

Drogi użytkowniku! Dziękujemy za pobranie aplikacji mObywatel. Prosimy, abyś przed rozpoczęciem korzystania z Aplikacji zapoznał się z regulaminem. Wyjaśnia on sposób i zasady działania Aplikacji, a także zawiera ważne informacje dotyczące Twoich danych osobowych i bezpieczeństwa.

Aplikacja mObywatel umożliwia wgląd do Twoich danych i ich pobranie z rejestru PESEL oraz Rejestru Dowodów Osobistych. Pobrane dane są przechowywane w zaszyfrowanej formie na Twoim urządzeniu mobilnym. Za pomocą Aplikacji możesz przekazywać Twoje dane innym osobom, umożliwić im potwierdzenie Twoich danych, a także pobierać od innych użytkowników Aplikacji ich dane.

Pamiętaj, że aplikacja nie jest dowodem osobistym i nie zastępuje dowodu osobistego.

Aplikacja umożliwia potwierdzenie Twoich danych osobistych (imienia, nazwiska czy wieku) w stosunkach prywatnych (np. w razie stłuczki, najmu roweru czy mieszkania). Potwierdzenie Twoich danych może być dokonane przez inną osobę posługującą się Aplikacją lub przez osobę posługującą się aplikacją mWeryfikator, udostępnianą na odrębnych zasadach. Wiarygodność danych zawartych w Aplikacji wynika z faktu, że dane pochodzą z rejestrów państwowych i zostały pobrane przez osobę, która została zidentyfikowana przez Państwo. Dane są też przechowywane i przesyłane za pomocą Aplikacji udostępnionej przez Państwo.

Nie jest natomiast możliwe posługiwanie się Aplikacją w stosunkach z administracją publiczną (np. przy kontroli drogowej czy wizyty w urzędzie) ani wtedy, gdy z przepisów prawa (ustawy, rozporządzenia itd.) wynika obowiązek okazania dowodu osobistego. Aplikacja nie uprawnia również do przekraczania granicy (np. w przypadku przekraczania granic państw UE i strefy Schengen).

Zwracamy uwagę, że korzystanie z Aplikacji nie zwalnia Cię 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.

W związku z udostępnieniem w Aplikacji usługi weryfikacji danych osobistych on-line Dostawca, którym jest Minister Cyfryzacji (ul. Królewska 27, 00-060 Warszawa), przetwarza dane użytkowników Aplikacji w celu umożliwienia świadczenia usługi weryfikacji danych on-line oraz zapewnienia bezpieczeństwa teleinformatycznego. W tych celach do Dostawcy przesyłane są dane obejmujące imię, nazwisko i sumę kontrolną utworzoną z numeru PESEL osoby weryfikującej i osoby, której dane są weryfikowane, a w przypadku weryfikacji Twoich danych on-line przez osobę posługującą się aplikacją mWeryfikator – identyfikator użytkownika aplikacji mWeryfikator oraz Twoje imię, nazwisko i sumę kontrolną utworzoną z numeru PESEL. Dane przesyłane są z urządzenia użytkownika dokonującego weryfikacji. Skorzystanie z usługi weryfikacji on-line jest dobrowolne i wymaga wywołania przez użytkownika odpowiedniej funkcji Aplikacji lub aplikacji mWeryfikator. Dostawca przetwarza również imię, nazwisko oraz numer PESEL użytkownika w związku z utworzeniem i zarządzaniem certyfikatem kryptograficznym, potwierdzającym autentyczność pobranych danych, który jest przypisany do użytkownika i urządzenia mobilnego, którym posługuje się użytkownik. Dane pobierane są z rejestru PESEL podczas aktywacji Aplikacji.

Do korzystania z Aplikacji niezbędne jest posiadanie Profilu Zaufanego (pz.gov.pl) oraz ważnego dowodu osobistego. Aplikacja jest bezpłatna. Aplikacja i związane z nią usługi są dostarczane przez Ministra Cyfryzacji. Korzystanie z Aplikacji (oraz pobranie danych do Aplikacji) jest dobrowolne. Postanowienia dotyczące zasad przetwarzania danych osobowych zostały zamieszczone w § 6 Regulaminu.

Regulamin aplikacji mObywatel

§ 1. Aplikacja

1. Dostawcą Aplikacji (dalej „**Dostawca**”) jest minister właściwy do spraw informatyzacji – Minister Cyfryzacji, ul. Królewska 27, 00-060 Warszawa.

2. **„Aplikacja”** to oprogramowanie Dostawcy pod nazwą „mObywatel”, przeznaczone do zainstalowania na urządzeniu mobilnym Użytkownika, z którego korzystanie odbywa się na warunkach określonych w tym Regulaminie.
3. **„mWeryfikator”** to oprogramowanie Dostawcy pod nazwą „mWeryfikator”, przeznaczone do zainstalowania na urządzeniu mobilnym, współpracujące z Aplikacją i umożliwiające potwierdzenie danych osobistych Użytkownika Aplikacji, z którego korzystanie odbywa się na odrębnie określonych zasadach.
4. Aplikacja pozwala na pobranie danych osobistych i wizerunku Użytkownika z Rejestru Dowodów Osobistych i rejestru PESEL i przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika. Za pośrednictwem Aplikacji dane Użytkownika przechowywane w Aplikacji mogą być w sposób bezpieczny okazywane innym Użytkownikom. Aplikacja umożliwia także weryfikację danych osobistych innych Użytkowników.
5. Wgląd do danych i pobranie danych poprzez Aplikację odbywa się:
 - 1) zgodnie z art. 65 ust. 3 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, która reguluje dostęp do danych w rejestrze dowodów osobistych. Zgodnie z tym przepisem „Osoba, której dane są przetwarzane w Rejestrze Dowodów Osobistych, ma prawo wglądu do swoich danych, przy wykorzystaniu środków komunikacji elektronicznej, po uwierzytelnieniu się w sposób określony w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;
 - 2) zgodnie z art. 45 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności, która reguluje dostęp do danych w rejestrze PESEL, który stanowi, że „osobie, której dane są przetwarzane w rejestrze PESEL, umożliwia się wgląd do rejestru w zakresie danych dotyczących tej osoby, przy wykorzystaniu środków komunikacji elektronicznej, po uwierzytelnieniu jej na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”
6. Dane prezentowane w Aplikacji nie stanowią dokumentu urzędowego ani nie posiadają mocy urzędowej.
7. Aplikacja służy do okazywania i weryfikowania danych osobistych Użytkownika w relacjach pomiędzy Użytkownikami.
8. Dla urządzeń mobilnych z systemem Android Aplikację można pobrać ze sklepu Google Play Store. Dla urządzeń mobilnych z systemem iOS Aplikację można pobrać ze sklepu Apple App Store.
9. Pobranie i korzystanie z Aplikacji jest nieodpłatne. Korzystanie przez Użytkownika z usług transmisji danych lub połączeń głosowych w związku z pobraniem lub korzystaniem z Aplikacji, może wiązać się z opłatami naliczanymi przez operatora telekomunikacyjnego, świadczącego Użytkownikowi usługi telekomunikacyjne.

§ 2. Użytkownicy

1. Użytkownikami Aplikacji (nazywanymi w Regulaminie **„Użytkownikami”** lub pojedynczo **„Użytkownikiem”**) mogą być wyłącznie osoby posiadające obywatelstwo polskie, które łącznie:
 - 1) posiadają ważny profil zaufany (dalej **„Profil Zaufany”**), który został potwierdzony zgodnie z rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej;
 - 2) posiadają ważny dowód osobisty, to jest dokument wydany zgodnie z ustawą z dnia 6 sierpnia 2010 r. o dowodach osobistych, który nie został utracony, uszkodzony lub unieważniony.
2. Użytkownikami Aplikacji mogą być wyłącznie osoby spełniające warunki określone w ust. 1 powyżej. W szczególności Użytkownikami Aplikacji nie mogą być osoby nieposiadające dowodu osobistego i posługujące się wyłącznie innym dokumentem stwierdzającym tożsamość, takim jak paszport lub karta pobytu.

3. Posługiwanie się Aplikacją przez Użytkowników jest dobrowolne. Dostawca informuje, że posiadanie Aplikacji i posługiwanie się nią nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej lub jakichkolwiek osób przebywających na terytorium Rzeczypospolitej Polskiej.

§ 3. Aktywacja Aplikacji

1. Przy pierwszym użyciu Aplikacji dokonywana jest aktywacja Aplikacji.
2. Aktywacja Aplikacji polega na:
 - 1) potwierdzeniu tożsamości Użytkownika przy użyciu Profilu Zaufanego;
 - 2) pobraniu danych Użytkownika z Rejestru Dowodów Osobistych i rejestru PESEL oraz zapisaniu ich w urządzeniu mobilnym Użytkownika;
 - 3) nadaniu przez Użytkownika indywidualnego hasła dostępu do Aplikacji.
3. Potwierdzenie tożsamości Użytkownika przy użyciu Profilu Zaufanego następuje z wykorzystaniem mechanizmu dwuskładnikowego uwierzytelniania i dokonywane jest przy użyciu hasła stałego, przypisanego do Profilu Zaufanego, oraz hasła jednorazowego, przesyłanego na numer telefonu przypisany do Profilu Zaufanego za pomocą wiadomości SMS lub innego dostępnego środka identyfikacji elektronicznej służącego do uwierzytelniania w Profilu Zaufanym.
4. Po pobraniu danych z Rejestru Dowodów Osobistych i rejestru PESEL automatycznie jest tworzony i pobierany do Aplikacji certyfikat kryptograficzny potwierdzający autentyczność pobranych danych (dalej „**Certyfikat**”). Certyfikat przypisany jest do Użytkownika i urządzenia mobilnego, którym posługuje się Użytkownik. Dla celu utworzenia Certyfikatu i zarządzania Certyfikatami Dostawca przetwarza dane osobowe Użytkownika obejmujące imię, nazwisko i jego numer PESEL pochodzące z rejestru PESEL.
5. Ważność Certyfikatu jest ograniczona w czasie i wynosi jeden rok od daty aktywacji Aplikacji.
6. Zakres pobieranych w czasie aktywacji i przechowywanych w urządzeniu mobilnym danych Użytkownika to:
 - 1) z Rejestru Dowodów Osobistych: zdjęcie, termin ważności dowodu osobistego, numer dowodu osobistego, organ wydający dowód osobisty;
 - 2) z rejestru PESEL: numer PESEL, imiona, nazwisko, data urodzenia Użytkownika.
7. Do potwierdzenia tożsamości Użytkownika przy użyciu Profilu Zaufanego, pobrania Certyfikatu oraz pobrania danych z Rejestru Dowodów Osobistych i rejestru PESEL niezbędne jest aktywne połączenie internetowe.
8. Użytkownik może dokonać aktywacji Aplikacji i pobrania danych z Rejestru Dowodów Osobistych i rejestru PESEL na nie więcej niż trzech urządzeniach mobilnych. Na jednym urządzeniu mobilnym można dokonać aktywacji i pobrać dane z Rejestru Dowodów Osobistych i rejestru PESEL tylko jednego Użytkownika.
9. Potwierdzenie tożsamości Użytkownika i pobranie danych z Systemu Rejestrów Publicznych nie powiedzie się, jeżeli Użytkownik nie spełnia warunków określonych w § 2 ust. 1 Regulaminu, w szczególności nie posiada Profilu Zaufanego, jego Profil Zaufany nie został potwierdzony lub utracił ważność, nie posiada ważnego dowodu osobistego lub w Rejestrze Dowodów Osobistych znajduje się informacja o zgłoszeniu jego zaginięcia lub uszkodzenia, bądź też w przypadku podjęcia próby aktywacji Aplikacji na czwartym i kolejnych urządzeniach mobilnych.
10. Dostęp do danych przechowywanych w Aplikacji jest zabezpieczony hasłem dostępu nadawanym przez Użytkownika podczas aktywacji. Nadane w trakcie aktywacji hasło dostępu powinno być przez Użytkownika chronione i nie powinno być udostępniane innym osobom.
11. Podanie hasła dostępu do Aplikacji jest wymagane każdorazowo po zaprzestaniu korzystania z niej przynajmniej na 5 (pięć) minut, a także po uruchomieniu Aplikacji po każdym jej wyłączeniu oraz

po każdym wyłączeniu urządzenia mobilnego. Trzykrotne wprowadzenie nieprawidłowego hasła będzie powodować czasową blokadę dostępu do Aplikacji.

§ 4. Funkcje Aplikacji

1. Z zastrzeżeniem postanowienia ust. 2 poniżej, prawidłowo aktywowana Aplikacja po zalogowaniu się z użyciem hasła dostępu do Aplikacji umożliwia Użytkownikowi korzystanie z następujących funkcjonalności:
 - 1) okazanie danych Użytkownika (funkcja „mTożsamość”);
 - 2) elektroniczne przekazanie danych Użytkownika (funkcja „Przełącz”);
 - 3) weryfikacja danych osobistych innego Użytkownika Aplikacji (funkcja „Sprawdź”);
 - 4) przechowywanie danych zweryfikowanych Użytkowników Aplikacji (funkcja „Historia”);
 - 5) odświeżenie danych Użytkownika;
 - 6) zarządzanie Certyfikatem;
 - 7) usunięcie danych z Aplikacji.
2. Dostawca informuje, że ze względu na ograniczenia techniczne, nie jest możliwa wymiana danych pomiędzy Aplikacją zainstalowaną na urządzeniu mobilnym z systemem iOS i Aplikacją zainstalowaną na urządzeniu mobilnym z systemem Android. W związku z powyższym funkcja dwustronnego elektronicznego przekazania danych, o której mowa w ust. 4 poniżej, oraz funkcja elektronicznej weryfikacji danych osobistych, opisana w ust. 6 poniżej, są dostępne wyłącznie w przypadku, w którym urządzenia mobilne Użytkownika przekazującego dane i Użytkownika pobierającego dane, są tego samego typu. Użytkownicy Aplikacji, posługujący się urządzeniem mobilnym z systemem iOS, nie mają również możliwości korzystania z funkcji elektronicznego przekazania danych użytkownikowi aplikacji mWeryfikator, o której mowa w ust. 11-14 poniżej.
3. Użytkownik może okazać osobie trzeciej jego dane osobiste na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu funkcji „mTożsamość” w Aplikacji. Ekran prezentacji danych, dostępny po wybraniu tej funkcji, uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
 - 1) ruchomego elementu graficznego, prezentującego biało-czerwoną flagę;
 - 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 orła białego z Godła Rzeczypospolitej Polskiej.
4. Elektroniczne przekazanie danych Użytkownika innemu Użytkownikowi Aplikacji umożliwia przesłanie niektórych danych dotyczących tego Użytkownika (zwanego dalej „**Użytkownikiem przekazującym dane**”) do urządzenia mobilnego, którym posługuje się inny Użytkownik, dokonujący odczytu tych danych (zwanego dalej „**Użytkownikiem pobierającym dane**”), połączone z potwierdzeniem poprawności Certyfikatu Użytkownika przekazującego dane. W tym celu Użytkownik dokonujący elektronicznego przekazania danych powinien:
 - 1) wybrać funkcję „Przełącz” w Aplikacji;
 - 2) po pojawieniu się odpowiedniego komunikatu wybrać i zaakceptować opcję „Obustronna wymiana danych”
 - 3) po wyświetleniu w Aplikacji graficznego kwadratowego kodu graficznego (dalej „Kod QR”) umożliwić innemu Użytkownikowi odczyt tego Kodu QR za pomocą aparatu fotograficznego urządzenia mobilnego, którym posługuje się Użytkownik pobierający dane. 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.

5. Po prawidłowym zeskanowaniu Kodu QR pomiędzy urządzeniami mobilnymi Użytkowników nawiązywane jest – w przypadku urządzeń mobilnych z systemem operacyjnym Android – połączenie Bluetooth, zaś w przypadku urządzeń mobilnych z systemem iOS – połączenie wybrane przez system iOS (Wi-Fi lub Bluetooth) i dokonywana jest weryfikacja czasu lokalnego 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, o którym mowa w ust. 4.3. powyżej, przekazanie danych zakończy się niepowodzeniem. Po nawiązaniu połączenia Aplikacja Użytkownika przekazującego dane weryfikuje poprawność Certyfikatu Użytkownika pobierającego dane i wyświetla, a następnie zapisuje niektóre jego dane w Aplikacji (funkcja „Historia”). Wyświetlone dane można dodatkowo zweryfikować on-line przy pomocy funkcji weryfikacji aktualności Certyfikatu. Po weryfikacji poprawności Certyfikatu Użytkownika pobierającego dane bądź – opcjonalnie – weryfikacji on-line aktualności Certyfikatu, Użytkownik przekazujący dane potwierdza zgodę na przesłanie ich do urządzenia Użytkownika pobierającego dane. Przesłanie danych jest możliwe co najmniej po pozytywnej weryfikacji poprawności Certyfikatu Użytkownika pobierającego dane.
6. Elektroniczna weryfikacja danych osobistych innego Użytkownika umożliwia potwierdzenie prawidłowości danych przekazanych przez innego Użytkownika przez weryfikację jego Certyfikatu oraz pobranie niektórych danych tego Użytkownika do własnego urządzenia mobilnego, co wiąże się z przekazaniem niektórych własnych danych. W tym celu Użytkownik pobierający dane innego Użytkownika powinien:
 - 1) wybrać funkcję „Sprawdź” w Aplikacji;
 - 2) po wyświetleniu ekranu skanera Kodów QR wyrazić zgodę na przekazanie swoich danych Użytkownikowi przekazującemu dane, a następnie odczytać Kod QR okazany przez Użytkownika przekazującego dane.
7. Po prawidłowym zeskanowaniu Kodu QR pomiędzy urządzeniami mobilnymi Użytkowników nawiązywane jest – w przypadku urządzeń mobilnych z systemem operacyjnym Android – połączenie Bluetooth, zaś w przypadku urządzeń mobilnych z systemem iOS – połączenie wybrane przez system iOS (Wi-Fi lub Bluetooth) i dokonywana jest weryfikacja czasu lokalnego 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, o którym mowa w ust. 6 pkt 2. powyżej, weryfikacja danych zakończy się niepowodzeniem. Po nawiązaniu połączenia Aplikacja Użytkownika pobierającego dane przesyła jego dane do Aplikacji Użytkownika przekazującego dane w celu sprawdzenia ważności Certyfikatu Użytkownika pobierającego dane. Dane Użytkownika pobierającego dane są przesyłane do urządzenia Użytkownika przekazującego dane tylko w przypadku potwierdzenia prawidłowości jego Certyfikatu. Po weryfikacji Certyfikatu i przekazaniu danych Użytkownika pobierającego dane, Użytkownik przekazujący dane potwierdza zgodę na przekazanie danych do Aplikacji Użytkownika pobierającego dane i następuje przekazanie danych Użytkownika przekazującego dane oraz weryfikacja poprawności jego Certyfikatu. Wyświetlone dane można dodatkowo zweryfikować on-line przy pomocy funkcji weryfikacji aktualności Certyfikatu. Po prawidłowym zakończeniu elektronicznej weryfikacji danych osobistych Użytkowników niektóre dane zweryfikowanego Użytkownika przekazującego dane zapisywane są w Aplikacji (funkcja „Historia”).
8. Przy korzystaniu z funkcji dwustronnego elektronicznego przekazania danych i elektronicznej weryfikacji danych osobistych pomiędzy Użytkownikami Aplikacji przekazywane są następujące dane:
 - 1) imiona i nazwisko;
 - 2) zdjęcie o zredukowanej jakości;
 - 3) seria i numer dowodu osobistego oraz organ go wydający.
9. Weryfikacja poprawności Certyfikatu dokonywana w związku ze skorzystaniem z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobistych nie wymaga aktywnego połączenia internetowego.

10. W przypadku konieczności weryfikacji aktualności Certyfikatu Użytkownika (jego ważności) przekazującego dane oraz Użytkownika pobierającego, należy wybrać funkcję „Weryfikuj”. Aby można było skorzystać z funkcji „Weryfikuj” urządzenie mobilne musi mieć aktywne połączenie internetowe.
11. Elektroniczne przekazanie danych Użytkownika użytkownikowi aplikacji mWeryfikator umożliwia przesłanie niektórych danych dotyczących Użytkownika do urządzenia mobilnego, którym posługuje się użytkownik aplikacji mWeryfikator, połączone z potwierdzeniem poprawności Certyfikatu Użytkownika przekazującego dane. W tym celu Użytkownik dokonujący elektronicznego przekazania danych powinien:
 - 1) wybrać funkcję „Przełącz” w Aplikacji;
 - 2) po pojawieniu się odpowiedniego komunikatu wybrać i zaakceptować opcję „Jednostronne przekazanie danych”;
 - 3) po wyświetleniu w Aplikacji graficznego kwadratowego kodu graficznego (dalej „Kod QR”) umożliwić innemu Użytkownikowi odczyt tego Kodu QR za pomocą aparatu fotograficznego urządzenia mobilnego, którym posługuje się Użytkownik pobierający dane. 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.
12. Po prawidłowym zeskanowaniu Kodu QR pomiędzy urządzeniami mobilnymi Użytkownika i użytkownika aplikacji mWeryfikator nawiązywane jest – w przypadku urządzeń mobilnych z systemem operacyjnym Android – połączenie Bluetooth, zaś w przypadku urządzeń mobilnych z systemem iOS – połączenie wybrane przez system iOS (Wi-Fi lub Bluetooth) i dokonywana jest weryfikacja czasu lokalnego 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, o którym mowa w ust. 11 pkt 3. powyżej, przekazanie danych zakończy się niepowodzeniem. Po nawiązaniu połączenia Aplikacja przekazuje do aplikacji mWeryfikator dane osoby Użytkownika przekazującego dane, umożliwiając ich wyświetlenie w aplikacji mWeryfikator oraz weryfikację poprawności jej certyfikatu. Użytkownik aplikacji mWeryfikator może dodatkowo zweryfikować przekazane dane on-line przy pomocy funkcji weryfikacji aktualności certyfikatu. Po prawidłowym zakończeniu elektronicznej weryfikacji danych osobistych Użytkownika dane dotyczące dokonanej weryfikacji zapisywane są w Aplikacji (funkcja „Historia”).
13. Przy korzystaniu z funkcji jednostronnego elektronicznego przekazania danych i elektronicznej weryfikacji danych osobistych, pomiędzy użytkownikiem Aplikacji a użytkownikiem aplikacji mWeryfikator przekazywane są następujące dane:
 - 1) imiona i nazwisko;
 - 2) zdjęcie o zredukowanej jakości.
14. Aplikacja mWeryfikator nie zapisuje danych Użytkownika Aplikacji, którego dane zostały zweryfikowane z wykorzystaniem tej aplikacji. Wszystkie dane dotyczące tego Użytkownika są usuwane z aplikacji mWeryfikator po wyjściu z ekranu wyświetlania danych.
15. Funkcja „Historia” pozwala na zapoznanie się z historią:
 - 1) pobranych danych osobistych, zawierającą daty pobrań oraz zapisane dane Użytkowników, którzy dokonywali weryfikacji zgodnie z ust. 4 i 5 powyżej;
 - 2) weryfikacji danych osobistych, zawierającą daty weryfikacji oraz zapisane dane Użytkowników zweryfikowanych zgodnie z ust. 6 i 7 powyżej;
 - 3) weryfikacji danych osobistych za pomocą aplikacji mWeryfikator, zawierająca identyfikator użytkownika aplikacji mWeryfikator oraz datę i czas przekazania danych zgodnie z ust. 12 powyżej.
16. Funkcja „Historia” przechowuje dane, o których mowa w ustępie poprzedzającym, przez okres:

- 1) 30 dni od daty ich zapisania w Aplikacji w zakresie danych wskazanych w ust. 15 pkt 1 i 2 powyżej;
 - 2) 1 roku od daty ich zapisania w Aplikacji w zakresie danych wskazanych w ust. 15 pkt 3 powyżej.
17. Funkcja odświeżenia danych Użytkownika (dostępna z menu Aplikacji), umożliwia ponowne pobranie danych Użytkownika z Rejestru Dowodów Osobistych i rejestru PESEL i zapisanie ich w urządzeniu mobilnym Użytkownika. Z funkcji tej należy korzystać po zmianie danych zawartych w Rejestrze Dowodów Osobistych lub rejestrze PESEL (np. zmiana nazwiska, zmiana dowodu osobistego).
18. Funkcja odświeżenia danych Użytkownika wymaga dokonania potwierdzenia tożsamości Użytkownika przy użyciu Profilu Zaufanego. Do odświeżenia danych Użytkownika odpowiednio stosuje się postanowienia § 3 ust. 2 do 3 i 6 do 9 Regulaminu.
19. Funkcja zarządzania Certyfikatem (dostępna z menu Aplikacji) umożliwia unieważnienie Certyfikatów Użytkownika. Po unieważnieniu Certyfikatu dla pojedynczego urządzenia mobilnego, dane przechowywane w Aplikacji są nadal dostępne dla Użytkownika. Nie jest jednak możliwe prawidłowe korzystanie z funkcji „Sprawdź” i „Przełącz”. W przypadku wybrania tych funkcji wyświetlać się będzie komunikat „Brak ważnego certyfikatu”.
20. 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 § 3 Regulaminu.

§ 5. Wymagania techniczne

1. Aplikacja jest przeznaczona na urządzenia mobilne:
 - 1) z systemem operacyjnym Android w wersji nie niższej niż 6.0 i dostępem do Google Play Store;
 - 2) nie starsze niż iPhone 5s, z systemem operacyjnym iOS w wersji nie niższej niż 11.0.3 i dostępem do Apple App Store.
2. Lista urządzeń z systemem operacyjnym Android, na których Aplikacja została przetestowana, dostępna jest pod adresem www.mobywutel.gov.pl/urzadzenia. Dostawca dokłada starań dla zapewnienia jak najszerszej kompatybilności Aplikacji z urządzeniami mobilnymi różnych producentów, ale nie gwarantuje, że Aplikacja będzie działać poprawnie na urządzeniach, na których nie została przetestowana.
3. Pobranie i aktywacja Aplikacji wymagają połączenia z siecią Internet. Połączenia z siecią Internet wymaga ponadto weryfikacja aktualności Certyfikatu innego Użytkownika oraz odświeżenie Certyfikatu w Aplikacji.
4. Aby Aplikacja działała poprawnie, urządzenie mobilne, na którym jest zainstalowana:
 - 1) musi mieć przynajmniej 100 MB wolnej pamięci;
 - 2) nie może mieć zainstalowanych modyfikacji systemu operacyjnego, w szczególności modyfikacji polegających na przełamaniu zabezpieczeń producenta urządzenia mobilnego lub producenta systemu operacyjnego (tzw. jailbreaking czy rooting);
 - 3) musi posiadać moduł łączności Bluetooth;
 - 4) musi umożliwiać nawiązanie połączenia z siecią Internet;
 - 5) musi posiadać aparat fotograficzny.
5. Dostawca informuje, że Aplikacja do prawidłowego działania wymaga, aby urządzenie mobilne umożliwiało jej w określonych sytuacjach dostęp do:

- 1) sieci Internet;
 - 2) aparatu;
 - 3) zdjęć/multimediów/plików;
 - 4) identyfikatora urządzenia mobilnego i informacji o połączeniu.
6. Dostawca informuje, że instalacja dostarczanych od czasu do czasu przez Dostawcę aktualizacji Aplikacji może być konieczna dla jej prawidłowego działania i należytego zabezpieczenia zawartych w niej danych. Dostawca rekomenduje instalowanie takich aktualizacji niezwłocznie po ich udostępnieniu za pomocą Google Play Store oraz Apple App Store.
7. Użytkownik powinien instalować uaktualnienia systemu operacyjnego zgodnie z zaleceniami producenta posiadanego urządzenia mobilnego oraz producenta systemu operacyjnego. Brak aktualizacji systemu operacyjnego lub Aplikacji może prowadzić do obniżenia poziomu bezpieczeństwa korzystania z Aplikacji, a nawet do wycieku danych z Aplikacji.

§ 6. Prywatność i bezpieczeństwo

1. Podstawą przetwarzania danych osobowych w Aplikacji oraz przez administratora danych (**Dostawcę** - Ministra właściwego do spraw informatyzacji) w systemie obsługującym działanie Aplikacji jest dobrowolna zgoda osoby której dane dotyczą. Pobranie Aplikacji oraz jej zainstalowanie wraz z potwierdzeniem regulaminu Aplikacji oraz uwierzytelnienie się Profilem Zaufanym, w celu pobrania danych z rejestrów państwowych do Aplikacji stanowi zgodę na przetwarzanie danych osobowych przez administratora danych w zakresie, o którym mowa w § 6 regulaminu.
2. Osobie, której dane dotyczą, przysługuje prawo odwołania zgody w każdym czasie, prawo dostępu do treści danych, prawo ich poprawiania oraz prawa przewidziane w art. 32 ust. 1 pkt 7 i 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, a po dniu 25 maja 2018 r. w art. 12-34 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1), w tym prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację.
3. Okazanie oraz elektroniczne przekazanie danych, jak również przekazanie danych Użytkownika pobierającego dane następuje dobrowolnie i w ramach realizacji uprawnień lub obowiązków Użytkownika w stosunku do innych Użytkowników.
4. W zakresie przetwarzania i ochrony danych, które Użytkownik uzyskał w toku elektronicznego okazywania danych osobistych bądź elektronicznego weryfikowania danych osobistych, Użytkownika obciąża obowiązek stosowania się do powszechnie obowiązujących przepisów prawa.
5. W przypadku zgubienia, kradzieży lub utraty z innych przyczyn urządzenia mobilnego, Użytkownik powinien niezwłocznie dokonać zgłoszenia tego faktu Dostawcy. Zgłoszenie może być dokonane telefonicznie, na numer telefonu 42 253 54 74.
6. Po zweryfikowaniu danych osobistych Użytkownika dokonującego zgłoszenia, o którym mowa w ust. 3 powyżej, Dostawca unieważni Certyfikat lub Certyfikaty przypisane do danego Użytkownika. Unieważnienie Certyfikatów uniemożliwia skorzystanie z funkcji odświeżenia Certyfikatu w Aplikacji.
7. Dostawca zaleca, aby w przypadku zakończenia korzystania z danego urządzenia mobilnego przez Użytkownika, przed przekazaniem urządzenia osobie trzeciej dokonać resetu danych w Aplikacji w sposób opisany w § 4 ust. 20 Regulaminu.
8. Aplikacja przechowuje następujące dane Użytkownika:

- 1) imiona i nazwiska;
 - 2) PESEL i data urodzenia;
 - 3) zdjęcie;
 - 4) termin ważności dowodu osobistego;
 - 5) seria i numer dowodu osobistego oraz organ, który go wydał;
9. Aplikacja przechowuje następujące dane Użytkowników, których dane osobiste zostały zweryfikowane elektronicznie:
- 1) imiona i nazwisko takich Użytkowników;
 - 2) zdjęcia takich Użytkowników o zredukowanej jakości;
 - 3) seria i numer dowodów osobistych takich Użytkowników oraz organ je wydający.
10. Dla celu utworzenia Certyfikatu podczas aktywacji Aplikacji oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Dostawca przetwarza dane obejmujące imię, nazwisko oraz numer PESEL Użytkownika. Dane pobierane są z rejestru PESEL podczas aktywacji Aplikacji.
11. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Przekaż”) innemu Użytkownikowi Aplikacji lub elektronicznej weryfikacji danych osobistych takiego Użytkownika funkcji (funkcja „Sprawdź”) Aplikacja przesyła do urządzenia mobilnego innego Użytkownika, z którym dochodzi do wymiany danych, następujące dane:
- 1) imiona i nazwisko Użytkownika;
 - 2) zdjęcie Użytkownika o zredukowanej jakości;
 - 3) seria i numer dowodu osobistego oraz organ go wydający.
12. Podczas korzystania z funkcji elektronicznego jednostronnego przekazania danych (funkcja „Przekaż”) użytkownikowi aplikacji mWeryfikator Aplikacja przesyła do urządzenia mobilnego użytkownika mWeryfikator następujące dane:
- 1) imiona i nazwisko Użytkownika;
 - 2) zdjęcie Użytkownika o zredukowanej jakości.
13. Dostawca gromadzi dane statystyczne dotyczące Aplikacji w zakresie:
- 1) liczby pobrań aplikacji;
 - 2) liczby aktualizacji aplikacji;
 - 3) liczby akcji odświeżenia danych i wydania Certyfikatów;
 - 4) liczby zgłoszonych utrat telefonów;
 - 5) liczby zgłoszonych problemów.
14. Z zastrzeżeniem ustępów następujących Dostawca nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z Aplikacji, danych o połączeniach między nimi, ani danych o Użytkownikach w związku z korzystaniem z funkcji weryfikacji on-line w aplikacji mWeryfikator. Dostawca nie gromadzi również informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobistych.
15. Dostawca przy skorzystaniu przez Użytkowników z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności Certyfikatu on-line) przez Użytkownika Aplikacji gromadzi następujące dane:

- 1) imiona i nazwisko Użytkownika korzystającego z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności Certyfikatu on-line);
 - 2) suma kontrolna utworzona z numeru PESEL Użytkownika korzystającego z funkcji weryfikacji aktualności Certyfikatu;
 - 3) numer Certyfikatu, o którego zweryfikowanie Użytkownik występuje.
16. Dostawca przy skorzystaniu z funkcji weryfikacji aktualności certyfikatu (sprawdzenie ważności certyfikatu on-line) za pomocą aplikacji mWeryfikator gromadzi następujące dane:
- 1) identyfikator użytkownika aplikacji mWeryfikator;
 - 2) numer certyfikatu Użytkownika przekazującego dane, weryfikowanego za pomocą aplikacji mWeryfikator.
17. Celem zbierania danych, o których mowa powyżej jest sprawdzenie poprawności obsługi procesu weryfikacji aktualności Certyfikatu oraz wykrycia błędów i luk bezpieczeństwa.
18. Dane, o których w ust. 15 i 16 są gromadzone wyłącznie w trakcie korzystania z funkcji wymienionych w ust. 15 i 16. Dostawca przechowuje dane osobowe przez okres ważności certyfikatu oraz przez okres jednego roku liczonego od daty wygaśnięcia certyfikatu. Dane nie są przetwarzane w celach marketingowych.
19. Dostawca umożliwia Użytkownikom pobranie z publicznych rejestrów danych osobowych opisanych w Regulaminie i okazywanie tych danych innym Użytkownikom, na wskazanych w Regulaminie zasadach. Pobrane przez Użytkowników w ramach korzystania z Aplikacji dane, w tym dane osobowe, są przechowywane na urządzeniu mobilnym Użytkownika i, z zastrzeżeniem ust. 15 i 16 powyżej, nie są przetwarzane przez Dostawcę.
20. Poza funkcjami elektronicznego przekazania danych oraz elektronicznej weryfikacji danych osobistych, Aplikacja nie oferuje funkcji eksportu ani importu danych.
21. Hasło dostępu do Aplikacji nie jest przechowywane w urządzeniu mobilnym Użytkownika. Dostawca nie umożliwia odtworzenia hasła dostępu do Aplikacji. W przypadku utraty hasła dostępu do Aplikacji niezbędne jest usunięcie Aplikacji z urządzenia mobilnego wraz ze wszystkimi danymi oraz ponowna instalacja i aktywacja Aplikacji.
22. Dostawca informuje, że dokłada najwyższej staranności w celu zapewnienia wysokiego poziomu bezpieczeństwa teleinformatycznego Aplikacji i danych Użytkowników. Jednakże Dostawca wskazuje, że ze względu na specyfikę technologii informatycznych w przyszłości może zostać ujawniona podatność Aplikacji na określone zagrożenia. Z tego względu Dostawca zaleca dokonywanie aktualizacji Aplikacji zgodnie z § 5 ust. 6 oraz wskazuje, że może od czasu do czasu wydawać publicznie dostępne zalecenia dotyczące zasad bezpieczeństwa związanych z korzystaniem z Aplikacji.

§ 7. Korzystanie z Aplikacji

1. Z chwilą instalacji Aplikacji Dostawca udziela Użytkownikowi niewyłącznej licencji na korzystanie z Aplikacji na warunkach określonych w niniejszym § 7. Udzielona licencja jest niewyłączna, nieprzenoszalna, nie uprawnia do udzielania dalszych licencji (sublicencji).
2. Licencja jest udzielana na czas nieoznaczony i bez ograniczeń terytorialnych.
3. Na podstawie udzielonej licencji Użytkownik jest uprawniony do zwielokrotniania Aplikacji w zakresie niezbędnym do jej zainstalowania i używania na posiadanych przez Użytkownika urządzeniach mobilnych, jeżeli czynności te są podejmowane dla celów korzystania z Aplikacji zgodnie z Regulaminem.
4. Z zastrzeżeniem ust. 3 powyżej oraz wyjątków wynikających z bezwzględnie obowiązujących przepisów prawa, Użytkownik nie jest uprawniony do zwielokrotniania Aplikacji w jakikolwiek inny

sposób lub tłumaczenia, przystosowywania, zmiany układu lub wprowadzania jakichkolwiek innych zmian w Aplikacji.

§ 8. Wsparcie techniczne i zgłoszenia Użytkowników

1. Wsparcie techniczne Aplikacji jest realizowane poprzez udostępnienie Użytkownikom telefonu kontaktowego, czynnego w godzinach 7.00-18.00 w dni robocze, pod numerem 42 253 54 74.
2. Ewentualne pytania, uwagi lub propozycje Użytkowników dotyczące Aplikacji i jej funkcjonalności, można kierować drogą elektroniczną na adres e-mail: mobywatel@mc.gov.pl.

§ 9. Odpowiedzialność

1. Dostawca informuje, że Użytkownik ponosi pełną odpowiedzialność za naruszenie prawa bądź szkodę wyrządzoną działaniem Użytkownika związanym z korzystaniem przez niego z Aplikacji, w szczególności posłużeniem się lub podaniem do wiadomości publicznej danych innych Użytkowników, uzyskanych za pomocą funkcji oferowanych przez Aplikację, w tym naruszenie ich dóbr osobistych, prywatności lub zasad przetwarzania danych osobowych.
2. Dostawca informuje, że nie ponosi odpowiedzialności za:
 - 1) szkody będące wynikiem niedokonania przez Użytkownika aktualizacji Aplikacji lub niezastosowania się do zaleceń, o których mowa w § 6 ust. 21 i 22 Regulaminu,
 - 2) szkody będące wynikiem korzystania przez Użytkownika z Aplikacji w sposób niezgodny z prawem lub niniejszym Regulaminem;
 - 3) jakość i dostępność usług telekomunikacyjnych, niezbędnych do korzystania z Aplikacji, świadczonych przez operatora telekomunikacyjnego, z którego usług korzysta Użytkownik;
 - 4) nieprawidłowości funkcjonowania Aplikacji wynikających z nieprawidłowości działania systemu operacyjnego lub urządzenia mobilnego, z którego korzysta Użytkownik.
3. Dostawca informuje, że Aplikacja udostępniana jest w wersji Produkcyjnej. Jednakże przewiduje się dalszy rozwój Aplikacji oraz wprowadzania nowych funkcji w przyszłości, co może powodować konieczność aktualizowania Aplikacji, w tym powstanie obowiązku potwierdzania zapoznania się z nowymi wersjami regulaminu. O rozszerzeniu funkcjonalności i wynikających stąd zmianach dla użytkownika Dostawca informuje w komunikatach prasowych lub na stronie internetowej obywatel.gov.pl w karcie usługi „mDokumenty. Potwierdzaj tożsamość smartfonem”.
4. Dostawca nie zapewnia również prawidłowego funkcjonowania Aplikacji po upływie terminu ważności Certyfikatu przypisanego do Aplikacji.
5. Dostawca informuje, że ze względu na specyfikę technologii informatycznych korzystanie z funkcji Aplikacji wymagających dostępu do sieci Internet (aktywacja Aplikacji, odświeżenie Certyfikatu, weryfikacja aktualności Certyfikatu innego użytkownika), może być realizowane z przerwami lub z ograniczeniami wynikającymi z mocy obliczeniowej infrastruktury informatycznej Dostawcy.

§ 10. Postanowienia końcowe

1. Użytkownik w każdym czasie jest uprawniony do zakończenia korzystania z Aplikacji poprzez jej odinstalowanie z Urządzenia mobilnego. Odinstalowanie Aplikacji jest równoznaczne z odwołaniem zgody na przetwarzanie danych osobowych z zastrzeżeniem § 6 ust. 18.
2. Regulamin może ulec zmianie wraz z kolejnymi wydaniami Aplikacji. Zmiana jest wiążąca dla Użytkowników, którzy zainstalują takie wydanie Aplikacji i zaakceptują zmienione brzmienie Regulaminu.
3. Regulamin jest udostępniony nieodpłatnie w Aplikacji, a ponadto za pośrednictwem strony www.mobywatel.gov.pl/regulamin-1-1-2 w formacie PDF, który umożliwia jego pobranie, utrwalenie i wydrukowanie.