Regulamin korzystania z Aplikacji mObywatel 2.0
– dostępne usługi, warunki użytkowania i warunki techniczne, postanowienia licencyjne, informacja o przetwarzaniu danych osobowych

Drogi Użytkowniku!
Dziękujemy za pobranie Aplikacji mObywatel. Warunkiem rozpoczęcia korzystania z Aplikacji mObywatel jest zapoznanie się i akceptacja Regulaminu, który wyjaśnia sposób i zasady działania oprogramowania, a także zawiera ważne informacje dotyczące bezpieczeństwa i ochrony danych osobowych. Załączniki do Regulaminu wyjaśniają kwestie korzystania z poszczególnych dokumentów i dostępnych usług Aplikacji oraz odnoszą się do zasad przetwarzania danych osobowych w poszczególnych usługach.

§ 1. Usługi i Funkcjonalności Aplikacji

1. W ramach Aplikacji dostępne są na urządzeniu mobilnym Użytkownika w Aplikacji następujące dokumenty i usługi, zwane dalej również pojedynczo „Dokumentem", „Usługą":
   1) **Dokument mObywatel** (dalej „mDowód"/ „dokument mDowód") – dokument mobilny stwierdzający tożsamość i obywatelstwo polskie użytkownika aplikacji mObywatel na terytorium Rzeczypospolitej Polskiej w relacjach wzajemnej fizycznej obecności stron. Dane użytkownika aplikacji mObywatel pobrane są z rejestru PESEL, o którym mowa w art. 6 ust. 1 Ustawy o ewidencji ludności. Wydawany użytkownikowi aplikacji mObywatel automatycznie, po ustaleniu jego tożsamości, w sposób określony w art. 4 ust. 1 Ustawy o aplikacji mObywatel na okres 5 lat.
   2) **Legitymacja szkolna –** usługa prezentacji dokumentu elektronicznego, o którym mowa w § 4 ust. 2 rozporządzenia Ministra Edukacji Narodowej z dnia 7 czerwca 2023 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych (Dz. U. poz. 1120) oraz § 4 ust. 5 rozporządzenia z dnia 16 kwietnia 2020 r. Ministra Kultury i Dziedzictwa Narodowego w sprawie świadectw, dyplomów państwowych i innych druków publicznych szkół i placówek artystycznych (Dz. U. poz. 813, z późn. zm.), wydawana w postaci dokumentu mobilnego, o którym mowa w art. 2 pkt 7 Ustawy o aplikacji mObywatel, która pozwala na pobranie danych osobowych Użytkownika, przechowywanie ich w zaszyfrowanej formie na urządzeniu mobilnym Użytkownika, okazywanie danych Użytkownika innym osobom;
   3) **Moje Pojazdy –** usługa Ministra, o której mowa w art. 3 ust. 1 pkt 1 i 3 Ustawy o aplikacji mObywatel, która pozwala na pobranie danych osobowych użytkownika powiązanych z danymi pojazdu ujawnionymi w bazie Centralnej Ewidencji Pojazdów oraz danych pojazdu zawartych w tej bazie i okazywane innym Użytkownikom w sposób bezpieczny. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
   4) **Legitymacja studencka** – usługa prezentacji dokumentu elektronicznego, o którym mowa w § 20 ust. 1 pkt 2 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz. U. z 2021 r. poz. 661), wydawana w postaci dokumentu mobilnego, o którym mowa w art. 2 pkt 7 Ustawy o aplikacji mObywatel, która pozwala na pobranie danych osobowych Użytkownika,

przechowywanie ich w zaszyfrowanej formie na urządzeniu mobilnym Użytkownika, okazywanie danych Użytkownika innym osobom;

5) **eRecepta** – usługa Ministra Zdrowia pozwalająca na dostęp, za pośrednictwem Aplikacji, do Internetowego Konta Pacjenta w zakresie prezentacji niezrealizowanych recept elektronicznych – dokumentów elektronicznych o których mowa w art. 2 ust. 6 lit. a ustawy o systemie informacji w ochronie zdrowia (Dz. U. 2022 poz. 1555). Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód albo Diia.pl;
6) **Polak za granicą** – usługa Ministra Spraw Zagranicznych pozwalająca na dostęp, za pośrednictwem Aplikacji, do informacji dla podróżujących przygotowanych przez polskie placówki dyplomatyczne we współpracy z Ministerstwem Spraw Zagranicznych. Szczegółowe zasady korzystania z usługi zostały określone odrębnie na stronie internetowej Ministra Spraw Zagranicznych pod adresem: https://www.gov.pl/dyplomacja/informacje-dla-podrozujacych/. Korzystanie z usługi wymaga aktywnego połączenia z Internetem. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
7) **mPrawo Jazdy i Punkty Karne** – usługa Ministra, – usługa Ministra, o której mowa w art. 3 ust. 1 pkt 1 Ustawy o aplikacji mObywatel, która pozwala na pobranie przez Użytkownika danych osobowych z usługi mObywatel i powiązanych z nimi uprawnień do kierowania pojazdami z bazy CEK oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika a także ich okazywanie. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
8) **MKA** – Małopolska Karta Aglomeracyjna lub usługa Małopolska Karta Aglomeracyjna lub usługa MKA – usługa online Zarządu Dróg Wojewódzkich w Krakowie (jednostki budżetowej Samorządu Województwa Małopolskiego), dostępna dla osób posiadających kartę MKA i konto w systemie MKA pod adresem: www.mka.malopolska.pl. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
9) **Bilkom – bilety kolejowe** – usługa online PKP pozwalająca na prezentację w aplikacji mObywatel biletów kolejowych zakupionych na bilkom.pl lub bilet.wielkopolskiebilety.pl. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
10) **Karta Dużej Rodziny** (**KDR**) – usługa Ministra Rodziny i Polityki Społecznej i Ministra, której wykorzystanie odbywa się na warunkach określonych w Ustawie o aplikacji mObywatel i art. 10 Ustawy o Karcie Dużej Rodziny. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód albo Legitymacja szkolna;
11) **Unijny Certyfikat COVID** – usługa Ministra Zdrowia zapewniająca na podstawie art. 7b ust. 1b ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia również w Aplikacji potwierdzenie, że dana osoba została zaszczepiona przeciw wirusowi SARS-Cov-2 i/lub uzyskała negatywny wynik testu na obecność wirusa SARS-Cov-2 i/lub przeszła COVID-19. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód albo Diia.pl;
12) **Legitymacja UUT** – usługa prezentacji dokumentu potwierdzającego uprawnienia jej posiadacza do korzystania z ulgowych usług transportowych, wydawanego przez PKP Intercity. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
13) **Diia.pl** – usługa Ministra, o której mowa w art. 10 Ustawy o pomocy obywatelom Ukrainy, dostępna na urządzeniu mobilnym Użytkownika w Aplikacji. Usługa pozwala

na pobranie danych osobowych Użytkownika z Rejestru oraz przechowywanie ich w zaszyfrowanej formie na urządzeniu mobilnym Użytkownika, a także okazywanie danych Użytkownika innym osobom w celu potwierdzenia jego tożsamości;

14) **Naruszenia środowiskowe** – usługa Głównego Inspektora Ochrony Środowiska pozwalająca na przesłanie, poprzez formularz umieszczony w Aplikacji, informacji o zdarzeniu mogącym mieć niekorzystny wpływ na środowisko. Usługa pozwala na raportowanie w szczególności:
a) porzucenia / nielegalnego zdeponowania / składowania /zakopywania / przetwarzania / odzyskiwania / unieszkodliwiania odpadów: niebezpiecznych, komunalnych, innych,
b) nielegalnego transportu odpadów niebezpiecznych i innych,
c) nielegalnego przywiezienia z zagranicy odpadów,
d) zanieczyszczenia wody, powietrza lub powierzchni ziemi substancjami zagrażającymi środowisku.
Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
15) **Złóż wniosek** – usługa Ministra, umożliwiająca za pomocą Aplikacji złożenie wniosku o wsparcie lub oświadczenia dla gospodarstw domowych w związku z sytuacją energetyczną i ciepłowniczą, udostępnionych na stronie ww.gov.pl. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
16) **Legitymacja emeryta-rencisty** – dokument mobilny, wydany przez terenową jednostkę organizacyjną Zakładu Ubezpieczeń Społecznych właściwą w sprawach wydawania decyzji dotyczących świadczeń lub ich wypłaty. Legitymacja emeryta-rencisty jest wydawana w formie:
a) spersonalizowanej karty identyfikacyjnej wykonanej z tworzywa sztucznego,
b) dokumentu elektronicznego przechowywanego i okazywanego przy użyciu Aplikacji.
Aby korzystać z mobilnej Legitymacji emeryta-rencisty wymagana jest aktywacja usługi mObywatel;
17) **Legitymacja adwokacka** – dokument mobilny wydany przez okręgową radę adwokacką na podstawie ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. 2022 r. poz. 1184) oraz uchwały nr 269/2022 Prezydium Naczelnej Rady Adwokackiej z dnia 8 grudnia 2022 r.
18) **Legitymacja poselska** – dokument mobilny wydany przez którego wykorzystywanie odbywa się na warunkach ustawy o aplikacji mObywatel oraz w ustawie z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
19) **Rejestr Uprawnień** – usługa Ministra, o której mowa w art. 15-16 Ustawy o aplikacji mObywatel, umożliwiająca prezentację za pomocą Aplikacji aktualnie posiadanych uprawnień przez obywateli. Uprawnienia obywateli do wykonywania czynności wydawane przez instytucje w ramach ich działalności statutowej. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
20) **Usługa e-Płatności** – pilotaż usługi online, skierowany do określonej grupy użytkowników, polegający na obsłudze elektronicznych Transakcji płatniczych udostępnionych w Aplikacji mObywatel;
21) **Aplikacja/Usługa mWeryfikator** - „mWeryfikator”, oprogramowanie Ministra Cyfryzacji, o którym mowa w art. 19 ust. 1 pkt 7 lit. a Ustawy o aplikacji mObywatel, stanowiące element publicznej aplikacji mobilnej. Umożliwia weryfikację danych

takich jak wizerunek, imię, nazwisko Użytkownika i posługującymi się w niej dostępnymi dokumentami oraz usługami;

2. Nie jest możliwe pobranie danych dokumentów jak i korzystanie z aplikacji mObywatel, jeżeli Użytkownik nie spełnia warunków technicznych określonych w Regulaminie. W szczególności nie ma ważnego środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl), nie ma aktywowanego dokumentu mObywatel.
3. Poza funkcją elektronicznego potwierdzania danych osobowych Aplikacja nie oferuje funkcji eksportu ani importu danych.
4. Szczegółowe zasady aktywacji, dezaktywacji i korzystania z głównych Usług oraz opis ich funkcji, a także informacji dotyczące przetwarzania danych osobowych Użytkownika określają załączniki do niniejszego Regulaminu.
5. Aktualny Regulamin jest udostępniony nieodpłatnie w Aplikacji, w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra skąd można go pobrać, utrwalić i wydrukować: https://mc.bip.gov.pl/aplikacja-mobywatel/informacje-o-aplikacji-mobywatel.html
6. Warunkiem rozpoczęcia korzystania z Aplikacji jest zapoznanie się i akceptacja Regulaminu.
7. Zasady korzystania z eRecepty określa odrębny regulamin Internetowego Konta Pacjenta Dostępny na stronie https://www.pacjent.gov.pl/warunki-korzystania-z-serwisu.
8. Zasady korzystania z Bilkom – bilety kolejowe określa odrębny regulamin dostępny na stronie https://bilkom.pl/regulamin.
9. Zgodnie z art. 21 ust. 1 Ustawy o aplikacji mObywatel, minister właściwy do spraw informatyzacji w Biuletynie Informacji Publicznej na swojej stronie podmiotowej zamieszcza oraz niezwłocznie aktualizuje:
   1) regulamin korzystania z aplikacji mObywatel;
   2) politykę świadczenia usług dla certyfikatów użytkownika aplikacji mObywatel;
   3) informacje dotyczące:
      a) usług udostępnianych w aplikacji mObywatel,
      b) usług czasowo zawieszonych,
      c) potwierdzania autentyczności, ważności, integralności oraz pochodzenia dokumentów mobilnych, w tym zabezpieczeń wizualnych tych dokumentów,
      d) udostępnianych metod unieważnienia certyfikatów użytkownika aplikacji mObywatel,
      e) ogólnych warunków świadczenia usług w aplikacji mObywatel, o których mowa w art. 15 ust. 3 Ustawy o aplikacji mObywatel, oraz listy usług świadczonych na tej podstawie.

§ 2. Definicje

1. **Minister** – minister właściwy do spraw informatyzacji, którego urząd obsługujący Ministerstwo Cyfryzacji posiada siedzibę w Warszawie, przy ul. Królewskiej 27.
2. **Aplikacja/ Aplikacja mObywatel** – bezpłatne i dobrowolne oprogramowanie Ministra pod nazwą „mObywatel 2.0” przeznaczone dla urządzeń mobilnych, w którym są udostępniane usługi świadczone przez podmioty publiczne oraz podmioty niepubliczne, z którego

korzystanie odbywa się na warunkach określonych w tym Regulaminie i Ustawie o aplikacji mObywatel.

3. **Użytkownik** – osoba fizyczna, której zapewniono możliwość korzystania z aplikacji mObywatel po uprzednim ustaleniu tożsamości tej osoby w sposób określony w ustawie o aplikacji mObywatel. Pojęcie może być używane w Regulaminie odpowiednio w liczbie mnogiej „Użytkownicy" lub w liczbie pojedynczej „Użytkownik".
4. **Certyfikat podstawowy / Certyfikat** – certyfikat, o którym mowa w art. 2 pkt 2 ustawy o aplikacji mObywatel – certyfikat użytkownika aplikacji mObywatel wydawany z dokumentem mObywatel, zgodnie z art. 10 ust. 2 Ustawy o aplikacji mObywatel, użytkownikowi aplikacji automatycznie z Profilem mObywatel zgodnie z art. 14 ust. 1 Ustawy o aplikacji mObywatel, pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika.
5. **System mObywatel/System teleinformatyczny Aplikacji** - system teleinformatyczny, który pozwala, przy użyciu publicznej aplikacji mobilnej, na pobranie dokumentu elektronicznego:
    1) zawierającego dane osobowe użytkownika publicznej aplikacji mobilnej pobrane z rejestrów publicznych;
    2) zawierającego dane dotyczące sytuacji prawnej użytkownika publicznej aplikacji mobilnej lub praw mu przysługujących;
6. zawierającego dane umożliwiające identyfikację rzeczy związanej z użytkownikiem publicznej aplikacji mobilnej;
7. **Instytucja** – podmiot prywatny lub publiczny, któremu Minister wydał certyfikat, pozwalający na zabezpieczenie oraz potwierdzenie pochodzenia danych przekazywanych pomiędzy systemem teleinformatycznym Aplikacji a systemem teleinformatycznym tego podmiotu.
8. **mWeryfikator** / **Aplikacja mWeryfikator** – oprogramowanie Ministra, stanowiące element systemu publicznej aplikacji mobilnej, współpracujące z głównymi Usługami i umożliwiające potwierdzenie danych osobowych w danej Usłudze. Szczegóły współpracy poszczególnych Usług z mWeryfikatorem regulują załączniki Regulaminu.
9. **Ustawa o aplikacji mObywatel –** ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234).
10. **Ustawa o pomocy obywatelom Ukrainy** – ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz. U. z 2022 poz. 583, z późn.zm.).
11. **Ustawa o ewidencji ludności** – ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. poz. 1191, z późn. zm.)
12. **Regulamin –** niniejszy regulamin aplikacji mObywatel, o którym mowa w art. 21 ust.1 pkt.1 Ustawy o aplikacji mObywatel.
13. **Ogólne rozporządzenie o ochronie danych** / **RODO** – rozporządzenie 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 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2).

14. **Rejestr** – rejestr osób które przybyły do Polski po 24 lutego 2022 r. w związku z wojną w Ukrainie, którym nadano numer PESEL, o którym mowa w art. 6 ust.1 Ustawy o pomocy obywatelom Ukrainy.
15. **Skrzynka odbiorcza** – skrzynka odbiorcza w Aplikacji, prezentująca wiadomości kierowane do konkretnego Użytkownika.
16. **Powiadomienie PUSH** – wiadomość przekazywana Użytkownikowi w formie powiadomienia wyświetlanego na ekranie telefonu, niezależnie od tego czy Aplikacja jest włączona.
17. **Profil mObywatel –** środek identyfikacji elektronicznej, o którym mowa w art. 3 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, obsługiwany przy użyciu usługi udostępnianej w aplikacji mObywatel, wydawany zgodnie z Art. 14 ust. 1-3 Ustawy o aplikacji mObywatel.

§ 3. Informacje ogólne

1. Pobranie Aplikacji i korzystanie z niej jest **nieodpłatne**.
2. Korzystanie przez Użytkownika z usług transmisji danych lub połączeń głosowych w związku z pobraniem lub korzystaniem z Aplikacji i Usług może wiązać się z opłatami naliczanymi przez operatora telekomunikacyjnego, który świadczy Użytkownikowi usługi telekomunikacyjne.
3. Posługiwanie się Aplikacją przez Użytkowników jest **dobrowolne**. Minister informuje, że posiadanie Aplikacji i posługiwanie się nią nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej lub jakichkolwiek osób przebywających na terytorium Rzeczypospolitej Polskiej.
4. Korzystanie z Aplikacji lub Usług 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.
5. Użytkownik Aplikacji jest uprawniony do korzystania z funkcjonalności odbierania Powiadomienia PUSH. Powiadomienie PUSH zawiera informację o przekazaniu wiadomości, w tym wiadomość pozwalającą na autoryzację czynności związanych z korzystaniem z profilu zaufanego. Pełna treść wiadomości dostępna jest w Skrzynce odbiorczej po zalogowaniu do Aplikacji lub – w przypadku wiadomości autoryzacyjnych – wyświetlana jest bezpośrednio po zalogowaniu do Aplikacji.
6. Użytkownik Aplikacji może wyłączyć funkcję otrzymywania Powiadomień PUSH dla Aplikacji korzystając z funkcji systemowych.
7. Do wysyłki Powiadomień PUSH jest wykorzystywane narzędzie Firebase Cloud Messaging: https://firebase.google.com/support/privacy.
8. Treść Powiadomień PUSH oraz narzędzia do ich wysyłki ustala Minister Cyfryzacji, który udostępnia dane Powiadomienie PUSH.

§ 4. Wymagania techniczne

1. W celu prawidłowego i pełnego korzystania z Aplikacji, Użytkownik powinien dysponować urządzeniem mobilnych typu smartfon z systemem:
    1) Android 7.0 lub wyższym i z dostępem do sklepu Google Play

       lub

    2) iOS 15.0 lub wyższym i z dostępem do sklepu App Store.
2. Minister 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 Internetem. Połączenia z Internetem wymaga ponadto aktualizacja danych w Aplikacji.
4. Aplikacja do prawidłowego działania wymaga:
    1) przynajmniej 100 MB wolnej pamięci;
    2) systemu operacyjnego pozbawionego modyfikacji, w szczególności modyfikacji polegających na przełamaniu zabezpieczeń producenta urządzenia mobilnego lub producenta systemu operacyjnego (tzw. jailbreaking czy rooting);
    3) dostępu do Internetu – w czasie instalacji, aktualizacji oprogramowania oraz aktywacji Aplikacji;
    4) udostępnienia lokalizacji (jednorazowo, tylko dla Android 8.1 i wyższej) – na potrzeby ustalenia identyfikatora interfejsu sieciowego;
    5) pozwolenia na dostęp do systemowej *Usługi telefon* (jednorazowo, tylko dla systemu Android) – na potrzeby ustalenia identyfikatora urządzenia (numer IMEI urządzenia).
5. Aplikacja nie jest przeznaczona do uruchamiania:
    1) na urządzeniu, którego modyfikacje pozwalają na ukrywanie przełamania zabezpieczeń producenta urządzenia lub producenta systemu operacyjnego (np. rooting, jailbreaking);
    2) na urządzeniu, którego bootloader został zmodyfikowany;
    3) na urządzeniu, którego system operacyjny został zmodyfikowany lub zastąpiony innym oprogramowaniem;
    4) w trybie klonowania lub podczas emulacji systemu operacyjnego;
    5) w środowisku, na którym zainstalowano oprogramowanie powszechnie uznawane za niebezpieczne;
    6) w środowisku, na którym zainstalowano oprogramowanie wykorzystujące rozwiązania stosowane przez oprogramowanie powszechnie uznawane za niebezpieczne;
    7) w środowisku, które zostało zmodyfikowane w celu wprowadzania w błąd odbiorców treści wyświetlanych przez Aplikację.
6. Aplikacja do pełnego działania wymaga, aby urządzenie mobilne umożliwiało jej w określonych sytuacjach dostęp do:
    1) aparatu - na potrzeby zeskanowania kodu QR aktywującego Legitymację szkolną lub studencką, zeskanowania kodu QR lub serii kodów QR w celu przekazania danych

za pomocą usługi mWeryfikator, zeskanowania kodu QR w celu przekazania danych do Instytucji;
2) modułu łączności Bluetooth lub Wi-Fi – na potrzeby nawiązania łączności w procesie przekazywanie danych po zeskanowaniu kodu QR do mWeryfikatora;
3) lokalizacji – na potrzeby odczytania identyfikatora urządzenia (lokalizacja wymagana wyłącznie podczas sprawdzania poprawności dokumentów z wykorzystaniem mWeryfikatora).

7. Instalacja dostarczanych okresowo przez Ministra aktualizacji Aplikacji może być konieczna dla jej prawidłowego działania i należytego zabezpieczenia zawartych w niej danych. Minister rekomenduje instalowanie takich aktualizacji niezwłocznie po ich udostępnieniu za pomocą sklepu Google Play Użytkownikom urządzeń z systemem Android lub App Store Użytkownikom urządzeń z systemem iOS
8. Użytkownik powinien instalować uaktualnienia systemu operacyjnego zgodnie z zaleceniami producenta swojego 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.

§ 5. Warunki bezpiecznego użytkowania Aplikacji

1. W przypadku zgubienia, kradzieży urządzenia mobilnego lub jego utraty z innych przyczyn, Użytkownik może unieważnić certyfikat:
    1) Samodzielnie za pomocą aplikacji mObywatel nawet na innym urządzeniu poprzez aktywację, co skutkuje automatycznym unieważnieniem istniejącego certyfikatu na poprzednim urządzeniu mobilnym;
    2) telefonicznie – dzwoniąc na numerem telefonu +48 42 253 54 74 czynnego całą dobę.
2. Minister zaleca, aby w przypadku zakończenia korzystania z danego urządzenia mobilnego przez Użytkownika, przed przekazaniem urządzenia osobie trzeciej, usunąć dane z usług zawartych w Aplikacji.
3. Hasło dostępu do Aplikacji nie jest przechowywane w postaci jawnej w urządzeniu mobilnym Użytkownika. Minister nie umożliwia odtworzenia hasła dostępu do Aplikacji. W przypadku utraty hasła dostępu do Aplikacji niezbędna jest ponowna aktywacja aplikacji (zależnie od preferencji Użytkownika skorzystanie z funkcji „Nie pamiętam hasła” lub ponowna instalacja aplikacji) oraz zastrzeżenie starego certyfikatu.
4. 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 spowoduje czasową blokadę dostępu do Aplikacji.
5. W przypadku urządzeń mobilnych obsługujących funkcję biometrii, dostęp do Aplikacji możliwy jest przy wykorzystaniu tej funkcji, przy czym:
    1) skorzystanie z funkcji biometrii nie zwalnia Użytkownika z obowiązku ustawienia hasła dostępu do Aplikacji;
    2) aktywacja biometrii wymaga zdefiniowania 4-cyfrowego kodu PIN;
    3) Użytkownik ma możliwość aktywacji uwierzytelniania biometrią bez PINu, przy czym:

a) Użytkownik akceptuje fakt, że ta metoda powoduje obniżenie poziomu zabezpieczeń Aplikacji,
b) hasło i PIN są zapisywane w Aplikacji w urządzeniu mobilnym, a Minister nie ponosi odpowiedzialności za szkody spowodowane błędami i zainstalowanym innym oprogramowaniem w systemie operacyjnym oraz błędy w samym urządzeniu,
c) część funkcjonalności i usług dostępnych w Aplikacji, będzie wymagała nadal podania PIN zdefiniowanego przez Użytkownika,
d) Użytkownik w trakcie procesu aktywacji uwierzytelniania biometrią bez PINu jest informowany o ryzyku, jakie niesie ze sobą zmiana metody uwierzytelniania i je akceptuje.

6. Minister informuje, że dokłada najwyższych starań, aby zapewnić wysoki poziom bezpieczeństwa teleinformatycznego Aplikacji i danych Użytkowników. Jednakże Minister wskazuje, że ze względu na specyfikę technologii informatycznych w przyszłości może zostać ujawniona podatność Aplikacji na określone zagrożenia. Z tego względu Minister zaleca aktualizowanie Aplikacji oraz wskazuje, że może wydawać publicznie dostępne zalecenia dotyczące zasad bezpieczeństwa związanych z korzystaniem z Aplikacji.
7. W przypadku wszystkich usług dostępnych w Aplikacji pobrane dane są przechowywane w zaszyfrowanej formie na urządzeniu mobilnym.

§ 6. Warunki licencyjne

1. Z chwilą instalacji Aplikacji Minister udziela Użytkownikowi niewyłącznej licencji na korzystanie z Aplikacji na warunkach określonych w niniejszym paragrafie oraz zgodnie z Regulaminem i Załącznikami. Udzielona licencja jest nieprzenaszalna oraz 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 zainstalowania aplikacji i używania jej na posiadanym przez Użytkownika urządzeniu mobilnym – jeżeli czynności te są podejmowane dla celów korzystania z Aplikacji zgodnie z Regulaminem i Załącznikami. Minister zastrzega, że ze względów bezpieczeństwa Usługi dostępne w Aplikacji, są możliwe do uruchomienia wyłącznie na jednym urządzeniu mobilnym.
4. Z zastrzeżeniem ust. 3 oraz wyjątków wynikających z bezwzględnie obowiązujących przepisów prawa, Użytkownik nie jest uprawniony do zwielokrotniania Aplikacji w jakikolwiek inny sposób lub jej tłumaczenia, przystosowywania, zmiany układu lub wprowadzania jakichkolwiek innych zmian.
5. Zakres udzielonej licencji obejmuje jednocześnie możliwość korzystania z Usług zdefiniowanych w § 1 ust. 1 Regulaminu oraz w Załącznikach.

§ 7. 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 telefonu +48 42 253 54 74.
2. Ewentualne pytania, uwagi lub propozycje Użytkowników dotyczące Aplikacji i jej funkcji można kierować drogą elektroniczną na adres e-mail: mobywatel-pomoc@coi.gov.pl. Pytania dotyczące usługi Unijny Certyfikat COVID oraz eRecepta należy kierować drogą

elektroniczną na adres: ikp-pomoc@cez.gov.pl Informacje dotyczące usługi Polak za granicą można uzyskać pod numerem telefonu 22 250 01 16.

§ 8. Funkcja Potwierdź swoje dane

1. Użytkownik dzięki funkcjonalności poszczególnych usług (mDowód, Diia.pl) może za pomocą aplikacji skorzystać z funkcji „Potwierdź swoje dane". Funkcja ta pozwala na przekazanie do weryfikacji Usługi mWeryfikator danych Użytkownika w postaci kodu QR lub w postaci 6 cyfrowego kodu.
2. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu danego dokumentu, a następnie funkcji „potwierdź swoje dane".
3. Ekran prezentacji danych uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
   1) ruchomego elementu polskiej flagi;
   2) elementu graficznego o zmiennej kolorystyce, uzależnionej od kąta pochylenia urządzenia mobilnego (hologram), w kształcie odpowiadającym Godłu Rzeczypospolitej Polskiej;
   3) elementy grafiki tła o zmiennej kolorystyce i napisach, uzależnionych od kąta pochylenia urządzenia mobilnego (hologram);
   4) elementu graficznego prezentującego aktualną datą i godzinę z dokładnością do zmieniających się sekund;
   5) elementu graficznego prezentującego datę pobrania danych tzw. „Stan na dzień".
4. Potwierdzenie danych przebiega w następujący sposób:
   1) Weryfikujący pokazuje kod. Weryfikowany skanuje kod, wyświetla się graficzny, kwadratowy kod QR, który zawiera informację o czasie jego wygenerowania;
   2) kod jest ważny 3 minuty od chwili jego wygenerowania. Po upływie tego czasu przekazanie danych wymaga ponownego wygenerowania Kodu QR;
   3) Po zamknięciu Aplikacji lub wygaśnięciu jej sesji, przekazanie danych wymaga ponownego wygenerowania kodu QR
   4) Weryfikujący przy uruchomionej Aplikacji mObywatel, odczytuje kod QR za pomocą aparatu fotograficznego swojego urządzenia mobilnego, którym się posługuje lub wpisuje otrzymany 6 cyfrowy kodu;
   5) następuje potwierdzenia danych zawartych w kodzie QR do urządzenia mobilnego osoby Weryfikującej.
   6) Po nawiązaniu połączenia Usługa mWeryfikator przekazuje do Aplikacji mObywatel osoby Weryfikowanej, dane Użytkownika, który go weryfikował.
   7) Usługa mWeryfikator i Aplikacja mObywatel nie przechowuje weryfikowanych danych, a jedynie informację o zdarzeniu.
   8) Po prawidłowym zakończeniu elektronicznej weryfikacji danych osobowych Użytkownika dane dotyczące dokonanej weryfikacji zapisywane są w weryfikowanej Usłudze/ Dokumencie (funkcja „Historia") Aplikacji mObywatel.

§ 9. Funkcja Przekaż

1. Funkcja „Przekaż"- (funkcjonalność dostępna dla: Legitymacja szkolna, Legitymacja studencka, Legitymacja adwokacka, Legitymacja emeryta-rencisty, Legitymacja posła, Karta Dużej Rodziny, Małopolska Karta Aglomeracyjna, Unijny Certyfikat COVID- za

pomocą danych z mDowodu) pozwala na elektroniczne przekazanie danych Użytkownika innemu Użytkownikowi aplikacji mWeryfikator.

2. Elektroniczne przekazanie danych Instytucji lub firmie.

   Funkcja ta pozwala na przekazanie danych Użytkownika do systemu teleinformatycznego Instytucji. W tym celu Użytkownik przekazujący dane:

   1) Wybiera odpowiedni dokument z jakiego chce przekazać dane
   2) Po wyborze dokumentu w dole ekranu funkcję „Przekaż”;
   3) następnie wybiera funkcję „Instytucji lub firmie” i przycisk „Przekaż”;
   4) Użytkownik skanuje kod QR Instytucji (okazany na stronie internetowej Instytucji – online lub w placówce Instytucji – on site);
   5) w usłudze mObywatel pojawia się komunikat o nawiązywaniu połączenia z Instytucją;
   6) pojawia się komunikat jakie dane i jakiej Instytucji zostaną przekazane;
   7) Użytkownik wybiera przycisk „Potwierdzam”;
   8) następuje przekazanie danych Użytkownika do Instytucji;
   9) pojawia się komunikat o wyniku przekazania danych.

3. Elektroniczne przekazanie danych Użytkownika użytkownikowi mWeryfikatora

   Funkcja „Przekaż” – dostępna jest dla dokumentów: legitymacja emeryta-rencisty, legitymacja ucznia, legitymacja studenta, legitymacja adwokacka, legitymacja poselska, KDR, legitymacja UUT, dokumenty lokalne (wydawane na podstawie WRU),
   Dla wybranego przez siebie dokumentu użytkownik:

   1) wybiera funkcję „Przekaż”;
   2) następnie wybiera funkcję „Osobie weryfikującej Twoją tożsamość” i przycisk „Przekaż”;
   3) w usłudze mObywatel wyświetli się graficzny, kwadratowy kod QR, który zawiera informację o czasie jego wygenerowania i jest ważny 3 minuty 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 swojego urządzenia mobilnego;
   5) następuje przekazanie danych zawartych w kodzie QR do urządzenia mobilnego użytkownika mWeryfikatora.

4. 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.

§ 10. Odpowiedzialność

1. Użytkownik ponosi pełną odpowiedzialność za naruszenie prawa bądź szkodę wyrządzoną swoim działaniem 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. Minister nie ponosi odpowiedzialności za:
    1) szkody będące wynikiem niewykonania przez Użytkownika aktualizacji Aplikacji lub niezastosowania się do zaleceń, o których mowa w § 5 Regulaminu bądź Załącznikach;
    2) szkody będące wynikiem korzystania przez Użytkownika z Aplikacji w sposób niezgodny z prawem lub niniejszym Regulaminem i Załącznikami;
    3) jakość i dostępność usług telekomunikacyjnych, niezbędnych do korzystania z Aplikacji, świadczonych przez operatora telekomunikacyjnego, z którego usług korzysta Użytkownik;
    4) nieprawidłowości funkcjonowania Aplikacji wynikające z nieprawidłowości działania systemu operacyjnego lub urządzenia mobilnego, z którego korzysta Użytkownik.
3. Minister przewiduje dalszy rozwój Aplikacji oraz wprowadzanie nowych funkcji w przyszłości, co może powodować konieczność aktualizowania Aplikacji. O rozszerzeniu funkcji i wynikających stąd zmianach dla Użytkownika Minister informuje w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra.
4. Minister nie zapewnia również prawidłowego funkcjonowania Usług po upływie terminu ważności certyfikatu przypisanego do: Profilu mObywatel albo usługi Legitymacja szkolna, albo Legitymacja studencka, albo Diia.pl.
5. Minister informuje, że ze względu na specyfikę technologii informatycznych korzystanie z funkcji Aplikacji wymagających dostępu do Internetu (aktywacja Aplikacji, aktualizacja danych), może być realizowane z przerwami lub z ograniczeniami wynikającymi z mocy obliczeniowej infrastruktury informatycznej Ministra.

§ 11. Klauzula informacyjna

1. Administratorem danych Użytkownika aplikacji mObywatel jest Minister, którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą przy ul. Królewskiej 27, 00-060 w Warszawie.
2. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: Kancelaria.Krolewska@cyfra.gov.pl lub na adres skrytki na ePUAP: /MAiC/SkrytkaESP.
3. Administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować we wszystkich sprawach związanych z przetwarzaniem danych osobowych: korespondencyjnie na adres: ul. Królewska 27, 00-060 Warszawa, bądź mailowo na adres: iod@mc.gov.pl.
    1) Podstawą przetwarzania danych osobowych przez administratora danych (Ministra Cyfryzacji) w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego:

2) w zakresie mDowodu, Profilu mObywatel i Certyfikatu realizacja obowiązku prawnego ciążącego na administratorze, to jest art. 6 ust. 1 lit. c RODO w związku z art. 7 ust. 1 i 2, art. 8 ust. 2 i 3, art. 10 ust. 1 i 2, art. 13, art. 14 Ustawy o aplikacji mObywatel;
3) w zakresie usługi Moje Pojazdy realizacja obowiązku prawnego ciążącego na administratorze, to jest art. 6 ust. 1 lit. c RODO, w związku z art.3 ust. 1 pkt 1 Ustawy o aplikacji mObywatel.
4) W zakresie Usługi mPrawo Jazdy realizacja obowiązku prawnego ciążącego na administratorze, to jest art. 6 ust. 1 lit. c RODO w związku z art. 3 ust. 1 pkt 1-3 Ustawy o aplikacji mObywatel.
5) W zakresie Usługi DIIA stanowi realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO w związku z art. 10 Ustawy o pomocy obywatelom Ukrainy
6) realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, polegającego na udostępnieniu usług podmiotów publicznych i niepublicznych na podstawie art. 15 i art. 16 Ustawy o aplikacji mObywatel.

4. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z RODO:
   1) prawo dostępu do treści danych;
   2) prawo ich poprawiania i sprostowania;
   3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   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.
5. Prawo do poprawienia lub sprostowania danych realizowane jest wyłącznie poprzez poprawienie danych znajdujących się w systemie teleinformatycznym zapewniających funkcjonowanie dokumentu mDowód oraz dotyczy danych, o których mowa w § 3 ust. 1– 3 Załącznika nr 1.
6. 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 albo na podstawie akceptacji przekazania danych osobowych do Instytucji.
7. 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.
8. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Potwierdź swoje dane”) do systemu teleinformatycznego Instytucji, Aplikacja przesyła wybrane dane osobowe, które są niezbędne do realizacji usługi oferowanej przez daną Instytucję. Zestaw danych jest uzależniony od oferowanej przez Instytucję usługi.

9. W celu utworzenia Certyfikatu oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister właściwy do spraw informatyzacji przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.
10. Minister właściwy do spraw informatyzacji przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.
11. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
12. Zgodnie z art. 20 ust. 3 Ustawy o aplikacji mObywatel Minister właściwy do spraw informatyzacji przetwarza dane osobowe użytkowników aplikacji mObywatel przez okres:
    1) 6 lat od dnia upływu ważności albo dnia unieważnienia certyfikatu użytkownika w przypadku danych, które są przetwarzane w systemie mObywatel;
    2) 20 lat od dnia unieważnienia profilu mObywatel – w przypadku danych, które są przetwarzane w systemie identyfikacji elektronicznej, w którym jest wydawany profil mObywatel. Dane nie są przetwarzane w celach marketingowych.
13. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu mDowód, 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. Historia działań Użytkownika zapisywana jest w jego urządzeniu mobilnym.
14. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), 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.
15. 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.
16. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

§ 11. Postanowienia końcowe

1. Minister informuje, że instalacja dostarczanych cyklicznie przez Ministra aktualizacji Aplikacji może być konieczna dla jej prawidłowego działania i należytego zabezpieczenia

zawartych w niej danych. Minister rekomenduje instalowanie takich aktualizacji niezwłocznie po ich udostępnieniu za pomocą sklepów z aplikacjami.
2. Użytkownik w dowolnym momencie może zakończyć korzystanie z Usług poprzez dezaktywowanie danej Usługi w Aplikacji (jeśli taka funkcjonalność jest dostępna) lub odinstalowanie Aplikacji z urządzenia mobilnego.
3. Użytkownik może w dowolnym momencie zakończyć korzystanie z Aplikacji, poprzez jej odinstalowanie z urządzenia mobilnego.
4. Regulamin jest udostępniony nieodpłatnie na stronie podmiotowej Ministra w Biuletynie Informacji Publicznej, która umożliwia jego pobranie, utrwalenie i wydrukowanie.
5. Regulamin może ulec zmianie wraz z kolejnymi wydaniami Aplikacji. Zmiana jest wiążąca dla Użytkowników, którzy zainstalują takie wydanie Aplikacji.
6. Jeżeli Użytkownik nie zgadza się ze zmianą postanowień Regulaminu, w każdym momencie może odinstalować Aplikację z urządzenia mobilnego.

Załączniki:

Załącznik nr 1 – dokument mDowód
Załącznik nr 2 – Usługa Legitymacja szkolna
Załącznik nr 3 – Usługa Moje Pojazdy
Załącznik nr 4 – Usługa Legitymacja studencka
Załącznik nr 5 – Usługa mPrawo Jazdy i Punkty Karne
Załącznik nr 6 – Usługa Karta Dużej Rodziny
Załącznik nr 7 – Usługa Unijny Certyfikat COVID (UCC)
Załącznik nr 8 – Usługa Legitymacja UUT – Legitymacja uprawniająca do Ulgowych Usług Transportowych
Załącznik nr 9 – Usługa Diia.pl
Załącznik nr 10 – Usługa Legitymacja emeryta-rencisty
Załącznik nr 11 – Usługa Legitymacja adwokacka
Załącznik nr 12 – Usługa Legitymacja poselska
Załącznik nr 13 – Usługa e-Płatności
Załącznik nr 14 – Usługa Rejestr Uprawnień
Załącznik nr 15 – Polityka prywatności aplikacji mObywatel

Załączniki do Regulaminu korzystania z Aplikacji mObywatel
Załącznik nr 1

Dokument mDowód

§ 1. Definicje
Profil mObywatel – o którym mowa w Regulaminie aplikacji.
Certyfikat podstawowy (zwany dalej „Certyfikatem") – o którym mowa w Regulaminie aplikacji.
Dokument mObywatel (zwany dalej "mDowód"/ „dokument mDowód) –
o którym mowa w Regulaminie aplikacji.

§ 2. Informacje ogólne
1. Dokument mDowód 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.
2. Za pomocą dokumentu mDowód możesz bezpiecznie:
   1) okazywać swoje dane innym osobom – tym samym potwierdzając swoją tożsamość,
   2) przekazać swoje dane podmiotom publicznym lub niepublicznym w celu skorzystania z oferowanych przez nie usług.
3. Postanowienia dotyczące zasad przetwarzania danych osobowych przy użyciu dokumentu mDowód zostały zamieszczone w § 11 Regulaminu Aplikacji.

§ 3. mDowód
1. Zgodnie z art. 7 ust. 1 Ustawy o aplikacji mObywatel mDowód zawiera dane użytkownika aplikacji mObywatel pobrane z rejestru PESEL, o którym mowa w art. 6 ust. 1 Ustawy o ewidencji ludności:
   1) nazwisko i imię (imiona);
   2) zdjęcie;
   3) numer PESEL;
   4) datę urodzenia;
   5) obywatelstwo;
   6) imię ojca;
   7) imię matki;
   8) Seria i nr dokumentu mDowód;
   9) Termin ważności dokumentu mDowód;
   10) Termin wydania dokumentu mDowód.
2. Fotografię użytkownika Aplikacji mObywatel pobraną z Rejestru Dowodów Osobistych, o którym mowa w art. 55 ust. 1 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych.

3. Za pośrednictwem dokumentu mDowód dane Użytkownika przechowywane w Aplikacji mObywatel mogą być w sposób bezpieczny okazywane innym osobom lub przekazane Instytucji lub Użytkownikowi mWeryfikatora.
4. Zgodnie z art.7 ust. 5 Ustawy o aplikacji mObywatel mDowód nie uprawnia do:
   1) przekraczania granicy państwowej,
   2) stwierdzenia tożsamości lub obywatelstwa polskiego w przypadku wystąpienia albo uzasadnionego przypuszczenia wystąpienia okoliczności, w których wykorzystanie tego dokumentu nie zapewni niezbędnego poziomu pewności i bezpieczeństwa stwierdzenia tożsamości lub obywatelstwa polskiego albo nie może być przeprowadzone w warunkach zapewniających taki poziom.
   3) zgodnie z art.83 ustawy o aplikacji mObywatel instytucje obowiązane, o których mowa w art. 2 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2023 r. poz. 1124), są obowiązane stosować przepisy ustawy w zakresie wykorzystywania dokumentu mObywatel jako środka bezpieczeństwa finansowego do identyfikacji klienta oraz weryfikacji jego tożsamości, od dnia 1 września 2023 r.

§ 4. Użytkownicy

1. Użytkownikiem mDowodu może zostać wyłącznie osoba fizyczna, która spełnia poniższe warunki:
   1) posiada numer PESEL;
   2) posiada obywatelstwo polskie;
   3) posiadają aktywny jeden z dostępnych środków identyfikacji elektronicznej wydany w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl) ;
   4) posiada aktywny certyfikat podstawowy.
2. Warunki uzyskania mDowodu przez osobę, która nie spełnia warunków w ust.1 określa ustawa o aplikacji mObywatel.

§ 5. Aktywacja dokumentu mDowód

1. Dla Użytkowników posiadających usługę mObywatel przed dniem 14 lipca 2023 r., warunkiem otrzymania mDowodu jest aktualizacja Aplikacji. Użytkownicy mają możliwość wyboru między aktywacją Aplikacji z profilem mObywatel, lub aktualizacji Aplikacji i tym samym korzystania z mDowodu na podstawie wcześniej uzyskanego certyfikatu.
   Użytkownicy mogą korzystać z certyfikatu wydanego do Usługi mObywatel do czasu jego wygaśnięcia.
2. Aktywacja dokumentu mDowód przez nowego Użytkownika polega na:
   1) zalogowaniu się do Aplikacji;
   2) potwierdzeniu tożsamości Użytkownika przy użyciu jednego z dostępnych środków identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl).

3. Po wykonaniu czynności opisanych w ust. 1, nastąpi automatyczne pobranie danych Użytkownika z Rejestru Dowodów Osobistych i rejestru PESEL oraz zaszyfrowanie i zapisanie ich w urządzeniu mobilnym Użytkownika.
4. Po pobraniu danych z Rejestru Dowodów Osobistych i rejestru PESEL automatycznie jest tworzony i pobierany Profil mObywatel. Certyfikat przypisany jest do Użytkownika i jego urządzenia mobilnego. W celu utworzenia Certyfikatu i zarządzania Certyfikatami Minister przetwarza dane osobowe Użytkownika – imiona, nazwisko, obywatelstwo i numer PESEL – pochodzące z rejestru PESEL.
5. Ważność Profil mObywatel jest ograniczona w czasie i wynosi nie więcej niż jeden rok od aty aktywacji usługi mObywatel i nie może być dłuższa niż data ważności mDowodu.
6. Do potwierdzenia tożsamości Użytkownika przy użyciu jednego z dostępnych środków identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl), pobrania Profil mObywatel oraz pobrania danych z Rejestru Dowodów Osobistych i rejestru PESEL niezbędne jest aktywne połączenie internetowe.
7. Użytkownik może aktywować i pobrać mDowód oraz profil mObywatel wyłącznie na jednym urządzeniu.
8. Dostęp do danych przechowywanych w usłudze mObywatel jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje dokumentu mDowód

1. Prawidłowo aktywowany dokument po zalogowaniu się z użyciem hasła dostępu do Aplikacji, umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych Użytkownika (moduł „mDowód”);
   2) elektroniczne przekazanie danych Użytkownika (funkcja „Potwierdź swoje dane”);
   3) przechowywanie informacji o przekazaniu danych do weryfikacji (funkcja „Historia”);
   4) aktualizowanie danych Użytkownika;
   5) zarządzanie Certyfikatem (funkcja „Wydane Certyfikaty”);
   6) usunięcia Dokumentu mDowód z Aplikacji (sekcja ”Dokumenty”, następnie ikona edycji i wybranie ikony „kosz”).

§ 7. Dostęp do usług online zależnych od dokumentu mDowód.

1. Przy pierwszym użyciu usług online zależnych od dokumentu mDowód dokonywana jest ich aktywacja. Aktywacja wymaga posiadania ważnego Profilu mObywatel za pomocą którego dane Użytkownika uwierzytelniane są w systemach teleinformatycznych Administratorów danych dla poszczególnych usług.
2. Dezaktywacja usług zależnych od dokumentu mDowód następuje poprzez dezaktywację-unieważnienie Profilu mObywatel.

Załącznik nr 2

Legitymacja szkolna

§ 1. Definicje:

1. **Legitymacja szkolna –** usługa prezentacji dokumentu elektronicznego, o którym mowa w § 4 ust. 2 rozporządzenia Ministra Edukacji Narodowej z dnia 7 czerwca 2023 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych (Dz.U. z 2023 r. poz. 1120) oraz § 4 ust 5 rozporządzenia z dnia 16 kwietnia 2020 r. Ministra Kultury i Dziedzictwa Narodowego w sprawie świadectw, dyplomów państwowych i innych druków publicznych szkół i placówek artystycznych (Dz. U. z 2020 r. poz. 813, z późn. zm.), wydawana w postaci dokumentu mobilnego, o którym mowa w art. 2 pkt 7 Ustawy o aplikacji mObywatel, która pozwala na pobranie danych osobowych Użytkownika, przechowywanie ich w zaszyfrowanej formie na urządzeniu mobilnym Użytkownika, okazywanie danych Użytkownika innym osobom.
2. **Certyfikat Ucznia** – poświadczenie, o którym mowa w art. 11 Ustawy o aplikacji mObywatel pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika wydany w ramach dokumentu mobilnego - Legitymacja szkolna.
3. **System** – system teleinformatyczny zapewniany przez Ministra Cyfryzacji, który pozwala na wydanie przez Dyrektora szkoły mobilnej Legitymacji szkolnej i wygenerowanie danych osobowych ucznia oraz danych potwierdzających status mobilnej Legitymacji szkolnej.
4. **Dyrektor** – Dyrektor szkoły, do której uczęszcza Uczeń lub upoważniona przez Dyrektora osoba wydająca mobilną Legitymację szkolną.

§ 2. Informacje ogólne

1. Usługa pozwala korzystać z mobilnej Legitymacji szkolnej, który ma taką samą funkcję i moc prawną, jak legitymacja wydana w wersji papierowej lub w postaci plastikowej karty (e-legitymacji). Za pomocą dokumentu mobilnego Legitymacji szkolnej możesz:
   1) potwierdzić, że jesteś uczniem danej szkoły;
   2) skorzystać z ulg i zwolnień, które przysługują po okazaniu legitymacji.
2. Ilekroć w załączniku pojawia się pojęcie pisane wielką literą i niezdefiniowane w Definicjach to mają one znaczenie nadane im przez Regulamin.
3. Dyrektor jest organem odpowiedzialnym za wydanie (aktywowanie) oraz ewentualne unieważnienie mobilnej Legitymacji szkolnej.

§ 3. Użytkownicy

1. Użytkownikami mobilnej Legitymacji szkolnej, mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
   1) posiadają nadany numer PESEL,
   2) są uczniami szkoły podstawowej, ponadpodstawowej, szkoły policealnej lub słuchaczami szkoły dla dorosłych, którym właściwi Dyrektorzy wydali mobilny dokument- Legitymację szkolną – zwani dalej w niniejszym załączniku **„Uczniami”** lub pojedynczo **„Uczniem”**.
2. Zabrania się Uczniowi:
   1) udostępniania Aplikacji w celu posłużenia się nią przez inną osobę;

2) udostępniania jednorazowego QR kodu oraz hasła otrzymanego od Dyrektora, umożlwiającego dostęp do Usługi.

§ 4. Aktywacja Usługi

1. Przy pierwszym użyciu Usługi dokonywana jest jej aktywacja.
2. Do przeprowadzenia aktywacji Usługi niezbędne jest aktywne połączenie internetowe.
3. Aktywacja Usługi polega na:
   1) nadaniu przez właściwego Dyrektora szkoły uprawnień w Systemie, wgraniu zdjęcia Ucznia w Systemie, wygenerowaniu kodu QR i jednorazowego kodu aktywującego Legitymację;
   2) zalogowaniu do Aplikacji;
   3) wczytaniu kodu QR oraz wpisaniu przez Ucznia (rodzica lub opiekuna prawnego) kodu aktywacyjnego Legitymacji;
   4) pobraniu danych osobowych Ucznia z Systemu.
4. Jednorazowy kod aktywacyjny oraz kod QR jest ważny 30 dni od momentu jego wygenerowania w Systemie.
5. Uczeń (rodzic lub opiekun prawny) może aktywować Usługę i pobrać dane Systemu wyłącznie na jednym urządzeniu mobilnym.
6. Po pobraniu danych z Systemu automatycznie jest tworzony i pobierany do Usługi Certyfikat Ucznia. Certyfikat przypisany jest do Ucznia i urządzenia mobilnego, którym posługuje się Uczeń. W celu utworzenia Certyfikatu i zarządzania Certyfikatami Minister przetwarza dane osobowe Ucznia: imię, nazwisko i numer PESEL.
7. Certyfikat Ucznia służy również do pobrania i podpisania danych w usłudze KDR, dla Uczniów posiadających Kartę Dużej Rodziny.
8. Ważność Certyfikatu Ucznia jest ograniczona w czasie. Certyfikat Ucznia jest wydawany na okres roku szkolnego lub semestru, w którym wydawana jest , związana z tym certyfikatem, legitymacja szkolna w postaci dokumentu mobilnego.
9. Nie jest możliwe nadanie uprawnień przez Dyrektora w Systemie oraz aktywacja Usługi – jeżeli Uczeń nie spełnia warunków określonych w § 3 ust. 1 niniejszego załącznika, w szczególności kiedy zostało zgłoszone zaginięcie lub uszkodzenie odpowiednio legitymacji lub e-legitymacji, bądź też w przypadku podjęcia próby aktywacji Usługi na kolejnym urządzeniu mobilnych.
10. Poza funkcjami elektronicznego przekazania danych oraz elektronicznej weryfikacji danych osobowych Aplikacja nie oferuje funkcji eksportu ani importu danych.

§ 5. Funkcje Legitymacji szkolnej

1. **Okazanie Legitymacji na ekranie urządzenia mobilnego**:
   1) zgodne z przepisami prawa okazanie mobilnej Legitymacji szkolnej ma skutek analogiczny jak okazanie legitymacji w postaci papierowej lub e-legitymacji;
   2) pozwala ocenić osobie uprawnionej do kontroli legitymacji prawdziwość Legitymacji szkolnej między innymi na podstawie następujących elementów graficznych:
      a) zdjęcia osoby legitymowanej,
      b) numeru legitymacji i wieku Ucznia, statusu: „ważna” lub „nieważna”,
      c) hologramu – którego wygląd pozwala na stwierdzenie, iż nie stanowi on statycznego obrazu, lecz jest faktycznie generowany przez Aplikację,
      d) flagi Polski – której wygląd pozwala na stwierdzenie, iż nie stanowi ona statycznego obrazu, lecz jest faktycznie generowana przez Aplikację,

e) czasu okazania.

§ 6. Unieważnianie Legitymacji i usuwanie danych Ucznia:

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.
2. Unieważnienie Legitymacji jest dokonywane przez Dyrektora, następuje ono w przypadku:
   1) utraty ważności wydanej Uczniowi legitymacji szkolnej albo e-legitymacji szkolnej;
   2) utraty Legitymacji na skutek uszkodzeń, niepoprawnego działania lub utraty urządzenia mobilnego, w którym przechowywana była Legitymacji;
   3) w przypadku przejścia Ucznia do innej szkoły;
   4) na wniosek pełnoletniego Ucznia lub rodziców niepełnoletniego Ucznia.

§ 7. Klauzula informacyjna

1. Administratorem danych zawartych w mobilnej Legitymacji jest Dyrektor, do której uczęszcza Uczeń. Minister Cyfryzacji w odniesieniu do tych danych jest podmiotem przetwarzającym.
2. We wszelkich sprawach dotyczących przetwarzania danych osobowych w mobilnej Legitymacji należy kontaktować się z właściwym Administratorem bądź powołanym przez niego Inspektorem Ochrony Danych.
3. Administratorem danych Użytkownika aplikacji mObywatel jest Minister Cyfryzacji, z siedzibą przy ul. Królewskiej 27, 00-060 w Warszawie.
4. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: Kancelaria.Krolewska@cyfra.gov.pl lub na adres skrytki na ePUAP: /MAiC/SkrytkaESP.
5. Administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować we wszystkich sprawach związanych z przetwarzaniem danych osobowych: korespondencyjnie na adres: ul. Królewska 27, 00-060 Warszawa, bądź mailowo na adres: iod@mc.gov.pl.
6. Podstawą przetwarzania danych osobowych dla Certyfikatu Ucznia przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, w związku z art. 69 ust. 2 ustawy o aplikacji mObywatel i porozumienia zawartego przez Ministra Cyfryzacji. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. Uczniowi przysługuje w dowolnym momencie prawo:
   1) prawo dostępu do treści danych;
   2) prawo ich poprawiania i sprostowania;
   3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

8. Uczniowi przysługuje również prawo do ograniczenia przetwarzania danych osobowych w przypadkach określonych w art. 18 Ogólnego rozporządzenie o ochronie danych. W takim przypadku Minister, na podstawie wniosku Ucznia, w systemie obsługującym Legitymacje oznaczy dane i nie będzie ich poza ich posiadaniem przetwarzał, nawet w celach statystycznych do czasu wyjaśnienia sprawy.
9. W przypadku zgubienia, kradzieży lub utraty z innych przyczyn urządzenia mobilnego, Uczeń powinien niezwłocznie dokonać zgłoszenia tego faktu Dyrektorowi.
10. Dla celu utworzenia Certyfikatu podczas aktywacji Usługi oraz zarządzania Certyfikatami Uczniów, w tym utrzymaniem listy aktywnych Certyfikatów, Minister przetwarza dane obejmujące imię, nazwisko, numer PESEL, numer legitymacji Ucznia.
11. Minister gromadzi dane statystyczne dotyczące Usługi w zakresie liczby:
    1) aktywacji Legitymacji;
    1) akcji wydania Certyfikatów Ucznia;
    2) unieważnionych Legitymacji;
    3) zgłoszonych problemów.
12. Z zastrzeżeniem ustępów następnych Minister nie przetwarza danych o połączeniach między urządzeniem mobilnym Ucznia używającego Legitymacji a użytkownikiem Aplikacji mWeryfikator. Minister nie gromadzi również informacji o skorzystaniu przez Uczniów z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych.
13. Minister przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu Ucznia (sprawdzenie ważności Certyfikatu Ucznia online) za pomocą Aplikacji mWeryfikator gromadzi następujące dane:
    1) identyfikator użytkownika Aplikacji mWeryfikator;
    2) numer Certyfikatu Ucznia przekazującego dane, weryfikowanego za pomocą Aplikacji mWeryfikator.
14. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji aktualności Certyfikatu oraz wykrycia ewentualnych błędów i luk bezpieczeństwa.
15. Dane, o których mowa w tym ustępie przechowywane są przez okres 6 lat od dnia ostatniej aktywności Użytkownika w systemie teleinformatycznym Aplikacji (art. 20 ust. 1 pkt. 1 ustawy o aplikacji mObywatel). Dane nie są przetwarzane w celach marketingowych.
16. Dane nie są przetwarzane w celach marketingowych.
17. Dane osobowe Ucznia będą mogły również być 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.
18. 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.
19. Dane osobowe Ucznia nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 3 do Regulaminu

Moje Pojazdy

§ 1. Definicje

1. **Usługa** – Usługa pod nazwą „Moje Pojazdy”, o której mowa w art. 3 ust. 1 pkt 1 Ustawy o aplikacji mObywatel, dostępna na urządzeniu mobilnym Użytkownika w Aplikacji, której wykorzystywanie odbywa się na warunkach określonych w Regulaminie i w Ustawie o aplikacji mObywatel oraz Prawie o ruchu drogowym.
2. **Ustawa Prawo o ruchu drogowym** – ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. 2023 poz. 1047 z późn. zm.).
3. **Dane pojazdu -** dane dotyczące Użytkownika oraz dane pojazdu lub pojazdów, którego użytkownik jest właścicielem lub współwłaścicielem ujawnionym w bazie CEP. Wszystkie dane dotyczące użytkownika i pojazdu są wyświetlane w Usłudze.
4. **Baza CEP -** Centralna ewidencja pojazdów**,** o której mowa w art. 80a Ustawy Prawo o ruchu drogowym, zawierająca dane, które są pobierane i wyświetlane w Usłudze.
5. **Certyfikat** – o którym mowa w Regulaminie aplikacji.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych pojazdu w ramach Usługi stanowi art. 80cb Prawa o ruchu drogowym w związku z art. 3 ust. 1 pkt 1 Ustawy o aplikacji mObywatel, zgodnie z którym Minister zapewnia działanie systemu teleinformatycznego, który pozwala, przy użyciu publicznej aplikacji mobilnej, na pobranie dokumentu elektronicznego zawierającego dane umożliwiające identyfikację rzeczy związanej z użytkownikiem publicznej aplikacji mobilnej.
2. Za aktualność danych zawartych w Usłudze odpowiada Użytkownik, który jest obowiązany do aktualizacji danych jeżeli dane te uległy zmianie i posiada o nich wiedzę. Zaleca się korzystanie z funkcji aktualizacji danych co najmniej raz na 3 miesiące.
3. Korzystanie z Usługi 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. Dane dostępne w Usłudze nie stanowią dowodu rejestracyjnego oraz nie są tożsame z dowodem rejestracyjnym ani go nie zastępują.
5. Postanowienia dotyczące zasad przetwarzania danych osobowych zostały zamieszczone w § 11 Regulaminu Aplikacji.

§ 3. Usługa Moje Pojazdy

1. Usługa pozwala na pobranie:
   1) danych osobowych Użytkownika powiązanych z danymi pojazdu ujawnionymi w bazie CEP,
   2) danych pojazdu zawartych w bazie CEP
   - oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika. Za pośrednictwem Usługi dane pojazdu przechowywane w Usłudze mogą być w sposób bezpieczny okazywane innym Użytkownikom.

2. Pobranie Usługi i korzystanie z niej jest nieodpłatne. Korzystanie przez Użytkownika z usług transmisji danych lub połączeń głosowych w związku z pobraniem lub korzystaniem z Usługi może wiązać się z opłatami naliczanymi przez operatora telekomunikacyjnego, który świadczy Użytkownikowi usługi telekomunikacyjne.
3. Wiarygodność danych dostępnych w Usłudze wynika z faktu, że dane pochodzą z rejestrów państwowych i zostały pobrane przez osobę, która została zidentyfikowana przez Ministra. Dane są też przechowywane i przesyłane za pomocą Aplikacji udostępnionej przez Ministra.
4. Nie jest natomiast możliwe posługiwanie się Usługą w stosunkach z administracją publiczną wtedy, gdy z przepisów prawa (ustawy, rozporządzenia itd.) wynika obowiązek okazania dowodu rejestracyjnego, polisy OC, karty pojazdu oraz pozwolenia czasowego.
5. Do korzystania z Usługi niezbędne jest posiadanie ważnego środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl).

§ 4. Użytkownicy

1. Użytkownikiem aplikacji mObywatel może zostać wyłącznie osoba fizyczna.
2. Użytkownikami mogą być wyłącznie osoby mające obywatelstwo polskie, które spełniają dwa poniższe warunki:
   1) posiadają aktywny jeden z dostępnych środków identyfikacji elektronicznej wydany w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl);
   2) posiadają aktywny Profil mObywatel.

§ 5. Aktywacja Usługi

1. Aktywację Usługi umożliwia dokument mDowód. Brak uprzedniego wyrażenia zgody przez Użytkownika na aktywację dokumentu mDowód uniemożliwia aktywację Usługi Moje Pojazdy.
2. Przy pierwszym użyciu Usługi dokonywana jest aktywacja Usługi.
3. Aktywacja Usługi polega na:
   1) zalogowaniu do Aplikacji;
   2) wybraniu z listy dostępnych usług „Moje Pojazdy”;
   3) potwierdzeniu tożsamości przy użyciu Certyfikatu;
   4) pobraniu danych Użytkownika z bazy CEP oraz zapisaniu ich w urządzeniu mobilnym Użytkownika.
4. Ważność Certyfikatu jest ograniczona w czasie i wynosi nie więcej niż jeden rok nie może być dłuższa niż data ważności mDowodu. Certyfikat wydawany jest zgodnie z art. 10 ust. 2 Ustawy o aplikacji mObywatel, użytkownikowi aplikacji automatycznie z Profilem mObywatel zgodnie z art. 14 ust. 1 Ustawy o aplikacji mObywatel.
5. Do pobrania danych z bazy CEP niezbędne jest aktywne połączenie internetowe.
6. Użytkownik może aktywować Usługę i pobrać dane z bazy CEP wyłącznie na jednym urządzeniu mobilny.

§ 6. Funkcje Usługi

1. Prawidłowo aktywowana Usługa po zalogowaniu się do Aplikacji umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych pojazdu („Moje Pojazdy”);
   2) aktualizowanie danych pojazdu (funkcja „Aktualizuj”);
2. Użytkownik może okazać osobie trzeciej dane pojazdu na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Usługi i po wybraniu funkcji „Moje Pojazdy”. Ekran prezentacji danych, dostępny po wybraniu tej funkcji, uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
   1. hologramu – którego wygląd pozwala na stwierdzenie, iż nie stanowi on statycznego obrazu, lecz jest faktycznie generowany przez Aplikację,
   2. flagi Polski – której wygląd pozwala na stwierdzenie, iż nie stanowi ona statycznego obrazu, lecz jest faktycznie generowana przez Aplikację,
3. Funkcja „Aktualizuj” umożliwia ponowne pobranie danych pojazdu przy użyciu Certyfikatu. **Zaleca się korzystanie z usługi aktualizacji danych co najmniej raz na 3 miesiące.**
4. W celu aktualizacji informacji o przebytych badaniach technicznych pojazdu lub informacji o nowym ubezpieczeniu OC należy wybrać przyciski funkcji „Aktualizuj”, dostępne w polach informacyjnych dotyczących wyżej wymienionych danych pojazdu.
5. Unieważnienie Certyfikatu usuwa jednocześnie dane dostępne w ramach Usługi.

Załącznik nr 4 do Regulaminu

Legitymacja studencka

Usługa pozwala korzystać z Legitymacji 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 Legitymacja studencka możesz:
- potwierdzić, że jesteś studentem danej uczelni,
- skorzystać z ulg i zwolnień, które przysługują po okazaniu legitymacji.

Ilekroć w załączniku pojawia się pojęcie pisane wielką literą i nie zdefiniowane w Definicjach to mają one znaczenie nadane im przez Regulamin.

§ 1. Definicje:

1. **Certyfikat Studenta**– poświadczenie, o którym mowa w art. 12 ust. 2 ustawy o aplikacji mObywatel pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika wydany w ramach dokumentu mobilnego- Legitymacja studencka.
2. **System** – system teleinformatyczny zapewniany przez Ministra Cyfryzacji, który pozwala na wydanie przez Dyrektora szkoły Legitymacji szkolnej i wygenerowanie danych osobowych ucznia oraz danych potwierdzających status Legitymacji studenckiej.
3. **Uczelnia** – uczelnia wydająca mobilną Legitymację studencką.

§ 2. Informacje ogólne

1. Usługa stanowi 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.

§ 3. Użytkownicy

1. Użytkownikami Usługi Legitymacja studencka, zwanej dalej „Legitymacją", mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
   1) mają nadany numer PESEL;
   2) są osobami, którym uczelnia wydała Legitymację – 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, umożlwiającego 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) nadaniu przez właściwą Uczelnię uprawnień w Systemie, wgraniu zdjęcia Studenta w Systemie, wygenerowaniu kodu QR i jednorazowego kodu aktywującego Legitymację;
   2) zalogowaniu do Aplikacji;
   3) wczytaniu kodu QR oraz wpisaniu przez użytkownika kodu aktywacyjnego Legitymacji;
   4) 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. Certyfikat jest wydawany na okres semestru, w którym jest wydawana, związana z tym certyfikatem legitymacja studencka w postaci dokumentu mobilnego.
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 Legitymacji

1. Okazanie Legitymacji na ekranie urządzenia mobilnego:
   1) zgodne z przepisami prawa okazanie mobilnej Legitymacji ma skutek analogiczny jak okazanie legitymacji studenckiej;
   2) pozwala ocenić osobie uprawnionej do kontroli legitymacji prawdziwość Legitymacji 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.

§ 6. Unieważnianie Legitymacji 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 Legitymacji jest dokonywane przez Uczelnię.

§ 7. Klauzula informacyjna

1. Administratorem danych zawartych w mobilnej Legitymacji jest Uczelnia, do której uczęszcza Student. Minister Cyfryzacji w odniesieniu do tych danych jest podmiotem przetwarzającym.
2. We wszelkich sprawach dotyczących przetwarzania danych osobowych w mobilnej Legitymacji należy kontaktować się z właściwym Administratorem bądź powołanym przez niego Inspektorem Ochrony Danych.
3. Administratorem danych Użytkownika aplikacji mObywatel jest Minister Cyfryzacji, z siedzibą przy ul. Królewskiej 27, 00-060 w Warszawie.
4. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: Kancelaria.Krolewska@cyfra.gov.pl lub na adres skrytki na ePUAP: /MAiC/SkrytkaESP.
5. Administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować we wszystkich sprawach związanych z przetwarzaniem danych osobowych: korespondencyjnie na adres: ul. Królewska 27, 00-060 Warszawa, bądź mailowo na adres: iod@mc.gov.pl.
6. Podstawą przetwarzania danych osobowych dla Certyfikatu Studenta przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, w związku z art. 69 ust. 1 ustawy o aplikacji mObywatel. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. Studentowi przysługuje w dowolnym momencie prawo:
   1) prawo dostępu do treści danych;
   2) prawo ich poprawiania i sprostowania;

3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

8. Studentowi przysługuje również prawo do ograniczenia przetwarzania danych osobowych w przypadkach określonych w art. 18 Ogólnego rozporządzenie o ochronie danych. W takim przypadku Minister, na podstawie wniosku Studenta, w systemie obsługującym Legitymacje oznaczy dane i nie będzie ich poza ich posiadaniem przetwarzał, nawet w celach statystycznych do czasu wyjaśnienia sprawy.
9. W przypadku zgubienia, kradzieży lub utraty z innych przyczyn urządzenia mobilnego, Student powinien niezwłocznie dokonać unieważnienia certyfikatu. Certyfikat można unieważnić:
   1) Samodzielnie za pomocą aplikacji mObywatel nawet w na innym urządzeniu poprzez aktywację, co skutkuje automatycznym unieważnieniem istniejącego certyfikatu.
   2) telefonicznie –dzwoniąc na numerem telefonu +48 42 253 54 74 czynnego w godzinach 7.00-18.00 w dni robocze.
10. Fakt unieważnienia Certyfikatu powinien zgłosić Uczelni.
11. Dla celu utworzenia Certyfikatu podczas aktywacji Usługi oraz zarządzania Certyfikatami Studentów, w tym utrzymaniem listy aktywnych Certyfikatów, Minister przetwarza dane obejmujące imię, nazwisko, numer PESEL, numer legitymacji Studenta.
12. Minister gromadzi dane statystyczne dotyczące Usługi w zakresie liczby:
   1) aktywacji Legitymacji;
   2) akcji wydania Certyfikatów Studenta;
   3) unieważnionych Legitymacji;
   4) zgłoszonych problemów.
13. Z zastrzeżeniem ustępów następnych Minister nie przetwarza danych o połączeniach między urządzeniem mobilnym Ucznia używającego Legitymacji a użytkownikiem Aplikacji mWeryfikator. Minister nie gromadzi również informacji o skorzystaniu przez Studentów z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych.
14. 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.
15. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji aktualności Certyfikatu oraz wykrycia ewentualnych błędów i luk bezpieczeństwa.
16. Dane, o których mowa w tym ustępie przechowywane są przez okres 6 lat od dnia ostatniej aktywności Użytkownika w systemie teleinformatycznym Aplikacji (art. 20 ust. 1 pkt. 1 ustawy o aplikacji mObywatel). Dane nie są przetwarzane w celach marketingowych.
17. Dane nie są przetwarzane w celach marketingowych.
18. Dane osobowe Studenta będą mogły również być 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.

19. 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.
20. Dane osobowe Studenta nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 5 Regulaminu

Usługa mPrawo Jazdy

§ 1. Definicje:

1. **CEK** – Centralna Ewidencja Kierowców, o której mowa w art. 100a Ustawy Prawo o ruchu drogowym.
2. **Punkty Karne** – usługa Ministra dostępna wraz z mPrawo Jazdy, która umożliwia prezentację liczby punktów, o których mowa w art. 98 ust. 1 ustawy o kierujących pojazdami otrzymanych przez Użytkownika za naruszenie przepisów ruchu drogowego.
3. **Ustawa o kierujących pojazdami** – ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2023 r. poz. 622).
4. **ustawa Prawo o ruchu drogowym** - ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. 2023 poz. 1047 z późn. zm.)..

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach mPrawo Jazdy i Punkty Karne stanowi art. 3 ust. 1 pkt 1-3 Ustawy o aplikacji mObywatel, zgodnie z którą 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 mPrawo Jazdy z danymi z CEK odpowiada Użytkownik, który jest obowiązany do aktualizacji danych, jeżeli dane te uległy zmianie i posiada o nich wiedzę. Zaleca się korzystanie z funkcji aktualizacji danych co najmniej raz na 3 miesiące.
3. Korzystanie z mPrawo Jazdy 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. Dane dostępne w mPrawo Jazdy nie stanowią prawa jazdy ani go nie zastępują.
5. Postanowienia dotyczące zasad przetwarzania danych osobowych zostały zamieszczone w § 11 Regulaminu Aplikacji.

§ 3. mPrawo Jazdy

1. mPrawo Jazdy pozwala na pobranie przez Użytkownika danych osobowych z usługi mObywatel i powiązanych z nimi uprawnień do kierowania pojazdami z bazy CEK oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie.
2. Wiarygodność danych dostępnych w mPrawo Jazdy wynika z faktu, że dane pochodzą z rejestrów państwowych i zostały pobrane przez osobę, która została uwierzytelniona przy użyciu środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego.
3. Do aktywacji i aktualizacji mPrawo Jazdy niezbędne jest posiadanie ważnego Certyfikatu.

§ 4. Użytkownicy

Użytkownikami korzystającymi z mPrawo Jazdy mogą być wyłącznie osoby mające obywatelstwo polskie, które spełniają trzy poniższe warunki:

1) posiadają ważny Certyfikat;
2) mają aktywowaną usługę mObywatel;
3) posiadają uprawnienia do kierowania pojazdami w rozumieniu przepisów Ustawy Prawo o ruchu drogowym.

§ 5. Aktywacja mPrawo Jazdy

1. Aktywacja mPrawo Jazdy polega na:
   1) zalogowaniu do Aplikacji;
   2) wybraniu z listy dostępnych usług „mPrawo Jazdy”;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu;
   4) pobraniu danych Użytkownika oraz danych jego uprawnień do kierowania pojazdami.
2. Ważność mPrawo Jazdy powiązana jest z ważnością Certyfikatu.
3. Certyfikat jest wykorzystywany do:
   1) potwierdzenia tożsamości Użytkownika
   2) podpisania danych w mPrawo Jazdy;
   3) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z CEK;
   4) zapewnienia, iż przekazywane dane w ramach mPrawo Jazdy są tożsame z danymi pobranymi z usługi mObywatel oraz CEK.
4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z CEK niezbędne jest aktywne połączenie internetowe.
5. Użytkownik może aktywować mPrawo Jazdy i pobrać dane wyłącznie na jednym urządzeniu mobilnym.
6. Poza funkcjami prezentacji uprawnień, przekazania w celu skorzystania z usług Instytucji, a także ich weryfikacji uprawnień - mPrawo Jazdy nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w mPrawo Jazdy jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje mPrawo Jazdy

1. Prawidłowo aktywowane mPrawo Jazdy umożliwia Użytkownikowi korzystanie, m. in. z następujących funkcji:
   1) okazanie uprawnień do kierowania pojazdami wraz z powiązanymi z nimi danymi Użytkownika (funkcja „mPrawo Jazdy”);
   2) przekazanie informacji o uprawnieniach do kierowania pojazdami wraz z powiązanymi z nimi danymi Użytkownika (funkcja „Przekaż”);
   3) aktualizacji informacji na temat uprawnień do kierowania pojazdami wraz z powiązanymi z nimi danymi Użytkownika (funkcja „Aktualizuj dane”);
   4) prezentacji Punktów Karnych (funkcja „Punkty karne”);
   5) usunięcia informacji o uprawnieniach do kierowania pojazdami z Aplikacji (funkcja „Odinstaluj usługę”).
2. Użytkownik może okazać innej osobie informacje o uprawnieniach do kierowania pojazdami oraz powiązanych z nimi danych osobowych na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu „mPrawo Jazdy”. Ekran prezentacji danych uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
   1) ruchomego elementu graficznego, prezentującego niebieska flagę z dwunastoma złotymi gwiazdami i skrótem „PL”;
   2) elementu graficznego o zmiennej kolorystyce, uzależnionej od kąta pochylenia urządzenia mobilnego (hologram), w kształcie odpowiadającym Godłu Rzeczypospolitej Polskiej;
   3) elementy grafiki tła o zmiennej kolorystyce i napisach, uzależnionych od kąta pochylenia urządzenia mobilnego (hologram);
   4) elementu graficznego prezentującego aktualną datą i godzinę z dokładnością do zmieniających się sekund;
   5) elementu graficznego prezentującego datę pobrania danych tzw. „Stan na dzień”.

§ 7. Punkty Karne

1. Aktywacja mPrawo Jazdy umożliwia Użytkownikowi dostęp do Punkty Karne.
2. Przy aktywacji mPrawo Jazdy dokonywana jest aktywacja Punktów Karnych. Aktywacja Punktów Karnych wymaga posiadania ważnego Certyfikatu usługi, za pomocą którego dane Użytkownika uwierzytelniane są w CEK.
3. Uwierzytelnienie w CEK umożliwia pobranie z CEK oraz prezentację w Aplikacji informacji, o której mowa w ust. 1.
4. Dezaktywacja Punktów Karnych następuje poprzez dezaktywację mPrawo Jazdy.

Załącznik nr 6 do Regulaminu
Karty Dużej Rodziny (KDR)

§ 1. Definicje:

1. **Certyfikat Ucznia–** poświadczenie, o którym mowa w art. 11 ust. 2 ustawy o aplikacji mObywatel pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika wydany w ramach dokumentu mobilnego- Legitymacja szkolna.
2. **Ustawa o Karcie Dużej Rodziny** – ustawa z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2021. poz. 1741, z późn. zm.).
3. **SI KDR** – system teleinformatyczny umożliwiający obsługę funkcjonalności związanych z kartami elektronicznymi, w szczególności zapewniający funkcjonalność pozwalającą na potwierdzenie uprawnień członków rodzin wielodzietnych oraz zapewniający usługi ułatwiające korzystanie z uprawnień przyznanych na podstawie Karty.
4. **Karta Dużej Rodziny lub Karta –** środek identyfikujący członka rodziny wielodzietnej, poświadczający prawo członka rodziny wielodzietnej do uprawnień ustalonych w trybie określonym w niniejszej ustawie lub przyznanych na podstawie przepisów odrębnych realizowanym m.in. przy użyciu publicznej aplikacji mobilnej, o której mowa w art. 10 Ustawy o Karcie Dużej Rodziny.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach KDR stanowią ustawa o aplikacji mObywatel i art. 10 ust. 1 d-e ustawy o Karcie Dużej Rodziny oraz art. 69 ust. 1 ustawy o aplikacji mObywatel i porozumienia zawartego przez Ministra Cyfryzacji.
2. Za zgodność danych zawartych w KDR odpowiada Użytkownik, który jest obowiązany do aktualizacji danych, jeżeli dane te uległy zmianie i posiada o nich wiedzę. Zaleca się korzystanie z funkcji aktualizacji danych co najmniej raz na 3 miesiące. W przypadku stwierdzenia, że dane znajdujące się na elektronicznej Karcie Dużej Rodziny są nieprawidłowe lub nieaktualne, należy zgłosić się do wójta, burmistrza lub prezydenta miasta w celu przyznania nowej Karty Dużej Rodziny z prawidłowymi danymi.
3. Aplikacja umożliwia pobranie KDR każdemu posiadaczowi Karty, który zaloguje się do aplikacji mObywatel, bez konieczności wnioskowania o nią.

§ 3. KDR

1. KDR pozwala na pobranie przez Użytkownika, danych z bazy SI KDR oraz z Usługi mObywatel oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub przekazywanie.
2. Wiarygodność danych dostępnych w KDR wynika z faktu, że dane pochodzą z rejestrów państwowych i systemu SI KDR i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem Ucznia lub Certyfikatem.
3. Posługiwanie się KDR przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej.
4. Do aktywacji i aktualizacji KDR niezbędne jest posiadanie ważnej Karty Dużej Rodziny oraz ważnego Certyfikatu lub Certyfikatu Ucznia.

§ 4. Użytkownicy

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

1) mają ważny Certyfikat lub Certyfikat Ucznia;
2) posiadają uprawnienia nadane zgodnie z Ustawą o Karcie Dużej Rodziny.

§ 5. Aktywacja KDR

1. Aktywacja KDR polega na:
   1) zalogowaniu do Aplikacji;
   2) wybraniu „KDR" z listy dostępnych usług;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu lub Certyfikatu Ucznia;
   4) pobraniu danych Użytkownika oraz jego uprawnień.
2. Ważność KDR powiązana jest z ważnością Certyfikatu lub Certyfikatu Ucznia.
3. Certyfikat oraz Certyfikat Ucznia są wykorzystywane do:
   1) pobrania i podpisania danych w KDR;
   2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z SI KDR;
   3) zapewnienia, że przekazywane dane w ramach KDR są tożsame z danymi pobranymi z SI KDR oraz usługi mObywatel lub Legitymacji szkolnej.
4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu lub Certyfikatu Ucznia oraz pobrania danych z SI KDR niezbędne jest aktywne połączenie internetowe.
5. Użytkownik posiadający usługę mObywatel może aktywować KDR i pobrać dane z SI KDR wyłącznie na jednym urządzeniu mobilnym. Na jednym urządzeniu mobilnym można aktywować i pobrać dane z SI KDR Użytkownika oraz osób powiązanych z Użytkownikiem.
6. Użytkownik posiadający Legitymację szkolną może aktywować KDR i pobrać dane z SI KDR tylko na jednym urządzeniu mobilnym.
7. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, KDR nie oferuje funkcji eksportu ani importu danych.
8. Dostęp do danych przechowywanych w KDR jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje KDR dla Użytkowników usługi mObywatel

1. Prawidłowo aktywowana usługa KDR umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych Użytkownika KDR oraz kodu QR (widok główny „KDR");
   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 kart osób powiązanych, przez które rozumie się osoby wskazane na wniosku o przyznanie Karty Dużej Rodziny jako członkowie rodziny Użytkownika i zarejestrowane przez wójta, burmistrza lub prezydenta miasta w SI KDR w sposób umożliwiający wyświetlanie przez rodzica/małżonka rodzica Kart członków rodziny (funkcja „Moi bliscy");

5) aktualizacji danych Użytkownika oraz osób powiązanych (funkcja „Aktualizuj”);
6) usunięcie KDR z Aplikacji (funkcja „Usuń KDR”).

2. Użytkownik może okazać innej osobie KDR oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu „KDR”. 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 KDR, 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 aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu.
4. Usunięcie KDR Użytkownika następuje również automatycznie w przypadku dezaktywacji Usługi mObywatel.

§ 7. Funkcje KDR dla Użytkowników Legitymacji szkolnej

1. Prawidłowo aktywowana usługa KDR umożliwia Użytkownikowi korzystanie, m. in. z następujących funkcji:
   1) okazanie danych Użytkownika oraz kodu QR (widok główny „KDR”);
   2) przekazanie danych Użytkownika w celu weryfikacji (funkcja „Przekaż”);
   3) przejście do Legitymacji szkolnej w celu potwierdzenia swoich danych osobowych (funkcja „Legitymacja”);
   4) aktualizacji informacji na temat uprawnień wraz z powiązanymi z nimi danymi Użytkownika (funkcja „Aktualizuj”);
   5) usunięcie KDR z Aplikacji (funkcja „Usuń KDR”).
2. Użytkownik może okazać innej osobie dane KDR oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu „KDR”. 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 KDR, 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 aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu Ucznia.
4. W przypadku dezaktywacji Certyfikatu Ucznia następuje automatyczne usunięcie KDR.

§ 8. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z SI KDR jest Minister Rodziny i Polityki Społecznej. Informacja o przetwarzaniu danych osobowych znajduje się na stronie internetowej Ministerstwa Rodziny i Polityki Społecznej pod adresem: https://www.gov.pl/web/rodzina/informacja-o-przetwarzaniu-danych-osobowych. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
2. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie oraz Certyfikacie Ucznia jest Minister Cyfryzacji, z siedzibą przy ul. Królewskiej 27, 00-060 w Warszawie.
3. Podstawą prawną przetwarzania danych osobowych jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, w związku z art. 2 pkt 2 lit b i art. 10 ust. 1e i 1f ustawy o Karcie Dużej Rodziny. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
4. Podstawa prawna przetwarzania danych osobowych dla Certyfikatu wskazana jest w Regulaminie Aplikacji, zaś dla Certyfikatu Ucznia w Załączniku nr 2.
5. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: Kancelaria.Krolewska@cyfra.gov.pl lub na adres skrytki na ePUAP: /MAiC/SkrytkaESP.
6. Administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować we wszystkich sprawach związanych z przetwarzaniem danych osobowych: korespondencyjnie na adres: ul. Królewska 27, 00-060 Warszawa, bądź mailowo na adres: iod@mc.gov.pl.
7. Administratorem danych osobowych uczniów, którym wydano Legitymację szkolną jest szkoła. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
8. We wszelkich sprawach dotyczących przetwarzania danych osobowych należy kontaktować się z właściwą szkołą lub właściwym Inspektorem Ochrony Danych.
9. W ramach usługi KDR w Aplikacji przechowuje się następujące dane Użytkownika:
   1) imię pierwsze posiadacza Karty oraz osób powiązanych;
   2) imię drugie posiadacza Karty oraz osób powiązanych;
   3) nazwisko posiadacza Karty oraz osób powiązanych;
   4) numer PESEL posiadacza Karty oraz osób powiązanych;
   5) wizerunek twarzy posiadacza Karty;
   6) numer karty posiadacza Karty oraz osób powiązanych;
   7) informacja na temat certyfikatu użytego do wydania danych;
   8) numer dokumentu tożsamości posiadacza Karty oraz osób powiązanych;
10. Osobie, której dane są przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 ustawy o aplikacji mObywatel, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych,:
    1) prawo dostępu do treści danych;
    2) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);

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.

11. Minister gromadzi dane statystyczne dotyczące KDR w zakresie liczby:
    1) aktywacji KDR;
    2) aktualizacji danych i wydania Certyfikatów;
    3) zgłoszonych utrat telefonów;
    4) zgłoszonych problemów.
12. Dane, o których w ust. 9, są przetwarzane wyłącznie w trakcie korzystania z funkcji wymienionych w Regulaminie. Dane, o których mowa w tym ustępie przechowywane są przez okres 6 lat od dnia ostatniej aktywności Użytkownika w systemie teleinformatycznym Aplikacji (art. 20 ust. 3 pkt. 1 ustawy o aplikacji mObywatel). Minister nie gromadzi informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych.
13. Dane osobowe, przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 ustawy o aplikacji mObywatel, nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
14. Dane osobowe, o których mowa w ust. 9, będą również przetwarzane 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 jako odpowiednio:
        a) podmiot przetwarzający dane osobowe,
        b) dalszy podmiot przetwarzający dane osobowe.
15. 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 7 do Regulaminu

Usługa Unijny Certyfikat COVID

Usługa Unijny Certyfikat COVID umożliwia prezentację potwierdzenia dokonania szczepienia przeciwko wirusowi SARS-CoV-2 i/lub uzyskania wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przejściu choroby COVID-19.

§ 1. Definicje:

1. **Ustawa o systemie informacji** – ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2022 r. poz. 1555, z późn. zm)),
2. **CEZ –** Centrum e-Zdrowia (CeZ) – państwowa jednostka budżetowa powołana przez Ministra Zdrowia, której głównym przedmiotem działalności jest realizacja zadań z zakresu budowy społeczeństwa informacyjnego, obejmujących organizację i ochronę

zdrowia oraz wspomaganie decyzji zarządczych ministra właściwego do spraw zdrowia na podstawie prowadzonych analiz.

3. **SI CEZ** – system informatyczny Centrum e-Zdrowia, zapewniający dostęp do danych niezbędnych do realizacji usługi **U**nijny **C**ertyfikat **C**OVID.
4. **Internetowe Konto Pacjenta (IKP)** – moduł systemu, o którym mowa w art. 7 ust. 1 Ustawy o systemie informacji w ochronie zdrowia, w którym są przetwarzane dane dotyczące usługobiorcy zawarte w Systemie Informacji Medycznej oraz Systemie Rejestru Usług Medycznych Narodowego Funduszu Zdrowia.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych z IKP, w tym w ramach usługi Unijny Certyfikat COVID stanowią:
   1) art. 3 ust. 1 pkt 1 ustawy o aplikacji mObywatel;
   2) art. 7b ust. 1a i 1b ustawy o systemie informacji;
2. Za zgodność i aktualność danych zawartych w usłudze Unijny Certyfikat COVID odpowiada Użytkownik, który jest obowiązany do ich aktualizacji. Konieczne jest aktualizowanie danych (kodu QR) po upływie terminu jego ważności w celu pobrania aktualnego zaświadczenia.
3. Korzystanie z usługi Unijny Certyfikat COVID 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 mObywatel umożliwia pobranie usługi Unijny Certyfikat COVID każdemu zaszczepionemu i/lub każdemu kto uzyskał ujemny wynik testu i/lub przebył chorobę COVID-19, użytkownikowi Aplikacji, posiadającemu aktywną usługę Diia.pl lub usługę mObywatel, który zaloguje się do Aplikacji.

§ 3. Usługa Unijny Certyfikat COVID

1. Usługa Unijny Certyfikat COVID pozwala na pobranie przez Użytkownika danych osobowych z Usługi Diia.pl albo Usługi mObywatel, pochodzących z IKP oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub przekazywanie.
2. Usługa Unijny Certyfikat COVID umożliwia pobranie przez Użytkownika Unijnych Certyfikatów COVID użytkownika oraz osób niepełnoletnich, których Użytkownik jest przedstawicielem ustawowym. Lista certyfikatów z zakładki „Dzieci" uwzględnia wyłącznie niepełnoletnich przypisanych do ubezpieczenia zdrowotnego Użytkownika Aplikacji.
3. Wiarygodność danych dostępnych w usłudze Unijny Certyfikat COVID wynika z faktu, że dane pochodzą z rejestrów państwowych i IKP i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
4. Do aktywacji i aktualizacji Usługi Unijny Certyfikat COVID niezbędne jest posiadanie w SI CEZ/IKP informacji o dokonaniu przez Użytkownika szczepienia przeciwko wirusowi SARS-CoV-2 i/lub informacji o uzyskanym ujemny wynik testu i/lub informacji o przebyciu choroby COVID-19 oraz posiadanie ważnej Usługi Diia.pl albo Usługi mObywatel.

§ 4. Użytkownicy

1. Użytkownikami korzystającymi z usługi Unijny Certyfikat COVID mogą być wyłącznie:
   1) osoby, mające obywatelstwo polskie i spełniają poniższe warunek:
      a) mają aktywowaną Usługę mObywatel;
      b) posiadają w SI CEZ/IKP informację o dokonaniu szczepienia przeciwko wirusowi SARS-CoV-2, i/lub informację o uzyskaniu ujemnego wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przejściu choroby COVID-19

   albo
   2) spełniają łączenie poniższe warunki:
      a) maja aktywną usługę Diia.pl;
      b) posiadają w SI CEZ/IKP informację o dokonaniu szczepienia przeciwko wirusowi SARS-CoV-2, i/lub informację o uzyskaniu ujemnego wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przejściu choroby COVID-19.

§ 5. Aktywacja usługi Unijny Certyfikat COVID

1. Aktywacja usługi Unijny Certyfikat COVID w systemie Aplikacji polega na:
   1) zalogowaniu do Aplikacji;
   2) naciśnięciu „Dodaj dokument”;
   3) wybraniu Unijny Certyfikat COVID (system automatycznie sprawdza czy Użytkownik posiada aktywną Usługę Diia.pl albo mDowód, w przypadku braku jednej z tych usług, Użytkownik będzie mógł aktywować brakującą Usługę). Brak aktywnej Usługi Diia.pl albo mDowód uniemożliwia korzystanie z Usługi Unijny Certyfikat COVID;
   4) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu;
   5) pobraniu z systemu mObywatel i SI CEZ/IKP danych dotyczących Użytkownika i danych dodatkowych dotyczących szczepienia i/lub wyniku ujemnego testu i/lub przybyciu choroby COVID-19 oraz odpowiedniego kodu QR.
2. Ważność Unijnego Certyfikatu COVID powiązana jest z ważnością Certyfikatu lub ważnością zaświadczenia o szczepieniu i/lub ważnością wyniku testu na obecność wirusa SARS-Cov-2 i/lub ważnością informacji o przejściu choroby COVID-19. W Usłudze Unijny Certyfikat COVID status ważności dokumentu będzie uzależniony od daty i czasu ważności UCC przekazanej z SI CEZ/IKP, a jej przekroczenie będzie sygnalizowane graficznie wewnątrz Usługi wraz z możliwością zaktualizowania danych.
3. Certyfikat jest wykorzystywany do:
   1) pobrania i podpisania danych w usłudze Unijny Certyfikat COVID;
   2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z IKP;
   3) zapewnienia, że przekazywane dane w ramach usług Unijny Certyfikat COVID są tożsame z danymi pobranymi z IKP oraz usługi mObywatel lub usługi Diia.pl.
4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z IKP niezbędne jest aktywne połączenie internetowe.
5. Użytkownik posiadający mDowód lub usługę Diia.pl może aktywować usługę Unijny Certyfikat COVID i pobrać dane z IKP wyłącznie na jednym urządzeniu mobilnym.
6. Poza funkcją prezentacji uprawnień oraz funkcją aktualizacji danych, usługa Unijny Certyfikat COVID nie oferuje funkcji eksportu ani importu danych.

7. Dostęp do danych przechowywanych w usłudze Unijny Certyfikat COVID jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje usługi Unijny Certyfikat COVID

1. Prawidłowo aktywowana usługa Unijny Certyfikat COVID umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie kodu/kodów QR zawierających dane przekazane z IKP;
   2) pobranie i okazanie kodu/kodów QR użytkownika oraz niepełnoletnich, których Użytkownik jest przedstawicielem ustawowym;
   3) przejście do mDowód albo usługi Diia.pl w celu potwierdzenia swoich danych osobowych; pobranie kodu QR potwierdzającego odbycie szczepienia wraz z datą jego ważności i uzyskania wyniku testu na obecność wirusa SARS-Cov-2 i informacji o przebytej chorobie COVID-19;
   4) zmianę języka z polskiego na angielski i odwrotnie albo zmianę języka z ukraińskiego na język angielski i odwrotnie;
   5) dodanie do aplikacji Apple (Portfela i Zdrowia) dostarczanej przez Apple Inc. - dostępna dla Użytkownika posiadającego Aplikację zainstalowaną na urządzeniu mobilnym typu smartfon z systemem iOS;
   6) usunięcie usługi Unijny Certyfikat COVID z Aplikacji.
2. Użytkownik może okazać innej osobie potwierdzenie dokonania szczepienia przeciwko wirusowi SARS-CoV-2 i/lub uzyskania wyniku testu na obecność wirusa SARS-Cov-2 i/lub informacji o przebytej chorobie COVID-19, na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu Unijny Certyfikat COVID.
3. Ważność kodu/kodów QR może być zweryfikowana poprzez funkcję „Przekaż".
4. Dodanie UCC do Apple (Portfela i Zdrowia) w aplikacji Portfel Apple wymaga wyrażenia zgody przez Użytkownika i akceptację ryzyka ewentualnego naruszenia prywatności w związku z możliwym przekazywaniem danych osobowych poza Europejski Obszar Gospodarczy, z czym wiąże się brak standardów ochrony danych osobowych wynikających z RODO.[1]
5. Usunięcie usługi Unijny Certyfikat COVID następuje również automatycznie w przypadku dezaktywacji usługi mObywatel albo usługi Diia.pl.

§ 7. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z IKP jest Minister Zdrowia. Informacja o przetwarzaniu danych osobowych znajduje się na stronie internetowej Ministerstwa Zdrowia pod adresem: https://www.gov.pl/web/zdrowie/dane-osobowe. Z administratorem danych można się kontaktować pod adresem: Ministerstwo Zdrowia, ul. Miodowa 15, 00-952 Warszawa lub elektronicznie, na adres: kancelaria@mz.gov.pl lub na adres skrytki ePUAP: /8tk37sxx6h/SkrytkaESP. Administrator wyznaczył Inspektora Ochrony Danych, z którym

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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, oraz Dz. Urz. UE L 127 z 23.05.2018 str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35).

można się kontaktować sprawach związanych z przetwarzaniem danych osobowych przez Ministra Zdrowia bezpośrednio pod adresem: iod@mz.gov.pl. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.

2. Administratorem danych osobowych Użytkownika pobieranych z usługi mObywatel albo usługi Diia.pl jest Minister właściwy do spraw informatyzacji, mający swą siedzibę 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. Podstawą przetwarzania danych osobowych w systemie teleinformatycznym obsługującym usługę Unijny Certyfikat COVID jest art. 6 ust 1 lit. e w związku z art. 7b ust. 1 a i 1 b ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2022 r. poz. 1555). Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
5. Podstawa prawna przetwarzania danych osobowych dla Certyfikatu wskazana jest w Regulaminie Aplikacji, zaś dla Certyfikatu Ucznia w Załączniku nr 2.
6. Usługa Unijny Certyfikat COVID przechowuje następujące dane Użytkownika lub osób niepełnoletnich, których Użytkownik jest przedstawicielem ustawowym:
   1) Dane zawarte w certyfikacie potwierdzającym szczepienie ochronne przeciw COVID-19:
   1) nazwisko (-a) i imię (imiona),
   2) data urodzenia,
   3) choroba lub czynnik chorobotwórczy: COVID-19 (co oznacza również SARS-CoV-2 lub jeden z jego wariantów),
   4) szczepionka / profilaktyka,
   5) szczepionkowy produkt leczniczy,
   6) posiadacz pozwolenia na dopuszczenie do obrotu lub wytwórca szczepionki,
   7) liczba w serii szczepień / dawek i całkowita liczba dawek w serii,
   8) data szczepienia, wskazująca datę ostatniej otrzymanej dawki,
   9) państwo członkowskie szczepienia,
   10) wystawca certyfikatu,
   11) niepowtarzalny identyfikator certyfikatu;
7. Dane zawarte w certyfikacje zawierającym wynik testu na obecność wirusa SARS-Cov-2:
   a) nazwisko (-a) i imię (imiona),
   b) data urodzenia,
   c) choroba lub czynnik chorobotwórczy: COVID-19 (co oznacza również SARS-CoV-2 lub jeden z jego wariantów),
   d) rodzaj testu,
   e) nazwa testu (opcjonalnie w przypadku testu NAAT),
   f) producent testu (nieobowiązkowo w przypadku testu NAAT),
   g) data i godzina pobrania próbki do badań,
   h) wynik testu,

i) ośrodek testowy lub placówka (nieobowiązkowe w przypadku szybkiego testu antygenowego),
j) państwo członkowskie, w którym wykonano test,
k) wystawca certyfikatu,
l) niepowtarzalny identyfikator certyfikatu;
   a. dane zawarte w potwierdzeniu przebycia choroby COVID-19:
   a) nazwisko (-a) i imię (imiona),
   b) data urodzenia,
   c) choroba lub czynnik chorobotwórczy, z którego Użytkownik wyzdrowiał: COVID-19 (czyli również SARS-CoV-2 lub jeden z jego wariantów),
   d) data pierwszego pozytywnego wyniku testu NAAT,
   e) państwo członkowskie, w którym wykonano test,
   f) wystawca certyfikatu,
   g) data od kiedy certyfikat jest ważny,
   h) data ważności certyfikatu (nie więcej niż 180 dni od daty pierwszego pozytywnego wyniku testu),
   i) niepowtarzalny identyfikator certyfikatu;

7. Osobie, której dane są przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 ustawy o aplikacji mObywatel przysługuje w dowolnym momencie – prawo do:
   1) uzyskania dostępu do swoich danych osobowych;
   2) żądania sprostowania swoich danych osobowych;
   3) wniesienia sprzeciwu wobec przetwarzania jego/jej danych osobowych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   4) żądania ograniczenia przetwarzania danych osobowych;
   5) prawo do wniesienia skargi do organu nadzorczego. Organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
8. Minister gromadzi dane statystyczne dotyczące usługi w zakresie liczby:
   1) aktywacji usługi Unijny Certyfikat COVID;
   2) akcji aktualizacji danych i wydania Certyfikatów;
   3) zgłoszonych utrat telefonów;
   4) zgłoszonych problemów.
9. Dane, o których w ust. 4 pkt 1-3 są przetwarzane wyłącznie w trakcie korzystania z usługi Unijny Certyfikat COVID, w celu dostarczenia Użytkownikom usługi umożliwiającej prezentację danych z IKP oraz zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
10. Dane, przechowywane są przez okres 6 lat od dnia ostatniej aktywności Użytkownika w systemie teleinformatycznym Aplikacji ((art. 20 ust. 1 pkt. 3 ustawy o aplikacji mObywatel).). Dane nie są przetwarzane w celach marketingowych.
11. Dane osobowe, przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 ustawy o aplikacji mObywatel, nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
12. Dane osobowe, , będą również przetwarzane przez:

13. Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa 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 8 do Regulaminu
Usługa Legitymacji Ulgowych Usług Transportowych

§ 1. Definicje:

1. **Certyfikat** – o którym mowa w art. 2 pkt 2 ustawy o aplikacji mObywatel – certyfikat użytkownika aplikacji mObywatel wydawany z dokumentem mObywatel, zgodnie z Art. 10. ust 2 ustawy o aplikacji mObywatel, użytkownikowi aplikacji automatycznie z Profilem mObywatel zgodnie z Art. 14 ust 1 ustawy o aplikacji mObywatel.
2. **Certyfikat Ucznia** – poświadczenie, o którym mowa w art. 11 ust. 2 ustawy o aplikacji mObywatel pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika wydany w ramach dokumentu mobilnego- Legitymacja 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 pożn. 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 Legitymacji UUT.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach Legitymacji UUT stanowi art. 19 ust. 1 ustawy o aplikacji mObywatel, 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 Legitymacji 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 Legitymacji UUT są nieprawidłowe lub nieaktualne, należy zgłosić się do Pracodawcy.
3. Korzystanie z Legitymacji 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 Legitymacji UUT posiadaczowi Legitymacji UUT, wskazanemu w Zasadach odprawy UUT i który zaloguje się do Aplikacji, bez konieczności wnioskowania o nią.

§ 3. Legitymacja UUT

1. Legitymacja 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 Legitymacji UUT pochodzą z Systemu UUT i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
3. Do aktywacji i aktualizacji Legitymacji UUT niezbędne jest posiadanie ważnej Legitymacji UUT oraz ważnego Certyfikatu.

§ 4. Użytkownicy

Użytkownikami korzystającymi z Legitymacji 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 Legitymacja UUT

1. Aktywacja Legitymacji UUT w Aplikacji polega na:
   1) zalogowaniu do Aplikacji;
   2) wybraniu „Legitymacja UUT” z listy dostępnych usług;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu lub Certyfikatu Ucznia;
   4) pobraniu danych Użytkownika oraz jego uprawnień.
2. Ważność Legitymacji UUT powiązana jest z ważnością Certyfikatu lub Certyfikatu Ucznia.
3. Certyfikat oraz Certyfikat Ucznia są wykorzystywane do:
   1) pobrania i podpisania danych w Legitymacji UUT;
   2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z Systemu UUT;
   3) zapewnienia, że przekazywane dane w ramach Legitymacji UUT są tożsame z danymi pobranymi z Systemu UUT oraz usługi mObywatel lub Legitymacji 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 Legitymację UUT i pobrać dane z Systemu UUT wyłącznie na jednym urządzeniu mobilnym. Na jednym urządzeniu mobilnym można aktywować i pobrać dane z Systemu UUT Użytkownika oraz osób powiązanych z Użytkownikiem.
6. Użytkownik posiadający Legitymację szkolną może aktywować Legitymację UUT i pobrać dane z Systemu UUT tylko na jednym urządzeniu mobilnym.
7. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Legitymacja UUT nie oferuje funkcji eksportu ani importu danych.
8. Dostęp do danych przechowywanych w Legitymacji UUT jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje Legitymacja UUT dla Użytkowników usługi mObywatel

1. Prawidłowo aktywowana usługa Legitymacja UUT umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych Użytkownika, o których mowa w § 8 ust. 3, oraz kodu QR (widok główny „Legitymacja 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 Legitymacji UUT z Aplikacji (funkcja „Usuń Legitymację UUT”).
2. Użytkownik może okazać innej osobie Legitymację UUT oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu usługi Legitymacja 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 Legitymacja 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 aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu.
4. Usunięcie Legitymacji UUT Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

§ 7. Funkcje Legitymacji UUT dla Użytkowników Legitymacji szkolnej

1. Prawidłowo aktywowana usługa Legitymacja UUT umożliwia Użytkownikowi korzystanie, m.in.
   z następujących funkcji:
   1) okazanie danych Użytkownika oraz kodu QR (widok główny „Legitymacja UUT”);
   2) przekazanie danych Użytkownika w celu weryfikacji (funkcja „Potwierdź swoje dane”);
   3) przejście do Legitymacji szkolnej w celu potwierdzenia swoich danych osobowych (funkcja „Legitymacja”);
   4) aktualizowanie informacji na temat uprawnień wraz z powiązanymi z nimi danymi Użytkownika (funkcja „Aktualizuj”);
   5) usunięcie Legitymacji UUT z Aplikacji (funkcja „Usuń Legitymację UUT”).
2. Użytkownik może okazać innej osobie dane Legitymacji UUT oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu „Legitymacja 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 Legitymacji 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 aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu Ucznia.
4. W przypadku dezaktywacji Certyfikatu Ucznia następuje automatyczne usunięcie Legitymacja UUT.

§ 8. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z Systemu UUT jest Pracodawca. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
   2. Administratorem danych osobowych Użytkownika pobieranych z usługi mObywatel albo usługi Diia.pl jest Minister właściwy do spraw informatyzacji, tj. Minister Cyfryzacji, którego urzędem obsługującym jest Ministerstwo Cyfryzacji z mający swą siedzibę 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 właściwego do spraw informatyzacji (Ministra Cyfryzacji) bezpośrednio pod adresem: iod@mc.gov.pl.
3. Administratorem danych osobowych uczniów, którym wydano Legitymację szkolną jest Szkoła. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.

4. Podstawą przetwarzania danych osobowych dla Certyfikatu Studenta przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, w związku z art. 69 ust. 1 ustawy o aplikacji mObywatel. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
5. Podstawa prawna przetwarzania danych osobowych dla Certyfikatu wskazana jest w Regulaminie Aplikacji, zaś dla Certyfikatu Ucznia w Załączniku nr 2.
6. W ramach usługi Legitymacja UUT w Aplikacji przechowuje się następujące dane:
   1) Zdjęcie;
   2) Imię (Imiona));
   3) Nazwisko;
   4) Seria;
   5) Numer;
   6) Typ relacji do karty;
   7) Typ posiadacza;
   8) Numer PESEL posiadacza UUT;
   9) Pracodawca;
   10) Kategoria OU;
   11) Klasa;
   12) Adnotacja;
   13) Informacja o dodatkowej uldze;
   14) Status;
   15) Kod pracodawcy;
   16) Ważny od;
   17) Ważny do;
   18) Obraz PNG kodu QR pobrany z CS PKP.
7. Osobie, której dane są przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 ustawy o aplikacji mObywatel, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych:
   1) prawo dostępu do treści danych;
   2) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   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.
8. Minister gromadzi dane statystyczne dotyczące Legitymacji UUT w zakresie liczby:
   1) aktywacji Legitymacji UUT;
   2) akcji aktualizacji danych i wydania Certyfikatów;
   3) zgłoszonych utrat telefonów;
   4) zgłoszonych problemów.

9. Dane, o których mowa w ust. 9 są przetwarzane wyłącznie w trakcie korzystania z Legitymacji UUT i w celu dostarczenia obywatelom usługi umożliwiającej prezentację danych z systemu UUT oraz zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
10. Dane, o których mowa w ust. 9 przechowywane są do roku od dnia utraty Legitymacji UUT. Dane nie są przetwarzane w celach marketingowych.
11. Minister nie gromadzi informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych.
12. Dane osobowe, przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 ustawy o aplikacji mObywatel, nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
13. Dane osobowe, o których mowa w ust. 9, będą również przetwarzane przez:
    1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa jako odpowiednio:
    2) Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa.

        1) podmiot przetwarzający dane osobowe,
        2) dalszy podmiot przetwarzający dane osobowe.
14. 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

§ 1. 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. w art. 4 ust. 4 pkt 1-15 oraz art. 6 ust. 5 pkt 2 i 3 ustawy o pomocy obywatelom Ukrainy oraz art. 8 pkt 24 i 24a lit. d Ustawy o ewidencji ludności.
1. 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.
2. Postanowienia dotyczące zasad przetwarzania danych osobowych zostały zamieszczone w § 11 Regulaminu Aplikacji

§ 2. Usługa Diia.pl

1. Usługa Diia.pl pozwala na pobranie danych osobowych i wizerunku Użytkownika (i jego podopiecznych) na podstawie art. 10 ust. 1 i ust. 1a Ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa. 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 w aplikacji mObywatel. Dane te są przechowywane i przesyłane za pomocą Aplikacji.

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, stwierdzających 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 30 dni (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. Do aktywacji i aktualizacji Diia.pl niezbędne jest posiadanie Profilu mObywatel.

§ 3. 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.

§ 4. Aktywacja Usługi

1. Przy pierwszym użyciu Diia.pl dokonywana jest aktywacja Usługi.
2. Usługa Diia.pl dla podopiecznych będzie możliwa do aktywacji wyłącznie wtedy, gdy w rejestrze PESEL przy danych dziecka zamieszczono numer PESEL opiekuna dziecka i Opiekun złożył oświadczenia o pozostawaniu dziecka pod jego władzą rodzicielską.

3. Składający oświadczenie zamieszcza w nim klauzulę następującej treści: ,,Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia."
4. Uwierzytelnienia przy użyciu certyfikatu podstawowego. Certyfikat wydawany jest z dokumentem mObywatel, zgodnie z art. 10 ust. 2 Ustawy o aplikacji mObywatel, użytkownikowi aplikacji automatycznie z Profilem mObywatel zgodnie z art. 14 ust. 1 ustawy o aplikacji mObywatel.
5. Aktywacja usługi Diia.pl przez Użytkownika polega na:
   1) zalogowaniu do Aplikacji;
   2) potwierdzeniu tożsamości Użytkownika przy użyciu Profilu mObywatel.
6. Po wykonaniu czynności opisanych w ust. 2, nastąpi automatyczne pobranie danych Użytkownika z Rejestru oraz zaszyfrowanie i zapisanie ich w urządzeniu mobilnym Użytkownika.
7. Brak akceptacji Regulaminu przez Użytkownika uniemożliwia aktywację Diia.pl.
8. 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.
9. Ważność Diia.pl powiązana jest z ważnością Certyfikatu.
10. Certyfikat jest wykorzystywany do:
    1) potwierdzenia tożsamości Użytkownika;
    2) podpisania danych w Diia.pl;
    3) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym Diia.pl
    4) zapewnienia, iż przekazywane dane w ramach Diia.pl są tożsame Rejestrem PESEL i Rejestrem Danych Kontaktowych.
11. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z rejestrów państwowych niezbędne jest aktywne połączenie internetowe.
12. Użytkownik może aktywować usługę Diia.pl, wyłącznie na jednym urządzeniu.
13. Poza funkcjami prezentacji uprawnień, przekazania w celu skorzystania z usługDiia.pl nie oferuje funkcji eksportu ani importu danych.
14. Dostęp do danych przechowywanych w Diia.pl jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 5. Funkcje usługi Diia.pl

1. Prawidłowo aktywowana usługa Diia.pl umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) Pobranie i okazanie danych użytkownika i jego dzieci
   2) uruchomienie usług:
      a) UCC
      b) e-Recpta
   3) przekazania danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);

4) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
5) usunięcie Usługi Diia.pl z Aplikacji (funkcja „Usuń Usługę Diia.pl”).

1. Użytkownik może okazać innej osobie Diia.pl swoje dane i powiązanych osób (sekcja Dzieci). Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu Usługi Diia.pl. Ekran prezentacji danych uwierzytelniają elementy zabezpieczeń wizualnych w postaci:
2. hologramu stanowiącego wizerunek orła ustalony jak dla godła Rzeczypospolitej Polskiej, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
3. ruchomego elementu graficznego prezentującego biało-czerwoną flagę Rzeczypospolitej Polskiej;
4. gilosza umieszczonego jako tło Diia.pl, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
5. zegara mierzącego aktualny czas liczony w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z upływem czasu.
6. Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
7. Usunięcie usługi Legitymacja poselska Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

Załącznik nr 10 do Regulaminu

Legitymacja emeryta-rencisty

§ 1. Definicje:

1. **Legitymacja emeryta-rencisty –** dokument wydany przez terenową jednostkę organizacyjną Zakładu Ubezpieczeń Społecznych właściwą w sprawach wydawania decyzji dotyczących świadczeń lub ich wypłaty. Legitymacja emeryta-rencisty jest wydawana w formie:
   1) Spersonalizowanej karty identyfikacyjnej wykonanej z tworzywa sztucznego, zwanej dalej „legitymacją”;
   2) Dokumentu elektronicznego przechowywanego i okazywanego przy użyciu aplikacji mobilnej mObywatel, o której mowa w art. 3 ust. 1 Ustawy o aplikacji mObywatel.
2. **Minister Rodziny i Polityki Społecznej** – minister właściwy do określenia wzoru legitymacji emeryta-rencisty w drodze rozporządzenia wydanego na podstawie art. 68 ust. 4 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 20222023 r. poz. 1230).
3. **Rejestr Zakładu Ubezpieczeń Społecznych (Rejestr ZUS)** – rejestr przechowujący dane Użytkowników posiadających ważną legitymację emeryta lub rencisty.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych mobilnej Legitymacji stanowi art. 3 ustawy o aplikacji mObywatel, 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 oraz § 3 ust. 1 pkt 2 rozporządzenia Ministra Rodziny i Polityki Społecznej z dnia 3 marca 2022 w sprawie legitymacji emeryta-rencisty, zgodnie z którym mobilna Legitymacja wydawana jest przez udostępnienie danych umożliwiające ich pobranie w ramach usługi pozwalającej na obsługę mobilnej Legitymacji przy użyciu publicznej aplikacji mobilnej.
2. Za zgodność danych zawartych w usłudze Legitymacja emeryta-rencisty 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 w Legitymacja, są nieprawidłowe lub nieaktualne, należy zgłosić się do Zakładu Ubezpieczeń Społecznych.
3. Korzystanie z mobilnej Legitymacji emeryta-rencisty 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 Legitymacji posiadaczowi, której dane znajdują się w Rejestrze ZUS. Pobranie mobilnej Legitymacji możliwe jest bez konieczności wnioskowania o nią oraz po zalogowaniu się do Aplikacji.
5. Instalacja dostarczanych cyklicznie przez Ministra aktualizacji Aplikacji jest konieczna dla jej prawidłowego działania i należytego zabezpieczenia zawartych w niej danych. Instalowanie takich aktualizacji powinno nastąpić niezwłocznie po ich udostępnieniu za pomocą sklepów z aplikacjami.

§ 3. Legitymacja emeryta-rencisty

1. Legitymacja emeryta-rencisty pozwala na pobranie przez Użytkownika danych z bazy Rejestru ZUS oraz z usługi mObywatel oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub przekazywanie.
2. Dane dostępne w usłudze mobilnej Legitymacji pochodzą z Rejestru ZUS oraz Usługi mObywatel i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem Podstawowym.
3. Posługiwanie się mobilną Legitymacją przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej.
4. Do aktywacji i aktualizacji Legitymacji emeryta-rencisty niezbędne jest posiadanie ważnego Certyfikatu Podstawowego.

§ 4. Użytkownicy

1. Użytkownikami korzystającymi z Legitymacji mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
   1) mają ważny Certyfikat podstawowy;
   2) posiadają ważną decyzję ZUS o przyznaniu lub zawiadomienie o podjęciu wypłaty emerytury lub renty.

§ 5. Aktywacja usługi Legitymacja emeryta - rencisty

1. Aktywacja usługi Legitymacja emeryta-rencisty w Aplikacji polega na:
   1) uruchomieniu aplikacji mObywatel i zalogowaniu się do niej;
   2) wybraniu „Legitymacja emeryta-rencisty" z listy dostępnych usług;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
   4) pobraniu danych Użytkownika oraz jego uprawnień.
2. Ważność Legitymacji powiązana jest z ważnością Certyfikatu.
3. Certyfikat podstawowy jest wykorzystywany do:
   1) pobrania i podpisania danych w mobilnej Legitymacji emeryta-rencisty;
   2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z rejestru ZUS;
   3) zapewnienia, że przekazywane dane w ramach usługi Legitymacja są tożsame z danymi pobranymi z Rejestru ZUS oraz usługi mObywatel.
   4) Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z Rejestru ZUS niezbędne jest aktywne połączenie internetowe.
4. Użytkownik może aktywować Mobilną Legitymację emeryta-rencisty i pobrać dane z Rejestru ZUS wyłącznie na jednym urządzeniu.
5. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Mobilna Legitymacja emeryta-rencisty nie oferuje funkcji eksportu ani importu danych.
6. Dostęp do danych przechowywanych w mobilnej Legitymacji jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje mobilnej Legitymacji emeryta - rencisty

1. Prawidłowo aktywowana usługa Legitymacja emeryta-rencisty umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych Użytkownika, o których mowa w § 7 ust. 7;
   2) przekazania danych Użytkownika w celu weryfikacji (funkcja „Przekaż");
   3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj");
   4) usunięcie mobilnej Legitymacji emeryta-rencisty z Aplikacji (funkcja „Usuń Legitymację emeryta-rencisty").
2. Użytkownik może okazać innej osobie mobilną Legitymację emeryta-rencisty. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu Legitymacji . 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) ruchomego elementu graficznego prezentującego biało-czerwoną flagę Rzeczypospolitej Polskiej;
3) gilosza umieszczonego jako tło mobilnej Legitymacja emeryta-rencisty, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
4) zegara mierzącego aktualny czas liczony w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z upływem czasu.

3. Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
4. usunięcie Legitymacji emeryta rencisty z Aplikacji (sekcja ”Dokumenty”, następnie ikona edycji i wybranie ikony „kosz”).

§ 7. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z Rejestru ZUS, o których mowa w ust. 7 jest ZUS, z siedzibą przy ul. Szamocka 3/5, 01-748, Warszawa. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
2. Wyżej wymieniony Administrator powołał Inspektora Ochrony Danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych korespondencyjnie na adres: Inspektor Ochrony Danych, Zakład Ubezpieczeń Społecznych, ul. Szamocka 3, 5, 01-748 Warszawa, bądź na adres e-mail: ODO@zus.pl.
3. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie podstawowym jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą mający swą siedzibę w Warszawie, przy ul. Królewskiej 27.
4. 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.
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym -– w sprawach związanych z przetwarzaniem danych osobowych -– można kontaktować się mailowo: iod@mc.gov.pl.
6. Podstawą przetwarzania danych osobowych dla Certyfikatu przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e RODO, w związku z art. 69 ust. 1 ustawy o aplikacji mObywatel w związku z zawartym przez Ministra Cyfryzacji porozumieniem. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach mobilnej Legitymacji emeryta-rencisty w Aplikacji przechowuje się następujące dane:
   1) imię (imiona) Użytkownika mobilnej Legitymacji;

2) nazwisko Użytkownika;
3) numer PESEL Użytkownika;
4) numer Legitymacji;
5) wizerunek twarzy Użytkownika;
6) rodzaj świadczenia;
7) termin ważności mobilnej Legitymacji;
8) Oznaczenie organu rentowego, który wydał mobilną Legitymację.

8. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych osobowych:

   1) prawo dostępu do treści danych;

   2) prawo ich poprawiania i sprostowania;

   3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);

   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.

2. 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 albo na podstawie akceptacji przekazania danych osobowych do Instytucji.

3. 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.

4. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Potwierdź swoje dane”) do systemu teleinformatycznego Instytucji, Aplikacja przesyła wybrane dane osobowe, które są niezbędne do realizacji usługi oferowanej przez daną Instytucję. Zestaw danych jest uzależniony od oferowanej przez Instytucję usługi.

5. W celu utworzenia Certyfikatu podczas aktywacji dokumentu mDowód oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister właściwy do spraw informatyzacji przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.

6. Minister właściwy do spraw informatyzacji przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.

    9) Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.

    10) Zgodnie z art. 20 ust. 3 pkt 1 ustawy o aplikacji mObywatel Minister właściwy do spraw informatyzacji przetwarza dane osobowe użytkowników aplikacji mObywatel przez okres :

7. 6 lat od dnia upływu ważności albo dnia unieważnienia certyfikatu użytkownika w przypadku danych, które są przetwarzane w systemie mObywatel.;

8. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu mDowód, danych o połączeniach między nimi ani danych o Użytkownikach w związku z korzystaniem z funkcji weryfikacji online w mWeryfikatorze.

9. Minister nie gromadzi również informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych. Historia działań Użytkownika zapisywana jest w jego urządzeniu mobilnym.

10. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:

    1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,

11. 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.

12. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 11 do Regulaminu

Legitymacja adwokacka

§ 1. Definicje:

1. **KRAiAA -** Krajowy Rejestr Adwokatów i Aplikantów Adwokackich, rejestr prowadzony

przez NRA, przechowujący dane wszystkich członków palestry: adwokatów, aplikantów adwokackich oraz adwokatów niewykonujących zawodu.

2. **Legitymacja adwokacka** – dokument wydany przez okręgową radę adwokacką na podstawie Ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz.U. 2022 poz. 1184) oraz uchwały nr 75/2010 Prezydium NRA z dnia 5 października 2010 roku w sprawie legitymacji adwokackich, o którym mowa w art. 3 ust. 1 ustawy o aplikacji mObywatel, dostępna na urządzeniu mobilnym Użytkownika w Aplikacji, której wykorzystywanie odbywa się na warunkach określonych w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel
3. **NRA** – Naczelna Rada Adwokacka.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach Legitymacji adwokackiej stanowi art. 3 ustawy o aplikacji mObywatel, zgodnie z którym Minister zapewnia działanie systemu teleinformatycznego, który pozwala, przy użyciu Aplikacji, na pobranie dokumentu elektronicznego zawierającego dane dotyczące sytuacji prawnej Użytkownika lub praw mu przysługujących.
2. Za zgodność danych zawartych w usłudze Legitymacja adwokacka 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 w Legitymacja, są nieprawidłowe lub nieaktualne, należy zgłosić się do okręgowej rady adwokackiej.
3. Korzystanie z mobilnej Legitymacji adwokackiej 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 Legitymacji adwokackiej posiadaczowi legitymacji adwokackiej, wskazanemu w KRAiAA, który zaloguje się do Aplikacji, bez konieczności wnioskowania o nią.
5. Instalacja dostarczanych cyklicznie przez Ministra aktualizacji Aplikacji jest konieczna dla jej prawidłowego działania i należytego zabezpieczenia zawartych w niej danych. Instalowanie takich aktualizacji powinno nastąpić niezwłocznie po ich udostępnieniu za pomocą sklepów z aplikacjami.

§ 3. Legitymacja adwokacka

1. Legitymacja adwokacka- pozwala na pobranie przez Użytkownika danych z KRAiAA oraz z usługi mObywatel oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub przekazywanie.
2. Dane dostępne w Legitymacji adwokackiej pochodzą z KRAiAA i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem podstawowym.

3. Posługiwanie się mobilną Legitymacją adwokacką przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej wykonujących zawód adwokata.
4. Do aktywacji i aktualizacji Legitymacji adwokackiej niezbędne jest posiadanie ważnego wpisu na listę aplikantów adwokackich, adwokatów lub prawników zagranicznych prowadzoną przez właściwą okręgową radę adwokacką.

§ 4. Użytkownicy

1. Użytkownikami korzystającymi z Legitymacji mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
   1) mają ważny Certyfikat podstawowy;
   2) posiadają wpis na listę aplikantów adwokackich, adwokatów lub prawników zagranicznych prowadzoną przez właściwą okręgową radę adwokacką.

§ 5. Aktywacja usługi Legitymacja adwokacka

1. Aktywacja usługi Legitymacja adwokacka w Aplikacji polega na:
   1) uruchomieniu aplikacji mObywatel i zalogowaniu się do niej,
   2) wybraniu „Legitymacja adwokacka” z listy dostępnych usług;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
   4) pobraniu danych Użytkownika oraz jego uprawnień.
2. Ważność Legitymacji powiązana jest z ważnością Certyfikatu Certyfikat podstawowy jest wykorzystywany do:
   1) pobrania i podpisania danych w mobilnej Legitymacji adwokackiej;
   2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z KRAiAA;
   3) zapewnienia, że przekazywane dane w ramach usługi Legitymacja adwokacka są tożsame z danymi pobranymi z KRAiAA oraz usługi mObywatel.
   4) Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z KRAiAA niezbędne jest aktywne połączenie internetowe.
3. Użytkownik może aktywować Mobilną Legitymację adwokacką i pobrać dane z KRAiAA wyłącznie na jednym urządzeniu.
4. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Mobilna Legitymacja adwokacka nie oferuje funkcji eksportu ani importu danych.
5. Dostęp do danych przechowywanych w mobilnej Legitymacji adwokackiej jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje mobilnej Legitymacji adwokackiej

1. Prawidłowo aktywowana usługa Legitymacja adwokacka umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych Użytkownika, o których mowa w § 7 ust. 7
   2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja

„Przekaż”);
3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
4) usunięcie mobilnej Legitymacji adwokackiej z Aplikacji (funkcja „Usuń Legitymację adwokacką”).

2. Użytkownik może okazać innej osobie mobilną Legitymację adwokacką. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu Legitymacji . 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) ruchomego elementu graficznego prezentującego biało-czerwoną flagę Rzeczypospolitej Polskiej;
   3) gilosza umieszczonego jako tło mobilnej Legitymacja adwokacka, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
   4) zegara mierzącego aktualny czas liczony w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z upływem czasu.
3. Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
4. usunięcie Legitymacji adwokackiej z Aplikacji można dokonać poprzez działanie (sekcja ”Dokumenty”, następnie ikona edycji i wybranie ikony „kosz”).
5. Usunięcie usługi Legitymacja adwokacka Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

§ 7. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z KRAiAA jest Naczelna Rada Adwokacka z siedzibą przy ul. Świętojerskiej 16, 00-202 Warszawa. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
2. Wyżej wymieniony Administrator wyznaczył Inspektora Ochrony Danych, z którym – w sprawach dotyczących przetwarzania danych osobowych - można kontaktować się korespondencyjnie: Naczelna Rada Adwokacka z siedzibą przy ul. Świętojerskiej 16, 00- 202 Warszawa z dopiskiem „Do inspektora ochrony danych” bądź mailowo: IOD@nra.pl
3. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie podstawowym jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą mający swą siedzibę w Warszawie, przy ul. Królewskiej 27.
4. 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.
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: iod@mc.gov.pl.
6. Podstawą przetwarzania danych osobowych dla Certyfikatu przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit

e RODO, w związku z art. 69 ust. 1 ustawy o aplikacji mObywatel w związku z zawartym przez Ministra Cyfryzacji porozumieniem. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.

7. W ramach mobilnej Legitymacji adwokackiej w Aplikacji przechowuje się następujące dane:
   1) Imię (imiona) mobilnej Legitymacji adwokackiej;
   2) nazwisko Użytkownika;
   3) wizerunek twarzy Użytkownika;
   4) numer wpisu na listę adwokatów/aplikantów adwokackich;
   5) data wydania dokumentu;
   6) data ważności dokumentu;
   7) nazwa izby adwokackiej;
   8) organ wydający legitymację;
   9) rodzaj uprawnienia.
5. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych osobowych:
   1) prawo dostępu do treści danych;
   2) prawo ich poprawiania i sprostowania;
   3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   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.
6. 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 albo na podstawie akceptacji przekazania danych osobowych do Instytucji.
7. 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.
8. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Przekaż") do systemu teleinformatycznego Instytucji, Aplikacja przesyła wybrane dane osobowe, które są niezbędne do realizacji usługi oferowanej przez daną Instytucję. Zestaw danych jest uzależniony od oferowanej przez Instytucję usługi.
9. W celu utworzenia Certyfikatu podczas aktywacji dokumentu mDowód oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister

właściwy do spraw informatyzacji przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.

10. Minister właściwy do spraw informatyzacji przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.
11. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
12. Zgodnie z art. 20 ust. 3 pkt 1 ustawy o aplikacji mObywatel Minister właściwy do spraw informatyzacji przetwarza dane osobowe użytkowników aplikacji mObywatel przez okres: 6 lat od dnia upływu ważności albo dnia unieważnienia certyfikatu użytkownika w przypadku danych, które są przetwarzane w systemie mObywatel;
13. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu mDowód, 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. Historia działań Użytkownika zapisywana jest w jego urządzeniu mobilnym.
14. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:
    1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
15. 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.
16. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 12 do Regulaminu

Legitymacja poselska

§ 1. Definicje:

1. **Legitymacja poselska –** dokument wydany przez Marszałka Sejmu na podstawie art. 45 Ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2022 r. poz. 1339)
2. **mobilna Legitymacja poselska** – usługa, o której mowa w art. 3 ust. 1 ustawy o aplikacji mObywatel, dostępna na urządzeniu mobilnym Użytkownika w Aplikacji, której wykorzystywanie odbywa się na warunkach określonych w Ustawie o aplikacji mObywatel oraz w ustawie z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora.

3. **SIS –** bazy danych Systemu Informacyjnego Sejmu zawierające dane dostępne w moblinej Legitymacji poselskiej.

§ 2. Informacje ogólne

1. Podstawę prawną pobrania danych mobilnej Legitymacji stanowi art. 3 ustawy o aplikacji mObywatel, 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 usłudze Legitymacja poselskiej 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 w Legitymacja, są nieprawidłowe lub nieaktualne, należy zgłosić się do Kancelarii Sejmu.
3. Korzystanie z mobilnej Legitymacji posła 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 Legitymacji posiadaczowi, której dane znajdują się w SIS. Pobranie mobilnej Legitymacji możliwe jest bez konieczności wnioskowania o nią oraz po zalogowaniu się do Aplikacji.
5. Instalacja dostarczanych cyklicznie przez Ministra aktualizacji Aplikacji jest konieczna dla jej prawidłowego działania i należytego zabezpieczenia zawartych w niej danych. Instalowanie takich aktualizacji powinno nastąpić niezwłocznie po ich udostępnieniu za pomocą sklepów z aplikacjami.

§ 3. Legitymacja poselska

1. Legitymacja poselska pozwala na pobranie przez Użytkownika danych z SIS oraz z usługi mObywatel oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub przekazywanie.
2. Dane dostępne w usłudze mobilnej Legitymacji pochodzą z SIS oraz Usługi mObywatel i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem Podstawowym.
3. Posługiwanie się mobilną Legitymacją przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej.
4. Do aktywacji i aktualizacji Legitymacji poselskiej niezbędne jest posiadanie ważnego Certyfikatu Podstawowego.

§ 4. Użytkownicy

1. Użytkownikami korzystającymi z Legitymacji mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
   1) mają ważny Certyfikat podstawowy;
   2) pełnią mandat posła w bieżącej kadencji Sejmu RP.

§ 5. Aktywacja usługi Legitymacja poselska

1. Aktywacja usługi Legitymacja w Aplikacji polega na:
    1. uruchomieniu aplikacji mObywatel i zalogowaniu się do niej,
    2. wybraniu „Legitymacja poselska” z listy dostępnych usług;
    3. potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
    4. pobraniu danych Użytkownika oraz jego uprawnień.
2. Ważność Legitymacji powiązana jest z ważnością Certyfikatu.
3. Certyfikat podstawowy jest wykorzystywany do:
    1) pobrania i podpisania danych w mobilnej Legitymacji poselskiej;
    2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z SIS;
    3) zapewnienia, że przekazywane dane w ramach usługi Legitymacja są tożsame z danymi pobranymi z SIS oraz usługi mObywatel.
4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z SIS niezbędne jest aktywne połączenie internetowe.
5. Użytkownik może aktywować Mobilną Legitymację poselską i pobrać dane z Rejestru ZUS wyłącznie na jednym urządzeniu.
6. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Mobilna Legitymacja nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w mobilnej Legitymacji jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje mobilnej Legitymacji poselskiej

1. Prawidłowo aktywowana usługa Legitymacja poselska umożliwia Użytkownikowi korzystanie z następujących funkcji:
    1) okazanie danych Użytkownika, o których mowa w § 7 ust. 7
    2) przekazania danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Przekaż”);
    3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
    4) usunięcie mobilnej Legitymacji poselskiej z Aplikacji (funkcja „Usuń Legitymację poselską”).
2. Użytkownik może okazać innej osobie mobilną Legitymację poselską. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu Legitymacji. 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) ruchomego elementu graficznego prezentującego biało-czerwoną flagę Rzeczypospolitej Polskiej;
    3) gilosza umieszczonego jako tło mobilnej Legitymacja poselska, w którym kolory zmieniają się pod wpływem zmiany położenia żyroskopu urządzenia;
    4) zegara mierzącego aktualny czas liczony w godzinach, minutach i sekundach,

zmieniający się dynamicznie wraz z upływem czasu.

5) Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
6) Usunięcie usługi Legitymacja poselska Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

§ 7. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z SIS jest Kancelaria Sejmu z siedzibą przy ul. Wiejskiej 4/6/8, 00-902, Warszawa. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
2. Wyżej wymieniony Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych korespondencyjnie na adres: Kancelaria Sejmu, ul. Wiejska 4/6/8, 00-902 Warszawa bądź na adres e-mail: iod@sejm.gov.pl.
3. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie jest Minister Cyfryzacji mający swą siedzibę w Warszawie, przy ul. Królewskiej 27.
4. 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.
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: iod@mc.gov.pl.
6. Podstawą przetwarzania danych osobowych w systemie teleinformatycznym obsługującym usługę mobilna Legitymacja poselska jest art. 6 ust 1 lit. e w związku z art. 45 ust. 1b Ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2022 r. poz. 1339). Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach mobilnej Legitymacji poselskiej w Aplikacji przechowuje się następujące dane:
   1) Imię (imiona) Użytkownika Legitymacji poselskiej;
   2) nazwisko Użytkownika;
   3) wizerunek twarzy Użytkownika;
   4) numer i data wydania Legitymacji poselskiej Użytkownika;
   5) numer kadencji Sejmu RP.
7. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych osobowych:
   1) prawo dostępu do treści danych;
   2) prawo ich poprawiania i sprostowania;
   3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   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.

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 albo na podstawie akceptacji przekazania danych osobowych do Instytucji.
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. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Potwierdź swoje dane") do systemu teleinformatycznego Instytucji, Aplikacja przesyła wybrane dane osobowe, które są niezbędne do realizacji usługi oferowanej przez daną Instytucję. Zestaw danych jest uzależniony od oferowanej przez Instytucję usługi.
11. W celu utworzenia Certyfikatu podczas aktywacji dokumentu mDowód oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister właściwy do spraw informatyzacji przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.
12. Minister właściwy do spraw informatyzacji przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.
13. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
14. Zgodnie z art. 20 ust. 3 pkt 1 ustawy o aplikacji mObywatel Minister właściwy do spraw informatyzacji przetwarza dane osobowe użytkowników aplikacji mObywatel przez okres: 6 lat od dnia upływu ważności albo dnia unieważnienia certyfikatu użytkownika w przypadku danych, które są przetwarzane w systemie mObywatel;
15. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu mDowód, danych o połączeniach między nimi ani danych o Użytkownikach w związku z korzystaniem z funkcji weryfikacji online w mWeryfikatorze.
16. Minister nie gromadzi również informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych. Historia działań Użytkownika zapisywana jest w jego urządzeniu mobilnym.
17. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:

1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,

23. 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.

24. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 13 do Regulaminu

Usługa e-Płatności

§ 1. Definicje:

1. **Usługa e-Płatności (PeP)** – usługa z wykorzystaniem platformy e- umożliwiająca wykonywanie przez obywateli opłat online za podatek od nieruchomości, udostępnionych w ramach Aplikacji mObywatel oraz ich podgląd.
2. **Zobowiązanie finansowe -–** zobowiązania podatkowe oraz opłaty cywilnoprawne udostępnianie obywatelom przez Organ podatkowy (urząd obsługujący ten organ) na portalu mObywatel.gov.pl i w Aplikacji mObywatel.
3. **EPO** – Elektroniczne potwierdzenie opłaty, które użytkownik aplikacji mObywatel będzie mógł pobrać w Aplikacji mObywatel.
4. **Transakcja płatnicza** – płatność wykonywana z wykorzystaniem kodu BLIK.

§ 2. Informacje ogólne

1. Uwierzytelnienie Użytkownika w celu dokonania Transakcji płatniczej w ramach usługi e- Płatności będzie odbywało się w oparciu o Certyfikat.

§ 3. Usługa e-Płatności

1. Interfejs użytkownika Usługi e-Płatności jest udostępniany w aplikacji mObywatel.
2. Do aktywacji i aktualizacji Usługi e-Płatności niezbędne jest posiadanie ważnego Certyfikatu.
3. Pobranie Usługi e-Płatności i korzystanie z niej jest nieodpłatne. Korzystanie przez Użytkownika z usług transmisji danych lub połączeń głosowych w związku z pobraniem lub korzystaniem z Usługi e-Płatności może wiązać się z opłatami naliczanymi przez operatora telekomunikacyjnego, który świadczy Użytkownikowi usługi telekomunikacyjne.
4. Korzystanie z Usługi e-Płatności jest dobrowolne.

§ 4. Użytkownicy

1. Użytkownik- osoba fizyczna, której zapewniono możliwość korzystania z aplikacji mObywatel po uprzednim ustaleniu tożsamości tej osoby w sposób określony w ustawie

o aplikacji mObywatel. Pojęcie może być używane w Regulaminie odpowiednio w liczbie mnogiej „Użytkownicy” lub w liczbie pojedynczej „Użytkownik”.

§ 5. Aktywacja Usługi e-Płatności

1. Aktywacja Usługi e-Płatności polega na:
   1) zalogowaniu do Aplikacji mObywatel;
   2) wybraniu „e-Płatności” z listy dostępnych usług;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu;
   4) pobraniu zobowiązań finansowych Użytkownika.
2. Ważność Usługi e-Płatności powiązana jest z ważnością Certyfikatu.
3. Certyfikat jest wykorzystywany do pobrania Usługi e-Płatności.
4. Do potwierdzenia tożsamości Użytkownika, ważności Certyfikatu oraz pobrania zobowiązań przy użyciu Usługi e-Płatności niezbędne jest aktywne połączenie internetowe.
5. Użytkownik może aktywować Usługę e-Płatności i pobrać dane z systemu teleinformatycznego organu podatkowego zintegrowanego z tą usługą za pomocą aplikacji mObywatel tylko na jednym urządzeniu mobilnym.
6. Usługa e-Płatności nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w Usłudze e-Płatności jest zabezpieczony hasłem w aplikacji mObywatel zgodnie z Regulaminem korzystania z aplikacji mObywatel.

§ 6. Funkcje w Usłudze e-Płatności dla Użytkowników

1. Prawidłowo aktywowana Usługa e-Płatności umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) opłacenia za pomocą szybkiej płatności BLIK zobowiązania finansowego udostępnionego przez Organ podatkowy (funkcja „Zapłać”);
   2) pobranie potwierdzenia przelewu – EPO (funkcja „Pobierz”/„Pobierz potwierdzenie”);
   3) przegląd wszystkich Transakcji płatnicza (funkcja „Historia płatności”);

§ 7. Klauzula informacyjna

1. Administratorem danych osobowych Użytkownika pobieranych z systemu Rejestr Uprawnień jest wydająca uprawnienie instytucja. Informacja o przetwarzaniu danych osobowych znajduje się na stronie internetowej danej instytucji.
2. Administratorem danych Użytkownika aplikacji mObywatel oraz Certyfikatu jest Minister Cyfryzacji, z siedzibą przy ul. Królewskiej 27, 00-060 w Warszawie.
3. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: Kancelaria.Krolewska@cyfra.gov.pl lub na adres skrytki na ePUAP: /MAiC/SkrytkaESP.
4. Administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować we wszystkich sprawach związanych z przetwarzaniem danych osobowych:

korespondencyjnie na adres: ul. Królewska 27, 00-060 Warszawa, bądź mailowo na adres: iod@mc.gov.pl.

5. W ramach usługi Rejestr Uprawnień w Aplikacji przechowuje się następujące dane Użytkownika:
   1) imię pierwsze posiadacza Uprawnienia;
   2) imię drugie posiadacza Uprawnienia;
   3) nazwisko posiadacza Uprawnienia;
   4) numer PESEL posiadacza Uprawnienia;
   5) wizerunek twarzy posiadacza Uprawnienia;
   6) nazwa instytucji;
   7) typ dokumentu;
   8) rodzaj Uprawnienia;
   9) numer Uprawnienia unikalny w ramach rodzaju uprawnienia;
   10) status Uprawnienia;
   11) termin ważności Uprawnienia.
6. Podstawą przetwarzania danych osobowych przez administratora danych (Ministra Cyfryzacji) jest:
7. Podstawą przetwarzania danych osobowych dla Certyfikatu Użytkownika przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, w związku z art. 69 ust. 1 ustawy o aplikacji mObywatel i porozumienia zawartego przez Ministra Cyfryzacji. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
8. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych osobowych:
   1) prawo dostępu do treści danych;
   2) prawo ich poprawiania i sprostowania;
   3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
   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.
   6) Prawo do poprawienia lub sprostowania danych realizowane jest wyłącznie poprzez poprawienie danych znajdujących się w systemie teleinformatycznym zapewniających funkcjonowanie dokumentu mDowód oraz dotyczy danych, o których mowa w § 3 ust. 1 - 3.
9. 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 albo na podstawie akceptacji przekazania danych osobowych do Instytucji.

10. 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.
11. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Potwierdź swoje dane") do systemu teleinformatycznego Instytucji, Aplikacja przesyła wybrane dane osobowe, które są niezbędne do realizacji usługi oferowanej przez daną Instytucję. Zestaw danych jest uzależniony od oferowanej przez Instytucję usługi.
12. W celu utworzenia Certyfikatu podczas aktywacji dokumentu mDowód oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister właściwy do spraw informatyzacji przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.
13. Minister właściwy do spraw informatyzacji przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.
14. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
15. Zgodnie z art. 20 ust. 3 ustawy o aplikacji mObywatel Minister właściwy do spraw informatyzacji przetwarza dane osobowe użytkowników aplikacji mObywatel przez okres: 6 lat od dnia upływu ważności albo dnia unieważnienia certyfikatu użytkownika – w przypadku danych, które są przetwarzane w systemie mObywatel;
16. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu mDowód, 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. Historia działań Użytkownika zapisywana jest w jego urządzeniu mobilnym.
17. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:
    1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
18. 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.
19. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 14 do Regulaminu

Rejestr Uprawnień (WRU)

§ 1. Definicje:

1. **Uprawnienie** – zestaw danych związanych z posiadanymi aktualnie uprawnień przez obywatela do wykonywania czynności oraz potwierdzających przysługujące im prawa.
2. **Instytucja** – wydaje Uprawnienia obywatelom w ramach swojej statutowej działalności.

§ 2. Informacje ogólne

1. Uwierzytelnienie Obywatela w celu pobrania Uprawnienia do aplikacji mObywatel będzie odbywało się w oparciu o certyfikat usługi mObywatel.

§ 3. Rejestr Uprawnień

1. Rejestr Uprawnień pozwala na pobranie przez Użytkownika danych o przysługujących świadczeniach użytkownikowi z bazy systemu Rejestru Uprawnień oraz z Usługi mObywatel oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich okazywanie lub udostępnianie.
2. Wiarygodność danych dostępnych w Rejestrze Uprawnień wynika z faktu, że dane pochodzą z rejestrów państwowych i systemu Rejestru Uprawnień będących we właściwości Jednostek Samorządów terytorialnych bądź Instytucji i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
3. Posługiwanie się Rejestrem Uprawnień przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej.
4. Do aktywacji i aktualizacji Rejestru Uprawnień niezbędne jest posiadanie ważnego Uprawnienia oraz ważnego Certyfikatu.
5. Dodanie nowej wersji rodzaju uprawnienia po stronie Rejestru Uprawnień nie będzie skutkowało automatyczną zmianą w mObywatelu, dopiero odświeżenie wybranego dokumentu w aplikacji mObywatel spowoduje pobranie najnowszej wersji Uprawnienia.

§ 4. Użytkownicy

1. Użytkownikami korzystającymi z Rejestru Uprawnień mogą być wyłącznie osoby mające obywatelstwo polskie oraz aktywny dowód osobisty, które spełniają dwa poniższe warunki:
   1) mają ważny Certyfikat
   2) posiadają aktywne uprawnienia nadane przez Instytucję zarejestrowane w systemie Rejestr Uprawnień.

§ 5. Aktywacja Rejestru Uprawnień

1. Aktywacja Rejestru Uprawnień polega na:
   1) zalogowaniu do Aplikacji;
   2) wybraniu „Rejestr Uprawnień” z listy dostępnych usług;
   3) potwierdzeniu tożsamości Użytkownika przy użyciu Certyfikatu;
   4) pobraniu danych Użytkownika oraz jego uprawnień.

2. Ważność Rejestru Uprawnień powiązana jest z ważnością Certyfikatu.
3. Certyfikat jest wykorzystywany do:
   1) pobrania i podpisania danych w Rejestrze Uprawnień;
   2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z Rejestru Uprawnień;
   3) zapewnienia, że przekazywane dane w ramach Uprawnienia są tożsame z danymi pobranymi z Rejestru Uprawnień oraz usługi mObywatel.
4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z systemu Rejestru Uprawnień niezbędne jest aktywne połączenie internetowe.
5. Użytkownik może aktywować Rejestr Uprawnień i pobrać dane z systemu Rejestru Uprawnień tylko na jednym urządzeniu mobilnym.
6. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Rejestr Uprawnień nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w Rejestrze Uprawnień jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

§ 6. Funkcje Rejestru Uprawnień dla Użytkowników usługi mObywatel

1. Prawidłowo aktywowana usługa Rejestru Uprawnień umożliwia Użytkownikowi korzystanie z następujących funkcji:
   1) okazanie danych Użytkownika Rejestru Uprawnień, o których mowa w §7 ust. 3, oraz kodu QR;
   2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji
   3) aktualizacji danych Użytkownika (funkcja „Aktualizuj”);
   4) usunięcie Rejestru Uprawnień z Aplikacji (funkcja „Usuń ”).
2. Użytkownik może okazać innej osobie Uprawnienie oraz kod QR na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu „Rejestr Uprawnień”. 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 Rejestru Uprawnień, 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 „Udostępnij” pozwala na przekazanie do weryfikacji Aplikacji mWeryfikator danych Użytkownika Rejestru Uprawnień w postaci kodu QR. Przekazanie danych przebiega w następujący sposób:
   1) Użytkownik w Rejestrze Uprawnień wywołuje funkcję „Udostępnij”,
   2) w Rejestrze Uprawnień 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.
5. Usunięcie Rejestru Uprawnień Użytkownika następuje również automatycznie w przypadku dezaktywacji Usługi mObywatel.

§ 7. Klauzula informacyjna

6. Administratorem danych osobowych Użytkownika pobieranych z systemu Rejestr Uprawnień jest wydająca uprawnienie Instytucja. Informacja o przetwarzaniu danych osobowych znajduje się na stronie internetowej danej instytucji. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
7. Administratorem danych Użytkownika aplikacji mObywatel oraz Certyfikatu jest Minister Cyfryzacji, z siedzibą przy ul. Królewskiej 27, 00-060 w Warszawie.
8. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: Kancelaria.Krolewska@cyfra.gov.pl lub na adres skrytki na ePUAP: /MAiC/SkrytkaESP.
9. Administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować we wszystkich sprawach związanych z przetwarzaniem danych osobowych: korespondencyjnie na adres: ul. Królewska 27, 00-060 Warszawa, bądź mailowo na adres: iod@mc.gov.pl.
10. W ramach usługi Rejestr Uprawnień w Aplikacji przechowuje się następujące dane Użytkownika:
    1) imię pierwsze posiadacza Uprawnienia;
    2) imię drugie posiadacza Uprawnienia;
    3) nazwisko posiadacza Uprawnienia;
    4) numer PESEL posiadacza Uprawnienia;
    5) wizerunek twarzy posiadacza Uprawnienia;
    6) nazwa instytucji;
    7) typ dokumentu;
    8) rodzaj Uprawnienia;
    9) numer Uprawnienia unikalny w ramach rodzaju uprawnienia;
    10) status Uprawnienia;
    11) termin ważności Uprawnienia.
20. Podstawą przetwarzania danych osobowych dla Certyfikatu Ucznia przez administratora danych (Ministra Cyfryzacji) jest realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, w związku z art. 15 i 69 ust. 1 ustawy o aplikacji mObywatel i porozumienia z Instytucją zawartego przez Ministra Cyfryzacji.

Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.

21. Osobie, której dane dotyczą, przysługuje w dowolnym momencie – zgodnie z Ogólnym rozporządzeniem o ochronie danych osobowych:
    1) prawo dostępu do treści danych;
    2) prawo ich poprawiania i sprostowania;
    3) prawo do sprzeciwu do przetwarzania danych (w odniesieniu do przetwarzania na podstawie art. 6 ust. 1 lit. e RODO);
    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.
22. Prawo do poprawienia lub sprostowania danych realizowane jest wyłącznie poprzez poprawienie danych znajdujących się w systemie teleinformatycznym zapewniających funkcjonowanie dokumentu mDowód oraz dotyczy danych, o których mowa w § 3 ust. 1 - 3.
23. 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 albo na podstawie akceptacji przekazania danych osobowych do Instytucji.
24. 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.
25. Podczas korzystania z funkcji elektronicznego przekazania danych (funkcja „Potwierdź swoje dane") do systemu teleinformatycznego Instytucji, Aplikacja przesyła wybrane dane osobowe, które są niezbędne do realizacji usługi oferowanej przez daną Instytucję. Zestaw danych jest uzależniony od oferowanej przez Instytucję usługi.
26. W celu utworzenia Certyfikatu podczas aktywacji dokumentu mDowód oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Minister właściwy do spraw informatyzacji przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.
27. Minister właściwy do spraw informatyzacji przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu (sprawdzenie ważności certyfikatu online) za pomocą mWeryfikatora gromadzi następujące dane: identyfikator użytkownika mWeryfikator.
28. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
29. Zgodnie z art. 20 ust. 3 pkt 1 ustawy o aplikacji mObywatel Minister właściwy do spraw informatyzacji przetwarza dane osobowe użytkowników aplikacji mObywatel przez okres:

6 lat od dnia upływu ważności albo dnia unieważnienia certyfikatu użytkownika – w przypadku danych, które są przetwarzane w systemie mObywatel;

30. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu mDowód, 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. Historia działań Użytkownika zapisywana jest w jego urządzeniu mobilnym.
31. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, to jest przez:
    1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
32. 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.
33. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.