UZASADNIENIE

Projekt ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw przewiduje wprowadzenie uproszczeń w przepisach będących w zakresie właściwości ministra właściwego do spraw informatyzacji. Kolejne zmiany polegają na uproszczeniu postępowań prowadzonych przez tego ministra dotyczących udostępnienia danych przez rezygnację z obowiązku wydawania decyzji administracyjnej, w sytuacjach gdy udostępnienie danych jest uzasadnione. W tym celu wprowadza się zmiany w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717) (art. 1 projektu), ustawie z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2024 r. poz. 1251) (art. 2 projektu), ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671 oraz z 2023 r. poz. 1234 i 1941) (art. 3 pkt 1 i pkt 2 lit. c projektu), ustawie z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2025 r. poz. 274) (art. 4 pkt 1 i 3 projektu), ustawie z dnia 28 listopada 2014 r. – Prawo o aktach stanu cywilnego (Dz. U. z 2025 r. poz. 594) (art. 5 projektu) oraz w ustawie z dnia 27 stycznia 2022 r. o dokumentach paszportowych (Dz. U. z 2024 r. poz. 1063) (art. 7 projektu), zaproponowano zmianę trybu udostępniania danych. Zgodnie z projektowanymi ww. przepisami, pozytywna odpowiedź na wniosek podmiotu ubiegającego się o udostępnienie skutkowałaby czynnością materialno-techniczną i nie wymagałaby przeprowadzenia procedury wydawania decyzji administracyjnej. Minister właściwy do spraw informatyzacji wydawałby decyzję jedynie w przypadku odmowy udostępnienia danych i cofnięcia zgody na udostępnianie danych – co oznacza, że strona będzie miało prawo kontroli negatywnego rozstrzygnięcia. Takie rozwiązanie przyczyni się do:

1. szybszego udostępniania danych;
2. odciążenia administracji publicznej od konieczności wydawania decyzji, jeżeli uwzględniają one w całości wniosek;
3. zmniejszenia formalności i skrócenia procedur.

Wprowadzenie ww. zmian nie spowoduje dodatkowych kosztów dla budżetu państwa.

Ponadto projekt ma na celu wprowadzenie podstaw prawnych dla rozwiązań, które zwiększą bezpieczeństwo obrotu prawnego i podniosą skuteczność weryfikacji tożsamości kontrahentów przez podmioty świadczące usługi w sektorze prywatnym.

Proponowane rozwiązanie udostępniania danych w formie czynności materialno-technicznej jest rozwiązaniem wystarczającym z punktu widzenia zapewnienia odpowiedniej ochrony danych osób, których one dotyczą gdyż czynność materialno-techniczna to działanie organu administracji publicznej, które służy do realizacji konkretnych zadań i jest związana z wykonywaniem konkretnych obowiązków i uprawnień, wynikających z przepisów prawa. Wykonanie tej czynności nie oznacza jednakże automatyzmu w procesie udostępniania danych z rejestrów ministra właściwego do spraw informatyzacji, bowiem czynność ta jako czynność z zakresu prawa administracyjnego jest podejmowana w sprawie indywidualnej, skierowana do oznaczonego podmiotu, dotyczy uprawnienia lub obowiązku tego podmiotu, samo zaś uprawnienie lub obowiązek, którego czynność dotyczy, jest określone w przepisie prawa powszechnie obowiązującego.

Każdorazowe udostępnianie danych będzie poprzedzone przeprowadzeniem, zgodnie w przepisami odpowiednio ustawy: o informatyzacji działalności podmiotów realizujących zadania publiczne, Prawo o ruchu drogowym, o dowodach osobistych, o ewidencji ludności Prawo o aktach stanu cywilnego oraz o dokumentach paszportowych, stosownego postępowania oraz sprawdzenia spełnienia warunków uzyskania danych, a zmienia się jedynie podstawa ich udostępniania nie w drodze decyzji, a czynności materialno-technicznej. Nie bez znaczenia pozostaje także fakt, że czynność materialno-techniczna jako czynność władztwa administracyjnego, rozumiana także jako jednostronne działania organu wykonującego administrację publiczną, stanowi czynność z zakresu administracji publicznej i jako taka podlega kontroli działalności administracji publicznej przez sądy administracyjne.

W art. 3 pkt 2 lit. a i b oraz pkt 3 projektu ustawy wprowadza się zmiany w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych.

W ww. projektowanych przepisach proponuje się wprowadzenie zmian prawnych, których głównym celem jest podniesienie skuteczności oraz bezpieczeństwa procesów ustalania tożsamości osób fizycznych przez zapewnienie warunków prawnych pozwalających na uzupełnienie tych procesów o weryfikację wizerunku twarzy osoby fizycznej z wizerunkiem tej osoby przechowywanym w Rejestrze Dowodów Osobistych (RDO).

Konsultacje przeprowadzane na przestrzeni lat przez Ministerstwo Cyfryzacji z dostawcami usług świadczonych w sektorze prywatnym prowadzą do konkluzji, że zapewnienie dostępu do danej biometrycznej, jaką stanowi wizerunek osoby fizycznej przechowywany w RDO, wpłynie pozytywnie na uszczelnienie procedur ustalania tożsamości osób fizycznych, co w rezultacie przełoży się na znaczne ograniczenie liczby wyłudzeń, które mają miejsce szczególnie w sektorze finansowym. Proceder tzw. „kradzieży tożsamości” realizowany jest głównie z wykorzystaniem imitacji dowodów osobistych. W takich przypadkach, sfałszowany dokument zawiera zdjęcie sprawcy oraz dane ofiary, pod którą podszywa się sprawca. Wobec powyższego sama weryfikacja danych zawartych w okazywanym dowodzie osobistym, a w niektórych przypadkach także zabezpieczeń fizycznych takiego dokumentu, może prowadzić usługodawcę do fałszywego przekonania o prawdziwości okazywanego dokumentu. Zapewnienie usługodawcom możliwości weryfikacji, oprócz danych jakie zawiera dowód osobisty, także zdjęcia, jakie zawiera autentyczny dokument, znacząco wpłynie na ukrócenie wyżej opisanego procederu, a samo rozwiązanie jest komplementarne do instytucji zastrzeżenia numeru PESEL, wpływając na ochronę osób, które z zastrzeżenia nie korzystają. Udostępnienie wizerunku nastąpi bez dodatkowej zgody osoby w procesie ustalenia tożsamości. Wprowadzenie zgody osoby powodowałoby, że w przypadku próby podszycia się, oszust w sposób naturalny nie wyrażałby zgody, co powodowałoby bezskuteczność rozwiązania. To podmiot weryfikujący tożsamość osoby, który staje się administratorem jej danych, decydować będzie o sposobach weryfikacji tożsamości. Pozyskana w projektowanym trybie fotografia nie podlega przechowywaniu i gromadzeniu przez podmiot, który ją pozyskał.

W art. 3 pkt 2 lit. a i b projektu ustawy wprowadza się zmiany w art. 68 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych polegające na:

1. uchyleniu w ust. 1 zdania drugiego, co ma na celu dostosowanie regulacji do rozszerzenia wydawanego raportu dotyczącego niezgodności danych z RDO;
2. dodaniu ust. 1a i 1b, które będą stanowić podstawę prawną do rozszerzenia dotąd wydawanego raportu dotyczącego niezgodności danych o wskazanie, która z danych jest niezgodna. Powyższy raport ma zapewnić sprawną obsługę klienta przez podmiot komercyjny np. bank oraz ją przyspieszyć, a także ograniczyć konieczność wizyty klienta banku lub w urzędzie w celu weryfikacji zapisu danych osoby widniejących w wydanym jej dowodzie osobistym. Rozszerzenie raportu weryfikacji mieści się w realizacji celu w jakim każdorazowo podmiot wnioskuje o weryfikację, jak również znajduje się w ramach celu, któremu służy ten tryb udostępniania. Tryb weryfikacji (ograniczonej teletransmisji) polega na ustaleniu, czy dowód osobisty o wskazanym zakresie danych istnieje czy też nie. Nie ma jednak przeszkód, aby podmiot weryfikujący, który, co należy podkreślić, na mocy decyzji wydanej przez Ministra Cyfryzacji jest do tego uprawniony, uzyskał również informację, która konkretnie dana jest niezgodna. Nadal nie jest to bowiem udostępnienie tej danej, a jedynie wskazanie, która z nich jest nieprawidłowa. W dalszym ciągu podmiot taki po uzyskaniu raportu niezgodności powinien podchodzić ostrożnie co do legalności tak zweryfikowanego dowodu osobistego. Celem nowelizacji jest wsparcie podmiotów sektora prywatnego w prowadzonej przez nie działalności tak, aby mogły wywiązywać się z ustawowo nałożonych na nie obowiązków, w tym weryfikować dane swoich klientów. Uzyskanie takiego raportu daje im dodatkowo możliwość zweryfikowania po swojej stronie, czy wszystkie dane zostały wpisane poprawnie i czy nie należy ich ponownie uzupełnić i zweryfikować, bez narażania klienta na niepotrzebne nieprzyjemności. Obecnie, jak również sygnalizuje Związek Banków Polskich, proces weryfikacji pomimo posługiwania się przez klienta ważnym dokumentem sprawia trudności i odbija się negatywnie na kliencie, w szczególności w przypadku występowania w danych osoby znaków diakrytycznych. Brak informacji, że negatywna weryfikacja spowodowana jest wadliwym wskazaniem określonej kategorii danych, często powoduje odesłanie klienta do urzędu w celu wyjaśnienia sprawy i weryfikacji zapisów danych osoby widniejących w rejestrze państwowym. Niejednokrotnie są to również zwykłe omyłki i literówki podczas wpisywania danych, które również powodują odesłanie klienta do urzędu. Problem ten obserwowany jest również z poziomu Ministerstwa Cyfryzacji, które w odpowiedzi na indywidualne zapytania osób fizycznych kierowane do niej bezpośrednio sprawdza sposób wprowadzenia zapytania przez podmioty weryfikujące. Sytuacje te dotyczą często spraw ważnych z punktu widzenia np. prowadzonej działalności gospodarczej i realizowanych w jej ramach operacji, gdzie istotny jest czas obsługi zlecenia.

W art. 3 w pkt 3 projektu ustawy dodaje się do ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych przepis art. 68a, w którym to przepisie:

1. w ust. 1 określa się warunki, na jakich będzie możliwe udostępnienie fotografii z RDO w trybie pełnej teletransmisji danych. W projekcie proponuje się przyjęcie dwustopniowego modelu dostępu usługodawcy do wizerunku twarzy. Zgodnie z przyjętymi założeniami, w pierwszym kroku usługodawca będzie musiał uzyskać pozytywny wynik weryfikacji danych zawartych w weryfikowanym dowodzie osobistym. Weryfikacja ta będzie odbywała się przy użyciu usługi sieciowej, udostępnianej przez Ministra Cyfryzacji, która funkcjonuje już obecnie na podstawie aktualnych przepisów zmienianej ustawy. Usługodawca ubiegający się o dostęp do wizerunku twarzy będzie musiał uprzednio uzyskać pozytywną decyzję Ministra Cyfryzacji warunkującą uzyskanie dostępu do danych zgromadzonych w RDO, w trybie weryfikacji danych, za pośrednictwem ww. usługi sieciowej. Dopiero po potwierdzeniu istnienia dowodu osobistego w wyżej opisany sposób, usługodawca będzie miał zapewnioną możliwość weryfikacji fotografii posiadacza dowodu osobistego, przechowywanej w Rejestrze Dowodów Osobistych, przy użyciu usługi sieciowej udostępnionej przez Ministra Cyfryzacji, w trybie pełnej teletransmisji;
2. w ust. 1–3 określa się także katalog podmiotów, które będą uprawnione do ubiegania się o dostęp do fotografii z RDO, i warunki, jakie będą musiały spełnić, by skorzystać z usługi. Katalog ten określono przez pryzmat wykonywanych zadań i czynności, w których niezbędna jest skuteczna weryfikacja tożsamości klienta. Tym samym posiadanie przez usługodawcę wyłącznie dostępu do danych zgromadzonych w RDO w drodze weryfikacji nie będzie stanowiło automatycznej przepustki do dostępu do wizerunku posiadacza dowodu osobistego, lecz zostanie ograniczone do wskazanego w projekcie kręgu podmiotów. Wśród podmiotów uwzględniono także instytucję tworzoną na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2024 r. poz. 1646, z późn. zm.) z uwagi na szczególną rolę tych podmiotów w sektorze finansowym. Instytucje te, takie jak Związek Banków Polskich czy Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa, pośredniczą dla banków lub swoich członków w dostępie do danych zgromadzonych w rejestrach publicznych. Taka sytuacja ma miejsce już obecnie w przypadku ZBP które przygotowało rozwiązanie techniczne za pośrednictwem którego banki weryfikują dane dowodu osobistego z Rejestrem Dowodów Osobistych. W przepisie art. 68a ust. 1 pkt 3 dodano tę instytucję, aby nie budziło wątpliwości interpretacyjnych, że może brać ona udział w procesie weryfikacji dowodu i uzyskiwania wizerunku osoby z Rejestru Dowodów Osobistych. Instytucje te nie dokonują weryfikacji i uzyskania wizerunku bezpośrednio na własne potrzeby lecz na potrzeby członków, których zrzeszają, np. banków. Dostęp do danych wywoływany jest przez konkretny bank a nie ZBP lecz następuje to z wykorzystaniem rozwiązania ZBP, który tym samym uczestniczy w przetwarzaniu danych osobowych. Spowodowało to konieczność umocowania tego podmiotu w ustawie;
3. w ust. 4 dookreślono, iż udostępnieniu na ww. zasadach podlega wyłącznie fotografia zamieszczona w ostatnim wydanym dowodzie osobistym, który w dniu dokonywania weryfikacji w trybie ograniczonej teletransmisji jest dokumentem ważnym. Nie będzie zatem możliwe pozyskiwanie fotografii, jeśli dowód jest z jakiejkolwiek przyczyny unieważniony, jak również do fotografii z poprzednich dowodów osobistych. Przyjęcie tego rozwiązania ma na celu umożliwienie weryfikacji tożsamości osoby wyłącznie na podstawie fotografii z aktualnego i ważnego dowodu osobistego. Dodatkowo ograniczono możliwość dostępu do fotografii wyłącznie w przypadku dokumentów wydanych, stąd też nawet w przypadku złożenia przez obywatela wniosku o nowy dokument – weryfikacji będą podlegały dane z poprzedniego – o ile jest on ważny;
4. w ust. 5 doprecyzowuje się, że udostępnienie fotografii z RDO w przypadku uprzedniej pozytywnej weryfikacji istnienia dowodu osobistego na podany przez Wnioskodawcę zestaw danych – w trybie ograniczonej teletransmisji danych – będzie nieodpłatne.

W art. 4 pkt 2, 4 i 5 projektu ustawy wprowadza się zmiany w ustawie z dnia 24 września 2010 r. o ewidencji ludności.

W art. 4 pkt 2 projektu ustawy wprowadza następujące zmiany w art. 48 ustawy dnia 24 września 2010 r. o ewidencji ludności:

1. dodawany ust. 1a będzie stanowił podstawę prawną do udostępnienia określonej grupie podmiotów informacji o seriach, numerach i datach ważności ważnych dowodów osobistych ich klientów wydanych na skutek zmiany dowodu osobistego. Dotąd konieczność zgłoszenia aktualizacji danych dotyczących dowodu osobistego spoczywała na kliencie instytucji. Brak zgłoszenia zmiany danych skutkował niemożnością realizacji czynności bankowej z powodu niezgodności danych (bank zweryfikował dane dotyczące dowodu osobistego i otrzymał zwrotnie informację, że dowód osobisty nie jest ważny). Przyczyni się to do zdjęcia z obywateli konieczności zgłaszania zmiany dowodu osobistego i zmniejszenia barier w dostępie do usług finansowych. Jednocześnie podmiot taki musi spełniać wskazane w ustawie przesłanki dotyczące bezpieczeństwa danych. Mechanizm oraz katalog podmiotów uprawnionych (banki oraz SKOK-i) określony został także przy uwzględnieniu celów ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, w szczególności środków bezpieczeństwa finansowego określonych w art. 34 tej ustawy. Instytucje obowiązane na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie. Określony w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu katalog podmiotów jest bardzo szeroki i obejmuje podmioty jak np. pośrednicy ubezpieczeniowi czy pośrednicy w obrocie nieruchomościami. W ocenie projektodawcy tak szeroki katalog podmiotów uprawnionych do uzyskiwania danych, jest jednak zbyt szeroki i powodujący wyższe ryzyko wycieku danych. Ryzyko to oceniono na tyle wysoko, aby katalog podmiotów ograniczyć do podmiotów dających rękojmię zaufania w najwyższym stopniu. Były to jednocześnie postulaty zgłaszane przez to środowisko. Projekt przewiduje także udostępnianie informacji o dacie ważności nowego dowodu osobistego co ma na celu umożliwienie weryfikacji czy klient dysponuje ważnym dokumentem i ewentualne monitowanie go o konieczności wymiany w przypadku zbliżającego się upływu terminu ważności. W świetle art. 34 ust. 4 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu instytucje obowiązane na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie, a zatem także informację o dacie ważności dokumentu;
2. dodawany ust. 1b doprecyzowuje, iż określone dane dotyczące dowodów osobistych klientów mogą być udostępnione również za pośrednictwem instytucji utworzonej na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, tak jak ma to miejsce np. w przypadku rejestru zastrzeżeń numerów PESEL.

W art. 4 pkt 4 projektu ustawy wprowadza zmianę w art. 53 pkt 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności, który będzie stanowił, iż udostępnienie np. bankom informacji o seriach, numerach i datach ważności ważnych dowodów osobistych ich klientów wydanych na skutek zmiany dowodu osobistego będzie realizowane odpłatnie.

W art. 4 pkt 5 projektu ustawy wprowadza się zmianę w art. 56 pkt 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności, polegającą na modyfikacji delegacji ustawowej dla Rady Ministrów do wydania rozporządzenia dotyczącego wysokości, sposobu i terminów uiszczenia opłat za udostępnienie danych z rejestru PESEL oraz sposobu ich dokumentowania poprzez objęcie zakresem rozporządzenia również opłaty za udostępnianie serii, numeru i daty ważności dowodu osobistego.

Zmiana w art. 6 polega na uchyleniu art. 37 i dodaniu przepisu art. 37a w ustawie z dnia 25 czerwca 2015 r. – Prawo konsularne (Dz. U. z 2023 r. poz. 1329) i ma na celu zastąpienie osobnych wykazów obywateli polskich przebywających w okręgu konsularnym, prowadzonych fakultatywnie przez konsulów, jednym rejestrem obywateli polskich przebywających za granicą, zwanym dalej „rejestrem podróżujących”, prowadzonym przez ministra właściwego do spraw zagranicznych, w celu wsparcia działań konsula, o których mowa w art. 36 zmienianej ustawy (wsparcie bezpiecznego i sprawnego opuszczenia zagrożonego obszaru w sytuacji zagrożenia dla życia lub bezpieczeństwa), a także działań, o których mowa w art. 18 pkt 8 zmienianej ustawy, w zakresie upowszechniania informacji o sytuacji w państwie przyjmującym, w szczególności o zdarzeniach mogących powodować zagrożenie dla życia lub bezpieczeństwa obywateli polskich. Powyższe cele, zawarte w przywołanych przepisach, stanowią tym samym uzasadnienie dla przetwarzania danych osobowych, o jakim mowa w art. 6 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

Dzięki ustawowemu uregulowaniu funkcjonowania ww. rejestru oraz powiązanej z nim usługi elektronicznej rejestracji podróży zagranicznej będzie możliwe jej udostępnienie w aplikacji mObywatel na zasadach określonych w art. 16 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275 i 1717). Obecnie usługa jest realizowana poprzez system Odyseusz prowadzony przez Ministerstwo Spraw Zagranicznych, funkcjonujący na zasadach określonych w regulaminie portalu internetowego (dane osobowe przetwarzane są w nim na podstawie art. 6 ust. 1 lit. a RODO, tj. za zgodą użytkownika). W nowym stanie prawnym zarówno rejestr, jak i usługa będą funkcjonować w ramach jednego systemu teleinformatycznego prowadzonego przez ministra właściwego do spraw zagranicznych, który będzie administratorem danych osobowych zgromadzonych rejestrze podróżujących. W projektowanym przepisie rozszerzono katalog danych osobowych przetwarzanych w ww. rejestrze. Będzie on obejmować imię (imiona), nazwisko, numer PESEL – jeżeli został nadany, adres miejsca pobytu za granicą, przewidywany okres pobytu za granicą – nie dłuższy niż 5 lat, oraz adres poczty elektronicznej lub numer telefonu komórkowego. Dane te będą zamieszczane, aktualizowane lub usuwane na wniosek obywatela polskiego (wypada zatem zauważyć, że ustawodawca uregulował również sytuację, w której obywatel nie będzie wyrażał dalszego życzenia co do ujęcia jego danych w systemie teleinformatycznym, gdyż np. zrezygnuje z planowanej podróży, wobec czego wystąpi o usunięcie danych).

Proponowana zmiana określa okres retencji danych rejestrze podróżujących wynoszący 14 dni od zakończenia przewidywanego pobytu w za granicą. Maksymalny okres zarejestrowanego pobytu za granicą wyniesie 5 lat – po upływie tego okresu obywatel będzie mógł ewentualnie ponownie zarejestrować swój pobyt. Dotychczasowy przepis art. 37 nie odnosił się do możliwości działania z wykorzystaniem systemów teleinformatycznych, które obecnie uważa się za standard w pracy konsula. Wprowadza się też możliwość udostępnienia danych z rejestru podróżnych organom innych państw lub innym podmiotom, w zakresie niezbędnym do prowadzenia przez konsula działań, o których mowa w art. 36 zmienianej ustawy (wsparcie bezpiecznego i sprawnego opuszczenia zagrożonego obszaru w sytuacji zagrożenia dla życia lub bezpieczeństwa), co niejednokrotnie może być niezbędne dla sprawnego przeprowadzenia ww. działań, w szczególności w sytuacji kryzysowej, obejmującej np. poszukiwania ofiar zdarzeń losowych przez miejscowe służby itp.

Jednocześnie planowane jest usunięcie art. 37 ustawy z dnia 25 czerwca 2015 r. – Prawo konsularne w aktualnym brzmieniu, przyznającego konsulowi kompetencję do prowadzenia wykazu obywateli polskich przebywających w okręgu konsularnym, w celu sprawnego przeprowadzenia działań, o których mowa w art. 36 przywołanej ustawy. Mając na uwadze, iż przepis ten nie jest stosowany w praktyce, nie jest potrzebne wprowadzenie regulacji przejściowych.

W ocenie projektodawcy nie zachodzi potrzeba zawarcia w projektowanych przepisach regulacji o charakterze przejściowym i dostosowującym związanych z utrzymaniem ważności decyzji wyrażających zgodę na udostępnienie danych, które zostały już wydane bądź zostaną wydane przed dniem wejścia w życie projektowanych przepisów ustaw, gdyż wprowadzane nie zmieniają co do zasady sposobu ubiegania się o udostępnianie danych.

Przewiduje się, że projektowane przepisy wejdą w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

1. art. 3 pkt 2 lit. a i b oraz pkt 3, art. 4 pkt 2, 4 i 5 oraz art. 9, które wejdą w życie z dniem 30 czerwca 2026 r.;
2. art. 6, który wchodzi w życie z dniem 17 kwietnia 2026 r.

Wejście w życie z dniem 30 czerwca 2026 r. regulacji dotyczących udostępniania wizerunku oraz aktualizacji danych o seriach i numerach oraz datach ważności dowodów osobistych wynika z konieczności przygotowania stosownych rozwiązań technicznych umożliwiających korzystania z takich usług przez podmioty uprawnione, w tym przygotowania mechanizmów rozliczalności przetwarzania danych osobowych.

Wejście w życie z dniem 17 kwietnia 2026 r. regulacji dotyczących rejestru podróżujących wynika z planowanego terminu uruchomienia projektowanej usługi wynikającego z harmonogramu projektu Rozbudowa systemu Odyseusz.

Projekt ustawy nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 1535), projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz z 2025 r. poz. 408), został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w zakładce Rządowy Proces Legislacyjny.

Projektowane regulacje nie stoją w sprzeczności z prawem Unii Europejskiej.

Projekt nie wymaga zasięgnięcia opinii, dokonania konsultacji oraz uzgodnienia z właściwymi organami i instytucjami Unii Europejskiej.