

Usługa mLegitymacja studencka - dostępne funkcje, ochrona danych osobowych

Usługa pozwala korzystać z mLegitymacji studenckiej – dokumentu elektronicznego, który ma taką samą funkcję i moc prawną, jak legitymacja wydana w wersji papierowej lub w postaci plastikowej karty (e-legitymacji). Za pomocą Usługi mLegitymacja studencka możesz:

- potwierdzić, że jesteś studentem danej uczelni,
- skorzystać z ulg i zwolnień, które przysługują po okazaniu legitymacji.

Ileokroć w załączniku pojawia się pojęcie pisane wielką literą i niezdefiniowane w definicjach to ma ono znaczenie nadane im przez Regulamin.

§ 1. Definicje:

1. **Certyfikat Studenta**– 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 studencka.
2. **System**– system teleinformatyczny zapewniany przez Ministra Cyfryzacji, który pozwala na wydanie przez rektora uczelni mLegitymacji studenckiej i wygenerowanie danych osobowych studenta oraz danych potwierdzających status mLegitymacji studenckiej.
3. **Uczelnia**– uczelnia wydająca mLegitymację studencką.

§ 2. Informacje ogólne

1. Usługa stanowi mLegitymację studencką – legitymację studencką, o której mowa w art. 74 ust. 4 Ustawy z dnia z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2022. poz. 574) – i jest dokumentem elektronicznym zawierającym dane dotyczące sytuacji prawnej użytkownika publicznej aplikacji mobilnej lub praw mu przysługujących, o którym mowa w art. 19e ust. 2 pkt 2 ustawy o informatyzacji.

§ 3. Użytkownicy

1. Użytkownikami Usługi mLegitymacja studencka, zwanej dalej „mLegitymacją”, mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
 - 1) mają nadany numer PESEL;
 - 2) są osobami, którym uczelnia wydała mLegitymację – zwani dalej „Studentami” lub pojedynczo „Studentem”.
2. Zabrania się Studentowi:
 - 1) udostępniania Aplikacji w celu posłużenia się nią przez inną osobę,
 - 2) udostępniania jednorazowego kodu QR oraz hasła otrzymanego od Uczelni, umożliwiającego dostęp do Usługi.

§ 4. Aktywacja Usługi

1. Przy pierwszym użyciu Usługi dokonywana jest aktywacja Usługi.
2. Do przeprowadzenia aktywacji Usługi niezbędne jest aktywne połączenie internetowe.
3. Aktywacja Usługi polega na:
 - 1) wystąpieniu przez Studenta do Uczelni o wydanie mLegitymacji;
 - 2) nadaniu przez właściwą Uczelnię uprawnień w Systemie, wgraniu zdjęcia Studenta w Systemie, wygenerowaniu kodu QR i jednorazowego kodu aktywującego mLegitymację;
 - 3) zalogowaniu do Aplikacji;
 - 4) wczytaniu kodu QR oraz wpisaniu przez użytkownika kodu aktywacyjnego mLegitymacji;
 - 5) pobraniu danych osobowych Studenta z Systemu.
4. Jednorazowy kod aktywacyjny oraz kod QR jest ważny 30 dni od momentu jego wygenerowania w systemie.
5. Student może aktywować Usługę i pobrać dane z Systemu wyłącznie na jednym urządzeniu mobilnym.
6. Po pobraniu danych z Systemu automatycznie jest tworzony i pobierany do Usługi Certyfikat Studenta. Certyfikat Studenta przypisany jest do Studenta i urządzenia mobilnego, którym posługuje się Student.
7. Ważność Certyfikatu Studenta jest ograniczona w czasie i jest tożsama z okresem ważności wydanej Studentowi odpowiednio legitymacji studenckiej.
8. Nie jest możliwe nadanie uprawnień przez Uczelnię w Systemie oraz aktywacja Usługi – jeżeli osoba nie spełnia warunków określonych w § 3 ust. 1 niniejszego załącznika Regulaminu, w szczególności kiedy zostało zgłoszone zaginięcie lub uszkodzenie odpowiednio legitymacji bądź też w przypadku podjęcia próby aktywacji Usługi na kolejnym urządzeniu mobilnych.
9. Poza funkcjami elektronicznego przekazania danych oraz elektronicznej weryfikacji danych osobowych Aplikacja nie oferuje funkcji eksportu ani importu danych.
10. Dostęp do danych przechowywanych w Usłudze jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 5. Funkcje mLegitymacji

1. Okazanie mLegitymacji na ekranie urządzenia mobilnego:
 - 1) zgodne z przepisami prawa okazanie mLegitymacji ma skutek analogiczny jak okazanie legitymacji studenckiej;

- 2) pozwala ocenić osobie uprawnionej do kontroli legitymacji prawdziwość mLegitymacji studenckiej między innymi na podstawie następujących elementów graficznych:
- a) zdjęcia osoby legitymowanej,
 - b) numeru legitymacji i wieku użytkownika,
 - c) statusu: „ważna” lub „nieważna”,
 - d) hologramu – którego wygląd pozwala na stwierdzenie, iż nie stanowi on statycznego obrazu, lecz jest faktycznie generowany przez Aplikację,
 - e) flagi Polski – której wygląd pozwala na stwierdzenie, iż nie stanowi ona statycznego obrazu, lecz jest faktycznie generowana przez Aplikację,
 - f) czasu okazania.

2. Przekazanie danych z usługi mLegitymacja do Aplikacji mWeryfikator.

- 1) Elektroniczne przekazanie danych Studenta użytkownikowi Aplikacji mWeryfikator umożliwia przesłanie niektórych danych w mLegitymacji do użytkownika Aplikacji mWeryfikator.
- 2) Student przekazujący dane powinien:
 - a) wybrać funkcję „Przekaż” w Aplikacji;
 - b) po pojawieniu się odpowiedniego komunikatu wybrać i zaakceptować opcję „Przekazanie danych”;
 - c) Po wyświetleniu w Aplikacji kwadratowego kodu graficznego (dalej „Kod QR”) Użytkownik Aplikacji mWeryfikator może odczytać ten Kod QR za pomocą aparatu fotograficznego jego urządzenia mobilnego. Kod QR zawiera informację o czasie i jest ważny 10 minut od chwili jego wygenerowania. Po upływie tego czasu przekazanie danych wymaga ponownego wygenerowania Kodu QR.
 - d) Po prawidłowym zeskanowaniu Kodu QR pomiędzy urządzeniami mobilnymi Studenta i użytkownika aplikacji mWeryfikator nawiązywane jest połączenie Bluetooth i dokonywana jest weryfikacja czasu urządzeń, który nie może się różnić o więcej, niż 5 (pięć) minut. W przypadku różnicy czasu większej niż 5 (pięć) minut lub w przypadku wygaśnięcia ważności Kodu QR przekazanie danych zakończy się niepowodzeniem.
 - e) Po nawiązaniu połączenia Aplikacja przekazuje do Aplikacji mWeryfikator dane Studenta przekazującego dane, umożliwiając ich wyświetlenie w Aplikacji mWeryfikator oraz weryfikację poprawności jej Certyfikatu. Użytkownik Aplikacji mWeryfikator może dodatkowo zweryfikować przekazane dane online przy pomocy funkcji weryfikacji aktualności Certyfikatu.

- f) Po prawidłowym zakończeniu elektronicznej weryfikacji danych osobowych Studenta dane dotyczące dokonanej weryfikacji zapisywane są w Usłudze mLegitymacja (funkcja „Historia”).
- 3) Przy korzystaniu z powyższej funkcji „Przełącz” przekazywane są następujące dane:
 - a) numer legitymacji oraz data jej wydania,
 - b) imię (imiona) i nazwisko Studenta,
 - c) wiek Studenta,
 - d) termin ważności mLegitymacji,
 - e) nazwa i adres uczelni,
 - f) zdjęcie o zredukowanej jakości.
- 4) Aplikacja mWeryfikator nie zapisuje danych Studenta, którego dane zostały zweryfikowane z wykorzystaniem tej aplikacji. Wszystkie dane dotyczące tego Studenta są usuwane z aplikacji mWeryfikator po wyjściu z ekranu wyświetlania danych.
- 3. Wszystkie przypadki przekazania danych użytkownikowi Aplikacji mWeryfikator są zapisane w „Historii”. Funkcja „Historia” pozwala na zapoznanie się z historią weryfikacji danych osobowych za pomocą Aplikacji mWeryfikator, zawierającej wyłącznie identyfikator użytkownika Aplikacji mWeryfikator oraz datę i czas przekazania danych.
- 4. Funkcja „Historia” przechowuje dane, o których mowa w ustępie poprzedzającym, przez okres 1 roku od daty ich zapisania w Usłudze.

§ 6. Unieważnianie mLegitymacji i usuwanie danych Studenta:

- 1. Funkcja usunięcia danych z Aplikacji (dostępna z menu Aplikacji) usuwa wszystkie dane przechowywane w Aplikacji oraz unieważnia Certyfikat. Po użyciu tej funkcji Aplikacja nie ulega odinstalowaniu z urządzenia mobilnego, jednak aby mogła być ponownie używana, wymaga ponownego aktywowania, zgodnie z § 4 niniejszego załącznika Regulaminu.
- 2. Unieważnienie mLegitymacji jest dokonywane przez Uczelnię. Następuje ono w przypadku:
 - 1) utraty ważności wydanej Studentowi legitymacji studenckiej;
 - 2) utraty mLegitymacji na skutek uszkodzeń, niepoprawnego działania lub utraty urządzenia mobilnego, w którym przechowywana była mLegitymacja;
 - 3) w przypadku przejścia Studenta do innej Uczelni;
 - 4) na wniosek Studenta.

§ 7. Prywatność i bezpieczeństwo

- 1. Podstawą przetwarzania danych osobowych w Aplikacji przez Ministra Cyfryzacji są artykuły 19f i 19h ustawy o informatyzacji.

2. Zgodnie z art. 19h ustawy o informatyzacji Minister Cyfryzacji przetwarza w systemie teleinformatycznym, o którym mowa w art. 19e, dane osobowe użytkowników publicznej aplikacji mobilnej w zakresie niezbędnym do obsługi dokumentów elektronicznych (mLegitymacji) oraz zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
3. Studentowi przysługuje w dowolnym momencie prawo:
 - 1) dostępu do treści danych,
 - 2) poprawiania i sprostowania danych przez Uczelnię,
 - 3) do usunięcia danych, np. za pomocą funkcji „usunięcia danych z Aplikacji”.
4. Studentowi przysługuje również prawo do ograniczenia przetwarzania danych osobowych w przypadkach określonych w art. 18 Ogólnego rozporządzenia o ochronie danych. W takim przypadku Minister, na podstawie wniosku Studenta, w systemie obsługującym mLegitymacje studenckie, oznaczy dane i nie będzie ich – poza ich posiadaniem – przetwarzał, nawet w celach statystycznych, do czasu wyjaśnienia sprawy.
5. Jeżeli Student nie chce dalej korzystać z mLegitymacji, może poprosić Uczelnię o jej unieważnienie.
6. W przypadku zgubienia, kradzieży lub utraty z innych przyczyn urządzenia mobilnego, Student powinien niezwłocznie zgłosić ten fakt Uczelni.
7. Aby utworzyć Certyfikat Studenta podczas aktywacji Usługi oraz zarządzać Certyfikatami Studenta, w tym utrzymaniem listy aktywnych Certyfikatów Studenta, Minister przetwarza dane Studenta: imię, nazwisko, numer legitymacji oraz numer PESEL.
8. Minister gromadzi dane statystyczne dotyczące Usługi w zakresie liczby:
 - 1) aktywacji mLegitymacji,
 - 2) akcji wydania Certyfikatów,
 - 3) unieważnionych mLegitymacji,
 - 4) zgłoszonych problemów.
9. Z zastrzeżeniem ustępów następnych Minister nie przetwarza danych o połączeniach między urządzeniem mobilnym Studenta używającego mLegitymacji a użytkownikiem Aplikacji mWeryfikator. Minister nie gromadzi również informacji o skorzystaniu przez Studentów z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych.
10. Minister przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu Studenta (sprawdzenie ważności Certyfikatu Studenta online) za pomocą Aplikacji mWeryfikator gromadzi następujące dane:
 - 1) identyfikator użytkownika Aplikacji mWeryfikator;
 - 2) numer Certyfikatu Studenta przekazującego dane, weryfikowanego za pomocą Aplikacji mWeryfikator.

11. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji aktualności Certyfikatu Studenta oraz wykrycia ewentualnych błędów i luk bezpieczeństwa.
12. Dane, o których mowa w tym paragrafie przechowywane są przez okres 6 lat od dnia ostatniej aktywności Użytkownika w systemie teleinformatycznym Aplikacji (art. 19h ustawy o informatyzacji). Dane nie są przetwarzane w celach marketingowych. Dane nie są przetwarzane w celach marketingowych.
13. Administratorem danych zawartych w mLegitymacji jest Uczelnia, do której uczęszcza Student.
14. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie Studenta 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.
15. Dane nie są przetwarzane w celach marketingowych.
16. Dane osobowe Użytkownika będą mogły również być przetwarzane odpowiednio 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 Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.