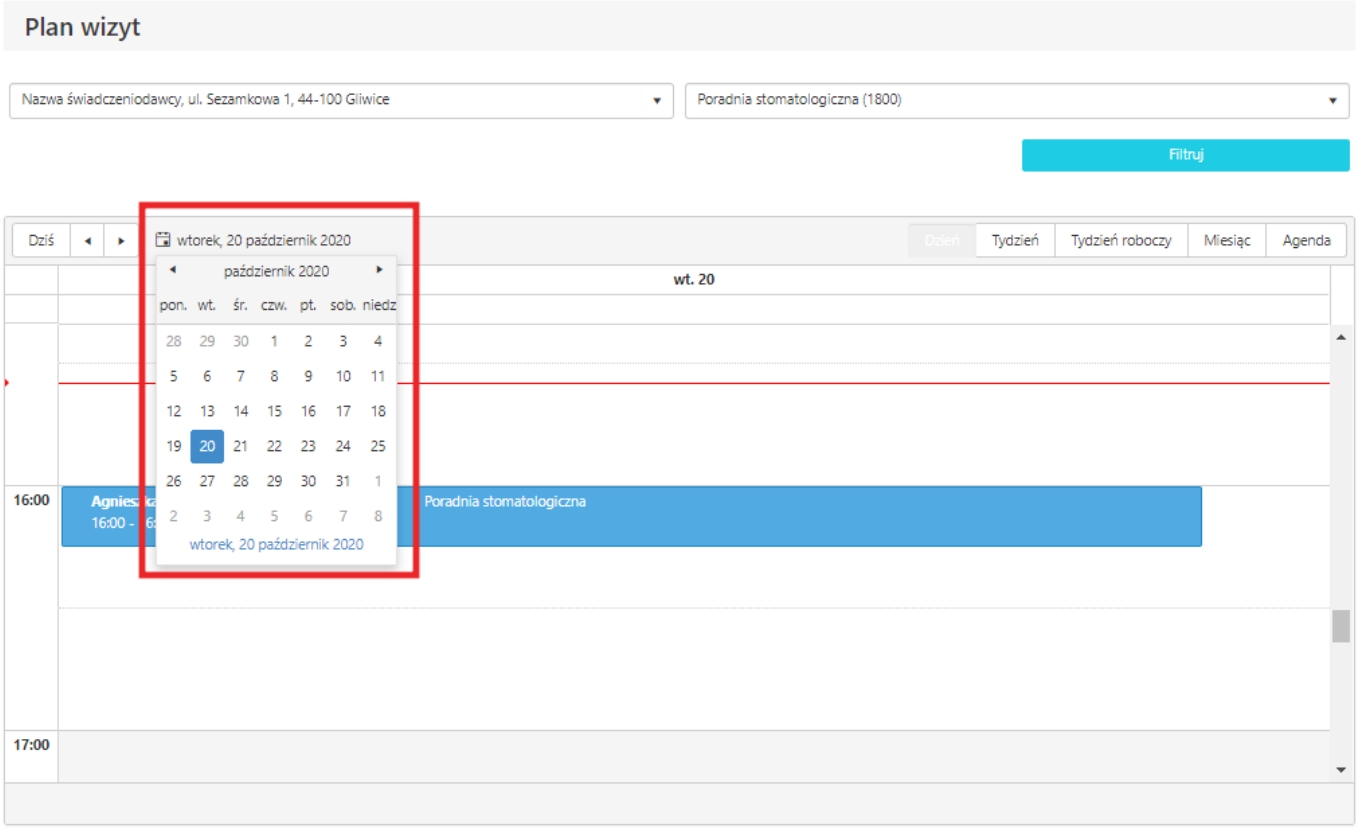


Rysunek 244: Przykładowy widok wyświetlających się rezerwacji dla zakładki „Agenda”

Po planie wizyt można poruszać się na kilka sposobów. Jednym z nich jest używanie przycisków „Dziś” oraz przycisków strzałek „Poprzedni” i „Następny”. Innym dostępnym sposobem, jest wybranie konkretnej daty w kalendarzu. Istnieje również funkcjonalność poruszania się po planie wizyt za pomocą strzałek na klawiaturze.

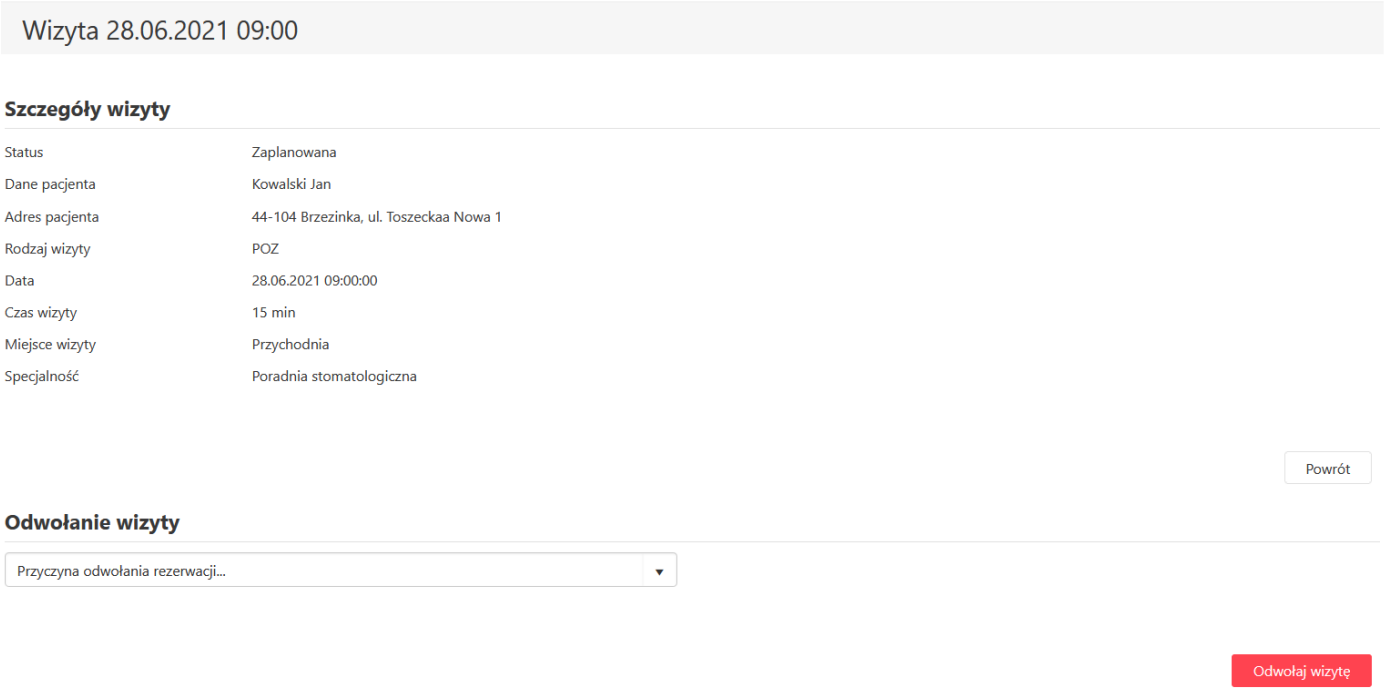


Rysunek 245: Widok przycisków "Dziś", "Poprzedni" i "Następny"



Rysunek 246: Widok kalendarza

Po kliknięciu na wybraną pozycję możliwe jest wyświetlenie informacji o wizycie oraz odwołanie wizyty po podaniu przyczyny.



Rysunek 247: Szczegóły wizyty wybranej z planu wizyt personelu

Wizyta 28.06.2021 09:00

Wizyta została odwołana.

Szczegóły wizyty

Status	Odwołana
Powód odwołania wizyty	Rezygnacja pacjenta
Dane pacjenta	Kowalski Jan
Adres pacjenta	44-104 Brzezinka, ul. Toszeckaa Nowa 1
Rodzaj wizyty	POZ
Data	28.06.2021 09:00:00
Czas wizyty	15 min
Miejsce wizyty	Przychodnia
Specjalność	Poradnia (gabinet) lekarza podstawowej opieki zdrowotnej

Powrót

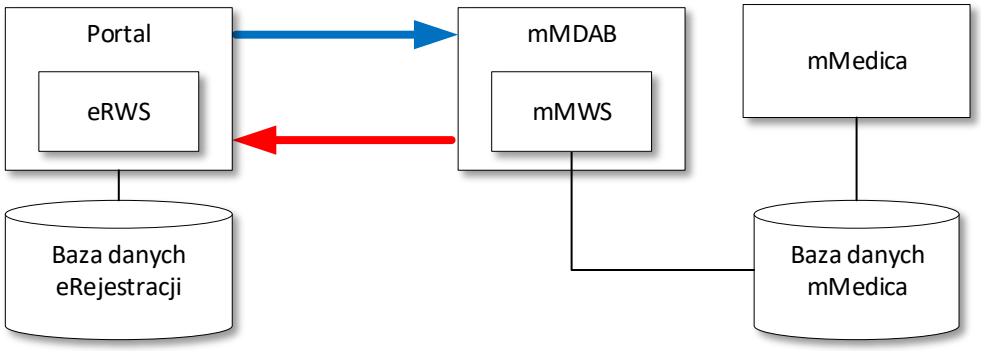
Rysunek 248: Szczegóły odwołanej wizyty wybranej z planu wizyt personelu

10. Komunikacja oraz synchronizacja danych

10.1. Modele komunikacji mMedica

Komunikacja pomiędzy oprogramowaniem mMedica a eRejestracja odbywa się za pośrednictwem usług mMWS (w mMDAB) oraz eRWS (wbudowanym w Portal). Komunikacje pomiędzy mMedica a eRejestracja należy rozpatrywać w zależności od kierunku przepływu danych:

1. eRejestracja -> mMedica – w tym rodzaju komunikacji eRejestracja inicjalizuje komunikację z oprogramowaniem mMedica. Portal łączy się z komponentem mMDAB, który przekierowuje wewnętrznie ruch do mMWS, który z kolei wprowadza zmiany na bazach danych mMedica. Na poniższym rysunku kolorem niebieskim oznaczono połączenia żądania, a kolorem czerwonym odpowiedzi.



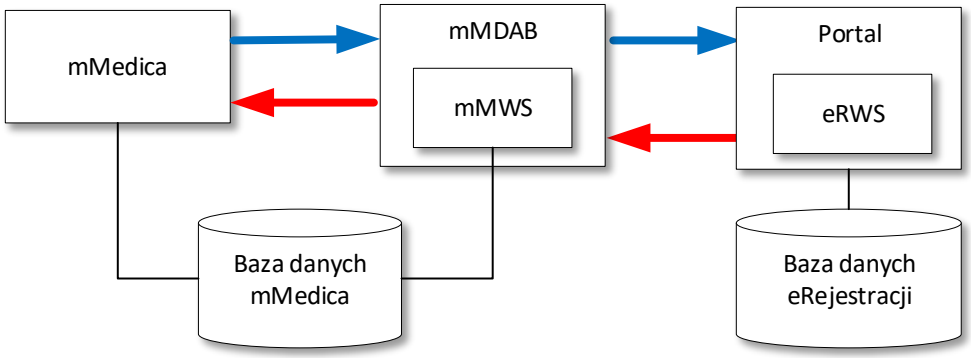
Rysunek 249: Model komunikacji eRejestracja -> mMedica

Przykłady komunikacji:

- dodawanie, odświeżanie, sprawdzanie statusu świadczeniodawcy,
- pobieranie konfiguracji połączenia z bramką SMS,
- pobieranie wolnych terminów, moich terminów oraz grafiku offline,
- operacje na terminach, zamawianie recept,
- wyświetlanie historii zamawianych recept,
- wyświetlanie wykonanych i planowanych szczepień użytkownika,
- wyświetlanie skierowań użytkownika,
- wyświetlanie wystawionych eRecept dla użytkownika,
- wyświetlanie zaleceń lekarskich z przeprowadzanych wizyt użytkownika,
- wyświetlenie eAnkiet użytkownika,
- tworzenie, edycja kont,
- aktualizacja danych użytkownika po logowaniu w Portalu,

- zmiana rodzaju logowania,
- import użytkownika z mMedica,
- tworzenie i odpinanie subkont,
- zmiana loginu użytkownika,
- synchronizacja terminów oraz kont powstałych lub zmienionych w trybie braku połączenia z bazą danych mMedica,
- zapis do rejestru wysłanych powiadomień (SMS),
- zmiana hasła usług sieciowych oraz ważności tokena bezpieczeństwa,
- import personelu medycznego z mMedica celem utworzenia konta w Portalu,
- zmiana kanału komunikacji dla teleporady,
- sprawdzenie, czy dane pacjenta są zweryfikowane,
- pobieranie identyfikatora pacjenta z bazy mMedica.

2. mMedica -> eRejestracja – w tym przypadku mMedica nawiązuje połączenie do komponentów eRejestracji - mMedica nawiązuje połączenie z mMDAB, który przekierowuje wewnętrznie ruch do mMWS. Natomiast mMWS nawiązuje połącznie z komponentem eRWS (wbudowanym w Portal), który dokonuje zmian na bazie danych eRejestracji. Na poniższym rysunku kolorem niebieskim przedstawiono połączenia żądania, a kolorem czerwonym odpowiedzi.



Rysunek 250: Model komunikacji mMedica -> eRejestracja

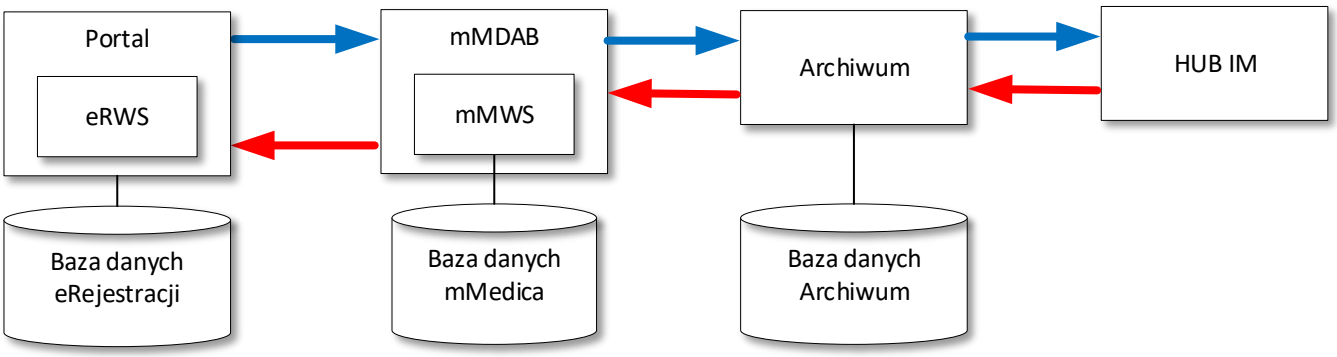
Przykłady komunikacji:

- tworzenie użytkownika w Portalu eRejestracja z poziomu programu mMedica,
- wymuszenie zmiany hasła użytkownika w Portalu eRejestracja,
- przekazywanie z mMedica do Portalu eRejestracja danych pacjenta do wykonania rezerwacji przez personel,
- wykonywanie procedur serwisowych na bazie eRejestracji za pomocą programu mMedica.

Uwaga: Należy pamiętać, że oprogramowanie posiada mechanizm sprawdzania kompatybilności wersji mMedica oraz eRejestracja, który może zablokować komunikacje.

10.2. Model komunikacji z eArchiwum

Integracja pomiędzy modułem eRejestracja a Archiwum odbywa się za pośrednictwem mMWS. Integracja wymaga poprawnej konfiguracji modułu Archiwum, właściwej konfiguracji modułu Archiwum w mMedica (adres usługi, hasło usług sieciowych). Na poniższym rysunku kolorem niebieskim przedstawiono żądania, z kolei kolorem czerwonym odpowiedzi.



Rysunek 251: Model komunikacji eRejestracja -> Archiwum

Przykłady komunikacji:

- wyszukiwanie udostępnionych przez personel w mMedica dokumentów medycznych użytkownika (wymaga licencji na moduł *eRejestracja+*),
- wyświetlanie oraz pobieranie udostępnionych przez personel w mMedica dokumentów medycznych użytkownika (wymaga licencji na moduł *eRejestracja+*),
- generacja PIN-u potrzebnego do rejestracji użytkownika w systemie *Informacje Medyczne*,
- awaryjne wyrejestrowanie użytkownika z systemu *Informacje Medyczne*,
- wyrażenie/wycofanie zgody użytkownika na komunikację z systemem *Informacje Medyczne*.

10.3. Model komunikacji z Chmurą dla zdrowia

Integracja pomiędzy modułem eRejestracja a Chmurą dla zdrowia odbywa się za pomocą danych uwierzytelniających pobranych z mMedica. W tym rodzaju komunikacji Portal eRejestracja łączy się bezpośrednio z Chmurą dla zdrowia.

Przykłady komunikacji dla eRepozytorium w chmurze:

- wyszukiwanie udostępnionych przez personel w mMedica dokumentów medycznych użytkownika za pomocą transakcji IHE ITI-18 (wymaga licencji na moduł *eRejestracja+*),
- wyświetlanie oraz pobieranie udostępnionych przez personel w mMedica dokumentów medycznych użytkownika za pomocą transakcji IHE ITI-43 (wymaga licencji na moduł *eRejestracja+*).

Przykłady komunikacji dla eAnkiet:

- pobieranie akcji ankietowych dla eAnkiet,
- generowanie eAnkiet na podsatwie pobranych akcji ankietowych,
- pobieranie statusów eAnkiet,
- pobieranie wypełnionych eAnkiet,
- rezygnacja z uzupełnienia eAnkiet.

10.4. Diagnostyka komunikacji

Diagnostyka podstawowa problemów opiera się na pozyskiwaniu informacji z Dziennika systemowego (opis w rozdziale *8.3.2. Dziennik systemowy*), w którym są zapisane informacje o błędach. Istnieje również możliwość diagnozy komunikacji z modułu eRejestracja do mMedica dla dodanych do Portalu świadczeniodawców przez Statusy świadczeniodawców (patrz: *8.3.1. Świadczeniodawcy).*

Diagnostyka zaawansowana polega na wykorzystaniu mechanizmów zawartych w usługach sieciowych mMDAB oraz mMWS Każda z usług posiada stronę statusu HTML, która wyświetla informacje związane z konfiguracją oraz stanem połączenia. Szczegółowy opis informacji zawartych na stronach statusu został przedstawiony w rozdziałach związanych z weryfikacją instalacji (*3.12. Weryfikacja instalacji* (Windows) *oraz 4.8. Weryfikacja instalacji* (Linux)).

10.5. Zasady synchronizacji danych z bazą mMedica

Poniżej przedstawiono zasady synchronizacji danych pomiędzy mMedica a eRejestracja:

1. Trwałe połączenie pomiędzy mMedica i eRejestracja następuje po dodaniu świadczeniodawcy w Portalu.
2. Specjalności, personel oraz słowniki terytorialne są aktualizowane w momencie dodawania lub odświeżania świadczeniodawcy w Portalu.
3. Po rejestracji użytkownika w Portalu jest on tworzony we wszystkich podłączonych bazach mMedica. Jeśli rejestracja nastąpiła poprzez utworzenie nazwy użytkownika i hasła oraz w konfiguracji portalu

wyłączona jest opcja „Tworzenie kont tradycyjnych bez weryfikacji danych w mMedica”, użytkownik jest dodawany do baz mMedica ze statusem „niezweryfikowany”. Oznacza to, że jego konto nie jest automatycznie scalane z istniejącym (jeśli istnieje) w bazie mMedica kontem.

4. Konta administracyjne w Portalu nie są przesyłane do bazy danych mMedica.
5. Podczas logowania użytkownika w Portalu, eRejestracja sprawdza we wszystkich podpiętych bazach mMedica (przez mMWS) najnowsze dane pacjenta i aktualizuje je w bazie danych eRejestracji jeśli dany użytkownik posiada status „zweryfikowany”.
6. Podczas zmiany danych pacjenta w Portalu zmiany są bezzwłocznie (w przypadku, w którym istnieje połączenie do bazy danych mMedica) przesyłane do bazy danych mMedica.
7. Wolne, moje terminy oraz lista leków dostępnych do zamówienia recepty są każdorazowo pobierane z bazy danych mMedica.
8. W przypadku braku połączenia z bazą danych mMedica wolne terminy pobierane są ze zbioru terminów pobranych do grafiku offline.
9. W przypadku przywrócenia połączenia z bazą danych mMedica następuje synchronizacja terminów, zmian w kontach użytkowników oraz rejestru wysłanych wiadomości SMS do bazy danych mMedica. Zmiana interwału sprawdzania, czy zostało przywrócone połączenie do bazy danych mMedica jest opisana w *8.3.9 Konfiguracja*.
10. W sytuacji, w której użytkownik tworzy konto w Portalu, a następnie rezerwuje termin u świadczeniodawcy, który nie istniał w Portalu w momencie tworzenia konta użytkownika, dane pacjenta zostaną przesłane do bazy danych mMedica w momencie rezerwacji terminu. Trzeba jednak pamiętać, że musi w Portalu być podpięty co najmniej jeden mMWS, aby użytkownik mógł stworzyć konto.
11. W szczególnych przypadkach może dojść do sytuacji, w której aplikacja podczas rejestracji użytkownika wykryje w bazie mMedica konto z przypisanym takim samym loginem do portalu eRejestracja, ale innymi danymi osobowymi. Spowoduje to utworzenie tak zwanego „konfliktu” użytkownika ze świadczeniodawcą. W takim przypadku zablokowana jest komunikacja użytkownika z bazą świadczeniodawcy (w tym synchronizacja danych).
12. Jeśli zaktualizowane po zalogowaniu pacjenta dane będą zawierały informację o dacie zgonu pacjenta, to jego konto w portalu eRejestracja zostanie zablokowane. W dzienniku systemowym pojawi się wpis informujący o blokadzie konta użytkownika.

11. Pobieranie danych diagnostycznych

Możliwe jest pobieranie danych diagnostycznych w formie XML lub JSON dotyczących działania komponentów mModułów. Zakres danych do pobrania jest tożsamy z danymi wyświetlanymi na stronach statusowych. Opis techniczny znajduje się w dokumencie pod odnośnikiem.

12. Rozwiązania częstych problemów

12.1. Nieprawidłowe hasło usług sieciowych (token)

Należy sprawdzić, czy hasło usług sieciowych wpisanie w Konfiguracji podstawowej Portalu (*8.3.9. Konfiguracja*) jest takie samo jak hasło wpisane w programie mMedica w Konfiguratorze (*8.1.1. Konfiguracja programu mMedica*). Szczególną uwagę należy zwrócić na wielkość liter, białe oraz specjalne znaki. Należy także zweryfikować, czy na wszystkich komputerach, na których zainstalowane są komponenty eRejestracji oraz bazy danych, jest ustawiona ta sama strefa czasowa. Jeżeli podczas komunikacji mMedica w kierunku eRejestracji nadal występuje problem z nieprawidłowym hasłem usług sieciowych, może to oznaczać zbyt małą wartość w parametrze „Ważność tokena przesyłanego do serwisu eRWS [s]” w Konfiguracji podstawowej Portalu. W przypadku, w którym problem występuje podczas komunikacji modułu eRejestracja z programem mMedica, należy zwiększyć wartość w „Czas ważności tokena” w Konfiguratorze mMedica. Jeśli świadczeniodawca został dodany do Portalu, to poprawność hasła usług sieciowych można zweryfikować na podstronie Świadczeniodawcy (patrz: *8.3.1. Świadczeniodawcy*).

12.2. Problem z brakiem licencji na moduł

W przypadku gdy licencja na moduł eRejestracja została dodana w programie mMedica, a mimo to występuje problem, należy w pierwszej kolejności sprawdzić, czy mMWS łączy się do poprawnej bazy danych mMedica (plik [mMWS]\appsettings.json). W sytuacji, w której licencja na moduł eRejestracja została dodana po instalacji modułu eRejestracja, możliwa jest sytuacja, w której mMWS zapamięta stan braku licencji. W takim wypadku najprościej jest zrestartować komponent według informacji zawartych w *3.15. Restartowanie i zatrzymywanie komponentów (Windows), 4.12. Restartowanie i zatrzymywanie komponentów (Linux).*

12.3. Nie pobierają się wolne terminy

Należy sprawdzić, czy zakres wyszukiwania terminów jest poprawny. Należy również pamiętać, iż pobrane zostaną wyłącznie terminy, których zakres jest odpowiedni dla wybranej wartości w „Zakres realizowanych świadczeń" w Konfiguracji podstawowej Portalu (patrz: *8.3.9. Konfiguracja*). Jeżeli w Dzienniku systemowym (*8.3.2. Dziennik systemowy*) nie zostały zapisane żadne błędy związane z pobieraniem wolnych terminów, należy zweryfikować, czy został poprawnie zdefiniowany harmonogram w programie mMedica (w szczególności wybór pola „Dostępność" w szablonach harmonogramów).

12.4. Brak terminów w grafiku offline

Należy sprawdzić, czy terminy przeznaczone do grafiku offline zostały oznaczone w szablonie harmonogramu programu mMedica jako dostępne wyłącznie dla eRejestracji.

12.5. Brak specjalności

Do Portalu pobierane są wyłącznie komórki organizacyjne, które mają aktualne kody na rok bieżący w programie mMedica.

12.6. Brak personelu

W pierwszej kolejności należy sprawdzić, czy w eRejestracji znajduje się specjalność, do której miał być przypisany członek personelu. Jeżeli nie ma takiej specjalności w „Zarządzaniu podmiotami w Portalu", należy zapoznać się z punktem *12.5. Brak specjalności*. Jeżeli specjalność znajduje się w Portalu, należy sprawdzić, czy członek personelu ma uprawnienia do wymaganej specjalności w programie mMedica.

12.7. Nieprawidłowe nazwy specjalności

Nazwy specjalności (komórek organizacyjnych) pobierane są z kodu cz. VIII ze struktury organizacyjnej programu mMedica. Administrator Portalu może je dowolnie zmienić (patrz: *8.3.11.1. Specjalności*).

12.8. Problem z dodaniem lub odświeżeniem świadczeniodawcy

Wszystkie błędy związane z dodawaniem lub odświeżaniem świadczeniodawcy są rejestrowane w Dzienniku systemowym Portalu (wraz z informacjami szczegółowymi, szczegóły w *8.3.2. Dziennik systemowy*). W przypadku instalacji modułu eRejestracja na dystrybucji Linux, należy również upewnić się, czy nie występują problemy z mMWS opisane w *4.8. Weryfikacja instalacji*. Dodatkowo, w przypadku, w którym mMWS

wykorzystuje protokół https, należy zaimportować jego certyfikat zgodnie z *4.5. Konfiguracja serwera oraz instalacja modułu*.

12.9. Zapomniane hasło do konta administratora

W przypadku, w którym zapomniano hasła do konta jedynego administratora, należy zgłosić się do Serwisu mMedica w celu otrzymania procedury serwisowej nadającej nowe hasło. Jeżeli w Portalu jest więcej niż jeden aktywny administrator, można za pomocą jego konta w Rejestrze użytkowników zmienić hasło innemu administratorowi (opis w *8.3.3. Rejestr użytkowników*).

12.10. Problem z wysyłaniem wiadomości e-mail (SMTP)

Problemy z wysyłaniem wiadomości email są rejestrowane w Dzienniku systemowym (patrz: *8.3.2. Dziennik systemowy*). Warto zweryfikować konfigurację z serwerem poczty wychodzącej (SMTP) wybierając funkcję wysyłania testowej wiadomości z poziomu Konfiguracja/Podstawowa/SMTP (zakładka), więcej informacji w podrozdziale *8.3.9.1.3. Konfiguracja SMTP*. W przypadku, w którym wiadomość nie została wysłana na adres administratora, należy sprawdzić ustawienia konfiguracji.

12.11. Problem z wysyłaniem wiadomości SMS

Problemy związane z wiadomościami SMS są zapisywane w Dzienniku systemowym (*8.3.2. Dziennik systemowy*). Możliwe jest ponowne pobranie konfiguracji połączenia z bramką SMS lub wysłanie testowej wiadomości na wybrany numer telefonu w Konfiguracja/Podstawowa/Bramka SMS (zakładka). Szczegółowe informacje konfiguracji bramki SMS zostały opisane w *8.3.9.1.4. Bramka SMS*

12.12. Problem z utworzeniem użytkownika w Portalu z poziomu mMedica

O ile treść zwracanego błędu w programie mMedica nie wskazuje na problem z walidacją danych, należy zweryfikować, czy adres mMWS, eRWS oraz hasło usług sieciowych są poprawnie skonfigurowane w Konfiguratorze mMedica (patrz: *8.1.1. Konfiguracja programu mMedica*).

12.13. Problem z wykonaniem procedury serwisowej

Problemy z wykonaniem procedury serwisowej są zapisywane w Dzienniku systemowym (*8.3.2. Dziennik systemowy*). Jeżeli taki wpis nie istnieje, należy sprawdzić, czy adres mMWS, eRWS oraz hasło usług sieciowych jest poprawnie skonfigurowane w Konfiguratorze mMedica (*8.1.1. Konfiguracja programu mMedica*).

12.14. Mapy nie wyświetlają się poprawnie

Najważniejszym krokiem jest wygenerowanie kluczy na stronie Google Maps (przycisk plusa w konfiguracji map) oraz jego późniejsze wklejenie w pole klucza (API Key). Pełen opis znajduje się w podrozdziale *8.3.10.6. Mapy*. Po zapisaniu konfiguracji należy odświeżyć stronę.

12.15. Wyłączanie powiadomień SMS

Istnieje możliwość wyłączenia powiadomień SMS dla danego świadczeniodawcy z poziomu Konfiguracja/Podstawowa/Brama SMS (zakładka), a także na poziomie poszczególnych specjalności podczas ich edycji w Portalu. Więcej informacji zostało umieszczonych w podrozdziałach *8.3.9.1.4. Bramka SMS* oraz *8.3.11.1. Specjalności*.

12.16. Zduplikowany personel

W przypadku zduplikowanego personelu w Portalu można użyć opcji powiązania, która pozwala na wyświetlanie w Portalu wyłącznie jednej osoby personelu zamiast kilku. Powiązanie dokonuje się z poziomu edycji personelu w Portalu (opis w *8.3.11.2. Personel*).

12.17. Zduplikowane specjalności

Zduplikowane specjalności pochodzące z programu mMedica można powiązać w Portalu z poziomu edycji specjalności. Powiązanie pozwala na wyświetlanie tylko jednej specjalności zamiast kilku (patrz: *8.3.11.1. Specjalności*).

12.18. Zmiana treść wiadomości e-mail lub SMS

Możliwa jest zmiana każdego z szablonów e-mail oraz SMS z poziomu Konfiguracja/Podstawowa/Szablony wiadomości (zakładka), więcej informacji w *8.3.9.3. Szablony wiadomości.*

Konfiguracja zezwala również na edycję stopki powiadomień po wybraniu wewnętrznej zakładki „Stopka wiadomości”.

12.19. Zmiana nazwy świadczeniodawcy

Z poziomu Konfiguracja/Zarządzanie podmiotami możliwa jest zmiana nazwy oraz adresu świadczeniodawcy. Odświeżenie świadczeniodawcy nie zmienia ustawionych danych świadczeniodawcy w Portalu.

12.20. Nieprawidłowe ustawienia Portalu – odtwórz. kopii bazy danych eRejestracji

W takim przypadku należy wykonać restart komponentów. Procedura restartowania została zawarta w *3.15. Restartowanie i zatrzymywanie komponentów (Windows), 4.12. Restartowanie i zatrzymywanie komponentów (Linux).*

12.21. Biała strona komponentu po instalacji przez instalator na IIS

Powodem takiej sytuacji jest zaznaczenie w instalatorze dla komponentu wymagania korzystania z SSL bez konfiguracji certyfikatu w IIS. Jeżeli wymaganie SSL zostało zaznaczone rozmyślnie, należy skonfigurować SSL zgodnie z *3.13.2. Konfiguracja certyfikatu SSL*. W innym przypadku istnieje możliwość wyłączenia opcji. W tym celu należy uruchomić Menedżer internetowych usług informacyjnych, następnie wybrać witrynę, w której zostały zainstalowane aplikacje (domyślnie „Default Web Site"), z panelu środkowego wybrać „Ustawienia protokołu SSL" i odznaczyć pole „Wymagaj protokołu SSL". Następnie kliknąć prawym przyciskiem myszy na witrynę (domyślnie „Default Web Site") i wybrać opcję „Edytuj powiązania…". Jeżeli w oknie brak jest typu „http" należy go dodać opcją „Dodaj…" z portem 80. Jeżeli na liście powiązań widnieje typ „https" to można go usunąć zaznaczając wiersz i wybierając opcję „Usuń". Dodatkowo należy zaznaczyć witrynę i w menu „Zarządzaj witryną sieci Web" wybrać opcję „Rozpocznij" jeśli witryna jest zatrzymana. Istnieje również możliwość późniejszej konfiguracji SSL zgodnie z podrozdziałem *3.13.2. Konfiguracja certyfikatu SSL*.

12.22. Błąd 403.4 na localhost lub na adresie komponentu na IIS

Rozwiązanie problemu zostało opisane w podrozdziale *12.21. Biała strona komponentu po instalacji przez instalator na IIS.*

12.23. Błąd 500.21 w IIS

Powodem błędu jest brak zainstalowanego modułu AspNetCoreModuleV2 dla IIS. Konieczne jest zainstalowanie lub zainstalowanie ponowne pakietu ASP.NET Core Windows Hosting – rozdział *3.4. Instalacja ASP .NET Core wraz z modułem* IIS. Warto również zapoznać się z rozdziałem dotyczącym ponownej instalacji ASP.NET Core Windows Hosting (patrz: *3.5. Instalacja IIS po instalacji ASP .NET* Core).

12.24. Błąd 502.19 w IIS

Opis błędu wraz z rozwiązaniem został opisane w rozdziale *12.23. Błąd 500.21 w IIS.*

12.25. Błąd 502.5 w IIS

Błąd najczęściej jest spowodowany brakiem zrestartowania usługi IIS po instalacji ASP.NET Core Windows Hosting (patrz: *3.4. Instalacja ASP .NET Core wraz z modułem* IIS lub *3.5. Instalacja IIS po instalacji ASP .NET* Core). Problem może również być wynikiem braku instalacji pakietu KB2533623 dla systemów Windows 7 SP1 oraz Windows Server 2008 R2 SP1 (więcej informacji w rozdziale *3.6. KB2533623 dla Windows 8.1,*). Innym powodem błędu może być brak uprawnień do odczytu folderu komponentu przez pulę aplikacji – punkt *18* z rozdziału *3.10.* Instalacja manualna.

12.26. Polecenie dotnet nie jest rozpoznawalne – Linux

Do poprawnego uruchomienia aplikacji wymagana jest instalacja środowiska ASP .NET Core. Proces instalacji opisany został w punkcie *6* w rozdziale *4.4. Instalacja wymaganego oprogramowania*. Jeżeli po dodaniu certyfikatu Microsoft, podczas próby zaktualizowania listy pakietów pojawi się problem związany z brakiem możliwości zweryfikowania podpisu. Oznacza to, pobierany jest certyfikat dla nie odpowiedniej wersji systemu. Przykładowy certyfikat dla Linux Ubuntu 20.04:

```
wget https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft-
prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
```

Na stronie https://docs.microsoft.com/pl-pl/dotnet/core/install/linux znajdują się instrukcje dla innych popularnych wersji systemu.

12.27. Status serwisu Main process exited – Linux

Błąd ten może wynikać z wielu przyczyn takich jak:

a) Brak uprawnień wykonywania dla pliku z rozszerzeniem .sh. Należy je wtedy dodać poprzez polecenie:

```
sudo chmod +x nazwa_pliku.sh
```

b) W pliku */etc/systemd/system/[*nazwa_serwisu*].service* została umieszczona błędna ścieżka do pliku wykonywalnego. Należy ją poprawić zgodnie z punktem *8* w *4.5. Konfiguracja serwera oraz instalacja modułu.*

c) W pliku *nazwa_pliku.sh* umieszczona została błędna ścieżka do pliku wykonywalnego. Należy ją poprawić zgodnie z punktem *7* w rozdziale *4.5. Konfiguracja serwera oraz instalacja modułu*.

12.28. Invalid command 'ProxyPreserveHost' – Linux

Jeżeli podczas sprawdzania statusu wyświetli się tego typu komunikat: „Invalid command 'ProxyPreserveHost', perhaps misspelled or defined by a module not included in the server configuration” oznacza to, że nie został udostępniony odpowiedni moduł Apache. Należy wtedy wykonać instrukcje zawarte w punkcie *4* w rozdziale *4.5. Konfiguracja serwera oraz instalacja modułu*.

12.29. Brak portu w statusie usługi – Linux

Jeśli podczas sprawdzania statusu serwisu poprzez polecenie:

```
sudo systemctl status nazwa_serwisu.service
```

pojawił się komunikat o uruchomieniu aplikacji, ale brak informacji na jakim porcie aplikacja została wystawiona. Najprawdopodobniej jest to związane z błędną konfiguracją komponentów. Więcej informacji można uzyskać uruchamiając plik wykonywalny *nazwa_pliku.sh* ręcznie. Poprzez komendę:

```
./nazwa_pliku.sh
```

W razie potrzeby należy poprawić konfigurację w pliku appsettings.json komponentu zgodnie z instrukcją *5. Konfiguracja aplikacji*. Możliwe jest również, że błąd wynika z braku odpowiedniego pakietu. Jeżeli podczas ręcznego uruchomienie wyświetlony zostanie komunikat o błędzie związanym z libunwind należy go zainstalować zgodnie z punktem *3* w rozdziale 4.4. Instalacja wymaganego oprogramowania.

12.30. Strona jest widoczna wyłącznie z komputera lokalnego

Należy sprawdzić, czy strona została właściwie powiązana z adresem, a także czy zapora ogniowa akceptuje ruch przychodzący na porcie działania usługi WWW.

12.31. Błąd podczas zapisu strony offline

Błąd związany z zapisem strony offline powinien zostać zapisany w dzienniku systemowy (patrz: *8.3.2. Dziennik systemowy*). Najczęstszą przyczyną błędów jest brak uprawnień do zapisu do folderu *[Ścieżka do Portalu]\Views\Shared\Custom* (opis w rozdziałach: *3.10. Instalacja manualna* (Windows), *4.2.* Instalacja (Linux)).

12.32. Błąd podczas zapisu własnego stylu strony

Błąd związany z zapisem definicji własnego stylu strony powinien zostać zapisany w dzienniku systemowym (patrz: *8.3.2. Dziennik systemowy*). Najczęstszym powodem błędu jest brak uprawnień do zapisu do

pliku *[Ścieżka do Portalu]\wwwroot\content\css\custom-site.min.css* (opis w rozdziałach: *3.10. Instalacja manualna* (Windows), *4.2.* Instalacja (Linux)).

12.33. Przekroczenie czasu realizacji operacji na bazie danych (timeout)

Możliwa jest edycja maksymalnego czasu wykonywania operacji na bazie danych dla każdego komponentu. W tym celu należy wpisać „CommandTimeout=WARTOSC" w pliku appsettings.config komponentu (sekcja „ConnectionString"). WARTOSC jest podawana w sekundach. Przykład dla 250 sekund:

```
"ConnectionString": "Server=localhost,5432;Database=ERMMEDICA;CommandTimeout=250;"
```

12.34. Problem z podpisem kwalifikowanym – Java

W razie problemów z obsługą podpisu kwalifikowanego (32-bitowa architektura oprogramowania Java JRE) należy:

1. Przejść do ścieżki instalacji Portalu a następnie do: wwwroot\Kir\ext.
2. W katalogu usunąć plik CCP11s.dll.
3. Zmienić nazwę pliku CCP11s.x32.dll na CCP11s.dll.

Warianty pliku CPP11s:

Nazwa pliku	Opis	Rozmiar
CCP11s.dll	Domyślny plik, preferowany dla Java 64-bit	Około 3,1 MB
CCP11s.x64.dll	Kopia pliku wersji 64-bitowej	
CCP11s.x86.dll	Plik preferowany dla Java 32bit	Około 1,7 MB

4. W katalogu usunąć plik Graphitep11.dll.
5. Zmienić nazwę pliku Graphitep1132.dll na Graphitep11.dll.

Warianty pliku Graphitep11:

Nazwa pliku	Opis	Rozmiar
Graphitep11.dll	Domyślny plik, preferowany dla Java 64-bit	Około 1,4 MB
Graphitep1132.dll	Plik preferowany dla Java 32bit	Około 1,1 MB

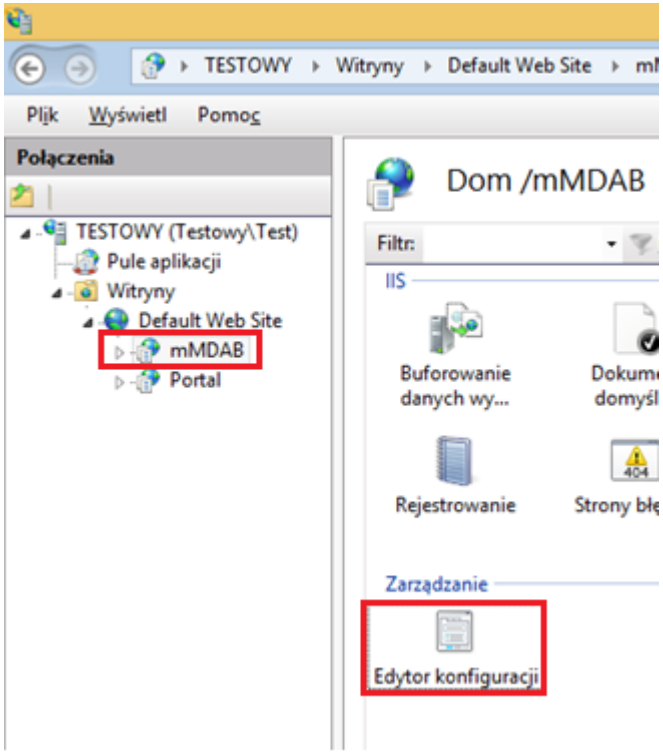
6. W katalogu usunąć plik libgraphite.dll.
7. Zmienić nazwę pliku libgraphite64.dll na libgraphite.dll.

Warianty pliku libgraphite:

Nazwa pliku	Opis	Rozmiar
libgraphite.dll	Domyślny plik, preferowany dla Java 64-bit	Około 2,7 MB
libgraphite32.dll	Plik preferowany dla Java 32bit	Około 2,5 MB

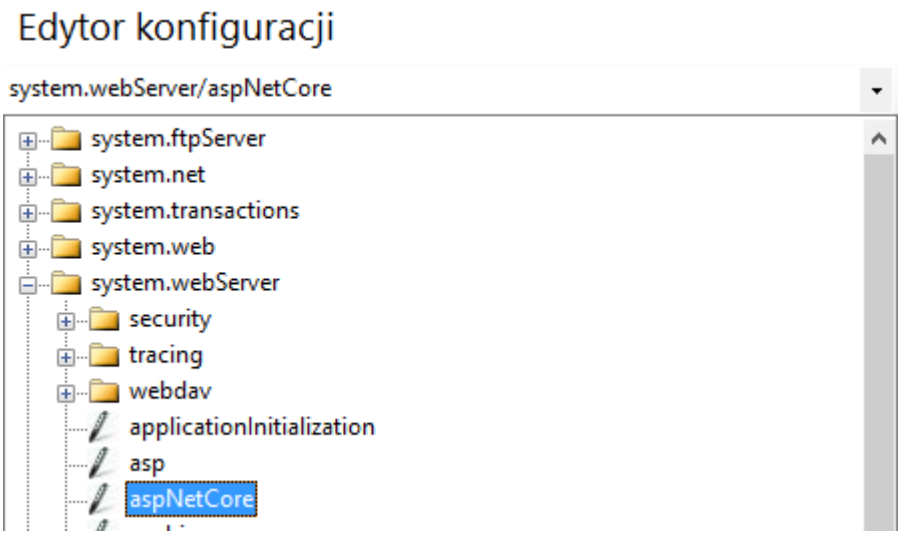
12.35. Problem z mMDAB i mMWS na IIS

Jeżeli podczas próby wejścia na stronę statusową np. http://localhost/mMDAB nie była ona dostępna, a możliwe jest wejście na stronę statusową mMWS np. http://localhost/mMDAB/mMWS to oznacza to najprawdopodobniej, że IIS jest błędnie skonfigurowany dla aplikacji mMDAB. Aby prawidłowo skonfigurować IIS należy w „Widoku funkcji” dla aplikacji mMDAB przejść do „Edytora konfiguracji”.



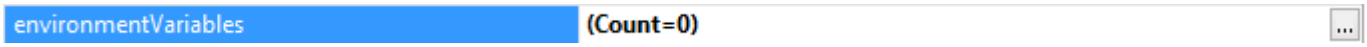
Rysunek 252: Edycja konfiguracji

Następnie z listy rozwijanej należy wybrać wewnątrz katalogu „system.webServer” sekcję aspNetCore.



Rysunek 253: IIS - Wybór odpowiedniej sekcji

W kolejnym kroku konieczne jest edytowanie sekcji environmentVariables.



Rysunek 254: IIS - Edycja zmiennych środowiskowych

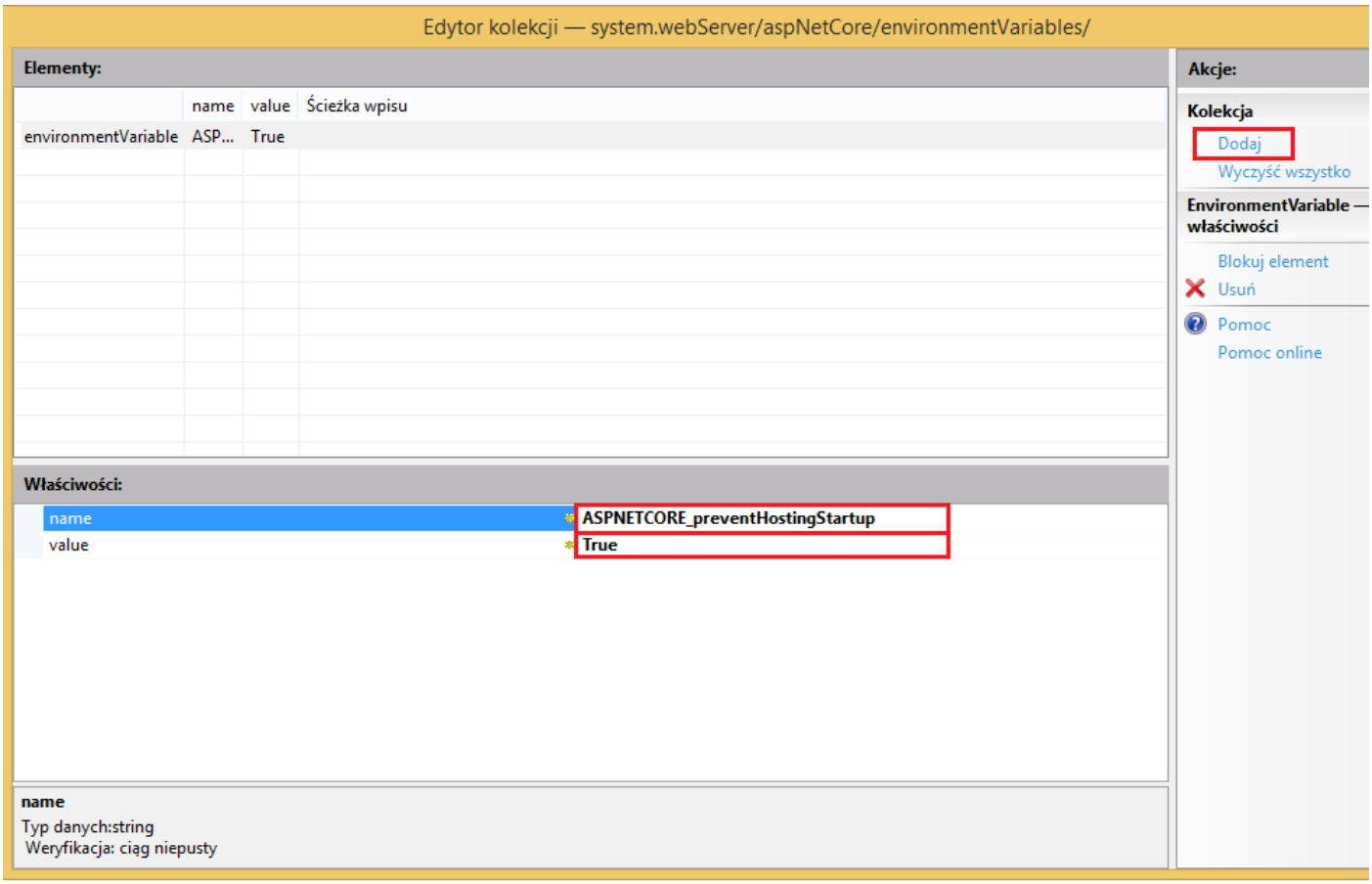
Podczas edycji należy dodać nową zmienną środowiskową poprzez przycisk „Dodaj” umieszczony po prawej stronie okna. W polu „name” należy wprowadzić:

```
ASPNETCORE_preventHostingStartup
```

Z kolei w polu „value” wartość:

```
True
```

Podobnie jak na poniższym zrzucie ekranu:



Rysunek 255: IIS - Dodawanie nowej zmiennej środowiskowej

Po wszystkim należy ponownie uruchomić komputer.

12.36. Brak pliku api-ms-win-crt-runtime-l1-1-0 – Windows

W przypadku błędu informującego o braku pliku api-ms-win-crt-runtime-l1-1-0 podczas uruchomienia któregoś z komponentów eRejestracji należy zainstalować lub zaktualizować pakiet „Universal C Runtime in Windows". Więcej informacji na stronie: https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows.

12.37. Błąd „Unspecified certificate from client" w mMedica

Jeśli w mMedica podczas komunikacji do mMWS (np. w teście połączenia) pojawia się błąd, w którego treści znajduje się fraza „Unspecified certificate from client" to oznacza, że niepoprawnie została skonfigurowana witryna zawierającą aplikację mMDAB. Powodem błędu jest ustawienie protokołu SSL dla witryny na opcjonalne lub obligatoryjne przesyłanie certyfikatu klienta.

Konfiguracja w IIS:

a) Przejść w IIS do witryny z aplikacją mMDAB.

b) Wybrać ze środkowego okna „Ustawienie protokołu SSL”.

c) Zmienić ustawienie „Certyfikaty klientów” na „Ignoruj”.

d) Zaleca się restart witryny.

Konfiguracja w apache:

a) Uruchomić w trybie edycji plik konfiguracyjny witryny mMDAB.

b) Usunąć opcję „SSLVerifyClient” lub ustawić ją na „none”.

c) Zapisać plik konfiguracyjny witryny.

d) Przeładować konfiguracje apache lub wykonać jego restart.