

## **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.

### **Definicje**

1. **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.
2. **CEK** – Centralna Ewidencja Kierowców, o której mowa w art. 100a ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym.
3. **CEP** - Centralna Ewidencja Pojazdów, o której mowa w art. 80a ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym.
4. **Certyfikat podstawowy / Certyfikat** – certyfikat użytkownika aplikacji mObywatel wydawany użytkownikowi aplikacji automatycznie z dokumentem mObywatel oraz Profilem mObywatel pozwalający na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika.
5. **Instytucja** – podmiot publiczny lub niepubliczny, któremu Minister wydał Certyfikat, pozwalający na zabezpieczenie oraz potwierdzenie pochodzenia danych przekazywanych pomiędzy systemem teleinformatycznym Aplikacji a systemem teleinformatycznym tego podmiotu.
6. **Minister, Minister Cyfryzacji** – minister właściwy do spraw informatyzacji, którego urząd obsługujący Ministerstwo Cyfryzacji posiada siedzibę w Warszawie, przy ul. Królewskiej 27.
7. **mWeryfikator webowy** – Internetowa usługa weryfikacji mDowodu – oprogramowanie Ministra, stanowiące element systemu publicznej aplikacji mobilnej, umożliwiające weryfikację mDowodu przy pomocy kryptograficznej weryfikacji tożsamości i dedykowanej strony internetowej: <https://weryfikator.mobywatel.gov.pl/>.
8. **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).

9. **Powiadomienie PUSH** – wiadomość przekazywana Użytkownikowi w formie powiadomienia wyświetlanego na ekranie urządzenia mobilnego, niezależnie od tego czy Aplikacja jest włączona.
10. **Profil mObywatel** – środek identyfikacji elektronicznej, wydawany zgodnie z art. 14 ust. 1-3 ustawy o aplikacji mObywatel.
11. **Regulamin** – niniejszy regulamin aplikacji mObywatel, o którym mowa w art. 21 ust.1 pkt 1 ustawy o aplikacji mObywatel.
12. **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.
13. **Skrzynka odbiorcza** – skrzynka odbiorcza w Aplikacji, prezentująca wiadomości kierowane do konkretnego Użytkownika.
14. **System mObywatel/System teleinformatyczny Aplikacji** - system teleinformatyczny zapewniający funkcjonalności niezbędne do działania aplikacji mObywatel oraz usług udostępnianych w tej aplikacji.
15. **Ustawa o aplikacji mObywatel** – ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275, z późn.zm.).
16. **Ustawa o ewidencji ludności** – ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 20252 r. poz. 274).
17. **Ustawa o kierujących pojazdami** – ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2024 r. poz. 1210, z późn. zm.).
18. **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 2024 r. poz. 167, z późn. zm.).
19. **Ustawa - Prawo o ruchu drogowym** – ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. 2024 r. poz. 1251).
20. **Ustawa o dowodach osobistych** – ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. z 2022 r. poz. 671, z późn.zm.)
21. **Użytkownik/Użytkownicy** – osoba fizyczna/osoby, której/ym zapewniono możliwość korzystania z aplikacji mObywatel po uprzednim ustaleniu tożsamości w sposób określony w ustawie o aplikacji mObywatel.
22. **Użytkownik/Użytkownicy mWeryfikatora webowego** – osoba fizyczna/osoby, której/ym zapewniono możliwość korzystania z mWeryfikatora webowego.

## **Dokumenty i usługi w 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** (inaczej **mDowód, dokument mDowód**) – dokument mobilny stwierdzający tożsamość i obywatelstwo polskie Użytkownika na terytorium Rzeczypospolitej Polskiej w relacjach wzajemnej fizycznej obecności stron. Wydawany Użytkownikowi 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 (legitymacji szkolnej), która pozwala na pobranie danych osobowych Użytkownika, przechowywanie ich w zaszyfrowanej formie na urządzeniu mobilnym Użytkownika, bezpieczne prezentowanie danych Użytkownika innym osobom lub podmiotom.
- 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 i powiązanych z nimi danych pojazdu z CEP i prezentowanie innym osobom lub podmiotom w sposób bezpieczny. Aby korzystać z tej usługi konieczny jest aktywny Dokument mObywatel.
- 4) **Legitymacja studencka** – Usługa prezentacji dokumentu elektronicznego (legitymacji studenckiej), 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, prezentowanie danych Użytkownika innym osobom lub podmiotom;
- 5) **Recepty** – 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 pkt 6 lit. a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2022 r. poz. 1555, z późn. zm.). 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, o której mowa w art. 3 ust. 1 pkt 1 ustawy o aplikacji mObywatel, która pozwala na pobranie przez Użytkownika danych osobowych (w tym danych osobowych) i powiązanych z nimi uprawnień do kierowania pojazdami z CEK, oraz przechowywanie ich w postaci zaszyfrowanej w

urządzeniu mobilnym Użytkownika, a także ich prezentowanie innym osobom lub podmiotom Użytkownikom w sposób bezpieczny. 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](http://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](http://bilkom.pl) lub [bilet.wielkopolskiebilety.pl](http://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) **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;
- 12) **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 prezentowanie danych Użytkownika innym osobom w celu potwierdzenia jego tożsamości;
- 13) **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;

- 14) **Dodatek gazowy** – 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](http://ww.gov.pl). Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
- 15) **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 prezentowanego przy użyciu Aplikacji. Aby korzystać z mobilnej Legitymacji emeryta-rencisty wymagana jest aktywacja usługi mObywatel;
- 16) **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.;
- 17) **Legitymacja poselska** – dokument mobilny wydany przez Marszałka Sejmu Rzeczypospolitej Polskiej, którego wykorzystywanie odbywa się na warunkach ustawy o aplikacji mObywatel oraz ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
- 18) **Rejestr Upnień** – usługa Ministra, o której mowa w art. 16 ustawy o aplikacji mObywatel, umożliwiająca prezentację w Aplikacji dokumentów potwierdzających uprawnienia obywatela, takiej jak np. karta mieszkańca lub lokalna karta seniora. Dokumenty wydawane są przez uprawnione do tego instytucje – np. urzędy gminy. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;
- 19) **Usługa e-Płatności** – pilotaż usługi online, skierowany do określonej grupy Użytkowników, polegający na obsłudze elektronicznych Transakcji płatniczych udostępnionych w Aplikacji mObywatel;
- 20) **Tymczasowe elektroniczne Prawo Jazdy (TePJ)** – dokument tworzony na okres 30 dni, bezpośrednio po zdanym egzaminie państwowym na prawo jazdy w systemie teleinformatycznym obsługującym CEK i udostępniany do pobrania w aplikacji mObywatel w ramach usługi Ministra, o której mowa w art. 3 ust. 1 pkt 1 ustawy o aplikacji mObywatel. Pozwala na pobranie przez Użytkownika danych osobowych i powiązanych z nimi uprawnień do kierowania pojazdami z CEK, oraz przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie innym osobom lub podmiotom Użytkownikom w sposób bezpieczny. Aby korzystać z tej usługi konieczny jest aktywny Dokument mDowód;

- 21) **Bezpieczny autobus** – usługa Ministra Cyfryzacji pozwalająca na sprawdzenie podstawowych danych na temat autobusu lub autokaru, w tym informacje na temat ważności badania technicznego, aktualności OC lub czy został oznaczony jako wycofany z ruchu;  
Aby sprawdzić dane konkretnego autobusu, należy zalogować się do aplikacji, wybrać usługę „Bezpieczny autobus”, wprowadzić numery tablicy rejestracyjnej pojazdu i kliknąć „sprawdź pojazd”, a następnie na ekranie pojawią się informacje na temat pojazdu.
- 22) **Historia Pojazdu** – usługa Ministra Cyfryzacji, umożliwiająca dostęp do informacji na temat historii pojazdu z uwzględnieniem danych ogólnych, technicznych i zdarzeń dotyczących pojazdu. W przypadku pojazdów importowanych, użytkownikowi prezentowane są również dane zagraniczne;
- 23) **Wybory, Centralny Rejestr Wyborców** – usługa Ministra Cyfryzacji, umożliwiająca wyświetlenie danych obywatela z Centralnego Rejestru Wyborców wraz z informacją o posiadaniu prawa wyborczego, listy zbliżających się wyborów oraz szczegółów dotyczących wydarzenia wyborczego (w tym informacji na temat siedziby obwodowej komisji wyborczej, do której obywatel został przypisany);
- 24) **Jakość powietrza** – usługa Ministra Cyfryzacji, umożliwiająca sprawdzenie stanu czystości powietrza w wybranych punktach na terenie Polski;  
Aby sprawdzić stan powietrza w konkretnej lokalizacji należy wybrać usługę „jakość powietrza” i wybrać z mapy najbliższy punkt pomiarowy.
- 25) **Mandaty** – usługa Ministra Finansów, umożliwiająca wyświetlenie informacji na temat otrzymanych mandatów fiskalnych w podziale na opłacone i nieopłacone. Dane pochodzą z Ministerstwa Finansów – Systemu e-Urząd Skarbowy. Szczegółowe informacje na jej temat znajdują się na stronie: <https://www.podatki.gov.pl/uslugi-online/>
- 26) **E-Wizyta w ZUS** – usługa Zakładu Ubezpieczeń Społecznych, umożliwiająca zapisanie się na wideo rozmowę z pracownikiem ZUS. Szczegółowe informacje na jej temat znajdują się na stronie: <https://www.zus.pl/e-wizyta>
- 27) **Zastrzeż PESEL** – Usługa Ministra, pozwalająca na zastrzeżenie osobie pełnoletniej numeru PESEL w celu zabezpieczenia się przed skutkami kradzieży tożsamości;
- 28) **Sprawdź PESEL** – Usługa Ministra, pozwalająca na sprawdzenie czy numer PESEL innej osoby pełnoletniej jest zastrzeżony. Sprawdzenie może nastąpić w imieniu własnym albo podmiotu trzeciego (np. firmy albo urzędu);
- 29) **Legitymacja radcy prawnego/aplikanta radcowskiego** - dokument mobilny, wydany przez Krajową Radę Radców Prawnych, na podstawie uchwały nr 68/VIII/2011 Krajowej Rady Radców Prawnych z dnia 1 października 2011 r., w sprawie wzoru legitymacji radcy prawnego, wzoru legitymacji aplikanta radcowskiego oraz wzoru legitymacji prawnika zagranicznego;

- 30) **PWZ pielęgniarki/PWZ położnej (Prawo wykonywania zawodu pielęgniarki, ograniczone prawo wykonywania zawodu pielęgniarki, prawo wykonywania zawodu położnej albo ograniczone prawo wykonywania zawodu położnej)** – dokument, o którym mowa w art. 41 ust. 1 zdanie pierwsze ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej, który umożliwia potwierdzenie uprawnień zawodowych pielęgniarki i położnej (Dz. U. z 2022 r. poz. 2702, z późn. zm.), udostępniany w postaci dokumentu mobilnego, o którym mowa w art. 2 pkt 7 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, zgodnie ze wzorem, określonym w rozporządzeniu wydanym na podstawie art. 41 ust. 2 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej.
- 31) **Firma** - Usługa Ministra Rozwoju i Technologii, umożliwiająca przedsiębiorcom, prowadzącym jednoosobową działalność gospodarczą, sprawdzenie podstawowych informacji dotyczących prowadzonej działalności, pobieranie zaświadczenia o wpisie do Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz w razie potrzeby udostępnienie danych do faktury w relacji wzajemnej fizycznej obecności stron.
- 32) **PWZ lekarza/ PWZ lekarza dentystry (Prawo wykonywania zawodu lekarza, albo prawo wykonywania zawodu lekarza dentystry)** – dokument, który umożliwia potwierdzenie uprawnień zawodowych lekarza i lekarza dentystry na podstawie art. 5 ust. 1 i 7, art. 5f oraz art. 7 ust. 1a, 2, 2e ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentystry (Dz. U. z 2023 r. poz. 152 z późn. zm.) oraz art. 113d ust. 1 pkt 1 ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa udostępniany w postaci dokumentu mobilnego, zgodnie ze wzorem, określonym w rozporządzeniu wydanym na podstawie art. 7e ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentystry.
- 33) **Bezpiecznie w sieci** – usługa NASK (Naukowej i Akademickiej Sieci Komputerowej - Państwowy Instytut Badawczy), umożliwiająca za pomocą aplikacji zgłaszanie złośliwych stron internetowych oraz incydentów bezpieczeństwa w sieci. Usługa zawiera także dostęp do Bazy Wiedzy - artykułów dot. cyberbezpieczeństwa przygotowanych przez NASK.
- 34) **Alert powodziowy** – usługa IMGW (Instytutu Meteorologii i Gospodarki Wodnej), umożliwiająca za pomocą aplikacji sprawdzenie informacji o stanie alarmowym rzek oraz otrzymanie wskazówek w jaki sposób postępować w przypadku zagrożenia powodziowego dla danego regionu.  
Aby sprawdzić dane, należy zalogować się do aplikacji, wybrać usługę „Alert powodziowy”, wybrać kafelek „stany alarmowe rzek”, a następnie pojawi się ekran z możliwością wyboru danego województwa lub zbiorcza informacja dla wszystkich regionów Polski.
- 35) **Legitymacja inżyniera budownictwa** – dokument mobilny, wydany przez Polską Izbę Inżynierów Budownictwa na podstawie uchwały nr PIIB/KR/0025/2024 Krajowej Rady Polskiej Izby Inżynierów Budownictwa z dnia 11 października 2024 r. w sprawie legitymacji inżynierów budownictwa w aplikacji mObywatel, potwierdzający posiadanie uprawnień wykonywania zawodu inżyniera budownictwa.

- 36) **Podpisz dokument** – usługa Ministra Cyfryzacji, umożliwiająca podpisywanie dokumentów w formacie pdf podpisem osobistym przy pomocy Certyfikatu Podpisu Osobistego umieszczonego w e-dowodzie Użytkownika.
- 37) **Uprawnienia kierowcy** – Usługa Ministra Cyfryzacji, umożliwiająca sprawdzenie uprawnień do kierowania pojazdami, zgodnie z art. 100a ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym.
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) czy nie ma aktywowanego dokumentu mObywatel.
  3. Poza funkcją elektronicznego potwierdzania danych osobowych Aplikacja nie daje Użytkownikowi możliwości modyfikacji lub pobierania danych.
  4. Szczegółowe zasady aktywacji, dezaktywacji Dokumentów 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 usługi Recepty 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>.

## Informacje ogólne

1. Pobranie Aplikacji i korzystanie z niej jest **dobrowolne i 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. Zbieranie danych innych użytkowników Aplikacji, posługiwanie się nimi czy ich publikacja podlegają ograniczeniom prawnym wynikającym m.in. z przepisów służących ochronie danych osobowych, dóbr osobistych i prywatności.
3. Aplikacja umożliwia wyświetlenie komunikatu PUSH Użytkownikowi. 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.

4. Użytkownik Aplikacji może wyłączyć funkcję otrzymywania Powiadomień PUSH dla Aplikacji korzystając z funkcji systemowych.
5. Do wysyłki Powiadomień PUSH jest wykorzystywane narzędzie Firebase Cloud Messaging: <https://firebase.google.com/support/privacy>.
6. Treść Powiadomień PUSH oraz narzędzia do ich wysyłki ustala Minister Cyfryzacji, który udostępnia dane Powiadomienie PUSH.
7. Użytkownik Aplikacji może sprawdzić swoje dane paszportowe (seria i numer dokumentu, data ważności, status oraz typ) korzystając z funkcji Dane paszportu.

### **Wymagania techniczne**

1. W celu prawidłowego i pełnego korzystania z Aplikacji, Użytkownik powinien dysponować urządzeniem mobilnym typu smartfon z systemem:
  - 1) Android 8.0 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 umożliwiała 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 przekazywania 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.

### **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 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, odinstalować Aplikację.
3. Hasło dostępu do Aplikacji nie jest przechowywane w postaci jawnej w urządzeniu mobilnym Użytkownika. Minister nie umożliwi 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.

## 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.

## 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.biznes@cyfra.gov.pl](mailto:mobywatel.biznes@cyfra.gov.pl) Pytania dotyczące usługi Recepty należy kierować drogą elektroniczną na adres: [ikp-pomoc@cez.gov.pl](mailto:ikp-pomoc@cez.gov.pl) Informacje dotyczące usługi Polak za granicą można uzyskać pod numerem telefonu [22 250 01 16](tel:222500116).

## Funkcja weryfikacji

1. Użytkownik dzięki funkcjonalności poszczególnych usług 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. W przypadku wybranych usług (Legitymacja szkolna, Legitymacja studencka) funkcja weryfikacji jest wywoływana poprzez naciśnięcie przycisku „Przełącz”.
3. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu danego dokumentu, a następnie funkcji „potwierdź swoje dane”.
4. Potwierdzenie danych przebiega w następujący sposób:
  - 1) Weryfikujący prezentuje 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/ Dokumentcie (funkcja „Historia”) Aplikacji mObywatel;
  - 9) Użycie mWeryfikatora webowego nie blokuje podstawowych funkcji systemu na urządzeniu Weryfikującego, takich jak utrwalanie obrazu;
  - 10) Aplikacja mObywatel dla systemu Android blokuje możliwość wykonywania zrzutów ekranów, tzw. screen shot’ów;
  - 11) Aplikacja mObywatel dla systemu iOS nie blokuje możliwości wykonania zrzutów ekranów, tzw. screen shot’ów.

## **Odpowiedzialność**

1. Użytkownik lub Użytkownik mWeryfikatora webowego ponosi pełną odpowiedzialność za naruszenie prawa bądź szkodę wyrządzoną swoim działaniem związanym z korzystaniem przez niego z Aplikacji lub mWeryfikatora webowego, w szczególności posłużeniem się lub podaniem do wiadomości publicznej danych innych Użytkowników, uzyskanych za pomocą funkcji oferowanych przez Aplikację lub mWeryfikatora webowego 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 lub mWeryfikatora webowego 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.

#### **Klauzula informacyjna**

1. Administratorem danych Użytkownika aplikacji mObywatel jest Minister Cyfryzacji, którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą przy ul. Królewskiej 27, 00-060 Warszawa.
2. Z Administratorem danych można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: [Kancelaria@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
3. Administrator danych 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@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
4. Podstawą przetwarzania danych osobowych przez Administratora danych w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego:
  1. 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;
  2. 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;

3. 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;
4. W zakresie Usługi Tymczasowe Elektroniczne Prawo 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.pl stanowi realizacja zadania w interesie publicznym, to jest art. 6 ust. 1 lit e. RODO, polegającego na umożliwieniu pobrania, przechowywania i prezentacji dokumentu elektronicznego w związku z art. 10 ustawy o pomocy obywatelom Ukrainy;
6. W zakresie Usługi Centralny Rejestr Wyborców 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;
7. W zakresie Usługi e-Wizyta w ZUS 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;
8. W zakresie Usługi Mandaty 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;
9. W zakresie wysyłania powiadomień PUSH w usłudze Zastrzeż PESEL, 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. 23b ust. 3 ustawy o ewidencji ludności.;
10. W zakresie Usług Zastrzeż PESEL i Sprawdź PESEL 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.
11. W zakresie Usług Legitymacja radcy prawnego/aplikanta radcowskiego, 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.
12. W zakresie Usługi Bezpieczny autobus, 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;
13. W zakresie Usługi Jakość powietrza, 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;
14. W zakresie Usługi Naruszenia środowiskowe, 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;

15. W zakresie Usług PWZ pielęgniarki/PWZ położnej, 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.
  16. W zakresie Usługi Firma, 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.
  17. W zakresie wyświetlania danych paszportu, 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;
  18. W zakresie usługi PWZ lekarza/ PWZ lekarza dentystry, 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;
  19. W zakresie usługi Bezpiecznie w sieci 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;
  20. W zakresie Usługi Alert powodziowy, 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;
  21. W zakresie Usługi Legitymacja inżyniera budownictwa, 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;
  22. W zakresie Usługi Podpisz dokument, 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;
  23. W zakresie usługi Uprawnienia kierowcy, 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;
5. 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 Administratora danych, w takim przypadku Administrator danych 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 Załącznika nr 1.

7. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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.
8. W zakresie przetwarzania i ochrony danych, które Użytkownik uzyskał w toku elektronicznego prezentowania danych osobowych bądź elektronicznego weryfikowania danych osobowych, Użytkownika obowiązuje stosowanie się do powszechnie obowiązujących przepisów prawa.
9. Aplikacja mObywatel przechowuje dane pozyskane w wyniku funkcji Przełącz dla usługi mObywatel przez 30 dni (przekazanie danych z aplikacji mObywatel do drugiej aplikacji mObywatel). Po upływie tego czasu Aplikacja automatycznie kasuje dane. Aplikacje mObywatel wydane po listopadzie 2020 roku nie oferują tej funkcji.
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. Historia weryfikacji przez mWeryfikatora i mWeryfikatora webowego jest dostępna w Aplikacji przez 12 miesięcy. mWeryfikator nie umożliwia zapisania danych Użytkownika Aplikacji, którego dane zostały zweryfikowane.
12. W celu utworzenia Certyfikatu oraz zarządzania Certyfikatami Użytkowników, w tym utrzymaniem listy aktywnych Certyfikatów, Administrator danych przetwarza dane – imię, nazwisko oraz numer PESEL Użytkownika – pobierane z rejestru PESEL podczas aktywacji dokumentu.
13. Administrator danych 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 Administrator danych 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.
16. Z zastrzeżeniem ustępów poprzedzających, Administrator danych 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. Administrator danych 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 będą również przetwarzane przez:

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.

### **Postanowienia końcowe**

1. 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.
2. Użytkownik może w dowolnym momencie zakończyć korzystanie z Aplikacji, poprzez jej odinstalowanie z urządzenia mobilnego.
3. Regulamin jest udostępniony nieodpłatnie na stronie podmiotowej Ministra w Biuletynie Informacji Publicznej, która umożliwia jego pobranie, utrwalenie i wydrukowanie.
4. Regulamin może ulec zmianie wraz z kolejnymi wydaniami Aplikacji. Zmiana jest wiążąca dla Użytkowników, którzy zainstalują takie wydanie Aplikacji.
5. 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 Legitymacja UUT – Ulgowe Usługi Transportowe

Załącznik nr 8 – Usługa Diia.pl

Załącznik nr 9 – Usługa Legitymacja emeryta-rencisty

Załącznik nr 10 – Usługa Legitymacja adwokacka

Załącznik nr 11 – Usługa Legitymacja poselska

Załącznik nr 12 – Usługa e-Płatności

Załącznik nr 13 – Usługa Rejestr Uprawnień

Załącznik nr 14 – Usługa Tymczasowe Elektroniczne Prawo Jazdy

Załącznik nr 15 – Usługa Centralny Rejestr Wyborców  
Załącznik nr 16 – Usługa Mandaty  
Załącznik nr 17 – Usługa e-Wizyta w ZUS  
Załącznik nr 18 – Usługa Zastrzeż PESEL  
Załącznik nr 19 – Usługa Sprawdź PESEL  
Załącznik nr 20 – Usługa Legitymacja radcy prawnego/aplikanta radcowskiego  
Załącznik nr 21 – Usługa PWZ pielęgniarki/PWZ położnej  
Załącznik nr 22 – Usługa Naruszenie środowiskowe  
Załącznik nr 23 – Usługa Firma  
Załącznik nr 24 – Usługa PWZ lekarza/ lekarza dentystry  
Załącznik nr 25 – Bezpiecznie w sieci  
Załącznik nr 26 – Legitymacja inżyniera budownictwa  
Załącznik nr 27 – Podpisz dokument  
Załącznik nr 28 – Uprawnienia kierowcy

## Załącznik nr 1

### Dokument mDowód

#### § 1. Definicje

1. **Profil mObywatel** – o którym mowa w Regulaminie aplikacji.
2. **Certyfikat podstawowy (zwany dalej „Certyfikatem”)** – o którym mowa w Regulaminie aplikacji.
3. **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) prezentować 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.
4. Każde działanie dotyczące potwierdzenia tożsamości, w tym przekazanie danych w celu weryfikacji, odbywa się z wyłączną zgodą użytkownika aplikacji mObywatel.

#### § 3. mDowód

1. Dokument mObywatel zawiera:
  - 1) dane użytkownika aplikacji mObywatel pobrane z rejestru PESEL:
    - a) nazwisko i imię (imiona),
    - b) numer PESEL,
    - c) datę urodzenia,
    - d) obywatelstwo,
    - e) imię ojca,
    - f) imię matki;
  - 2) fotografię użytkownika aplikacji mObywatel pobraną z Rejestru Dowodów Osobistych.
2. Seria, nr, data wydania i termin ważności dokumentu:
  - 1) Termin ważności dokumentu mDowód;
  - 2) Termin wydania dokumentu mDowód.
3. 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.

4. Za pośrednictwem dokumentu mDowód dane Użytkownika przechowywane w Aplikacji mObywatel mogą być w sposób bezpieczny prezentowane innym osobom lub przekazane Instytucji.
5. 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 usługi dokument mDowód**

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. Aby aktywować mDowód należy:
  - 1) zalogować się do Aplikacji;

- 2) potwierdzić tożsamość 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 Profilu mObywatel jest ograniczona w czasie i wynosi nie więcej niż jeden rok od daty 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 Profilu 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**

Prawidłowo aktywowany dokument po zalogowaniu się z użyciem hasła dostępu do Aplikacji, umożliwia Użytkownikowi korzystanie z następujących funkcji:

- 1) prezentowanie 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. 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, prezentowanie 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 zaprezentowaniu 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 usługi Legitymacja szkolna**

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, umożliwiającego 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. Prezentowanie Legitymacji na ekranie urządzenia mobilnego:**

- 1) zgodne z przepisami prawa prezentowanie mobilnej Legitymacji szkolnej ma skutek analogiczny jak prezentowanie 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 prezentowania.

## **§ 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 Szkoła, 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
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@cyfra.gov.pl](mailto:iod.mc@cyfra.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 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. Dane, o których mowa w art. 20 ust. 3 pkt 1 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;

13. Dane nie są przetwarzane w celach marketingowych.
14. Dane osobowe będą również przetwarzane 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 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. z 2023 r. 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 § 10 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 prezentowane 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 prezentowania 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 usługi Moje Pojazdy**

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. Aby aktywować usługę Moje pojazdy należy:
  - 1) zalogować do Aplikacji;
  - 2) wybrać z listy dostępnych usług „Moje Pojazdy”;
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 mobilnym.

## § 6. Funkcje Usługi

1. Prawidłowo aktywowana Usługa po zalogowaniu się do Aplikacji umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) prezentowanie danych pojazdu („Moje Pojazdy”);
  - 2) aktualizowanie danych pojazdu (funkcja „Aktualizuj”);
2. Użytkownik może zaprezentować 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

#### § 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 Rektora uczelni Legitymacji studenckiej i wygenerowanie danych osobowych studenta oraz danych potwierdzających status Legitymacji studenckiej.
3. **Uczelnia** – uczelnia wydająca mobilną Legitymację studencką.

#### § 2. Informacje ogólne

Usługa stanowi Legitymację studencką – usługę prezentacji dokumentu elektronicznego (legitymacji studenckiej), 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 2023 r. poz. 2787); 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, prezentowanie danych Użytkownika innym osobom lub podmiotom.

#### § 3. Użytkownicy usługi Legitymacja studencka

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, umożliwiającego dostęp do Usługi.

#### § 4. Aktywacja Usługi

1. Przy pierwszym użyciu Usługi dokonywana jest aktywacja Usługi.
2. Do przeprowadzenia aktywacji Usługi niezbędne jest aktywne połączenie internetowe.
3. Aktywacja Usługi polega na:

- 1) 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. Prezentowanie Legitymacji na ekranie urządzenia mobilnego:
  - 1) zgodne z przepisami prawa prezentowanie mobilnej Legitymacji ma skutek analogiczny jak prezentowanie 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 prezentowania.

## **§ 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
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@cyfa.gov.pl](mailto:iod.mc@cyfa.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 RODO. 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. 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.
14. Dane nie są przetwarzane w celach marketingowych.
15. Dane osobowe będą również przetwarzane przez:
  - 1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa.
16. 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.
17. Dane osobowe Studenta nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 5 do Regulaminu

### Usługa mPrawo Jazdy

#### § 1. 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 § 10 Regulaminu Aplikacji.

#### § 2. 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 prezentowanie.
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.

#### § 3. Użytkownicy usługi mPrawo Jazdy

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 o kierujących pojazdami

#### **§ 4. Aktywacja mPrawo Jazdy**

1. Aby aktywować usługę mPrawo Jazdy należy:
  - 1) zalogować się do Aplikacji;
  - 2) wybrać z listy dostępnych usług „mPrawo Jazdy”;
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.

#### **§ 5. Funkcje mPrawo Jazdy**

1. Prawidłowo aktywowane mPrawo Jazdy umożliwia Użytkownikowi korzystanie, m. in. z następujących funkcji:
  - 1) prezentowanie 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 „Potwierdź swoje dane”);
  - 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 zaprezentować 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 niebieską flagę z dwunastoma złotymi gwiazdami i skrótem „PL”;
- 2) elementu graficznego o zmiennej kolorystyce, uzależnionej od kąta pochylenia urządzenia mobilnego (hologram), w kształcie odpowiadającym Godłowi Rzeczypospolitej Polskiej;
- 3) elementy grafiki tła o zmiennej kolorystyce i napisach, uzależnionych od kąta pochylenia urządzenia mobilnego (hologram);
- 4) elementu graficznego prezentującego aktualną datę i godzinę z dokładnością do zmieniających się sekund;
- 5) elementu graficznego prezentującego datę pobrania danych tzw. „Stan na dzień”.

## **§ 6. Punkty Karne**

1. Punkty Karne to usługa Ministra dostępna wraz z mPrawo Jazdy, która umożliwia prezentację liczby punktów, o których mowa w art. 98 ust. 1 ustawy o kierujących pojazdami przypisanych kierowcy za naruszenie przepisów ruchu drogowego.
2. Aktywacja mPrawo Jazdy umożliwia Użytkownikowi dostęp do Punkty Karne.
3. 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.
4. Uwierzytelnienie w CEK umożliwia pobranie z CEK oraz prezentację w Aplikacji informacji, o której mowa w ust. 1.
5. 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 2024 r. poz. 1212).
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 oraz ust. 1d-1e ustawy o Karcie Dużej Rodziny oraz art. 69 ust. 1 ustawy o aplikacji mObywatel.
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, przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie 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 usługi Karta Dużej Rodziny**

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. Aby aktywować usługę KDR należy:
  - 1) zalogować się do Aplikacji;
  - 2) wybrać „KDR” z listy dostępnych usług;
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) prezentowanie danych Użytkownika KDR oraz kodu QR (widok główny „KDR”);
  - 2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - 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 zaprezentować 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) prezentowanie danych Użytkownika oraz kodu QR (widok główny „KDR”);
  - 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) aktualizacji informacji na temat uprawnień wraz z powiązаныmi z nimi danymi Użytkownika (funkcja „Aktualizuj”);
  - 3) usunięcie KDR z Aplikacji (funkcja „Usuń KDR”).
2. Użytkownik może zaprezentować 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
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@cyrfa.gov.pl](mailto:iod.mc@cyrfa.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 RODO:
  - 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 art. 20 ust. 3 pkt 1 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;
13. Minister nie gromadzi informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych. Dane nie są przetwarzane w celach marketingowych.

14. Dane osobowe, przetwarzane w systemie teleinformatycznym, o którym mowa w art. 19 ust. 1 stawy o aplikacji mObywatel, nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
15. Dane osobowe będą również przetwarzane przez:  
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.

## Załącznik nr 7 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 późn. zm.
4. **PKP Intercity lub PKP** – „PKP Intercity” Spółka Akcyjna z siedzibą w Warszawie (KRS 0000296032, NIP 526 25 44 258) będąca dystrybutorem ulgowych usług transportowych zgodnie z Porozumieniem w sprawie ulgowych usług transportowych zawartym w dniu 27 listopada 2013 r. oraz podmiotem odpowiedzialnym za wydawanie Legitymacji UUT.
5. **Pracodawca** – PKP Intercity lub podmiot, który wystąpił do PKP Intercity o wydanie Legitymacji UUT dla Użytkownika.
6. **System UUT** – system PKP Intercity przechowujący przekazane przez pracodawców dane Użytkowników posiadających Legitymację UUT.
7. **Zasady odprawy UUT** – dokument wewnętrzny, ustalony przez pasażerskich przewoźników kolejowych, na podstawie Porozumienia w sprawie ulgowych usług transportowych z dnia 27 listopada 2013 r., który obowiązuje wyłącznie przy przejazdach osób uprawnionych do UUT pociągami tych przewoźników, wskazujący m.in. katalog osób uprawnionych do korzystania z 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, przechowywane ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie 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 usługi Legitymacja UUT**

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. Aby aktywować Legitymację UUT należy:
  - 1) zalogować do Aplikacji;
  - 2) wybrać „Legitymacja UUT” z listy dostępnych usług;
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) prezentowanie 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 „Potwierdź swoje dane”);
  - 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 zaprezentować 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) prezentowanie 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 powiązаныmi z nimi danymi Użytkownika (funkcja „Aktualizuj”);
  - 5) usunięcie Legitymacji UUT z Aplikacji (funkcja „Usuń Legitymację UUT”).
2. Użytkownik może zaprezentować 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) gilosa 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 Legitymacji 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 Dii.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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl). Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować w sprawach związanych z przetwarzaniem danych osobowych przez Ministra właściwego do spraw informatyzacji (Ministra Cyfryzacji) bezpośrednio pod adresem: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)

3. W ramach usługi Legitymacja UUT w Aplikacji przechowuje się następujące dane:
  - 1) Wizerunek twarzy użytkownika;
  - 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.
4. 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.
5. 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.
6. Dane, o których mowa w ust. 8, 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.
7. Dane, o których mowa w ust. 8, przechowywane są do roku od dnia utraty Legitymacji UUT. Dane nie są przetwarzane w celach marketingowych.

8. Minister nie gromadzi informacji o skorzystaniu przez Użytkowników z funkcji elektronicznego przekazania danych.
9. 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.
10. Dane osobowe będą również przetwarzane 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.

## Załącznik nr 8 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 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.
2. Korzystanie z Diia.pl nie zwalnia Użytkownika z obowiązków wynikających z przepisów prawa. Zbieranie danych innych użytkowników, posługiwanie się nimi czy ich publikacja podlegają ograniczeniom prawnym wynikającym m.in. z przepisów służących ochronie danych osobowych, dóbr osobistych i prywatności.
3. Postanowienia dotyczące zasad przetwarzania danych osobowych zostały zamieszczone w § 10 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 prezentowane 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 usługi Diia.pl**

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. Aby aktywować usługę Diia.pl należy:
  - 1) zalogować do Aplikacji;
  - 2) potwierdzić tożsamość 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 usług Diia.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 prezentowanie danych użytkownika i jego dzieci,
  - 2) uruchomienie usług:
    - a) UCC,
    - b) Recepty;
  - 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”).
2. Użytkownik może zaprezentować 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:
  - 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 Diia.pl, 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.

## Załącznik nr 9 do Regulaminu

### Legitymacja emeryta-rencisty ZUS

#### § 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 prezentowanego 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 2023 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 r. w sprawie legitymacji emeryta-rencisty (Dz. U. poz. 560), 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 Legitymacji, 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.

#### **§ 4. Użytkownicy usługi Legitymacja emeryta-rencisty**

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.

#### **§ 3. Legitymacja emeryta-rencisty**

1. Legitymacja emeryta-rencisty pozwala na pobranie przez Użytkownika danych z bazy Rejestru ZUS oraz z usługi mObywatel, przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie 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.

#### **§ 5. Aktywacja usługi Legitymacja emeryta - rencisty**

1. Aby aktywować usługę Legitymacja emeryta-rencisty należy:
  - 1) zalogować się do aplikacji mObywatel;
  - 2) wybrać „Legitymacja emeryta-rencisty” z listy dostępnych usług;
2. Ważność Legitymacji powiązana jest z ważnością Certyfikatu.
3. Certyfikat podstawowy jest wykorzystywany do:
  - 1) pobrania i podpisania danych w 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 Legitymację emeryta-rencisty i pobrać dane z Rejestru ZUS wyłącznie na jednym urządzeniu.
  5. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, 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 Legitymacji emeryta - rencisty**

1. Prawidłowo aktywowana usługa Legitymacja emeryta-rencisty umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;
  - 2) przekazania danych Użytkownika w celu weryfikacji (funkcja „Przełącz”);
  - 3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - 4) usunięcie mobilnej Legitymacji emeryta-rencisty z Aplikacji (funkcja „Usuń Legitymację emeryta-rencisty”).
2. Użytkownik może zaprezentować innej osobie 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 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@mc.gov.pl
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym — w sprawach związanych z przetwarzaniem danych osobowych — można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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 Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach 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 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.
2. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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 prezentowania 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.
  - 1) Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
  - 2) 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. Dane nie są przetwarzane w celach marketingowych.
7. 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.
8. 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.
9. 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,
10. 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.
11. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.



## Załącznik nr 10 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. z 2024 r. poz. 1564) 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 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 Legitymacji, są nieprawidłowe lub nieaktualne, należy zgłosić się do okręgowej rady adwokackiej.
3. Korzystanie z 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, przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie 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 usługi Legitymacja adwokacka**

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. Aby aktywować usługę Legitymacja adwokacka należy:
  - 1) zalogować się do aplikacji mObywatel;;
  - 2) wybrać „Legitymacja adwokacka” z listy dostępnych usług;
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 Legitymację adwokacką i pobrać dane z KRAiAA wyłącznie na jednym urządzeniu.
4. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Legitymacja adwokacka nie oferuje funkcji eksportu ani importu danych.

5. Dostęp do danych przechowywanych w 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) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;
  - 2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - 3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - 4) usunięcie mobilnej Legitymacji adwokackiej z Aplikacji (funkcja „Usuń Legitymację adwokacką”).
2. Użytkownik może zaprezentować 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) gilosa umieszczonego jako tło Legitymacji adwokackiej, 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](mailto: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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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. 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 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.
6. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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 prezentowania 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 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. 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,
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 11 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 2024 r. poz. 907).
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 mobilnej 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, przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie 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 usługi Legitymacja poselska**

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

#### **§ 5. Aktywacja usługi Legitymacja poselska**

3. Aby aktywować usługę Legitymacja poselska należy:
  - a) Zalogować się do aplikacji mObywatel;
  - b) wybrać „Legitymacja poselska” z listy dostępnych usług;
4. Ważność Legitymacji powiązana jest z ważnością Certyfikatu.
5. Certyfikat podstawowy jest wykorzystywany do:
  - a) pobrania i podpisania danych w mobilnej Legitymacji poselskiej;
  - b) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z SIS;
  - c) 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 wyłącznie na jednym urządzeniu.
6. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Legitymacja nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w Legitymacji jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

#### **§ 6. Funkcje Legitymacji poselskiej**

1. Prawidłowo aktywowana usługa Legitymacja poselska umożliwia Użytkownikowi

korzystanie z następujących funkcji:

- 1) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;
  - 2) przekazania danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - 3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - 4) usunięcie mobilnej Legitymacji poselskiej z Aplikacji (funkcja „Usuń Legitymację poselską”).
2. Użytkownik może prezentować innej osobie 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](mailto: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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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 .

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. Prezentowanie oraz elektroniczne przekazanie danych następują dobrowolnie. Prezentowanie 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 prezentowania 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. Dane nie są przetwarzane w celach marketingowych.
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 12 do Regulaminu

### Usługa ePłatności

#### § 1. Definicje:

1. **Usługa ePłatności (PeP)** – usługa z wykorzystaniem platformy ePłatności umożliwiająca wykonywanie przez obywateli opłat online w zakresie objętym pilotażem, 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 lub karty płatniczej.

#### § 2. Informacje ogólne

1. Usługa ePłatności umożliwia uiszczenie opłat:
  - a) wystawionych przez urzędy do aplikacji mObywatel;
  - b) wystawionych przy okazji wizyty w urzędzie oraz zainicjowanych przez urzędnika;
  - c) utworzonych przez obywatela na własne potrzeby, przed wizytą w urzędzie (tzw. skarbowe).
2. Metody płatności uzależnione są od integracji urzędu. Usługa w aplikacji mObywatel przewiduje następujące metody:
  - a) BLIK;
  - b) BLIK bez kodu;
  - c) Karta płatnicza.

#### § 3. Usługa ePłatności

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

#### **§ 4. Użytkownicy usługi ePłatności**

Użytkownikami korzystającymi z usługi ePłatności mogą być wyłącznie osoby, które, spełniają poniższe warunki:

- a) mają ważny Certyfikat;
- b) mają aktywowany dokument mDowód;

#### **§ 5. Aktywacja Usługi ePłatności**

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

#### **§ 6. Funkcje w Usłudze ePłatności dla Użytkowników**

1. Prawidłowo aktywowana Usługa e-Płatności umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - a) opłacenia za pomocą szybkiej płatności BLIK lub karty płatniczej zobowiązania finansowego udostępnionego przez Organ podatkowy (funkcja „Zapłać”);
  - b) tworzenia płatności przez obywatela na własne potrzeby, przed wizytą w urzędzie (funkcja Utwórz płatność);
  - c) pobranie potwierdzenia przelewu – EPO (funkcja „Pobierz”/ „Pobierz potwierdzenie”);
  - d) przegląd wszystkich Transakcji płatnicza (funkcja „Historia płatności”).

#### **§ 7. Klauzula informacyjna**

1. Administratorem danych Użytkownika aplikacji mObywatel oraz Certyfikatu jest Minister 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)

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@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl).
4. 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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
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) 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.
6. 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. Dane nie są przetwarzane w celach marketingowych.
7. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji, to jest przez: Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa.
8. 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.
9. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 13 do Regulaminu

### Rejestr Upoważnień (WRU)

#### § 1. Definicje:

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

#### § 2. Informacje ogólne

1. Uwierzytelnienie obywatela w celu pobrania Upoważnienia do aplikacji mObywatel będzie odbywało się w oparciu o certyfikat usługi mObywatel.
2. Usługa Rejestr Upoważnień jest przeznaczona dla podmiotów, które nie posiadają rozwiązań technicznych (API) oraz własnych rejestrów danych, umożliwiających integrację z Aplikacją mObywatel.

#### § 3. Rejestr Upoważnień

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

#### § 4. Użytkownicy usługi Rejestr Upoważnień

Użytkownikami korzystającymi z Rejestru Upoważnień 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. Aby aktywować usługę Rejestr Uprawnień należy:
  - 1) Zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Rejestr Uprawnień” z listy dostępnych usług;
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) prezentowanie 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 zaprezentować 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 „Potwierdź swoje dane” pozwala na przekazanie do weryfikacji usłudze mWeryfikator danych Użytkownika Rejestru Upoważnień w postaci kodu QR. Przekazanie danych przebiega w następujący sposób:
  - 1) Użytkownik w Rejestrze Upoważnień wywołuje funkcję „Potwierdź swoje dane”;
  - 2) w Rejestrze Upoważnień 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 Upoważnień Użytkownika następuje również automatycznie w przypadku dezaktywacji Usługi mObywatel.

## **§ 7. Klauzula informacyjna**

1. Administratorem danych osobowych Użytkownika pobieranych z systemu Rejestr Upoważnień jest wydająca upoważnienie Instytucja. Informacja o przetwarzaniu danych osobowych znajduje się na stronie internetowej danej instytucji. W odniesieniu do tych danych Minister Cyfryzacji jest podmiotem przetwarzającym.
2. Administratorem danych Użytkownika aplikacji mObywatel, Certyfikatu oraz danych osobowych pracowników Podmiotów obsługujących Rejestr Upoważnień 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
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@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
5. W ramach usługi Rejestr Upoważnień w Aplikacji przechowuje się następujące dane Użytkownika:
  - 1) imię pierwsze posiadacza Upoważnienia;
  - 2) imię drugie posiadacza Upoważnienia;
  - 3) nazwisko posiadacza Upoważnienia;
  - 4) numer PESEL posiadacza Upoważnienia;
  - 5) wizerunek twarzy posiadacza Upoważnienia;
  - 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 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. 15 i 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. 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.
8. 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. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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 prezentowania 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 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. Dane nie są przetwarzane w celach marketingowych.
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, 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

### Usługa Tymczasowe elektroniczne Prawo Jazdy

#### § 1. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach dokumentu Tymczasowe elektroniczne Prawo Jazdy stanowi art. 10a ustawy o kierujących pojazdami.
2. 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
3. Tymczasowe elektroniczne Prawo Jazdy jest dokumentem elektronicznym stwierdzającym uprawnienie do kierowania pojazdem na podstawie art. 4 ust. 1a ustawy o kierujących pojazdami.
4. Posiadanie Tymczasowego elektronicznego prawa jazdy nie zwalnia użytkownika z dopełnienia formalności związanych z wydaniem prawa jazdy we właściwym wydziale komunikacji.
5. Użytkownik, któremu wydano prawo jazdy, albo którego Tymczasowe elektroniczne prawo jazdy jest unieważnione jest zobowiązany do skorzystania z funkcji „Aktualizuj” w celu usunięcia Tymczasowego elektronicznego prawa jazdy z widoku w aplikacji.
6. Prowadzenie pojazdu po upływie okresu ważności Tymczasowego elektronicznego Prawa Jazdy a przed wydaniem prawa jazdy podlega karze na podstawie art. 95 § 2 ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 2023 r. poz. 2119, z późn. zm.).

#### § 2. Tymczasowe elektroniczne Prawo Jazdy

1. Tymczasowe elektroniczne Prawo Jazdy powstaje w wyniku pobrania przez Użytkownika danych osobowych z usługi mObywatel i powiązanych z nimi uprawnień do kierowania pojazdami z bazy CEK.
2. Wiarygodność danych dostępnych w Tymczasowym elektronicznym Prawie 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 przyłączonego do Węzła Krajowego (login.gov.pl) bezpośrednio albo za pośrednictwem węzła transgranicznego.
3. Nie jest możliwe posługiwanie się Tymczasowym elektronicznym Prawem Jazdy poza terytorium RP.
4. Do aktywacji i aktualizacji Tymczasowego elektronicznego Prawa Jazdy niezbędne jest posiadanie ważnego Certyfikatu.

### **§ 3. Użytkownicy usługi Tymczasowe elektroniczne Prawo Jazdy**

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

- 1) posiadają ważny Certyfikat;
- 2) mają aktywowany dokument mDowód lub legitymację szkolną;
- 3) uzyskały pozytywny wyniku egzaminu państwowego.

### **§ 4. Aktywacja Tymczasowego elektronicznego Prawa Jazdy**

1. Aby aktywować Tymczasowe elektroniczne Prawo Jazdy należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać z listy dostępnych usług „mPrawo Jazdy (również tymczasowe)”;
2. Ważność Tymczasowego elektronicznego Prawa Jazdy powiązana jest z ważnością Certyfikatu.
3. Certyfikat jest wykorzystywany do:
  - 1) potwierdzenia tożsamości Użytkownika;
  - 2) podpisania danych w Tymczasowym elektronicznym Prawie Jazdy;
  - 3) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z CEK;
  - 4) zapewnienia, iż przekazywane dane w ramach Tymczasowego elektronicznego Prawa 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 Tymczasowe elektroniczne Prawo Jazdy i pobrać dane z CEK na jednym urządzeniu.
6. Poza funkcjami prezentacji uprawnień, przekazania w celu skorzystania z usług Instytucji, a także ich weryfikacji uprawnień - Tymczasowe elektroniczne Prawo Jazdy nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w Tymczasowym elektronicznym Prawie Jazdy jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

### **§ 5. Funkcje Tymczasowego elektronicznego Prawa Jazdy**

1. Prawidłowo aktywowana usługa Tymczasowe elektroniczne Prawo Jazdy umożliwia Użytkownikowi korzystanie, m.in. z następujących funkcji:
  - 1) prezentowanie danych Użytkownika;
  - 2) przekazania danych Użytkownika w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - 3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - 4) usunięcie Tymczasowego Prawa Jazdy z Aplikacji (funkcja „Usuń Tymczasowe Prawo Jazdy”).

2. Użytkownik może zaprezentować innej osobie Tymczasowe elektroniczne Prawo Jazdy; funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu usługi Tymczasowe elektroniczne Prawo Jazdy. 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) gilosa umieszczonego jako tło Tymczasowego elektronicznego Prawa Jazdy, 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 Usługi Tymczasowe elektronicznego Prawo Jazdy następuje również automatycznie w przypadku unieważnienia Certyfikatu lub Certyfikatu wydanego uczniowi z Legitymacją szkolną. Usługa Tymczasowe elektroniczne Prawo Jazdy jest również usuwana, gdy Użytkownik skorzysta z funkcji „Aktualizuj”, a zostało mu już wydane prawo jazdy.

## Załącznik nr 15 do Regulaminu

### Centralny Rejestr Wyborców

#### § 1. Informacje ogólne

1. Wydarzenia wyborcze – należy przez to rozumieć wybory do Sejmu i Senatu, wybory Prezydenta Rzeczypospolitej, wybory do Parlamentu Europejskiego w Rzeczypospolitej Polskiej, wybory do organów stanowiących jednostek samorządu terytorialnego oraz wybory wójtów, burmistrzów i prezydentów miast, a także referenda ogólnokrajowe i referenda lokalne.
2. Uwierzytelnienie obywatela w celu pobrania Uprawnienia do aplikacji mObywatel będzie odbywało się w oparciu o certyfikat usługi mObywatel, Certyfikat wydany uczniowi z Legitymacją szkolną lub Certyfikat wydany użytkownikowi z Legitymacją studencką.
3. W zakresie Usługi Centralny Rejestr Wyborców 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;

#### § 2. Centralny Rejestr Wyborców

1. Centralny Rejestr Wyborców pozwala na pobranie przez Użytkownika danych na temat posiadania czynnego prawa wyborczego, wyświetlenie listy zbliżających się wydarzeń wyborczych oraz ich szczegółów, a także wyświetlenie danych obywatela znajdujących się w Centralnym Rejestrze Wyborców.
2. Wiarygodność danych dostępnych w Centralnym Rejestrze Wyborców wynika z faktu, że dane pochodzą z rejestru państwowego i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem lub Certyfikatem wydanym uczniowi z Legitymacją szkolną.
3. Posługiwanie się Centralnym Rejestrem Wyborców przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem.

#### § 3. Użytkownicy Usługi Centralny Rejestr Wyborców

1. Użytkownikami korzystającymi z Centralnego Rejestru Wyborców mogą być wyłącznie osoby, które spełniają poniższe warunki:
  - 1) mają ważny Certyfikat lub Certyfikat wydany uczniowi z Legitymacją szkolną.
  - 2) posiadają obywatelstwo polskie oraz ukończyli 17 lat lub są mieszkańcami Unii Europejskiej (innych niż Polska) lub Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, którzy dopisali się do spisu wyborców.
  - 3) zostały wpisane do Centralnego Rejestru Wyborców.
2. Użytkownicy, którzy nie zostali wpisani do Centralnego Rejestru Wyborców (w tym obywatele polscy, którzy nie ukończyli 17 roku życia), przy próbie skorzystania z usługi

otrzymają komunikat, że w Centralnym Rejestrze Wyborców nie ma ich danych.

#### **§ 4. Aktywacja Centralnego Rejestru Wyborców**

1. Aby aktywować Centralny Rejestr Wyborców należy:
  - 1) Zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Centralny Rejestr Wyborców” z listy dostępnych usług;
2. Certyfikat jest wykorzystywany do:
  - 1) pobrania i podpisania danych w Centralnym Rejestrze Wyborców;
  - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z Centralnego Rejestru Wyborców;
  - 3) zapewnienia, że przekazywane dane w ramach Upewnienia są tożsame z danymi pobranymi z Centralnego Rejestru Wyborców oraz usługi mObywatel.
3. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z systemu Centralnego Rejestru Wyborców niezbędne jest aktywne połączenie internetowe.
4. Użytkownik może aktywować Centralny Rejestr Wyborców i pobrać dane tylko na jednym urządzeniu mobilnym.

#### **§ 5. Funkcje Centralnego Rejestru Wyborców dla Użytkowników usługi mObywatel**

1. Prawidłowo aktywowana usługa Centralnego Rejestru Wyborców umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) sprawdzenie czy Użytkownik posiada czynne prawa wyborcze;
  - 2) wyświetlenie listy zbliżających się wydarzeń wyborczych;
  - 3) Wyświetlenie danych użytkownika znajdujących się w Centralnym Rejestrze Wyborców;
  - 4) Wyświetlenie szczegółów wydarzenia wyborczego.
2. Aplikacja mObywatel nie przechowuje danych Użytkownika pobranych przez usługę Centralnego Rejestru Wyborców.
3. Usługa Centralny Rejestr Wyborców nie umożliwia Użytkownikowi wykonania następujących czynności:
  - 1) zmiany miejsca głosowania;
  - 2) zmiany stałego obwodu głosowania;
  - 3) zgłoszenia zamiaru głosowania przez pełnomocnika;
  - 4) zgłoszenia zamiaru głosowania korespondencyjnego.
4. Czynności wymienione w § 5 ust. 3 realizowane są przez dedykowane usługi online.

## Załącznik nr 16 do Regulaminu

### Usługa Mandaty

#### § 1. Informacje ogólne

1. Uwierzytelnienie obywatela w celu pobrania Uprawnienia do aplikacji mObywatel będzie odbywało się w oparciu o certyfikat usługi mObywatel.
2. W zakresie Usługi Tymczasowe Elektroniczne Prawo 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;

#### § 2. Mandaty

1. Usługa Mandaty pozwala na pobranie przez Użytkownika danych na temat otrzymanych mandatów fiskalnych w podziale na opłacone i nieopłacone.
2. Wiarygodność danych dostępnych w usłudze Mandaty wynika z faktu, że dane pochodzą z Systemu e-Urząd Skarbowy i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
3. Posługiwanie się usługą Mandaty przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem.
4. Dane udostępnianie w usłudze Mandaty nie stanowią mandatu ani go nie zastępują.

#### § 3. Użytkownicy usługi Mandaty

Użytkownikami korzystającymi z usługi Mandaty mogą być wyłącznie osoby, które spełniają poniższe warunki:

- 1) mają ważny Certyfikat;
- 2) mają aktywowany dokument mDowód.

#### § 4. Aktywacja usługi Mandaty

1. Aby aktywować usługę Mandaty należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Mandaty” z listy dostępnych usług;
2. Certyfikat jest wykorzystywany do:
  - 1) pobrania i podpisania danych w usłudze Mandaty;
  - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z usługi Mandaty;
3. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych niezbędne jest aktywne połączenie internetowe.
4. Użytkownik może aktywować usługę tylko na jednym urządzeniu mobilnym.

## **§ 5. Funkcje usługi Mandaty dla Użytkowników usługi mObywatel**

1. Prawidłowo aktywowana usługa Mandaty umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) Wyświetlenie listy mandatów nieopłaconych;
  - 2) Wyświetlenie listy mandatów opłaconych;
  - 3) Wyświetlenie szczegółów mandatu.
2. Aplikacja mObywatel nie przechowuje danych Użytkownika pobranych przez usługę Mandaty.
3. Usługa Mandaty nie umożliwia Użytkownikowi opłacenia mandatów.

## Załącznik nr 17 do Regulaminu

### Usługa e-Wizyta w ZUS

#### § 1. Informacje ogólne

Uwierzytelnienie obywatela w celu pobrania Uprawnienia do aplikacji mObywatel będzie odbywało się w oparciu o certyfikat usługi mObywatel, Certyfikat wydany uczniowi z Legitymacją szkolną, Certyfikat wydany użytkownikowi z Legitymacją studencką lub Certyfikat wydany użytkownikowi wraz z Diia.pl.

#### § 2. e-Wizyta w ZUS

1. Usługa e-Wizyta w ZUS pozwala na umówienie użytkownika na wideorozmowę z pracownikiem ZUS, weryfikację statusu wizyty oraz zarządzanie rezerwacją.
2. Dane wprowadzone przez użytkownika są przekazywane do systemu informatycznego ZUS.
3. Posługiwanie się usługą e-Wizyta w ZUS przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem.
4. 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. Użytkownicy usługi e-Wizyta w ZUS

Użytkownikami korzystającymi z usługi e-Wizyta w ZUS mogą być wyłącznie osoby, które spełniają poniższe warunki:

- 1) mają ważny Certyfikat, Certyfikat wydany uczniowi z Legitymacją szkolną, Certyfikat wydany użytkownikowi z Legitymacją studencką lub Certyfikat wydany użytkownikowi wraz z Diia.pl.
- 2) mają aktywowany dokument mDowód, Legitymację szkolną, Legitymację studencką lub dokument Diia.pl.

#### § 4. Aktywacja usługi e-Wizyta w ZUS

Aby aktywować usługę e-Wizyta w ZUS należy:

- 1) zalogować się do Aplikacji mObywatel;
- 2) wybrać „e-Wizyta w ZUS” z listy dostępnych usług;

## **§ 5. Funkcje usługi e-Wizyta w ZUS dla Użytkowników usługi mObywatel**

1. Prawidłowo aktywowana usługa e-Wizyta w ZUS umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) Umówienie wizyty w tematach:
    - a) Potwierdzenie profilu PUE i świadczenia dla rodzin (500+ i inne),
    - b) Emerytury i renty krajowe – także w języku PJM,
    - c) Emerytury i renty międzynarodowe,
    - d) Zasiłki i zwolnienia lekarskie – także w języku PJM,
    - e) Ulgi i umorzenia,
    - f) Firmy i pracownicy;
  - 2) Prezentację umówionych wizyt;
  - 3) Weryfikację szczegółów e-Wizyty;
  - 4) Odwołanie e-Wizyty;
  - 5) Dołączenie do wizyty.
2. Aplikacja mObywatel nie przechowuje danych Użytkownika pobranych przez usługę e-Wizyta w ZUS.
3. Usługa e-Wizyta w ZUS służy wyłącznie do umówienia wizyty. Obsługa wideorozmowy jest realizowana przez dedykowane rozwiązania ZUS.

## **§ 6. Klauzula informacyjna**

1. Administratorem danych osobowych w zakresie imienia, nazwiska, numeru PESEL, adresu poczty elektronicznej, numeru telefonu, imienia i nazwiska opiekuna faktycznego i prawnego, imienia i nazwiska tłumacza jest Zakład Ubezpieczeń Społecznych z siedzibą przy ul. Szamocka 3,5, 01-748 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 siedziby Administratora bądź na adres e-mail: [odo@zus.pl](mailto:odo@zus.pl). Administratorem danych osobowych w zakresie imienia, nazwiska, numeru PESEL jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą przy ul. Królewskiej 27, 00-060 Warszawa.
3. Z administratorem można kontaktować się korespondencyjnie na adres siedziby bądź drogą elektroniczną na adres: [Kancelaria@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
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@cyrfa.gov.pl](mailto:iod.mc@cyrfa.gov.pl)

5. 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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
6. 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.
7. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez: Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
8. 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.
9. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
10. Dane nie są przetwarzane w celach marketingowych.

## Załącznik nr 18 do Regulaminu

### Usługa Zastrzeż PESEL

#### § 1. Informacje ogólne

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

#### § 2. Zastrzeż PESEL

1. Usługa pozwala na: weryfikację i zmianę statusu zastrzeżenia numeru PESEL, pobranie przez Użytkownika danych na temat zastrzeżenia swojego numeru PESEL, zmian statusu zastrzeżenia numeru PESEL oraz informacji kto i kiedy sprawdzał czy jego numer PESEL jest zastrzeżony.
2. Wiarygodność danych dostępnych w usłudze wynika z faktu, że pochodzą one z rejestru państwowego i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
3. Posługiwanie się Usługą Zastrzeż PESEL przez Użytkowników jest dobrowolne, nieodpłatne i nie jest prawnym obowiązkiem.

#### § 3. Użytkownicy

Użytkownikami korzystającymi z Zastrzeż PESEL mogą być wyłącznie osoby, które spełniają poniższe warunki:

- 1) mają ważny Certyfikat.
- 2) są pełnoletnie i posiadają pełną zdolność do czynności prawnych.

#### § 4. Aktywacja usługi Zastrzeż PESEL

1. Aby aktywować usługę Zastrzeż PESEL należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Zastrzeż PESEL” z listy dostępnych usług;
2. Certyfikat jest wykorzystywany do:
  - 1) pobrania i podpisania danych w usłudze Zastrzeż PESEL;
  - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z rejestru zastrzeżeń numerów PESEL;
  - 3) zapewnienia, że przekazywane dane w ramach Uprawnienia są tożsame z danymi pobranymi z rejestru zastrzeżeń numerów PESEL oraz usługi mObywatel.
3. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z rejestru zastrzeżeń numerów PESEL niezbędne jest aktywne połączenie internetowe.
4. Użytkownik może aktywować Usługę i pobrać dane tylko na jednym urządzeniu mobilnym.

## **§ 5. Funkcje rejestru zastrzeżeń numerów PESEL dla Użytkowników usługi mObywatel**

1. Prawidłowo aktywowana usługa Zastrzeż PESEL umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) Zastrzeżenie i cofnięcie zastrzeżenia numeru PESEL;
  - 2) Przeglądanie historii zastrzeżeń swojego numeru PESEL;
  - 3) Przeglądanie historii weryfikacji zastrzeżenia swojego numeru PESEL.
2. Usługa Zastrzeż PESEL nie umożliwia Użytkownikowi wykonania następujących czynności:
  - 1) zastrzeżenia jego numeru PESEL przez pełnomocnika;
  - 2) zastrzeżenia i cofnięcia zastrzeżenia jego numeru PESEL przez opiekuna prawnego albo kuratora.
3. Czynności wymienione w § 5 ust. 2 realizowane są w dowolnym urzędzie gminy.

## **§ 7. Klauzula informacyjna**

1. Administratorem danych Użytkownika aplikacji mObywatel oraz Certyfikatu jest Minister 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl)
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@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
4. 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. Ponadto art. 23b ustawy o ewidencji ludności, w szczególności ust. 3 który stanowi, że: Minister właściwy do spraw informatyzacji jest administratorem rejestru zastrzeżeń numerów PESEL.
5. 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.
  - 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.

6. 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. Dane nie są przetwarzane w celach marketingowych.
7. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:  
Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
8. 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.
9. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 19 do Regulaminu

### Sprawdź PESEL

#### § 1. Informacje ogólne

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

#### § 2. Sprawdz PESEL

1. Usługa pozwala na sprawdzenie czy numer PESEL innej osoby pełnoletniej jest lub był zastrzeżony.
2. Wiarygodność danych dostępnych w usłudze wynika z faktu, że dane pochodzą z rejestru państwowego i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem.
3. Posługiwanie się Usługą przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem.

#### § 3. Użytkownicy

Użytkownikami korzystającymi z Sprawdz PESEL mogą być wyłącznie osoby, które spełniają poniższe warunki:

- 1) mają ważny Certyfikat.
- 2) są pełnoletnie i posiadają pełną zdolność do czynności prawnych.

#### § 4. Aktywacja usługi Sprawdz PESEL

1. Aby aktywować usługę Sprawdz PESEL należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Sprawdz PESEL” z listy dostępnych usług;
2. W przypadku sprawdzania statusu zastrzeżenia numeru PESEL w imieniu firmy lub instytucji użytkownik podaje dodatkowe dane identyfikujące ten podmiot:
  - 1) nr NIP, REGON lub KRS;
  - 2) nazwę firmy lub instytucji;
  - 3) dane adresowe firmy lub instytucji (miejscowość, kod pocztowy, ulicę, numer domu, numer lokalu).
3. Certyfikat jest wykorzystywany do:
  - 1) pobrania i podpisania danych w usłudze Sprawdz PESEL;
  - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z rejestru zastrzeżeń numerów PESEL;
  - 3) zapewnienia, że przekazywane dane w ramach Uprawnienia są tożsame z danymi pobranymi z rejestru zastrzeżeń numerów PESEL oraz usługi mObywatel.

4. Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z rejestru zastrzeżeń numerów PESEL niezbędne jest aktywne połączenie internetowe.
5. Użytkownik może aktywować Usługę i pobrać dane tylko na jednym urządzeniu mobilnym.

#### **§ 5. Funkcje rejestru zastrzeżeń numerów PESEL dla Użytkowników usługi mObywatel**

Prawidłowo aktywowana usługa Sprawdź PESEL umożliwia Użytkownikowi korzystanie z następujących funkcji:

- 1) Sprawdzenie statusu zastrzeżenia numeru PESEL w imieniu własnym albo firmy lub instytucji i sprawdzenie statusu zastrzeżenia numeru PESEL w obecnej chwili albo w danym dniu z przeszłości.

#### **§ 6. Klauzula informacyjna**

1. Administratorem danych Użytkownika aplikacji mObywatel oraz Certyfikatu jest Minister 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@cyfra.gov.pl](mailto:Kancelaria@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@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
4. 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. 3 ust. 1 pkt 1-3 ustawy o aplikacji mObywatel.
5. 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.
  - 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.

6. 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. Dane nie są przetwarzane w celach marketingowych.
7. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:  
Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
8. 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.
9. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 20 do Regulaminu

### Legitymacja radcy prawnego/aplikanta radcowskiego

#### § 1. Definicje:

1. **KRRP** - Krajowy Rejestr Radców Prawnych
2. **Radca prawny** – osoba wpisana na listę radców prawnych, o której mowa w przepisach ustawy z dnia 6 lipca 1982 r. o radcach prawnych.
3. **Aplikant radcowski** – osoba wpisana na listę aplikantów radcowskich, która wykonuje zadania określone w art. 35 ustawy z dnia 6 lipca 1982 r. o radcach prawnych.
4. **Legitymacja radcy prawnego/aplikanta radcowskiego** – dokument wydany przez Okręgową Izbę Radców Prawnych na podstawie ustawy z dnia 6 lipca 1982 r. o radcach prawnych ( Dz. U. z 2024 r. poz. 499) oraz uchwały nr 68/VIII/2011 KRRP z dnia 1 października 2011 roku w sprawie wzoru legitymacji radcy prawnego, wzoru legitymacji aplikanta radcowskiego oraz wzoru legitymacji prawnika zagranicznego, 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.
5. **OIRP** – Okręgowa Izba Radców Prawnych.

#### § 2 Informacje ogólne

1. Podstawę prawną pobrania danych w ramach Legitymacji radcy prawnego/aplikanta radcowskiego 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 radcy prawnego/aplikanta radcowskiego 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 aplikacji mObywatel, są nieprawidłowe lub nieaktualne, należy zgłosić się do Okręgowej Izby Radców Prawnych.
3. 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 radcy prawnego/aplikanta radcowskiego posiadaczowi legitymacji radcy prawnego/aplikanta radcowskiego, wpisanemu na listę radców prawnych lub listę aplikantów radcowskich.
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 radcy prawnego/aplikanta radcowskiego**

1. Legitymacja radcy prawnego/aplikanta radcowskiego umożliwia pobranie przez Użytkownika danych z KRRP celem wyświetlania legitymacji.
2. Dane dostępne w Legitymacji radcy prawnego/aplikanta radcowskiego pochodzą z KRRP i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem podstawowym.
3. Posługiwanie się mobilną Legitymacją radcy prawnego/aplikanta radcowskiego przez Użytkowników jest dobrowolne
4. Do aktywacji i aktualizacji Legitymacji rady prawnego/aplikanta radcowskiego niezbędne jest posiadanie ważnego wpisu na listę aplikantów radcowskich, radców prawnych lub prawników zagranicznych prowadzoną przez właściwą Okręgową Izbę Radców Prawnych.

### **§ 4. Aktywacja usługi Legitymacja radcy prawnego/aplikanta radcowskiego**

1. Aby aktywować usługę Legitymacja radcy prawnego/aplikanta radcowskiego w Aplikacji należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Legitymacja radcy prawnego/aplikanta radcowskiego” z listy dostępnych usług;
2. Certyfikat podstawowy jest wykorzystywany do:
  - 1) pobrania i podpisania danych w mobilnej Legitymacji radcy prawnego/aplikanta radcowskiego;
  - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z KRRP;
  - 3) zapewnienia, że przekazywane dane w ramach usługi Legitymacja radcy prawnego/aplikanta radcowskiego są tożsame z danymi pobranymi z KRRP oraz usługi mObywatel;
  - 4) Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z KRRP niezbędne jest aktywne połączenie internetowe.
3. Użytkownik może aktywować Legitymację radcy prawnego/aplikanta radcowskiego i pobrać dane z KRRP wyłącznie na jednym urządzeniu.
4. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, Legitymacja radcy prawnego/aplikanta radcowskiego nie oferuje funkcji eksportu ani importu danych.
5. Dostęp do danych przechowywanych w Legitymacji radcy prawnego/aplikanta radcowskiego jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

## **§ 5. Funkcje mobilnej Legitymacji radcy prawnego/aplikanta radcowskiego**

1. Prawidłowo aktywowana usługa Legitymacja radcy prawnego umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;
  - 2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - 3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - 4) usunięcie mobilnej Legitymacji radcy prawnego/aplikanta radcowskiego z Aplikacji (funkcja „Usuń Legitymację radcy prawnego”).
2. Użytkownik może zaprezentować innej osobie mobilną Legitymację radcy prawnego/aplikanta radcowskiego. 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) gilosa umieszczonego jako tło Legitymacji radcy prawnego/aplikanta radcowskiego, 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 radcy prawnego/aplikanta radcowskiego z Aplikacji można dokonać poprzez działanie (sekcja” Dokumenty”, następnie ikona edycji i wybranie ikony „kosz”).
5. Usunięcie usługi Legitymacja radcy prawnego/aplikanta radcowskiego Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

## **§ 6. Klauzula informacyjna**

1. Administratorem danych osobowych, w rozumieniu Rozporządzenia 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 („RODO”), jest Krajowa Izba Radców Prawnych z siedzibą w Warszawie. 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: jest Krajowa Izba Radców Prawnych z siedzibą przy ul. Powązkowskiej 15, 01-797 Warszawa z dopiskiem „Do inspektora ochrony danych” bądź mailowo: [iod@kirp.pl](mailto:iod@kirp.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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach mobilnej Legitymacji radcy prawnego/aplikanta radcowskiego w Aplikacji przechowuje się następujące dane:
  - 1) Imię (imiona) Użytkownika mobilnej Legitymacji radcowskiej/aplikanta radcowskiego;
  - 2) nazwisko Użytkownika;
  - 3) wizerunek twarzy Użytkownika;
  - 4) numer wpisu na listę radów prawnych/aplikantów radcowskich;
  - 5) data wydania dokumentu;
  - 6) data ważności dokumentu;
  - 7) nazwa izby radcowskiej;
  - 8) organ wydający legitymację;
  - 9) rodzaj uprawnienia.
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.

9. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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 prezentowania 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 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. Dane nie są przetwarzane w celach marketingowych.
16. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu legitymacja radcy prawnego/aplikanta radcowskiego, 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:  
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. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 21 do Regulaminu

### PWZ pielęgniarki/PWZ położnej

#### § 1. Definicje:

1. Naczelna Izba Pielęgniarek i Położnych (NIPIP) - jednostka organizacyjna samorządu zawodowego pielęgniarek i położnych;
2. Naczelna Rada Pielęgniarek i Położnych (NRPIP) - organ NIPIP, który prowadzi Centralny Rejestr Pielęgniarek i Położnych;
3. Centralny Rejestr Pielęgniarek i Położnych (CRPIP) – rejestr, w którym gromadzone są dane pielęgniarek i położnych posiadających prawo wykonywania zawodu pielęgniarki lub położnej, prowadzony na podstawie art. 43 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej.
4. PWZ Pielęgniarki/ PWZ położnej – prawo wykonywania zawodu pielęgniarki/położnej

#### § 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach PWZ pielęgniarki/ PWZ położnej 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 PWZ pielęgniarki/ PWZ położnej 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 aplikacji mObywatel, są nieprawidłowe lub nieaktualne, należy zgłosić się do NRPIP.
3. Korzystanie z PWZ pielęgniarki/ PWZ położnej 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 PWZ pielęgniarki/ PWZ położnej posiadaczowi uprawnień, wskazanemu w Centralnym Rejestrze Pielęgniarek i Położnych, 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.
6. Korzystanie z dokumentu PWZ pielęgniarki/ PWZ położnej przeznaczone jest zarówno dla obywateli Polski posługujących się mDowodem, jak i dla użytkowników Diia.

### **§ 3. PWZ pielęgniarki/ PWZ położnej**

1. PWZ pielęgniarki/ PWZ położnej – pozwala na pobranie przez Użytkownika danych z Centralnego Rejestru Pielęgniarek i Położnych oraz z usługi mObywatel, przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie lub przekazywanie.
2. Dane dostępne w PWZ pielęgniarki/ PWZ położnej pochodzą z Centralnego Rejestru Pielęgniarek i Położnych i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem podstawowym.
3. Posługiwanie się mobilnym dokumentem PWZ pielęgniarki/ PWZ położnej przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej wykonujących zawód pielęgniarki lub położnej.
4. Do aktywacji i aktualizacji PWZ pielęgniarki/ PWZ położnej niezbędne jest wpisanie do Centralnego Rejestru Pielęgniarek i Położnych, na podstawie danych przekazanych do tego rejestru przez okręgowe rady pielęgniarek i położnych na podstawie art. 48 ust. 7 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej.

### **§ 4. Użytkownicy usługi PWZ pielęgniarek/ PWZ położnych**

1. Aby aktywować usługę PWZ pielęgniarki/ PWZ położnej w Aplikacji należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać „PWZ pielęgniarki/ PWZ położnej” z listy dostępnych usług;
2. Certyfikat podstawowy jest wykorzystywany do:
  - 1) pobrania i podpisania danych w PWZ pielęgniarki/ PWZ położnej;
  - 2) zabezpieczenia (zaszyfrowania) danych zawartych w dokumencie elektronicznym pobieranym z CRPIP;
  - 3) zapewnienia, że przekazywane dane w ramach usługi PWZ pielęgniarki/ PWZ położnej są tożsame z danymi pobranymi z CRPIP oraz usługi mObywatel;
  - 4) Do potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu oraz pobrania danych z CRPIP niezbędne jest aktywne połączenie internetowe.
3. Użytkownik może aktywować PWZ pielęgniarki/ PWZ położnej i pobrać dane z CRPIP wyłącznie na jednym urządzeniu.
4. Poza funkcjami prezentacji uprawnień, a także ich weryfikacji, PWZ pielęgniarki/ PWZ położnej nie oferuje funkcji eksportu ani importu danych.
5. Dostęp do danych przechowywanych w PWZ pielęgniarki/ PWZ położnej jest zabezpieczony hasłem w Aplikacji zgodnie z Regulaminem.

### **§ 5. Funkcje PWZ pielęgniarki/ PWZ położnej**

1. Prawidłowo aktywowana usługa PWZ pielęgniarki/ PWZ położnej umożliwia Użytkownikowi korzystanie z następujących funkcji:
  - 1) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;

- 2) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - 3) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - 4) usunięcie PWZ pielęgniarki/ PWZ położnej z Aplikacji (funkcja „Usuń PWZ Pielęgniarki/ PWZ Położnej”).
2. Użytkownik może zaprezentować innej osobie PWZ pielęgniarki/ PWZ położnej. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu dokumentu. 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) gilosa umieszczonego jako tło PWZ pielęgniarki/ PWZ położnej, 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 PWZ pielęgniarki/ PWZ położnej z Aplikacji można dokonać poprzez działanie (sekcja ”Dokumenty”, następnie ikona edycji i wybranie ikony „kosz”).
5. Usunięcie usługi PWZ pielęgniarki/ PWZ położnej Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

## **§ 6. Klauzula informacyjna**

1. Administratorem danych osobowych, w rozumieniu Rozporządzenia 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 („RODO”), jest Naczelna Izba Pielęgniarek i Położnych z siedzibą w Warszawie. 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: jest Naczelna Izba Pielęgniarek i Położnych z siedzibą przy ul. Pory 78 lok. 10, 02-757 Warszawa z dopiskiem „Do inspektora ochrony danych” bądź mailowo: [iod@nipip.pl](mailto:iod@nipip.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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl).

5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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 Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach PWZ pielęgniarki/ PWZ położnej w Aplikacji przechowuje się następujące dane:
  - 1) Imię (imiona) Użytkownika PWZ pielęgniarki/ PWZ położnej;
  - 2) nazwisko Użytkownika;
  - 3) wizerunek twarzy Użytkownika;
  - 4) numer wpisu na listę pielęgniarek i położnych;
  - 5) data wydania dokumentu;
  - 6) data ważności dokumentu;
  - 7) nazwa izby pielęgniarek i położnych;
  - 8) organ wydający legitymację;
  - 9) rodzaj uprawnienia.
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.
9. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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 prezentowania 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 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. Dane nie są przetwarzane w celach marketingowych.
16. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu PWZ pielęgniarce/PWZ położnej, 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. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 22 do Regulaminu

### Usługa Naruszenie środowiskowe

#### § 1. Informacje ogólne

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

#### § 2. Naruszenie środowiskowe

1. Usługa Naruszenie środowiskowe pozwala użytkownikowi na zgłoszenie wydarzenia, które może źle wpłynąć na środowisko.
2. Dane wprowadzone przez użytkownika są przekazywane do systemu informatycznego Głównego Inspektoriatu Ochrony Środowiska.
3. Posługiwanie się usługą Naruszenie środowiskowe przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem.
4. Pobranie usługi Naruszenie środowiskowe i korzystanie z niej jest nieodpłatne. Korzystanie przez Użytkownika z usług transmisji danych lub połączeń głosowych w związku z pobraniem lub korzystaniem z usługi Naruszenie środowiskowe może wiązać się z opłatami naliczanymi przez operatora telekomunikacyjnego, który świadczy Użytkownikowi usługi telekomunikacyjne.

#### § 3. Użytkownicy usługi Naruszenie środowiskowe

Użytkownikami korzystającymi z usługi Naruszenie środowiskowe mogą być wyłącznie osoby, które spełniają poniższe warunki:

- a) mają ważny Certyfikat;
- b) mają aktywowany dokument mDowód.

#### § 4. Aktywacja usługi Naruszenie środowiskowe

Aby aktywować usługę Naruszenie środowiskowe należy:

- 1) zalogować się do Aplikacji mObywatel;
- 2) wybrać „Naruszenie środowiskowe” z listy dostępnych usług.

#### § 5. Funkcje usługi Naruszenie środowiskowe dla Użytkowników usługi mObywatel

1. Prawidłowo aktywowana usługa Naruszenie środowiskowe umożliwia Użytkownikowi wysłanie zgłoszenia w zakresie jednego z rodzajów naruszeń:
  - 1) porzucenie odpadów;
  - 2) nielegalne przetwarzanie odpadów;
  - 3) zanieczyszczenie substancjami;

- 4) nielegalny transport odpadów;
  - 5) nielegalny transport odpadów z zagranicy;
  - 6) inne zdarzenia mogące negatywnie wpłynąć na środowisko.
2. Aplikacja mObywatel nie przechowuje danych Użytkownika, przekazanych za pośrednictwem usługi Naruszenie środowiskowe.
  3. Usługa Naruszenie środowiskowe służy wyłącznie do zgłoszenia naruszenia środowiskowego.
  4. Usługa Naruszenie środowiskowe umożliwia użytkownikowi wysłanie zgłoszenia z zachowaniem poufności (bez przesyłania danych osobowych do systemu informatycznego Głównego Inspektoriatu Ochrony Środowiska).

## **§ 6. Klauzula informacyjna**

1. Administratorem danych osobowych w zakresie imienia, nazwiska, numeru PESEL, adresu, adresu poczty elektronicznej, numeru telefonu jest Główny Inspektoriat Ochrony Środowiska z siedzibą przy ul. Bitwy Warszawskiej 1920 r. 3, 02-362 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 siedziby Administratora bądź na adres e-mail: [iod@gios.gov.pl](mailto:iod@gios.gov.pl). Administratorem danych osobowych w zakresie imienia, nazwiska, numeru PESEL jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą przy ul. Królewskiej 27, 00-060 Warszawa.
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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
6. 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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
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. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:
  9. 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.
  10. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
  11. Dane nie są przetwarzane w celach marketingowych.

## Załącznik nr 23 do Regulaminu

### Usługa Firma

#### § 1. Informacje ogólne

1. Usługa dostępna w aplikacji mObywatel, która umożliwia wyświetlanie danych jednoosobowej działalności gospodarczej, pobieranie zaświadczenia o wpisie do Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz udostępnianie danych do faktury.

#### § 2. Użytkownicy

2. Usługa "Firma" jest dostępna dla użytkowników prowadzących jednoosobową działalność gospodarczą, posiadających ważny certyfikat mDowodu w aplikacji mObywatel.

#### § 3. Aktywacja usługi Firma

Aktywacja usługi polega na:

1. Zalogowaniu się do aplikacji mObywatel
2. wybraniu „Firma” z listy dostępnych usług;

#### § 4. Funkcje usługi Firma dla Użytkowników usługi mObywatel

1. Usługa "Firma" pozwala na:
  - a) wyświetlanie danych jednoosobowej działalności gospodarczej (wizytówka firmy);
  - b) pobieranie zaświadczenia o wpisie do Centralnej Ewidencji i Informacji o Działalności Gospodarczej;
  - c) udostępnianie danych do faktury w ramach relacji wzajemnej fizycznej obecności stron.

#### § 5. Klauzula informacyjna

1. Administratorem danych osobowych pobranych z Centralnej Ewidencji i Informacji Działalności Gospodarczej (*imię i nazwisko; numer PESEL; dodatkowe określenia, które przedsiębiorca włącza do firmy, o ile przedsiębiorca takich używa; oznaczenie „w spadku”, jeżeli został ustanowiony zarząd sukcesyjny; numer identyfikacyjny REGON, jeżeli posiada; numer identyfikacji podatkowej (NIP), jeżeli posiada, oraz informacje o jego unieważnieniu lub uchyleniu; adres do doręczeń oraz – jeżeli przedsiębiorca takie miejsce posiada – adres stałego miejsca wykonywania działalności gospodarczej; dane dotyczące adresu są zgodne z oznaczeniami Dziennik Ustaw – 7 – Poz. 1342 1 2 3 kodowymi przyjętymi w krajowym rejestrze urzędowym podziału terytorialnego kraju, o ile to w danym przypadku możliwe; dane kontaktowe przedsiębiorcy, w szczególności adres poczty elektronicznej, adres strony internetowej, numer telefonu, o ile dane te zostały zgłoszone przez przedsiębiorcę we wniosku o wpis do CEIDG; przedmiot*

*wykonywanej działalności gospodarczej według Polskiej Klasyfikacji Działalności (PKD) na poziomie podklasy, w tym jeden przedmiot przeważającej działalności; data rozpoczęcia wykonywania działalności gospodarczej; numer identyfikacji podatkowej (NIP) oraz numer identyfikacyjny REGON spółki cywilnej, o ile przedsiębiorca zawarł umowę takiej spółki; data zawieszenia i wznowienia wykonywania działalności gospodarczej; data zaprzestania wykonywania działalności gospodarczej, o ile została zgłoszona we wniosku o wpis do CEIDG; informacja o wykreśleniu przedsiębiorcy z CEIDG) jest Minister właściwy do spraw gospodarki z siedzibą w Warszawie (00-507) ul. Pl. Trzech Krzyży 3/5. 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 siedziby Administratora bądź na adres e-mail: [iod@mrit.gov.pl](mailto:iod@mrit.gov.pl).
3. Administratorem danych osobowych w zakresie imienia, nazwiska, numeru PESEL jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą przy ul. Królewskiej 27, 00-060 Warszawa.
4. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie podstawowym jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą mającą swą siedzibę w Warszawie, przy ul. Królewskiej 27.
5. Z administratorem można się kontaktować na podany wyżej adres lub na adres: ul. Królewska 27, 00-060 Warszawa lub elektronicznie na adres: [kancelaria@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
6. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
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 c. 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.
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.

9. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:
10. 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.
11. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu. Dane nie są przetwarzane w celach marketingowych.

## Załącznik nr 24 do Regulaminu

### PWZ lekarza/PWZ lekarza dentysty

#### § 1. Definicje:

1. Naczelna Izba Lekarska (NIL) - jednostka organizacyjna samorządu zawodowego reprezentująca lekarzy i lekarzy dentystów na szczeblu państwowym;
2. PWZ lekarza/ PWZ lekarza dentysty - prawo wykonywania zawodu lekarza/lekarza dentysty;
3. Centralny Rejestr Lekarzy i Lekarzy Dentystów Rzeczypospolitej Polskiej (CRL) – rejestr, w którym gromadzone są dane lekarzy i lekarzy dentystów posiadających prawo wykonywania zawodu lekarza lub lekarza dentysty, prowadzony na podstawie art. 50 ustawy z dnia 2 grudnia 2009 r. o izbach lekarskich (Dz.U. z 2021 r. poz. 1342).

#### § 2. Informacje ogólne

1. Podstawę prawną pobrania danych w ramach PWZ lekarza/ PWZ lekarza dentysty stanowi art. 7c ust. 2a-2c ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty w zw. z 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 PWZ lekarza/ PWZ lekarza dentysty 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 aplikacji mObywatel, są nieprawidłowe lub nieaktualne, należy zgłosić się do NIL.
3. Korzystanie z dokumentu PWZ lekarza/ PWZ lekarza dentysty 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 PWZ lekarza/ PWZ lekarza dentysty posiadaczowi uprawnień, wskazanemu w Centralnym Rejestrze Lekarzy i Lekarzy Dentystów Rzeczypospolitej Polskiej, 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.
6. Korzystanie z dokumentu PWZ lekarza/ PWZ lekarza dentysty przeznaczone jest zarówno dla obywateli Polski posługujących się mDowodem, jak i dla użytkowników Diia.

### **§ 3. PWZ lekarza/ lekarza dentysty**

1. PWZ lekarza/ PWZ lekarza dentysty – pozwala na pobranie przez Użytkownika danych z Centralnego Rejestru Lekarzy i Lekarzy Dentystów Rzeczypospolitej Polskiej oraz z usługi mObywatel, przechowywanie ich w postaci zaszyfrowanej w urządzeniu mobilnym Użytkownika, a także ich prezentowanie lub przekazywanie.
2. Dane dostępne w PWZ lekarza/ PWZ lekarza dentysty pochodzą z CRL i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem podstawowym.
3. Posługiwanie się mobilnym dokumentem PWZ lekarza/ PWZ lekarza dentysty przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem obywateli Rzeczypospolitej Polskiej wykonujących lekarza i lekarza dentysty.
4. Do aktywacji i aktualizacji PWZ lekarza/ PWZ lekarza dentysty niezbędne jest, aby użytkownik uzyskał prawo do wykonywania zawodu i został wpisany do rejestru prowadzonego przez właściwą okręgową radę lekarską zgodnie z art. 8 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty.

### **§ 4. Użytkownicy usługi PWZ lekarza/ lekarza dentysty**

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

### **§ 5. Funkcje PWZ lekarza/ PWZ lekarza dentysty**

1. Prawidłowo aktywowana usługa PWZ lekarza/ PWZ lekarza dentysty umożliwia Użytkownikowi korzystanie z następujących funkcji:

- a) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;
  - b) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - c) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - d) usunięcie PWZ lekarza/ PWZ lekarza dentysty z Aplikacji (funkcja „Usuń PWZ lekarza/ PWZ lekarza dentysty”).
2. Użytkownik może zaprezentować innej osobie PWZ lekarza/ PWZ lekarza dentysty. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu dokumentu. 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) gilosa umieszczonego jako tło PWZ lekarza/ PWZ lekarza dentysty, 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 PWZ lekarza/ PWZ lekarza dentysty z Aplikacji można dokonać poprzez działanie (sekcja „Dokumenty”, następnie ikona edycji i wybranie ikony „kosz”).
  5. Usunięcie usługi PWZ lekarza/ PWZ lekarza dentysty Użytkownika następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

## **§ 6. Klauzula informacyjna**

1. Administratorem danych osobowych, w rozumieniu Rozporządzenia 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 („RODO”), jest Naczelna Izba Lekarska z siedzibą w Warszawie. 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: jest Naczelna Izba Lekarska z siedzibą przy ul. Jana III Sobieskiego 110, 00-764 Warszawa z dopiskiem „Do inspektora ochrony danych” bądź mailowo: [iod@nil.org.pl](mailto:iod@nil.org.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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl).
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach PWZ lekarza/ PWZ lekarza dentystry w Aplikacji przechowuje się następujące dane:
  - 1) Imię (imiona) Użytkownika PWZ lekarza/ PWZ lekarza dentystry;
  - 2) nazwisko Użytkownika;
  - 3) wizerunek twarzy Użytkownika;
  - 4) numer wpisu na listę lekarzy i lekarzy dentystry;
  - 5) data wydania dokumentu;
  - 6) data ważności dokumentu;
  - 7) nazwa izby lekarskiej;
  - 8) organ wydający dokument;
  - 9) rodzaj uprawnienia.
19. 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.
20. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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.
21. W zakresie przetwarzania i ochrony danych, które Użytkownik uzyskał w toku elektronicznego prezentowania danych osobowych bądź elektronicznego weryfikowania

danych osobowych, Użytkownika obowiązuje stosowanie się do powszechnie obowiązujących przepisów prawa.

22. 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.
23. 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.
24. 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.
25. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji oraz wykrycia błędów i luk bezpieczeństwa.
26. 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. Dane nie są przetwarzane w celach marketingowych.
27. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z dokumentu PWZ Pielęgniarki/PWZ Położnej, 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.
28. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez: Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
29. 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. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## **Załącznik nr 25 do Regulaminu**

### **Usługa Bezpiecznie w sieci**

#### **§ 1. Informacje ogólne**

1. Usługa Bezpiecznie w sieci umożliwia zgłaszanie złośliwych wiadomości oraz incydentów bezpieczeństwa, które Użytkownicy napotykają w Internecie.
2. Usługa zawiera funkcje edukacyjną w postaci Bazy wiedzy przygotowanej przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK).
3. Z poziomu usługi można przejść do ustawień powiadomień push dot. alertów bezpieczeństwa, jeśli użytkownik ma je wyłączone.
4. Dane wprowadzone przez użytkownika są przekazywane do CERT Polska.
5. Posługiwanie się usługą Bezpiecznie w sieci przez Użytkowników jest dobrowolne i nie jest prawnym obowiązkiem.

#### **§ 2. Użytkownicy usługi Bezpiecznie w sieci**

1. Użytkownikami korzystającymi z usługi Bezpiecznie w sieci mogą być osoby, które spełniają poniższe warunki:
  - a) mają ważny Certyfikat;
  - b) posiadają Certyfikat (mDowód, legitymacja studencka, legitymacja szkolna, Diia.pl).

#### **§ 3. Aktywacja usługi Bezpiecznie w sieci**

1. Aktywacja usługi polega na:
  - a) zalogowaniu do Aplikacji;
  - b) wybraniu „Bezpiecznie w sieci” z listy dostępnych usług.

#### **§ 4. Funkcje usługi Bezpiecznie w sieci**

1. Usługa Bezpiecznie w sieci umożliwia użytkownikowi korzystanie z następujących funkcji:
  - a) Zgłaszanie zdarzeń, które naruszają bezpieczeństwo w sieci;
  - b) złośliwych stron internetowych (próbę wyłudzenia danych osobowych lub pieniędzy);
  - c) zgłaszanie podejrzanych wiadomości SMS lub e-mail dotyczących treści lub nadawcy wiadomości, załączników do wiadomości, szantażu lub phishingu;
  - d) zgłaszanie podejrzenia oszustw (fałszywe sklepy internetowe i inne próby podszywania się pod firmy lub instytucje);
  - e) zgłaszania innych zdarzeń, które naruszają bezpieczeństwo w sieci.
    - 1) Korzystanie z Bazy wiedzy, która zawiera treści dotyczące bezpiecznego poruszania się w sieci, jak chronić swoje dane i unikać zagrożeń w Internecie;
    - 2) Aktywowanie alertów z ostrzeżeniami o zagrożeniach w Internecie w

postaci powiadomień PUSH.

2. Aplikacja mObywatel nie przechowuje danych Użytkownika, przekazanych za pośrednictwem usługi Bezpiecznie w sieci.
3. Usługa Bezpiecznie w sieci służy wyłącznie do zgłoszenia niebezpiecznych incydentów oraz kształtowania dobrych praktyk w zakresie bezpiecznego korzystania z sieci.
4. Usługa umożliwia użytkownikowi wysłanie zgłoszenia z zachowaniem poufności (bez przesyłania danych osobowych).

## **§ 5. Klauzula informacyjna**

11. Administratorem danych osobowych w zakresie zgłaszania incydentów bezpieczeństwa przez Użytkownika w związku z korzystaniem z usługi „Bezpiecznie w sieci” jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy z siedzibą przy ul. Kolskiej 12, 01-045 Warszawa. Informacje dotyczące zasad przetwarzania danych osobowych w związku ze zgłaszaniem i obsługą incydentów bezpieczeństwa znajdują się w Polityce Prywatności dostępnej na stronie [www.cert.pl](http://www.cert.pl).
12. Wyżej wymieniony Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych korespondencyjnie na adres siedziby Administratora bądź na adres e-mail: [iod@nask.pl](mailto:iod@nask.pl).
13. 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.
14. Z administratorem można się kontaktować na podany wyżej adres lub na adres: ul. Królewska 27, 00-060 Warszawa lub elektronicznie na adres: [kancelaria@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
15. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl)
16. 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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
17. 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.

18. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:
  19. 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.
  20. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
12. Dane nie są przetwarzane w celach marketingowych.

## Załącznik nr 26 do Regulaminu

### Usługa Legitymacja inżyniera budownictwa

#### § 1. Definicje

1. **Polska Izba Inżynierów Budownictwa (PIIB)** – nazwa własna uchwalona przez Krajowy Zjazd Izby wybrana dla krajowej jednostki organizacyjnej samorządu zawodowego na podstawie ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (Dz.U. z 2023 r. poz. 551).
2. **Legitymacja inżyniera budownictwa** - dokument mobilny, wydawany członkom Polskiej Izby Inżynierów Budowlanych na podstawie uchwały nr PIIB/KR/0025/2024 Krajowej Rady Polskiej Izby Inżynierów Budownictwa z dnia 11 października 2024 r. w sprawie legitymacji inżynierów budownictwa w aplikacji mObywatel, potwierdzający posiadanie uprawnień wykonywania zawodu inżyniera budownictwa.

#### § 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 inżyniera budownictwa 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 Legitymacji, są nieprawidłowe lub nieaktualne, należy zgłosić się do Polskiej Izby Inżynierów Budownictwa.
3. Korzystanie z mobilnej Legitymacji inżyniera budownictwa 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, którego dane znajdują się we właściwej Okręgowej Izbie Inżynierów Budownictwa. 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 inżyniera budownictwa

1. Legitymacja inżyniera budownictwa umożliwia pobranie przez Użytkownika danych z systemu dziedzinowego PIIB celem wyświetlenia legitymacji.
2. Dane dostępne w Legitymacji inżyniera budownictwa pochodzą z PIIB i zostały pobrane przez osobę, która została uwierzytelniona Certyfikatem podstawowym.

3. Posługiwanie się mobilną Legitymacją przez Użytkowników jest dobrowolne.
4. Do aktywacji i aktualizacji Legitymacji inżyniera budownictwa niezbędne jest członkostwo w Polskiej Izbie Inżynierów Budownictwa.

#### **§ 4. Użytkownicy**

1. Dokument jest dostępny zarówno dla obywateli Polski posługujących się mDowodem jak i dla użytkowników Diia, posiadających członkostwo w Polskiej Izbie Inżynierów Budownictwa.

#### **§ 5. Funkcje Legitymacji inżyniera budownictwa**

1. Prawidłowo aktywowana Legitymacja inżyniera budownictwa możliwi Użytkownikowi korzystanie z następujących funkcji:
  - a) prezentowanie danych Użytkownika, o których mowa w § 7 ust. 7;
  - b) przekazanie danych Użytkownika oraz osób powiązanych w celu weryfikacji (funkcja „Potwierdź swoje dane”);
  - c) aktualizowanie danych Użytkownika (funkcja „Aktualizuj”);
  - d) usunięcie dokumentu z Aplikacji (funkcja „Usuń legitymację inżyniera budownictwa”).
2. Użytkownik może zaprezentować dokument innej osobie. Funkcja dostępna jest po uruchomieniu Aplikacji i po wybraniu dokumentu. 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) gilosa umieszczonego jako tło legitymacji inżyniera budownictwa, 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.
6. Funkcja aktualizacji danych wymaga potwierdzenia tożsamości Użytkownika przy użyciu Certyfikatu podstawowego.
7. Usunięcia dokumentu z Aplikacji Użytkownik może dokonać poprzez działanie (sekcja Legitymacja inżyniera budownictwa). Usunięcie następuje również automatycznie w przypadku dezaktywacji usługi mObywatel.

#### **§ 6. Klauzula informacyjna**

1. Administratorem danych osobowych, w rozumieniu Rozporządzenia 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 („RODO”),

jest Polska Izba Inżynierów Budownictwa z siedzibą w Warszawie. 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 z dopiskiem: „Ochrona Danych Osobowych” na adres Polskiej Izby Inżynierów Budownictwa, 00-793 Warszawa, ul. Kujawska, bądź mailowo: [IOD@piib.org.pl](mailto:IOD@piib.org.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@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl).
5. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.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. 16 ust. 9 ustawy o aplikacji mObywatel. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
7. W ramach Legitymacji inżyniera budownictwa w Aplikacji przechowuje się następujące dane:
  - 1) Imię (imiona) użytkownika;
  - 2) nazwisko użytkownika;
  - 3) wizerunek twarzy użytkownika;
  - 4) nazwa(właściwej Okręgowej Izby Inżynierów Budownictwa, w której inżynier jest wpisany na listę członków ;
  - 5) numer PESEL użytkownika;
  - 6) numer członkowski;
  - 7) data ważności zaświadczenia o przynależności do izby inżynierów budownictwa ;
  - 8) informacja o posiadaniu wymaganego ubezpieczenia OC;
  - 9) typ dokumentu;
  - 10) status;
  - 11) wewnętrzny identyfikator dokumentu.
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.
9. Prezentowanie oraz elektroniczne przekazanie danych następuje dobrowolnie. Prezentowanie 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 prezentowania 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 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. Dane nie są przetwarzane w celach marketingowych.
16. Z zastrzeżeniem ustępów poprzedzających, Minister właściwy do spraw informatyzacji nie przetwarza danych osobowych gromadzonych przez Użytkowników w ramach korzystania przez nich z Legitymacji inżyniera budownictwa, 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: 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. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## Załącznik nr 27

### Usługa Podpisz dokument

#### § 1. Definicje

1. **Certyfikat Podpisu Zaawansowanego** (Certyfikat Podpisu Osobistego) – zgodnie z art. 2 ust. 2 ustawy o dowodach osobistych, to poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu osobistego do posiadacza dowodu osobistego, potwierdzające dane tego posiadacza.
2. **e-dowód** – polski dowód osobisty, o którym mowa w art. 4 ustawy o dowodach osobistych, zawierający warstwę elektroniczną, o której mowa w art. 12a tej ustawy.
3. **Kod PIN2** – kod, którego użycie umożliwia wykonanie operacji złożenia podpisu osobistego (kod 6-cyfrowy – PIN2 za pomocą e-dowodu. Kody PIN są blokowane po 3 błędnych próbach użycia ich).
4. **Kod PUK** – kod, który umożliwia odblokowanie kodów PIN. Kod PUK jest blokowany po 3 próbach użycia go. Odblokowanie kodu PUK nie jest możliwe.
5. **NFC** (ang. Near-Field Communication) – standard bezprzewodowej komunikacji radiowej, używany w urządzeniach mobilnych np. do płatności zbliżeniowych.
6. **Numer CAN** – numer, o którym mowa w art. 2 ust. 1 pkt 6 ustawy o dowodach osobistych. Jest to 6-cyfrowy numer widoczny na e-dowodzie, który chroni e-dowód przed niepowołanym odczytem bezprzewodowym
7. **Podpis osobisty** – podpis, o którym mowa w zgodnie z art. 2 pkt 9 ustawy o dowodach osobistych.

#### § 2. Informacje ogólne

1. Usługa Podpisz dokument – usługa udostępniana na podstawie art. 3 ust 1. ustawy o aplikacji mObywatel, umożliwiająca podpisywanie dowolnych dokumentów w formacie pdf podpisem osobistym przy pomocy Certyfikatu Podpisu Osobistego umieszczonego w e-dowodzie użytkownika.
2. Korzystanie z Usługi wymaga podania nr CAN, a także nr PIN2. Brak ustawionego kodu PIN uniemożliwiają realizację Usługi. Kod PIN po raz pierwszy ustala Użytkownik osobiście, zgodnie z przepisami ustawy o dowodach osobistych we właściwym urzędzie obsługującym sprawy obywatelskie. Przekroczenie liczby błędnych wprowadzeń kodu PIN2 blokuje go.
3. Usługa umożliwia odblokowanie nr PIN2 w procesie podpisywania dokumentu za pomocą kodu PUK. Przekroczenie liczby błędnych wprowadzeń PUK blokuje go, co uniemożliwia dalsze korzystanie z warstwy elektronicznej e-dowodu.
4. Usługa umożliwia również zmianę kodu PIN do podpisu osobistego w procesie podpisywania dokumentów eDowodem.
5. Aby podpisać dokument pdf podpisem osobistym niezbędne jest połączenie online.

**Komentarz [MS1]:** Kod pin czy kod pin2?

**Komentarz [MS2]:** Do weryfikacji mamy kod PIN2 powyżej. Czy to dwa różne kody tj PIN i PIN2?

6. Do aktywacji i aktualizacji Usługi Podpisz dokument niezbędne jest posiadanie ważnego Certyfikat Podpisu Osobistego.
7. Pobranie Usługi Podpisz dokument i korzystanie z niej jest nieodpłatne. Korzystanie przez Użytkownika z usług transmisji danych lub połączeń głosowych w związku z pobraniem lub korzystaniem z Usługi Podpisz dokument może wiązać się z opłatami naliczanymi przez operatora telekomunikacyjnego, który świadczy Użytkownikowi usługi telekomunikacyjne.
8. Korzystanie z Usługi Podpisz dokument jest dobrowolne.
9. Usługa nie obejmuje:
  - a) odczytu danych z warstwy graficznej e-dowodu.
  - b) fotografowania e-dowodu, ani jakiegokolwiek jego części.

### **§ 3. Użytkownicy usługi Podpisz dokument**

Z usługi Podpisz dokument może skorzystać Użytkownik, który ukończył 18 lat i posiada e-dowód: z aktywną warstwą elektroniczną, z Certyfikatem Podpisu Osobistego oraz z ustawionym PIN2.

### **§ 4. Aktywacja usługi Podpisz dokument**

1. Aby aktywować usługę Podpisz dokument należy:
  - 1) zalogować się do Aplikacji mObywatel;
  - 2) wybrać „Podpisz dokument” z listy dostępnych usług;
  - 3) potwierdzić tożsamość Użytkownika przy użyciu Certyfikatu Podpisu Osobistego.
2. Do potwierdzenia tożsamości Użytkownika, ważności Certyfikatu Podpisu Osobistego oraz podpisania dokumentu przy użyciu Usługi Podpisz dokument niezbędne jest aktywne połączenie internetowe.

### **§ 5. Funkcje usługi Podpisz dokument**

Prawidłowo aktywowana usługa Podpisz dokument umożliwia Użytkownikowi korzystanie z funkcji podpisanie dokumentu w formacie .pdf podpisem osobistym znajdującym się w e-dowodzie. Ponadto usługa umożliwia zmianę kodu PIN.

#### **Zmiana kodu PIN2**

1. W przypadku gdy Użytkownik nie pamięta kodu PIN2 do podpisu osobistego, może za pomocą kodu PUK dokonać zmiany swojego 6-cio cyfrowego kodu PIN2. Opcja resetowania kodu dostępna jest w dwóch miejscach w aplikacji mObywatel:
  - Usługa podpisz dokument (proces popisywania dokumentów);
  - Z pozycji dokumentu mDowód.

2. Użytkownik może również dokonać zmiany kodu PIN2 do podpisu osobistego na inny (bez potrzeby podawania PUK), jeżeli pamięta wcześniejszy kod PIN2. Aby to zrobić należy:
  - otworzyć **mDowód** w aplikacji mObywatel.
  - W mDowodzie należy wybrać skrót **Dane dowodu osobistego**, a następnie nacisnąć **Pokaż dane**.
  - Następnie nacisnąć **Zmień PIN do podpisu osobistego**.
  - Wpisać dotychczasowy **6-cyfrowy PIN** do podpisu osobistego w e-dowodzie (tzw. PIN2).
  - Wprowadzić **numer CAN** e-dowodu.
  - Następnie należy wpisać **nowy PIN2** do podpisu osobistego dwa razy w przeznaczonych do tego polach.
  - Po wpisaniu nowego kodu wymagane jest przyłożenie e-dowodu do **anteny NFC** z tyłu urządzenia, żeby zatwierdzić zmianę. Dokument powinien pozostać przyłożony do telefonu do czasu potwierdzenia zmiany kodu PIN2 na ekranie aplikacji.

## 6. Klauzula informacyjna

1. Administratorem danych Użytkownika aplikacji mObywatel oraz Certyfikatu jest Minister 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@cyfra.gov.pl](mailto:Kancelaria@cyfra.gov.pl).
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@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl).
4. 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 c RODO w związku z art. 3 ust. 1 pkt 1-3 ustawy o aplikacji mObywatel.
5. W ramach usługi Podpisz dokument w aplikacji przechowuje się następujące dane:
  - 1) imię (imiona),
  - 2) nazwisko,
  - 3) numer PESEL,
  - 4) datę urodzenia,
  - 5) obywatelstwo,
  - 6) datę i miejsce zamieszkania.
6. 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.
- 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.
7. 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. Dane nie są przetwarzane w celach marketingowych.
8. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez: Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
9. 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.
10. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

## **Załącznik nr 28 do Regulaminu**

### **Usługa Uprawnienia kierowcy**

#### **§ 1. Informacje ogólne**

1. Podstawę prawną pobrania danych w ramach usługi Uprawnienia kierowcy stanowi art. 3 ust. 1 pkt 1 ustawy o aplikacji mObywatel, zgodnie z którą Minister zapewnia działanie systemu teleinformatycznego, który pozwala, przy użyciu publicznej aplikacji mobilnej, na pobranie danych osobowych tego użytkownika niezbędnych do realizacji usługi oraz danych dotyczących sytuacji prawnej tego użytkownika lub praw mu przysługujących.
2. Usługa umożliwia sprawdzenie uprawnień do kierowania pojazdami, zgodnie z art. 100a ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym
3. Dane w zakresie uprawnień kierowcy pochodzą z Centralnej Ewidencji Kierowców (CEK).

4. Warunkiem uzyskania informacji o uprawnieniach kierowcy jest podanie imienia i nazwiska kierowcy oraz numeru blankietu/numeru identyfikującego dokument prawa jazdy, tymczasowego prawa jazdy lub pozwolenia na kierowanie tramwajem.
5. Wyszukiwanie odbywa się wyłącznie po uprzednim podaniu kompletu w/w danych. W odpowiedzi użytkownik otrzymuje informacje o uprawnieniach zapisanych w danym dokumencie lub informację, że na podstawie wskazanych danych uprawnienia nie zostały odnalezione.

## **§ 2. Użytkownicy**

Użytkownikami korzystającymi z usługi Uprawnienia kierowcy mogą być osoby, które posiadają ważny Certyfikat (mDowód, legitymacja studencka, legitymacja szkolna, Diia.pl).

## **§ 3. Aktywacja Uprawnienia kierowcy**

1. Aby aktywować usługę Uprawnienia kierowcy należy:
  - a) Zalogować się do Aplikacji mObywatel;
  - b) wybrać „Uprawnienia kierowcy” z listy dostępnych usług;
2. Ważność usługi powiązana jest z ważnością Certyfikatu.
3. Certyfikat jest wykorzystywany do pobrania usługi Uprawnienia kierowcy.
4. Do korzystania z usługi niezbędne jest aktywne połączenie internetowe.
5. Użytkownik za pomocą aplikacji mObywatel może aktywować usługę i pobrać dane z systemu tylko na jednym urządzeniu mobilnym.
6. Usługa Uprawnienia kierowcy nie oferuje funkcji eksportu ani importu danych.
7. Dostęp do danych przechowywanych w usłudze Uprawnienia kierowcy jest zabezpieczony hasłem w aplikacji mObywatel zgodnie z Regulaminem korzystania z aplikacji mObywatel.

## **§ 4. Funkcje w Usłudze Zastrzeż dokument**

Prawidłowo aktywowana usługa umożliwia Użytkownikowi weryfikację uprawnień swoich lub innego kierowcy, które są zapisane w dokumencie prawa jazdy, tymczasowego prawa jazdy lub pozwolenia na kierowanie tramwajem.

## **§ 5. Klauzula informacyjna**

1. Administratorem danych w zakresie: typu dokumentu (odpowiednio: prawo jazdy, tymczasowe prawo jazdy lub pozwolenie na kierowanie tramwajem), serii i numeru blankietu, statusu dokumentu, daty ważności dokumentu, organu wydającego, kategorii uprawnień oraz daty ważności uprawnienia jest Minister Cyfryzacji którego urzędem obsługującym jest Ministerstwo Cyfryzacji z siedzibą przy ul. Królewskiej 27, 00-060 Warszawa.
2. 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.

3. Z administratorem można się kontaktować na podany wyżej adres lub na adres: ul. Królewska 27, 00-060 Warszawa lub elektronicznie na adres: [kancelaria@cyfra.gov.pl](mailto:kancelaria@cyfra.gov.pl)
4. Administrator wyznaczył Inspektora Ochrony Danych, z którym - w sprawach związanych z przetwarzaniem danych osobowych - można kontaktować się mailowo: [iod.mc@cyfra.gov.pl](mailto:iod.mc@cyfra.gov.pl).
5. 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. Minister Cyfryzacji przetwarza dane osobowe w celu udostępnienia usług w aplikacji i zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
6. 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.
7. Dane osobowe Użytkownika będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora, którym jest Minister Cyfryzacji), to jest przez:
8. 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.
9. Dane osobowe Użytkownika nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
10. Dane nie są przetwarzane w celach marketingowych.