

Usługa mLegitymacji Ulgowych Usług Transportowych

§ 1. Definicje:

1. **Certyfikat** – poświadczenie, o którym mowa w art. 19e ust. 2a ustawy o informatyzacji, pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika, wydawane w ramach Usługi mObywatel.
2. **Certyfikat Ucznia** – poświadczenie, o którym mowa w art. 19e w ust. 2b pkt 1 ustawy o informatyzacji, pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika wydany w ramach usługi mLegitymacja szkolna.
3. **Legitymacja UUT** – dokument wydany przez PKP Intercity i potwierdzający uprawnienia jego posiadacza do korzystania z ulgowych usług transportowych zgodnie z Porozumieniem w sprawie ulgowych usług transportowych zawartym w dniu 27 listopada 2013 r. z późn. zm.
4. **PKP Intercity lub PKP** – „PKP Intercity” Spółka Akcyjna z siedzibą w Warszawie (KRS 0000296032, NIP 526 25 44 258) będąca dystrybutorem ulgowych usług transportowych zgodnie z Porozumieniem w sprawie ulgowych usług transportowych zawartym w dniu 27 listopada 2013 r. oraz podmiotem odpowiedzialnym za wydawanie Legitymacji UUT.
5. **Pracodawca** – PKP Intercity lub podmiot, który wystąpił do PKP Intercity o wydanie Legitymacji UUT dla Użytkownika.
6. **System UUT** - system PKP Intercity przechowujący przekazane przez pracodawców dane Użytkowników posiadających Legitymację UUT.
7. **Zasady odprawy UUT** – dokument wewnętrzny, ustalony przez pasażerskich przewoźników kolejowych, na podstawie Porozumienia w sprawie ulgowych usług transportowych z dnia 27 listopada 2013 r., który obowiązuje wyłącznie przy przejazdach osób uprawnionych do UUT pociągami tych przewoźników, wskazujący m.in. katalog osób uprawnionych do korzystania z mLegitymacji UUT.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach mLegitymacji UUT stanowi art. 19e ust. 2 pkt 3 ustawy o informatyzacji, zgodnie z którym Minister zapewnia działanie systemu teleinformatycznego, który pozwala, przy użyciu publicznej aplikacji mobilnej, na pobranie dokumentu elektronicznego zawierającego dane dotyczące sytuacji prawnej Użytkownika lub praw mu przysługujących.
2. Za zgodność danych zawartych w mLegitymacji UUT odpowiada Użytkownik, który jest zobowiązany do aktualizacji danych, jeżeli dane te uległy zmianie i posiada o nich wiedzę. W przypadku stwierdzenia, że dane znajdujące się na mLegitymacji UUT są nieprawidłowe lub nieaktualne, należy zgłosić się do Pracodawcy.

3. Korzystanie z mLegitymacji UUT nie zwalnia z obowiązków wynikających z przepisów prawa. Zbieranie danych innych Użytkowników, posługiwanie się nimi czy ich publikacja podlegają ograniczeniom prawnym wynikającym, m.in. z przepisów służących ochronie danych osobowych, dóbr osobistych i prywatności.
4. Aplikacja umożliwia pobranie mLegitymacji UUT posiadaczowi Legitymacji UUT, wskazanemu w Zasadach odprawy UUT i który zaloguje się do Aplikacji, bez konieczności wnioskowania o nią.

§ 3. mLegitymacja UUT

1. mLegitymacja UUT pozwala na pobranie przez Użytkownika, danych z bazy Systemu UUT oraz z Usługi mObywatel oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub przekazywanie.
2. Dane dostępne w mLegitymacji UUT pochodzą z Systemu UUT i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
3. Do aktywacji i aktualizacji mLegitymacji UUT niezbędne jest posiadanie ważnej Legitymacji UUT oraz ważnego Certyfikatu.

§ 4. Użytkownicy

Użytkownikami korzystającymi z mLegitymacji UUT mogą być wyłącznie osoby mające obywatelstwo polskie, które spełniają dwa poniższe warunki:

- 1) mają ważny Certyfikat;
- 2) posiadają aktualną i ważną Legitymację UUT.

§ 5. Aktywacja mLegitymacja UUT

1. Aktywacja mLegitymacji UUT w Aplikacji polega na:
 - 1) zalogowaniu do Aplikacji;
 - 2) wybraniu „mLegitymacja UUT” z listy dostępnych usług;
 - 3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu lub Certyfikatu Ucznia;
 - 4) pobraniu danych Użytkownika oraz jego uprawnień.
2. Ważność mLegitymacji UUT powiązana jest z ważnością Certyfikatu lub Certyfikatu Ucznia.
3. Certyfikat oraz Certyfikat Ucznia są wykorzystywane do:
 - 1) pobrania i podpisania danych w mLegitymacji UUT;
 - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z Systemu UUT;
 - 3) zapewnienia, że przekazywane dane w ramach mLegitymacji UUT są tożsame z danymi pobranymi z Systemu UUT oraz usługi mObywatel lub mLegitymacji szkolnej.
4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu lub Certyfikatu Ucznia oraz pobrania danych z Systemu UUT niezbędne jest aktywne połączenie internetowe.
5. Użytkownik posiadający usługę mObywatel może aktywować mLegitymację UUT i pobrać dane z Systemu UUT na nie więcej niż trzech urządzeniach mobilnych. Na jednym

urządzeniu mobilnym można aktywować i pobrać dane z Systemu UUT Użytkownika oraz osób powiązanych z Użytkownikiem.

6. Użytkownik posiadający mLegitymację szkolną może aktywować mLegitymację UUT i pobrać dane z Systemu UUT tylko na jednym urządzeniu mobilnym.
7. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, mLegitymacja UUT nie oferuje funkcji eksportu ani importu danych.
8. Dostęp do danych przechowywanych w mLegitymacji UUT jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje mLegitymacja UUT dla Użytkowników usługi mObywatel

1. Prawidłowo aktywowana usługa mLegitymacja UUT umożliwia Użytkownikowi korzystanie z następujących funkcji:
 - 1) okazanie danych Użytkownika, o których mowa w § 8 ust. 3, oraz kodu QR (widok główny „mLegitymacja UUT”);
 - 2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Przekaż”);
 - 3) przejście do usługi mObywatel w celu potwierdzenia swoich danych osobowych (funkcja „mObywatel”);
 - 4) prezentacja Legitymacji UUT dzieci lub współmałżonka Użytkownika, w sposób umożliwiający wyświetlanie przez Użytkownika Legitymacji UUT członków jego rodziny posiadających także Legitymacje UUT (funkcja „Moi bliscy”);
 - 5) aktualizowanie danych Użytkownika oraz osób powiązanych (funkcja „Aktualizuj”); 6) usunięcie mLegitymacji UUT z Aplikacji (funkcja „Usuń mLegitymację UUT”).
2. Użytkownik może okazać innej osobie mLegitymację UUT oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu usługi mLegitymacja UUT. Ekran prezentacji danych uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
 - 1) hologramu stanowiącego wizerunek orła ustalony jak dla godła Rzeczypospolitej Polskiej, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
 - 2) gilosza umieszczonego jako tło mLegitymacja UUT, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
 - 3) zegara mierzącego aktualny czas liczony w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z biegiem czasu.
3. Funkcja „Przekaż” pozwala na przekazanie do weryfikacji aplikacji mWeryfikator danych Użytkownika mLegitymacji UUT oraz danych mLegitymacji UUT pozostałych członków jego rodziny w postaci kodu QR . Przekazanie danych przebiega w następujący sposób:
 - 1) Użytkownik w mLegitymacji UUT wywołuje funkcję „Przekaż”;
 - 2) Użytkownik wybiera mLegitymację UUT osoby, której dane chce przekazać do aplikacji mWeryfikator;

- 3) w mLegitymacji UUT wyświetla się graficzny, kwadratowy kod QR, który zawiera informację o czasie jego wygenerowania. Po zamknięciu Aplikacji lub wygaśnięciu jej sesji, przekazanie danych wymaga ponownego wygenerowania kodu QR;
- 4) użytkownik mWeryfikatora odczytuje kod QR za pomocą aparatu fotograficznego urządzenia mobilnego, którym się posługuje;
- 5) następuje przekazanie danych zawartych w kodzie QR do urządzenia mobilnego użytkownika mWeryfikatora. mWeryfikator nie przechowuje pobranych danych.
4. Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu.
5. Usunięcie mLegitymacji UUT Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

§ 7. Funkcje mLegitymacji UUT dla Użytkowników mLegitymacji szkolnej

1. Prawidłowo aktywowana usługa mLegitymacja UUT umożliwia Użytkownikowi korzystanie, m.in. z następujących funkcji:
 - 1) okazanie danych Użytkownika oraz kodu QR (widok główny „mLegitymacja UUT”);
 - 2) przekazanie danych Użytkownika w celu weryfikacji (funkcja „Przekaż”);
 - 3) przejście do mLegitymacji szkolnej w celu potwierdzenia swoich danych osobowych (funkcja „mLegitymacja”);
 - 4) aktualizowanie informacji na temat uprawnień wraz z powiązanymi z nimi danymi Użytkownika (funkcja „Aktualizuj”);
 - 5) usunięcie mLegitymacji UUT z Aplikacji (funkcja „Usuń mLegitymację UUT”).
2. Użytkownik może okazać innej osobie dane mLegitymacji UUT oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu „mLegitymacja UUT”. Ekran prezentacji danych uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
 - 1) hologramu stanowiącego wizerunek orła ustalony jak dla godła Rzeczypospolitej Polskiej, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
 - 2) gilosza umieszczonego jako tło mLegitymacji UUT, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
 - 3) zegara mierzącego aktualny czas liczony w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z biegiem czasu.
3. Funkcja „Przekaż” pozwala na przekazanie do weryfikacji Aplikacji mWeryfikator zakodowanych w mLegitymacji UUT danych Użytkownika w postaci kodu QR. Przekazanie danych przebiega w następujący sposób:
 - 1) Użytkownik w mLegitymacji UUT wywołuje funkcję „Przekaż”;
 - 2) w mLegitymacji UUT wyświetla się graficzny, kwadratowy kod QR, który zawiera informację o czasie jego wygenerowania. Po zamknięciu Aplikacji lub wygaśnięciu jej sesji, przekazanie danych wymaga ponownego wygenerowania kodu QR;

- 3) użytkownik mWeryfikatora odczytuje kod QR za pomocą aparatu fotograficznego urządzenia mobilnego, którym się posługuje;
- 4) następuje przekazanie danych zawartych w kodzie QR do urządzenia mobilnego użytkownika mWeryfikatora. mWeryfikator nie przechowuje pobranych danych.
4. Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu Ucznia.
5. W przypadku dezaktywacji Certyfikatu Ucznia następuje automatyczne usunięcie mLegitymacja UUT.

§ 8. Prywatność i bezpieczeństwo

1. Administratorem danych osobowych Użytkownika pobieranych z Systemu UUT jest Pracodawca.
2. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie oraz Certyfikacie Ucznia jest Minister mający swą siedzibę w Kancelarii Prezesa Rady Ministrów, al. Ujazdowskie 1/3, 00-583 Warszawa. Z administratorem można się kontaktować na podany wyżej adres lub na adres ul. Królewska 27, 00-060 Warszawa lub elektronicznie, na adres: Kancelaria.Krolewska@mc.gov.pl lub na adres skrytki ePUAP: /MAiC/SkrytkaESP. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować sprawach związanych z przetwarzaniem danych osobowych przez Ministra bezpośrednio pod adresem: iod@mc.gov.pl.
3. Administratorem danych osobowych uczniów, którym wydano mLegitymację szkolną jest Szkoła.
4. W ramach usługi mLegitymacja UUT w Aplikacji przechowuje się następujące dane:
 - 1) pierwsze imię Użytkownika Legitymacji UUT oraz osób powiązanych;
 - 2) drugie imię Użytkownika oraz osób powiązanych;
 - 3) nazwisko Użytkownika oraz osób powiązanych;
 - 4) numer PESEL Użytkownika oraz osób powiązanych;
 - 5) wizerunek twarzy Użytkownika;
 - 6) seria i numer mLegitymacji UUT Użytkownika oraz osób powiązanych;
 - 7) Pracodawca;
 - 8) kategoria Użytkownika;
 - 9) klasa wagonu;
 - 10) status mLegitymacji UUT Użytkownika oraz osób powiązanych;
 - 11) informacja na temat Certyfikatu użytego do wydania danych;
 - 12) termin ważności mLegitymacji UUT Użytkownika oraz osób powiązanych.
5. Osobie, której dane są przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19e ust. 2 ustawy o informatyzacji, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych, w tym w szczególności z art. 6 ust. 1 lit. e:
 - 1) prawo dostępu do treści danych;
 - 2) prawo do sprzeciwu do przetwarzania danych;

- 3) prawo do ograniczenia przetwarzania danych osobowych przez Ministra; w takim przypadku Minister oznaczy te dane i nie będzie ich przetwarzał w systemie do czasu wyjaśnienia sprawy (poza ich przechowywaniem);
 - 4) prawo do wniesienia skargi do organu nadzorczego.
6. Minister gromadzi dane statystyczne dotyczące mLegitymacji UUT w zakresie liczby:
 - 1) aktywacji mLegitymacji UUT;
 - 2) akcji aktualizacji danych i wydania Certyfikatów;
 - 3) zgłoszonych utrat telefonów;
 - 4) zgłoszonych problemów.
7. Dane, o których mowa w ust. 4 są przetwarzane wyłącznie w trakcie korzystania z mLegitymacji UUT i w celu dostarczenia obywatelom usługi umożliwiającej prezentację danych z systemu UUT oraz zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
8. Dane, o których mowa w ust. 4 przechowywane są do roku od dnia utraty Legitymacji UUT. Dane nie są przetwarzane w celach marketingowych.
9. Minister nie gromadzi informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych.
10. Dane osobowe, przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19e ust. 2 ustawy o informatyzacji, nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
11. Dane osobowe, o których mowa w ust. 4, będą również przetwarzane przez: Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa jako odpowiednio:
 - 1) podmiot przetwarzający dane osobowe,
 - 2) dalszy podmiot przetwarzający dane osobowe.
12. Dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej.

Załącznik nr 9 do Regulaminu

Usługi Diia.pl w aplikacji mObywatel - dostępne funkcje, ochrona danych osobowych

Za pomocą usługi Diia.pl możesz bezpiecznie:

- okazywać swoje dane innym osobom – tym samym potwierdzając swoją tożsamość,
- przekazać swoje dane podmiotom publicznym lub niepublicznym w celu skorzystania z oferowanych przez nie usług.

§ 1. Definicje:

1. **Certyfikat Diia.pl** – certyfikat kryptograficzny, o którym mowa w art. 19e ust. 2a ustawy o informatyzacji, stanowiący poświadczenie autentyczności danych Użytkownika pobranych z Rejestru w ramach usługi Diia.pl.
2. **Profil Zaufany** - środek identyfikacji elektronicznej wydany w systemie identyfikacji elektronicznej przyłączony do węzła krajowego albo za pośrednictwem węzła transgranicznego.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych osobowych w ramach Diia.pl stanowi art. 10 ustawy o pomocy obywatelom Ukrainy zgodnie z którym możliwe jest pobranie aktualnych danych, o których mowa w art. 4 ust. 4 pkt 1-15 oraz art. 5 ust. 5 pkt 2 i 3 ustawy o pomocy obywatelom Ukrainy oraz art. 8 pkt 23 i 24a lit. d ustawy z dnia 24 września 2010 r. o ewidencji ludności .
2. Korzystanie z Diia.pl nie zwalnia Użytkownika z obowiązków wynikających z przepisów prawa. Zbieranie danych innych użytkowników, posługiwanie się nimi czy ich publikacja podlegają ograniczeniom prawnym wynikającym m.in. z przepisów służących ochronie danych osobowych, dóbr osobistych i prywatności.

§ 3. Usługa Diia.pl

1. Usługa Diia.pl pozwala na pobranie danych osobowych i wizerunku Użytkownika z Rejestru oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika. Za pośrednictwem Diia.pl dane Użytkownika przechowywane w Usłudze mogą być w sposób bezpieczny okazywane innym osobom lub Użytkownikowi mWeryfikatora.
2. Wiarygodność danych dostępnych w Usłudze Diia.pl wynika z faktu, że dane pochodzą z Rejestru i zostały pobrane przez osobę, która została zidentyfikowana przez Rzeczpospolitą Polską. Dane te są przechowywane i przesyłane za pomocą Aplikacji udostępnionej przez Rzeczpospolitą Polską.

3. Nie jest możliwe posługiwanie się Diia.pl w stosunkach z administracją publiczną wtedy, gdy z przepisów prawa (ustawy, rozporządzenia) wynika obowiązek przedstawienia innych dokumentów stwierdzających tożsamość Użytkownika, stwierdzanych prawo Użytkownika do pobytu na terytorium Rzeczypospolitej Polskiej lub innych praw przysługujących Użytkownikowi.
4. Diia.pl spełnia rolę dokumentu pobytowego i umożliwia Użytkownikom przekraczanie granic zewnętrznych i podróżowanie w strefie Schengen przez 90 dni (w okresie 180 dni) wraz z ważnym dokumentem podróży (np. paszportem). Przy czym wyjazd z Polski na okres dłuższy niż 1 miesiąc (bez względu na to czy w ramach czy poza strefą Schengen) pozbawia uprawnień wynikających z ustawy o pomocy obywatelom Ukrainy, w tym prawa posługiwania się Diia.pl
5. Posługiwanie się Diia.pl przez Użytkowników jest dobrowolne. Minister informuje, że aktywacja Diia.pl i posługiwanie się nią nie jest prawnym obowiązkiem osób przebywających na terytorium Rzeczypospolitej Polskiej.
6. Skorzystanie z usługi weryfikacji online jest dobrowolne. Weryfikowany Użytkownik korzysta z odpowiedniej funkcji Diia.pl, a Użytkownik mWeryfikatora z odpowiedniej funkcji mWeryfikatora.
7. Do aktywacji i aktualizacji Diia.pl niezbędne jest posiadanie Profilu zaufanego.

§ 4. Użytkownicy

1. Użytkownikami Diia.pl mogą być wyłącznie osoby, które spełniają poniższe warunki:
 - 1) przebywają legalnie na terytorium Rzeczypospolitej Polskiej zgodnie z przepisami ustawy o pomocy obywatelom Ukrainy i deklarują zamiar pozostania na terytorium Rzeczypospolitej Polskiej;
 - 2) ich wyjazd na terytorium Rzeczypospolitej Polskiej został zarejestrowany przez właściwy organ Straży Granicznej;
 - 3) mają nadany numer PESEL,
 - 4) posiadają Profil Zaufany.

§ 5. Aktywacja Usługi

1. Przy pierwszym użyciu Diia.pl dokonywana jest aktywacja Usługi.
2. Aktywacja usługi Diia.pl przez Użytkownika polega na:
 - 1) zalogowaniu do Aplikacji;
 - 2) potwierdzeniu tożsamości Użytkownika przy użyciu Profilu Zaufanego.
3. Po wykonaniu czynności opisanych w ust. 2, nastąpi automatyczne pobranie danych Użytkownika z Rejestru oraz zaszyfrowanie i zapisanie ich w urządzeniu mobilnym Użytkownika.
4. Brak akceptacji Regulaminu przez Użytkownika uniemożliwia aktywację Diia.pl.

5. Po pobraniu danych z Rejestru automatycznie jest tworzony i pobierany Certyfikat Diia.pl. Certyfikat Diia.pl przypisany jest do Użytkownika i urządzenia mobilnego, którym posługuje się Użytkownik. W celu utworzenia Certyfikatu Diia.pl i zarządzania Certyfikatami Minister przetwarza dane osobowe Użytkownika – imiona, nazwisko i numer PESEL – pochodzące z Rejestru.
6. Ważność Certyfikatu Diia.pl jest ograniczona w czasie i wynosi nie więcej niż jeden rok od daty aktywacji usługi Diia.pl.
7. Do potwierdzenia tożsamości Użytkownika przy użyciu Profilu Zaufanego, pobrania Certyfikatu Diia.pl oraz pobrania danych z Rejestru niezbędne jest aktywne połączenie internetowe.
8. Użytkownik może aktywować Diia.pl i pobrać dane z Rejestru na nie więcej niż trzech urządzeniach mobilnych jednocześnie. Na jednym urządzeniu mobilnym można aktywować i pobrać dane z Rejestru tylko jednego Użytkownika.
9. Nie jest możliwe pobranie danych z Rejestru, jeżeli Użytkownik nie spełnia warunków określonych w § 4 ust. 1 Regulaminu, w szczególności nie posiada Profilu Zaufanego, bądź też w przypadku podjęcia próby aktywacji usługi mObywatel na czwartym i kolejnych urządzeniach mobilnych.
10. Poza funkcją elektronicznego przekazania danych osobowych Aplikacja nie oferuje funkcji eksportu ani importu danych.
11. Dostęp do danych przechowywanych w usłudze Diia.pl jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje usługi Diia.pl

1. Z zastrzeżeniem postanowienia ust. 2 poniżej, prawidłowo aktywowana usługa Diia.pl po zalogowaniu się z użyciem hasła dostępu do Aplikacji umożliwia Użytkownikowi korzystanie z następujących funkcji:
 - 1) okazanie danych Użytkownika (moduł „Diia.pl”);
 - 2) elektroniczne przekazanie danych Użytkownika (funkcja „Przełącz”);
 - 3) przechowywanie informacji o przekazaniu danych do weryfikacji (funkcja „Historia”);
 - 4) aktualizowanie danych Użytkownika;
 - 5) zarządzanie Certyfikatem;
 - 6) usunięcie usługi Diia.pl.
2. Użytkownik może okazać osobie trzeciej swoje dane osobowe na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i wybraniu „Diia.pl”. Ekran prezentacji danych uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
 - 1) ruchomego elementu graficznego, prezentującego niebiesko-żółtą flagę Ukrainy;

- 2) elementu graficznego o zmiennej kolorystyce, uzależnionej od kąta pochylenia urządzenia mobilnego (hologramu), w kształcie odpowiadającym godłu Rzeczypospolitej Polskiej;
 - 3) grafiki tła (znaku wodnego) stanowiącego stylizowany rysunek Trójzębu z Herbu Ukrainy.
3. **Korzystanie z funkcji „Przekaż”.** Funkcja ta pozwala na elektroniczne przekazanie danych Użytkownika (zwanego dalej „Użytkownikiem przekazującym dane”):
- 1) Instytucji,
 - 2) Osobie weryfikującej Twoją tożsamość (Użytkownikowi mWeryfikatora).
4. **Elektroniczne przekazanie danych do Instytucji.** Funkcja ta pozwala na przekazanie danych Użytkownika do systemu teleinformatycznego Instytucji. W tym celu Użytkownik przekazujący elektronicznie dane powinien:
- 1) wybrać funkcję „Przekaż Instytucji lub firmie” i przycisk „Przekaż”;
 - 2) Użytkownik skanuje Kod QR Instytucji (okazany na stronie internetowej Instytucji – online lub w placówce instytucji – onsite);
 - 3) w usłudze Diia.pl pojawia się komunikat o nawiązywaniu połączenia z Instytucją;
 - 4) pojawia się komunikat jakie dane i jakiej Instytucji zostaną przekazane;
 - 5) Użytkownik wybiera przycisk „Potwierdzam”;
 - 6) następuje przekazanie danych Użytkownika do Instytucji;
 - 7) pojawia się komunikat o wyniku przekazania danych.
5. **Elektroniczne przekazanie danych Użytkownika użytkownikowi mWeryfikatora** umożliwia przesłanie niektórych danych osobowych Użytkownika wymienionych w § 9 ust.2 do urządzenia mobilnego, którym posługuje się Użytkownik mWeryfikatora. Czynność ta jest połączona z potwierdzeniem poprawności Certyfikatu Użytkownika przekazującego dane. W tym celu Użytkownik przekazujący dane elektronicznie powinien:
- 1) wybrać funkcję „Przekaż”;
 - 2) następnie wybiera funkcję „Osobie weryfikującej Twoją tożsamość” i przycisk „Przekaż”;
 - 3) w usłudze Diia.pl wyświetli się graficzny, kwadratowy Kod QR, który zawiera informację o czasie jego wygenerowania i jest ważny 10 minut od chwili jego wygenerowania. Po upływie tego czasu przekazanie danych wymaga ponownego wygenerowania Kodu QR. Również po zamknięciu Aplikacji lub wygaśnięciu jej sesji, przekazanie danych wymaga ponownego wygenerowania Kodu QR,
 - 4) użytkownik mWeryfikatora odczytuje Kod QR za pomocą aparatu fotograficznego urządzenia mobilnego, którym się posługuje,

- 5) następuje przekazanie danych zawartych w Kodzie QR do urządzenia mobilnego Użytkownika mWeryfikatora.
6. Przy korzystaniu z funkcji elektronicznej weryfikacji danych osobowych, pomiędzy Użytkownikiem a Użytkownikiem mWeryfikatora przekazywane są następujące dane:
- 1) imię (imiona) i nazwisko,
 - 2) zdjęcie o zredukowanej jakości,
 - 3) data i godzina wymiany danych,
 - 4) status Certyfikatu Diia.pl.
7. mWeryfikator nie zapisuje danych Użytkownika, którego dane zostały zweryfikowane z wykorzystaniem usługi mObywatel. Wszystkie dane dotyczące tego Użytkownika są usuwane z mWeryfikatora po wyjściu z ekranu wyświetlania danych.
8. **Funkcja „Historia”** pozwala na zapoznanie się z historią weryfikacji danych osobowych za pomocą mWeryfikatora, zawierającą identyfikator Użytkownika mWeryfikatora oraz datę i czas przekazania danych.
9. Funkcja „Historia” przechowuje dane, o których mowa w ustępie poprzedzającym, przez 1 rok od daty ich zapisania w usłudze Diia.pl.
10. **Funkcja aktualizacji danych Użytkownika** (dostępna z menu usługi Diia.pl), umożliwia ponowne pobranie danych Użytkownika z Rejestru oraz zapisanie ich w urządzeniu mobilnym Użytkownika. Z funkcji tej należy korzystać po zmianie danych zawartych w Rejestrze.
11. Funkcja aktualizacji danych Użytkownika wymaga potwierdzenia tożsamości Użytkownika przy użyciu Profilu Zaufanego. Do aktualizacji danych Użytkownika odpowiednio stosuje się postanowienia §5 niniejszego załącznika.
12. **Funkcja zarządzania Certyfikatem** (dostępna z menu usługi Diia.pl) umożliwia unieważnienie Certyfikatów Diia.pl. Po unieważnieniu Certyfikatu Diia.pl dla pojedynczego urządzenia mobilnego dane przechowywane w usłudze mObywatel nie są dostępne dla Użytkownika. Nie jest także możliwe prawidłowe korzystanie z funkcji „Przełącz”. W przypadku wybrania tej funkcji wyświetlać się będzie komunikat „Brak ważnego Certyfikatu”.
13. **Funkcja usunięcia danych** (dostępna z menu usługi Diia.pl) usuwa wszystkie dane przechowywane w usłudze mObywatel oraz unieważnia Certyfikat Diia.pl. Po użyciu tej funkcji usługa Diia.pl nie ulega odinstalowaniu z urządzenia mobilnego, jednak aby mogła być ponownie używana, wymaga ponownego aktywowania, zgodnie z Regulaminem.

§ 7. Dostęp do usług online eRecepta

1. Certyfikat usługi Diia.pl umożliwia prezentację za pośrednictwem Aplikacji wydanej Użytkownikom usługi online eRecepta.
2. Przy pierwszym użyciu usługi online dokonywana jest jej aktywacja. Aktywacja wymaga posiadania ważnego Certyfikatu usługi Diia.pl, za pomocą którego dane Użytkownika uwierzytelniane są w systemach teleinformatycznych usługodawcy, Centrum e-Zdrowia.
3. Uwierzytelnienie Użytkownika w systemie, o którym mowa w ust. 2, umożliwia prezentację w Aplikacji:
 - 1) niezrealizowanych recept wystawionych Użytkownikowi w wersji elektronicznej. Korzystanie przez Użytkownika z systemu, o którym mowa w zdaniu 1, odbywa się na zasadach określonych odrębnie przez Ministra Zdrowia w Regulaminie Internetowego Konta Pacjenta.
4. Dezaktywacja usług następuje poprzez dezaktywację usługi mObywatel.

§ 8. Dostęp do usługi Unijny Certyfikat COVID UA

1. Certyfikat usługi Diia.pl umożliwia prezentację za pośrednictwem Aplikacji potwierdzenia, że dana osoba została zaszczepiona przeciw wirusowi SARS-Cov-2 i/lub uzyskała ujemny wynik testu na obecność wirusa SARS-Cov-2 i/lub przeszła COVID-19 (usługa UCC).
2. Przy pierwszym użyciu usługi Unijny Certyfikat COVID dokonywana jest jej aktywacja. Aktywacja usługi wymaga posiadania ważnego Certyfikatu usługi Diia.pl, za pomocą którego dane Użytkownika uwierzytelniane są w systemie teleinformatycznym Ministerstwa Zdrowia, którego dostawcą jest Centrum e-Zdrowia (IKP).
3. Uwierzytelnienie Użytkownika w systemie, o którym mowa w ust. 2, umożliwia prezentację w Aplikacji potwierdzenia, że dana osoba została zaszczepiona przeciw wirusowi SARS-Cov-2 i/lub uzyskała ujemny wynik testu na obecność wirusa SARS-Cov-2 i/lub przeszła COVID-19.

Dezaktywacja usługi Unijny Certyfikat COVID następuje poprzez dezaktywację usługi Diia.pl.

§ 9. Prywatność i bezpieczeństwo

1. Minister jest administratorem danych osobowych Użytkownika, mający swą siedzibę w Kancelarii Prezesa Rady Ministrów, al. Ujazdowskie 1/3, 00-583 Warszawa.
2. Z administratorem można się kontaktować na podany wyżej adres lub na adres ul. Królewska 27, 00-060 Warszawa lub elektronicznie, na adres: Kancelaria.Krolewska@mc.gov.pl, lub na adres skrytki ePUAP: /MAiC/SkrytkaESP.
3. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować sprawach związanych z przetwarzaniem danych osobowych przez Ministra właściwego

do spraw informatyzacji (Ministra Cyfryzacji) bezpośrednio pod adresem:
iod@mc.gov.pl.

4. W usłudze Diia.pl i w Aplikacji przechowuje się następujące dane Użytkownika:
 - 1) imię (imiona);
 - 2) nazwisko;
 - 3) datę urodzenia;
 - 4) miejsce urodzenia;
 - 5) kraj urodzenia;
 - 6) obywatelstwo
 - 7) płeć;
 - 8) numer PESEL;
 - 9) fotografię;
 - 10) Status Cudzoziemca;
 - 11) seria i numer dokumentu tożsamości cudzoziemca;
 - 12) data ważności dokumentu.
5. Podstawą przetwarzania danych osobowych w Diia.pl przez administratora danych (**Ministra**) w systemie obsługującym działanie Diia.pl jest art. 6 ust. 1 lit. e Ogólnego rozporządzenia o ochronie danych, w związku z art. 19 h ustawy o informatyzacji.
6. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych:
 - 1) prawo dostępu do treści danych;
 - 2) prawo ich poprawiania i sprostowania;
 - 3) prawo do sprzeciwu do przetwarzania danych;
 - 4) prawo do ograniczenia przetwarzania danych osobowych przez Ministra, w takim przypadku Minister oznaczy te dane i nie będzie ich przetwarzał w systemie do czasu wyjaśnienia sprawy (poza ich przechowywaniem).
 - 5) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
7. Prawo do poprawienia lub sprostowania danych realizowane jest wyłącznie poprzez poprawienie danych znajdujących się w systemie teleinformatycznym zapewniających funkcjonowanie usługi mObywatel oraz dotyczy danych, o których mowa w ust. 4.
8. Okazanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Okazanie oraz elektroniczne przekazanie danych, o których mowa w zdaniu poprzedzającym, następuje w ramach realizacji uprawnień lub obowiązków Użytkownika w stosunku do innych Użytkowników.

9. W zakresie przetwarzania i ochrony danych, które Użytkownik uzyskał w toku elektronicznego okazywania danych osobowych bądź elektronicznego weryfikowania danych osobowych, Użytkownika obowiązuje stosowanie się do powszechnie obowiązujących przepisów prawa.
10. W celu utworzenia Certyfikatu podczas aktywacji Diia.pl oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister przetwarza dane – imiona, nazwisko, kraj oraz numer PESEL Użytkownika – pobierane z Rejestru podczas aktywacji usługi.
11. Minister przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.
12. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
13. Minister gromadzi dane statystyczne dotyczące Diia.pl w zakresie liczby:
 - 1) aktywacji usługi mObywatel,
 - 2) akcji aktualizacji danych i wydania Certyfikatów,
 - 3) zgłoszonych utrat telefonów,
 - 4) zgłoszonych problemów.
14. Minister przetwarza dane osobowe wskazane w ustępach poprzedzających przez okres 6 lat od dnia ostatniej aktywności w Aplikacji. Dane nie są przetwarzane w celach marketingowych.
15. Z zastrzeżeniem ustępów poprzedzających Minister nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z Diia.pl, danych o połączeniach między nimi ani danych o Użytkownikach w związku z korzystaniem z funkcji weryfikacji online w mWeryfikatorze. Minister nie gromadzi również informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych.
16. Dane osobowe, o których mowa w tym paragrafie, mogą być również przetwarzane przez podmioty przetwarzające w imieniu administratora (Ministra), to jest przez:
 - 1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
 - 2) Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa.
17. Dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej.
18. Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.