

UZASADNIENIE

I. Cel ustawy.

W dobie coraz bardziej powszechnego dostępu do Internetu standardem stało się świadczenie usług online. Jednakże dla dostawcy takiej usługi częstym mankamentem jest brak bezpośredniego kontaktu ze świadczeniobiorcą oraz wynikająca z tego wątpliwość dotycząca deklarowanej tożsamości i wieku osoby, na rzecz której świadczona jest usługa. Problem pojawia się także w przypadku, gdy wymaganym elementem usługi świadczonej online jest złożenie przez świadczeniobiorcę oświadczenia woli, które powinno być opatrzone przez składającego podpisem. Panaceum na powyższe problemy stały się dwa narzędzia: mechanizmy uwierzytelniania oraz podpis elektroniczny.

Dlatego też celem ustawy jest zapewnienie każdemu obywatelowi bezpiecznego narzędzia do komunikacji elektronicznej z administracją, służbą zdrowia i podmiotami komercyjnymi. Takim narzędziem ma być nowy dowód osobisty, nieodpłatny, państwowy środek identyfikacji elektronicznej. Dokument ten będzie w sposób jednoznaczny i niezaprzeczalny potwierdzał tożsamość obywatela, będzie też służył do uwierzytelnienia w e-usługach administracji publicznej oraz do podpisywania dokumentów elektronicznych, a także pozwalał potwierdzać obecność w systemach teleinformatycznych. Nowy dowód będzie posiadał aplikację ICAO (dokument podróży z cechą biometryczną „zdjęcie twarzy”). Nowy dowód osobisty będzie zawierał w warstwie elektronicznej dane, które, wraz z danymi znanymi wyłącznie posiadaczowi tego dowodu, pozwolą zarówno na uwierzytelnienie go w systemach teleinformatycznych, w ramach których świadczone są usługi online, jak i na opatrywanie dokumentów elektronicznych podpisem elektronicznym. Podpis elektroniczny będzie rozwiązaniem analogicznym do znanego już i używanego, zarówno w administracji, jak i w biznesie, kwalifikowanego podpisu elektronicznego. Podpis, zwany „podpisem osobistym”, będzie stanowił zaawansowany podpis elektroniczny w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014” lub „rozporządzeniem eIDAS”, i będzie mógł być składany bez konieczności dostępu do Internetu.

Poza zaawansowanym podpisem osobistym w nowym dokumencie znajdzie się także

przestrzeń na zamieszczanie kwalifikowanego certyfikatu podpisu elektronicznego wydawanego przez dostawców komercyjnych.

Upowszechnienie profilu osobistego zapewniającego identyfikację i uwierzytelnianie w systemach teleinformatycznych oraz podpisu osobistego służącego do podpisywania elektronicznych oświadczeń woli ma usprawnić procesy przede wszystkim organach administracji publicznej, doprowadzić do poprawy obsługi obywatela, podnosząc jednocześnie jej bezpieczeństwo. Popularyzacja e-usług przełoży się z kolei na mniejsze obciążenie urzędów. Certyfikat potwierdzania obecności umożliwiający m.in. potwierdzanie odbioru świadczeń medycznych w sposób elektroniczny, przyczyni się do uszczelnienia systemu opieki zdrowotnej i pozwoli wygospodarować oszczędności na inne świadczenia.

Polska jest jednym z niewielu krajów europejskich, w którym nie wydano jeszcze dowodu osobistego z warstwą elektroniczną. Dowód elektroniczny funkcjonuje już w Austrii, Belgii, Chorwacji, Portugalii, Estonii, Finlandii, Francji, Hiszpanii, Litwie, Niemczech, Szwecji, na Węgrzech, czy we Włoszech. Dokument ten jest najczęściej wykorzystywany do identyfikacji i uwierzytelniania oraz do składania elektronicznego podpisu. Z funkcjonalności elektronicznych korzystają osoby dorosłe, najczęściej na zasadach dobrowolności (Hiszpania, Luksemburg). Podobne rozwiązania przyjęto w projektowanej ustawie.

Projektowana ustawa realizuje wcześniejsze zamierzenia w tym zakresie, których do tej pory nie udało się urzeczywistnić. Wdrożenie dowodu osobistego z warstwą elektroniczną ujęte było w Planie Informatyzacji Państwa na lata 2007 – 2010, który przewidywał wprowadzenie wielofunkcyjnego elektronicznego dokumentu tożsamości z funkcją uwierzytelnienia zgodną z wytycznymi i wymogami ustanowionymi w tym zakresie na poziomie UE (Dyrektywą PE i Rady 1999/93/WE z 13.XII.1999 w sprawie wspólnotowych ram w zakresie podpisów elektronicznych) w ramach projektu „pl.ID – polska ID karta”. Dowód miał być wykorzystywany do uwierzytelniania obywateli w systemach teleinformatycznych administracji publicznej i służby zdrowia. Zakres projektu obejmował ponadto uporządkowanie rejestrów państwowych, w szczególności rejestru PESEL oraz zapewnienie odpowiedniej infrastruktury centralnej i gminnej do obsługi procesu wydawania dowodów osobistych, jak również informatyzację rejestrów urzędów stanu cywilnego. Wartość projektu pl.ID oszacowano na 370 mln zł, co oznacza, że zgodnie z rozporządzeniem UE nr 1083/2006 ustanawiającym przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającym

rozporządzenie (WE) nr 1260/1999, projekt ten miał status „dużego projektu” i podlegał zatwierdzeniu przez Komisję Europejską (KE). Decyzję w tej sprawie Komisja Europejska wydała w dniu 7 czerwca 2010 r. Zgodne z decyzją dowód osobisty miał:

- 1) być wielofunkcyjnym elektronicznym dokumentem z funkcją uwierzytelniania, zgodnym ze wspólnymi wytycznymi i wymogami ustanowionymi przez właściwe organy UE;
- 2) zapewniać możliwość wykorzystania dowodu w kontaktach z administracją publiczną oraz służbą zdrowia;
- 3) personalizacja graficzna i elektroniczna dowodu osobistego miała być zgodna z międzynarodowymi wymogami technicznymi i odbywać się zgodnie z zasadami neutralności technologicznej.
- 4) wyposażony w zaawansowany certyfikat służący do składania „podpisu osobistego”;
- 5) zgodny z normami i dyrektywami UE regulującymi kwestie elektronicznego zabezpieczenia dokumentu, elektronicznego systemu identyfikacji osób fizycznych i ochrony danych osobowych;
- 6) posiadać certyfikat zapisany na karcie dowodu osobistego ważny przez okres ważności dokumentu;
- 7) powinna zostać wdrożona infrastruktura klucza publicznego do celów realizacji usług związanych z elektronicznym podpisem składanym przy pomocy dowodu osobistego. Zaawansowany certyfikat powinien być wydawany przez wewnętrzne centrum certyfikacji (dla transakcji obywatel-urząd, w tym transakcji online).
- 7) przestrzeń umożliwiającą wgranie dodatkowego kwalifikowanego certyfikatu wydawanego przez dostawców komercyjnych (dla transakcji obywatel – instytucja prywatna).

Tym samym, realizacja projektu w ww. kształcie stała się zobowiązaniem strony polskiej. Celem wdrożenia dowodu osobistego z warstwą elektroniczną, 6 sierpnia 2010 r. została uchwalona ustawa o dowodach osobistych (Dz. U. Nr 167 poz. 1131). W 2012 r. Komitet Rady Ministrów do spraw Cyfryzacji rekomendował przesunięcie terminu wdrożenia elektronicznej warstwy dowodu osobistego do czasu zakończenia prac nad modernizacją i uporządkowaniem rejestrów państwowych, wdrożenia elektronicznych usług publicznych oraz zakończenia prac na poziomie UE nad rozporządzeniem w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS). 1 marca 2015 r. uruchomiony został System Rejestrów Państwowych, który stanowi integrację rejestru PESEL, Rejestru Dowodów Osobistych oraz nowo zbudowanego Rejestru Aktów Stanu Cywilnego. KE nie zmodyfikowała pierwotnej

decyzji zatwierdzającej finansowanie projektu pl.ID z 2010 r., podtrzymując oczekiwanie w stosunku do strony polskiej wdrożenia dowodu osobistego z warstwą elektroniczną. KE podkreśliła, że ostateczne rozliczenie projektu będzie możliwe po rozpoczęciu wydawania dowodów osobistych z warstwą elektroniczną.

Mając na uwadze stanowisko KE, jak również jej wytyczne dotyczące zamykania programów operacyjnych z perspektywy 2007-2013, pod koniec 2015 r. poinformowano KE o planowanej kontynuacji projektu pl.ID w formule tzw. projektu niefunkcjonującego aż do czasu rozpoczęcia wdrażania dowodów elektronicznych. Zgodnie z ww. wytycznymi, ostateczny termin zakończenia projektów realizowanych w tej formule to 31 marca 2019 r. KE podkreśliła, że do tego czasu Polska powinna rozpocząć wydawanie dowodów osobistych z warstwą elektroniczną. W przypadku niezakończenia projektu w wyznaczonym czasie bądź odstąpienia od jego realizacji beneficjent będzie zobligowany do zwrotu 85% kwoty wydatków uznanych dotychczas za kwalifikowane (kwotę 148, 4 mln zł.) wraz z odsetkami. W efekcie Rada Ministrów przyjęła w sierpniu 2018 r. dokument „Koncepcja: e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych”, stanowiący podstawę dla projektowanej ustawy, która uwzględni wytyczne KE z 2010 r.

Nowy dowód osobisty będzie realizował następujące funkcjonalności:

- 1) identyfikację i uwierzytelnianie posiadacza dokumentu w zewnętrznych systemach informatycznych;
- 2) możliwość złożenia podpisu zaawansowanego pod elektronicznym oświadczeniem woli;
- 3) potwierdzanie obecności posiadacza dowodu osobistego w zewnętrznych systemach teleinformatycznych, w tym w szczególności w systemach służby zdrowia;
możliwość przekraczania granic (dokument podróży zgodny z ICAO) przez automatyczne bramki na lotniskach w UE.

W dokumencie tym znajdzie się też przestrzeń umożliwiającą zamieszczenie kwalifikowanego certyfikatu podpisu elektronicznego zgodnego z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE.L 2014 Nr 257).

Niniejszy projekt wpisuje się też w działania Unii Europejskiej w zakresie zwiększenia

bezpieczeństwa dokumentów. W grudniu 2016 r. Komisja Europejska skierowała do Parlamentu Europejskiego i Rady komunikat pn. Plan działania na rzecz wzmocnienia europejskiej reakcji na przestępstwa przeciwko wierzytelności dokumentów. Przyjęty plan działań dotyczy zwiększenia bezpieczeństwa dokumentów podróży wobec nadużywania i podrabiania krajowych dowodów tożsamości wydawanych przez państwa członkowskie oraz dokumentów pobytu wydawanych obywatelom Unii przebywającym w innym państwie członkowskim i członkom ich rodzin.

Nowe dowody osobiste będą wydawane od marca 2019 r. Wymiana obecnie obowiązujących dowodów osobistych na dowody z warstwą elektroniczną będzie dotyczyła dowodów osobistych z określonym terminem ważności, czyli tych dowodów osobistych jakie będą w obiegu do końca 2028 r. Wymiana dokumentów oznacza olbrzymie wyzwanie organizacyjne, pociągające za sobą znaczące koszty (ponad 31 mln dokumentów do wymiany z powodu upływu terminu ważności, powiększone o dowody wymieniane z innych przyczyn). Dlatego też proces wymiany został rozłożony na okres 10 lat i potrwa do 2029 r.

II. Szczegółowe rozwiązania.

Projektowana ustawa, nie wprowadza zmian w zakresie podstawowych zasad wydawania dowodów osobistych. Nowelizacja ogranicza się do uregulowania zagadnień związanych z funkcjonalnościami warstwy elektronicznej dowodu osobistego.

II 1. Przepisy ogólne Zmiany w tej części polegają na dostosowaniu zakresu przedmiotowego ustawy (art. 1 pkt 2a), funkcji dowodu osobistego (art. 4) oraz definicji podstawowych do nowych rozwiązań. Wprowadzono definicje (art. 2): certyfikatu identyfikacji i uwierzytelniania, certyfikatu podpisu osobistego, certyfikatu potwierdzenia obecności, numeru CAN, podpisu osobistego, profilu osobistego oraz polityki świadczenia usług. Definicje: „personalizacja dowodu osobistego” oraz „uszkodzenie dowodu osobistego” zostały dostosowane do dokumentu z warstwą elektroniczną. Zmiana dotycząca art. 8 wynika jedynie z potrzeby uwzględnienia wszystkich zadań określonych w ustawie, realizowanych przez organy gmin jako zadania zlecone z zakresu administracji rządowej, bez ich wymieniania.

II 2. Zakres danych zawartych w dowodzie osobistym oraz funkcjonalności jego warstwy elektronicznej.

Dodane w tym rozdziale przepisy regulują kwestie związane z zamieszczeniem w dowodzie

osobistym warstwy elektronicznej i jej funkcjonalnościami. W art. 10a wskazano, że oprócz warstwy graficznej dowód osobisty zawiera również warstwę elektroniczną. Przepis ten wymienia wszystkie funkcjonalności nowego dowodu osobistego. Dostęp uprawnionych podmiotów do warstwy elektronicznej będzie umożliwiał potwierdzenie prawdziwości danych zamieszczonych w warstwie graficznej. Nowy dokument będzie też umożliwiał: uwierzytelnienie posiadacza dowodu osobistego w systemach teleinformatycznych (certyfikat identyfikacji i uwierzytelnienia), potwierdzenie obecności posiadacza dowodu osobistego w określonym czasie i miejscu lub udziału w usługach (certyfikat potwierdzenia obecności) oraz składanie podpisu osobistego (certyfikat podpisu osobistego). Dowód osobisty będzie też zawierał przestrzeń umożliwiającą zamieszczenie kwalifikowanego certyfikatu podpisu elektronicznego.

Wszystkie dowody osobiste będą wyposażone w certyfikat potwierdzenia obecności. Natomiast certyfikat identyfikacji i uwierzytelnienia będzie zamieszczony w dowodach osobistych osób posiadających pełną zdolność do czynności prawnych oraz osób posiadających ograniczoną zdolność do czynności prawnych (art. 12a ust. 2). Certyfikat podpisu osobistego będą posiadały dowody osobiste wydane osobom, które posiadają pełną zdolność do czynności prawnych i przy składaniu wniosku o wydanie dowodu osobistego nie wyraziły sprzeciwu na zamieszczenie tego certyfikatu, oraz osobom małoletnim, które w okresie ważności dowodu osobistego ukończą 18 rok życia, jeżeli rodzic, opiekun prawny lub kurator tej osoby przy składaniu wniosku o wydanie dowodu osobistego nie wyraził sprzeciwu na zamieszczenie tego certyfikatu (art. 12 a ust. 3). Zasadą ma być, że każdy dowód osobisty osoby posiadającej pełną zdolność do czynności prawnych oraz osoby posiadającej ograniczoną zdolność do czynności prawnych będzie wyposażony w funkcjonalność podpisu osobistego (certyfikat podpisu osobistego), ale dla osób, które nie będą chciały korzystać z tej funkcjonalności, projekt przewiduje, możliwość złożenia sprzeciwu. W sytuacji, gdy już po wydaniu takiego dowodu, jego posiadacz uzna potrzebę korzystania z osobistego podpisu elektronicznego, będzie mógł wystąpić o wymianę dowodu (art. 46 ust. 1 pkt 5b).

Zakres danych warstwy elektronicznej pokrywa się z zakresem warstwy graficznej, z wyłączeniem numeru CAN, zapewniającego nawiązanie bezpiecznego połączenia pomiędzy warstwą elektroniczną dowodu osobistego a urządzeniem lub systemem teleinformatycznym, za pośrednictwem czytnika kart. Numer ten jest jedyną daną dodaną w stosunku do dotychczasowej zawartości warstwy graficznej dowodu osobistego (art. 12 pkt 2 lit. e).

Uwzględnienie jednej, obowiązkowej cechy biometrycznej w postaci wizerunku twarzy, stanowiącej powtórzenie elektronicznej funkcjonalności paszportu biometrycznego, zgodnie z zaleceniami ICAO DOC9303 dla dokumentów typu TD1 MRTD, umożliwi elektroniczne odczytanie zakresu informacyjnego tych samych danych, co uwidocznione w warstwie wizualnej dokumentu (bez informacji technicznych, np. numeru CAN, zapisu w polu MRZ). Przedmiotowa funkcjonalność umożliwi automatyzację procesu przejścia posiadacza dokumentu przez kontrolę graniczną.

Projektowany przepis art. 12b stanowi, że dostęp do danych zamieszczonych w warstwie graficznej, zawsze jest kontrolowany przez posiadacza dokumentu. Udostępnienie danych następuje wyłącznie na żądanie uprawnionych organów lub za zgodą wyrażoną przez posiadacza dowodu osobistego. Natomiast przepis art. 12c stanowi, że e-Dowód gwarantuje bezpieczeństwo danych zawartych w warstwie elektronicznej przed skopiowaniem kluczy prywatnych powiązanych z certyfikatami zamieszczonymi w dowodzie oraz umożliwia zweryfikowanie, że dane te są zamieszczone przez uprawniony do tego organ.

Użycie osobistego podpisu elektronicznego, dla podmiotu publicznego będzie wywoływało taki sam skutek jak podpis własnoręczny, a w przypadku innego podmiotu taki sam skutek zaistnieje, o ile podmiot ten i posiadacz dowodu osobistego wyrażą na to zgodę (art. 12d). Należy się spodziewać, że możliwość posługiwania się osobistym podpisem elektronicznym na równi z podpisem własnoręcznym, czy kwalifikowanym podpisem elektronicznym, uwzględniając obowiązek posiadania dowodu osobistego przez pełnoletnich obywateli Rzeczypospolitej Polskiej, zamieszkujących na jej terytorium (obowiązujący art. 5 ust. 2), przyczyni się do upowszechnienia komunikacji elektronicznej obywateli nie tylko z administracją i służbą zdrowia, ale także z podmiotami komercyjnymi.

W art. 12e wymienione zostały dane jakie będzie zawierał certyfikat identyfikacji i uwierzytelnienia oraz certyfikat osobistego podpisu elektronicznego, a także certyfikat potwierdzania obecności. Dane te będą pozwalały w sposób niezaprzeczalny na weryfikację czynności elektronicznych dokonywanych z wykorzystaniem dowodu osobistego. Ważność certyfikatów będzie taka sama jak dowodu osobistego, tj. 5 i 10 lat (art. 12f ust. 1), poza wymienionymi wyjątkami. Pierwszy dotyczy dowodów osobistych z zamieszczonym certyfikatem podpisu osobistego, wydanych osobom posiadającym ograniczoną zdolność do czynności prawnych. W takim przypadku, ważność tego certyfikatu rozpocznie się z chwilą ukończenia 18 roku życia przez posiadacza dowodu osobistego (art.12f ust. 2). Drugi wyjątek przewiduje, że ważność certyfikatów może być krótsza przy zachowaniu ważności warstwy

graficznej dowodu osobistego (art. 12i). Ponieważ certyfikaty będą użytkowane przez cały okres ważności dowodu osobistego, należało przyjąć rozwiązanie szczególne, które umożliwi niezwłoczną reakcję na sytuację uzasadnionego podejrzenia prawdopodobnego naruszenia praw obywateli związanego z naruszeniem bezpieczeństwa wykorzystania warstwy elektronicznej dowodu osobistego. Źródeł takiego zagrożenia nie da się przewidzieć i precyzyjnie opisać dla tak długiego czasu. W celu ochrony praw obywateli minister właściwy do spraw wewnętrznych będzie mógł w takiej sytuacji unieważnić certyfikaty zamieszczone w warstwie elektronicznej dowodu osobistego przy zachowaniu ważności warstwy graficznej dowodu osobistego. Dowód nadal będzie wypełniał funkcję potwierdzania tożsamości, ale nie będzie mógł być wykorzystany jako dokument podróży. Minister właściwy do spraw wewnętrznych będzie mógł przedłużyć ważność warstwy graficznej dowodów osobistych. Taka sytuacja może zaistnieć, jeżeli unieważnienie certyfikatów będzie dotyczyło dużej liczby dowodów, w tym dokumentów z krótkim terminem ważności, i nie będzie możliwa ich szybka wymiana. Minister może także zdecydować o wydawaniu, przez określony czas, dowodów osobistych niezawierających warstwy graficznej, jeżeli przygotowanie prawidłowo działających rozwiązań technicznych, będzie tego wymagało. Decyzję w sprawie unieważnienia certyfikatów, przedłużeniu ważności dowodów osobistych oraz harmonogram wymiany dowodów osobistych, a także informację o okresie, w którym będą wydawane dowody osobiste niezawierające w warstwie elektronicznej certyfikatów identyfikacji i uwierzytelnienia, certyfikatu podpisu osobistego oraz certyfikatu potwierdzenia obecności, minister właściwy do spraw wewnętrznych ogłosi w drodze obwieszczenia. Jest to najszybsza forma zakomunikowania o dokonaniu zmiany w zakresie ważności wydanych dowodów osobistych. Niezależnie od tego, minister podejmie inne środki mające na celu dotarcie z tą informacją do wszystkich zainteresowanych obywateli. Przepisy dotyczące działań ministra właściwego do spraw wewnętrznych wynikających z art. 12i odnoszą się wyłącznie do certyfikatów zamieszczanych przez ministra właściwego do spraw wewnętrznych, tj. certyfikatu identyfikacji i uwierzytelnienia, certyfikatu podpisu osobistego i certyfikatu potwierdzenia obecności. Nie odnoszą się do kwalifikowanego certyfikatu podpisu elektronicznego, dla którego przewidziano w dowodzie osobistym jedynie przestrzeń, umożliwiającą jego zamieszczenie.

Projektowany art. 12g przewiduje możliwość zawieszenia i cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego. Zawieszenie certyfikatów zawsze spowoduje zawieszenie ważności dowodu osobistego. Czynności

dokonane w okresie zawieszenia albo unieważnienia certyfikatów nie wywołają skutków prawnych (art. 12g). Natomiast późniejsze cofnięcie zawieszenia certyfikatów nie wpłynie na ważność czynności dokonanej w okresie zawieszenia (art. 12 g i art. 12h). Uwzględniając zasady zawieszania i cofania zawieszenia certyfikatów, opisane szczegółowo w projektowanym rozdziale 3a, posiadacz dowodu osobistego każdorazowo będzie decydował o zawieszeniu i cofnięciu zawieszenia certyfikatów wpływając bezpośrednio na ważność czynności dokonywanych z użyciem certyfikatów.

Minister właściwy do spraw wewnętrznych będzie odpowiedzialny za wydawanie certyfikatów i zapewnienie możliwości ich weryfikacji (art. 12j) oraz za określenie i opublikowanie polityki świadczenia usług dla dowodu osobistego z warstwą elektroniczną (art.12k ust. 1). Posiadacz dowodu osobistego będzie obowiązany postępować zgodnie z zasadami określonymi w opublikowanym przez ministra właściwego do spraw wewnętrznych dokumencie określającym techniczne i organizacyjne rozwiązania dotyczące sposobu, zakresu oraz warunków tworzenia, wydawania i używania certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego (art. 12k ust. 2).

Regulacje związane z wymaganiami dla warstwy elektronicznej oraz sposobem wydawania i używania certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego zostaną określone przez ministra właściwego do spraw wewnętrznych w rozporządzeniu (art. 12l).

Przepisy dotyczące zawieszania i cofania zawieszenia certyfikatów, tak samo, jak działania ministra właściwego do spraw wewnętrznych opisane wyżej, odnoszą się wyłącznie do certyfikatów zamieszczanych przez ministra właściwego do spraw wewnętrznych, tj. certyfikatu identyfikacji i uwierzytelnienia, certyfikatu podpisu osobistego i certyfikatu potwierdzenia obecności. Nie odnoszą się do kwalifikowanego certyfikatu podpisu elektronicznego, dla którego przewidziano w dowodzie osobistym jedynie przestrzeń, umożliwiającą jego zamieszczenie. Zamieszczenie w dowodzie osobistym kwalifikowanego certyfikatu podpisu elektronicznego wraz z danymi do składania podpisu oraz korzystanie z tego podpisu odbywa się na ryzyko posiadacza dowodu osobistego oraz dostawcy usługi zaufania. W przypadku unieważnienia dowodu osobistego z przyczyn określonych w ustawie skutkującego niemożnością korzystania z tego certyfikatu, Skarb Państwa nie ponosi kosztów związanych z zakupem nowego kwalifikowanego certyfikatu podpisu elektronicznego (art. 12a ust. 3).

II 3. Zasady wydawania dowodu osobistego.

Projektowane zmiany w zakresie składania wniosku o wydanie dowodu osobistego dotyczą porządkowej zmiany w zakresie art. 24 ust. 3 polegającej na uspołnieniu przepisów regulujących zasady składania wniosków i zgłoszeń, a także doprecyzowaniu, że wniosek o wydanie dowodu osobistego, składa się „osobiście”. Z uwagi na kwestionowanie przez obywateli, przy obecnym brzmieniu przepisu, obowiązku osobistego składania wniosku o wydanie dowodu osobistego, doprecyzowano ten przepis. Jednocześnie dokonując zmiany w zakresie przepisu art. 28 ust. 1 pkt 11 umożliwiono opatrzenie wniosku składanego w formie dokumentu elektronicznego - osobistym podpisem elektronicznym. Zakres wniosku uzupełniono o możliwość wyrażenia sprzeciwu na zamieszczenie w warstwie elektronicznej dowodu osobistego certyfikatu osobistego podpisu elektronicznego oraz złożenia żądania wydania koperty z kodem umożliwiającym odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego w alfabecie Braille'a (art. 28 pkt 13 i 14).

W związku z wprowadzeniem dowodu osobistego zawierającego warstwę elektroniczną, odbiór dowodu będzie się wiązał z wydaniem kodu umożliwiającego odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego. Organ gminy zapewni też posiadaczowi dowodu osobistego warunki pozwalające na ustalenie kodów umożliwiających identyfikację elektroniczną i złożenie podpisu osobistego oraz odbiór kodu umożliwiającego odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego (art. 30 ust. 1a). Odbiór dowodu osobistego zawierającego certyfikat identyfikacji i uwierzytelnienia oraz certyfikat podpisu osobistego, a także odbiór kodu umożliwiającego odblokowanie tych certyfikatów i dokonanie czynności ustalenia kodów umożliwiających identyfikację elektroniczną i złożenie podpisu osobistego będzie następował osobiście (art. 30 ust. 3). Dzięki temu zapewnione zostanie uwierzytelnienie na poziomie wysokim w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE. Przewidziana możliwość odbioru dowodu osobistego przez pełnomocnika dotyczy wyłącznie odbioru dowodu osobistego bez odbioru kodu umożliwiającego odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego bez możliwości dokonania czynności ustalenia ww. kodów. Pełnomocnik będzie mógł dokonać odbioru

dowodu osobistego w sytuacji gdy przeszkoda uniemożliwiająca osobisty odbiór dowodu osobistego powstała po złożeniu wniosku o wydanie dowodu osobistego. Przewidziano także możliwość odbioru dokumentu w miejscu pobytu wnioskodawcy, o ile miejsce pobytu tej osoby położone jest na terenie gminy, w przypadku gdy wnioskodawca złożył wniosek w formie dokumentu elektronicznego i nie może osobiście odebrać dowodu osobistego z powodu choroby, niepełnosprawności lub innej niedającej się pokonać przeszkody, która powstała po dniu złożenia wniosku o wydanie dowodu osobistego. Obecnie obowiązujące przepisy przewidują jedynie możliwość przyjęcia wniosku o wydanie dowodu osobistego w miejscu pobytu wnioskodawcy i w takiej sytuacji ustanowienie pełnomocnika do odbioru dokumentu tylko w przypadku, gdy w chwili składania wniosku ma miejsce sytuacja uniemożliwiająca osobiste złożenie wniosku. Podczas stosowania przepisów ustawy, okazało się jednak, że nie rozwiązuje to wszystkich możliwych przypadków braku możliwości osobistego udziału w procedurze odbioru dowodu osobistego.

II 4. Zawieszanie i cofanie zawieszenia certyfikatów zamieszczonych w dowodzie osobistym.

Czynności wykonane z użyciem osobistego podpisu elektronicznego oraz certyfikatu identyfikacji i uwierzytelnienia w okresie zawieszenia albo po ich unieważnieniu nie wywołają skutków prawnych (art. 12g). Projekt przewiduje możliwość zawieszania certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego, jeżeli posiadacz dokumentu czasowo utracił nad nim kontrolę (art. 32a), zawieszenie certyfikatów powoduje zawieszenie ważności dowodu osobistego (art. 12). Zawieszenie następuje na 7 dni kalendarzowych od dnia zgłoszenia. Jeżeli w tym okresie nie nastąpi cofnięcie zawieszenia, certyfikaty oraz dowód osobisty podlegają unieważnieniu z mocy prawa.

Przepisy dodanego rozdziału 3a regulują zasady zawieszania i cofania zawieszenia certyfikatów zamieszczonych w dowodzie osobistym. Zgłoszenia zawieszenia będzie mógł dokonać posiadacz dowodu osobistego mający pełną zdolność do czynności prawnych, a w imieniu osoby nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do czynności prawnych - rodzic, opiekun prawny lub kurator, a także pełnomocnik legitymujący się pełnomocnictwem szczególnym do dokonania takiej czynności (art. 32a ust.1 - 3). Przewidziana forma zgłoszenia obejmuje wszystkie możliwe warianty, tj. zgłoszenie osobiste w organie gminy, w formie dokumentu elektronicznego lub bezpośrednio w Rejestrze Dowodów Osobistych po uwierzytelnieniu (art. 32b ust. 1). Zgłaszający

zawieszenie będzie otrzymywał nieodpłatnie zaświadczenie potwierdzające datę i godzinę zgłoszenia (art. 32b ust. 2 – 4). Taki sam tryb postępowania będzie miał zastosowanie w przypadku cofania zawieszenia certyfikatów. Minister właściwy do spraw wewnętrznych będzie wydawał certyfikaty oraz zapewniał możliwość ich weryfikacji (art.12j), będzie więc także organem właściwym do zawieszania i cofania zawieszenia certyfikatów na podstawie danych wprowadzanych do Rejestru Dowodów Osobistych, odpowiednio, przez organy gmin przyjmujące zgłoszenia lub osobę zgłaszającą zawieszenie przy wykorzystaniu dedykowanej do tego usługi elektronicznej udostępnionej przez ministra właściwego do spraw informatyzacji (art. 32e). Wspomniana usługa elektroniczna umożliwi zawieszenie i cofnięcie zawieszenia certyfikatów bez udziału pracownika organu gminy, bezpośrednio przez posiadacza dowodu osobistego po jego uwierzytelnieniu w sposób określony w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

II 5. Wymiana i unieważnianie dowodu osobistego

W rozdziale regulującym kwestie wymiany i unieważniania dowodu osobistego uzupełniono przepis art. 46 o dodatkowe przesłanki do wydania dowodu osobistego wynikające z wprowadzenia do dowodów osobistych warstwy elektronicznej, tj. związane z unieważnieniem dowodu osobistego w wyniku unieważnienia certyfikatów zamieszczonych w warstwie elektronicznej, żądaniem obywatela wymiany dowodu osobistego na dowód z warstwą elektroniczną lub na dowód z certyfikatem identyfikacji i uwierzytelnienia (osoba, która ukończyła 13 rok życia i będzie chciała wymienić dowód z tym certyfikatem; rozwiązanie to może się przyczynić do zwiększenia liczby osób . które będą korzystać z tej funkcjonalności) lub na dowód z certyfikatem osobistego podpisu elektronicznego w sytuacji, gdy posiadacz dysponuje dowodem bez tego certyfikatu (składając wniosek zgłosił sprzeciw na zamieszczenie tego certyfikatu) lub na żądanie obywatela, w którego dowodzie osobistym został zamieszczony certyfikat osobistego podpisu elektronicznego, ale nie jest on ważny, pomimo uzyskania pełnoletniości przez posiadacza tego dowodu osobistego (przypadek małoletniej kobiety wchodzącej w związek małżeński – od 16 roku życia), w przypadku ubezwłasnowolnienia (utruty pełnej zdolności do czynności prawnych) posiadacza dowodu osobistego, w którego dowodzie osobistym w warstwie elektronicznej został zamieszczony certyfikat osobistego podpisu elektronicznego. Dla tego przypadku przewidziano obowiązek

kuratora lub opiekuna prawnego posiadacza dowodu osobistego, powiadomienia organu dowolnej gminy o ubezłasnowolnieniu całkowitym lub częściowym posiadacza takiego dowodu osobistego (art. 49a). Brak możliwości korzystania z certyfikatów identyfikacji i uwierzytelnienia lub certyfikatu podpisu elektronicznego także będzie stanowił przesłankę do wymiany dowodu osobistego.

Przewidziano możliwość zgłoszenia utraty lub uszkodzenia dowodu osobistego w formie dokumentu elektronicznego bezpośrednio w Rejestrze Dowodów Osobistych po uwierzytelnieniu się w sposób określony w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Takie działanie umożliwi niezwłoczne unieważnienie dowodu bez udziału urzędnika, a więc również w dni wolne od pracy (art. 47 ust. 3a i art. 50 ust. 3 pkt 10). Taką samą możliwość przewidziano w opisanym wcześniej przypadku zgłaszania zawieszenia i przywrócenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego (art. 50 ust. 3 pkt 9). Zapewniono również unieważnienie dowodu osobistego w przypadku zgłoszenia Policji utraty dowodu osobistego w wyniku przestępstwa (art. 50 ust. 3 pkt 11). Projektowane przepisy przewidują, że w przypadku zgłoszenia Policji utraty dowodu osobistego w wyniku przestępstwa, dowód osobisty będzie unieważniany z dniem zgłoszenia. Unieważnienie dowodu w Rejestrze Dowodów Osobistych ma następować w takim przypadku na podstawie informacji otrzymywanych za pośrednictwem Krajowego Systemu Informacji Policji i Krajowego Systemu Informatycznego. Systemy te nie posiadają funkcjonalności odnotowywania czasu, w jakim nastąpiło zgłoszenie utraty, a rejestrują jedynie datę zgłoszenia oraz datę i czas wprowadzenia zdarzenia do tych systemów, które mogą się różnić. Z tych względów odpowiednio dla tego przypadku w art. 50 ust. 3 pkt 11 wskazano, że unieważnienie dowodu osobistego nastąpi z dniem zgłoszenia. W art. 50 ust. 3 dodano również wskazanie czasu, w którym następuje unieważnienie dowodu osobistego w przypadku gdy minister właściwy do spraw wewnętrznych przedłuży ważność warstwy graficznej dowodów osobistych oraz w przypadku orzeczenia sądu o ubezłasnowolnieniu posiadacza dowodu osobistego, którego dowód osobisty w warstwie elektronicznej miał zamieszczony certyfikat osobistego podpisu elektronicznego.

W wyniku wprowadzonych zmian wskazano również organy właściwe do unieważnienia dowodu osobistego, tj. ministra właściwego do spraw informatyzacji, który prowadzi Rejestr Dowodów Osobistych, w przypadku zgłoszenia Policji utraty dowodu osobistego oraz w przypadku dokonania zgłoszenia utraty lub uszkodzenia dowodu bezpośrednio w Rejestrze

Dowodów Osobistych, oraz organ gminy, który otrzymał orzeczenie o ubezwłasnowolnieniu posiadacza dowodu osobistego. Uzupełniono również przepis art. 51 ust. 2 o wskazanie, że dowód osobisty podlega unieważnieniu z mocy prawa również w wyniku unieważnienia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego, z wyłączeniem przypadku przedłużenia przez ministra właściwego do spraw wewnętrznych ważności warstwy graficznej dowodu osobistego.

Przepis art. 53 dotyczący prowadzonego przez ministra właściwego do spraw informatyzacji wykazu unieważnionych dowodów osobistych został uzupełniony o dane o zawieszonych dowodach. Na podstawie dowodu osobistego w czasie jego zawieszenia, tak jak na podstawie dowodu unieważnionego, nie powinny być dokonywane żadne czynności, dlatego powszechnie dostępny wykaz uzupełniono o te dane.

Dodano przepis art. 53a dotyczący utylizacji dowodów osobistych z warstwą elektroniczną. Chodzi o skuteczne zniszczenie danych zawartych w warstwie elektronicznej dowodu osobistego, celem uniemożliwienia ich wykorzystania.

Upoważnienie dla ministra właściwego do spraw wewnętrznych do określenia w porozumieniu z ministrem właściwym do spraw informatyzacji w rozporządzeniu wzoru nowego dowodu osobistego oraz zasad wydawania dowodów osobistych i wzorów formularzy uzupełniono o nowy wzór informacji o zawartości certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego, a także o określenie sposobu i trybu utylizacji dowodów osobistych z warstwą elektroniczną oraz blankietów tych dowodów osobistych.

II 6. Rejestr Dowodów Osobistych i udostępnianie danych.

Zakres danych gromadzonych w Rejestrze Dowodów Osobistych uzupełniono o dane dotyczące nowych statusów dowodu osobistego, tj. datę i czas zawieszenia, datę i czas cofnięcia zawieszenia oraz datę ważności wynikającą z decyzji ministra właściwego do spraw wewnętrznych o unieważnieniu certyfikatów zamieszczonych w warstwie elektronicznej (certyfikatu identyfikacji i uwierzytelnienia, certyfikatu podpisu osobistego oraz certyfikatu potwierdzenia obecności) oraz o przedłużeniu ważności dowodów osobistych (art. 12i ust. 3). W rejestrze znajdzie się także informacja o statusie warstwy elektronicznej dowodu osobistego. Przechowywanie tej informacji będzie konieczne z uwagi na rozwiązania przewidziane w projektowanym art. 12i, tj. możliwość unieważnienia przez ministra właściwego do spraw wewnętrznych certyfikatów zamieszczonych w warstwie elektronicznej

przy zachowaniu ważności warstwy graficznej dowodu osobistego.

W zakresie przepisów dotyczących postępowania z dokumentacją związaną z dowodami osobistymi dodano jedynie, że w kopercie dowodowej będzie przechowywana również koperta z kodem umożliwiającym odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego (art. 62 ust. 4 pkt 5). Koperta będzie przechowywana do czasu jej odbioru przez posiadacza dowodu osobistego.

Projektowane przepisy, w wyniku poszerzenia statusów dowodu osobistego o „zawieszenie”, wprowadzają również zmiany dotyczące udostępniania danych. Udostępnienie danych z wykazu unieważnionych (i zawieszonych) dowodów osobistych, będzie dotyczyło również zawieszonych dowodów osobistych (art. 74).

Niezależnie od projektowanych zmian związanych z wdrożeniem e-Dowodu przewidziano rezygnację z dwuinstancyjności postępowań prowadzonych na podstawie art. 52. Decyzja wydana na podstawie tego przepisu posiada rygor natychmiastowej wykonalności, zatem podlega natychmiastowemu wykonaniu z mocy prawa, niezależnie od tego, czy strona wniosła odwołanie, czy też nie. W wyniku tej decyzji, dowód osobisty jest unieważniony i nie ma możliwości cofnięcia tego unieważnienia nawet w przypadku, gdy wojewoda wyda rozstrzygnięcie stwierdzające unieważnienie za nieuzasadnione. Stosunkowo niewielka jest też liczba odwołań od decyzji wydawanych przez organy gmin – z 520 decyzji w sprawach dowodów osobistych wydanych przez organy gmin w 2016 r. jedynie 8 zostało zaskarżonych do wojewody, a 3 decyzje wojewody zostały zaskarżone do WSA, z czego jedno rozstrzygnięcie sąd administracyjny uchylił. Uwzględniając te dane, odstąpienie od zasady dwuinstancyjności nie powinno utrudniać sprawowania nadzoru przez wojewodów i ministra właściwego do spraw wewnętrznych nad organami niższego stopnia.

IV. Zmiany w przepisach obowiązujących.

Uwierzytelnianie to proces przeprowadzany przez usługodawcę w celu potwierdzenia tożsamości usługobiorcy. Przeprowadzenie tego procesu wymaga, aby usługobiorca uprzednio zidentyfikował się w systemie teleinformatycznym, czyli zadeklarował swoją tożsamość. Jeżeli usługa wymaga potwierdzenia tożsamości użytkownika jako określonej osoby fizycznej, to mechanizm uwierzytelniania musi wykorzystywać w tym celu określony „środek identyfikacji elektronicznej”, a więc materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę, takie jak np.: imię, nazwisko, data urodzenia i numer

PESEL. Usługodawca musi mieć zaufanie do danych identyfikujących osobę fizyczną, zawartych w takim środku identyfikacji elektronicznej, stąd też uprzednio musi sam dokonać wiarygodnego ich ustalenia na przykład na podstawie dowodu tożsamości okazanego przez świadczeniobiorcę w trakcie jego wizyty w jednej z placówek usługodawcy. Ten sam usługodawca może także podjąć decyzję, iż bardziej opłacalnym jest skorzystanie z mechanizmu uwierzytelnienia udostępnianego przez inny podmiot, który zarządza systemem identyfikacji elektronicznej, w ramach którego wydaje własny środek identyfikacji elektronicznej.

Kolejnym narzędziem, stosowanym w usługach online jest podpis elektroniczny, który w najprostszej formie stanowi dane w postaci elektronicznej, określające tożsamość osoby składającej podpis, które są dołączone lub logicznie powiązane z podpisywanym dokumentem elektronicznym, i które użyte są przez podpisującego jako podpis. Co do zasady wymagane jest, aby taki podpis elektroniczny był unikalnie przyporządkowany podpisującemu, aby mógł być złożony przy użyciu danych, których podpisujący może z dużą dozą pewności użyć pod wyłączną swoją kontrolą oraz aby był tak powiązany z podpisanym dokumentem elektronicznym, że każda późniejsza zmiana dokonana w tym dokumencie będzie mogła być wykryta dowodząc tym samym o nieważności złożonego na tym dokumencie podpisu elektronicznego.

Odbierając dowód osobisty w urzędzie gminy obywatel otrzyma możliwość posługiwania się przyporządkowanym mu środkiem identyfikacji elektronicznej, zwanym dalej „profilem osobistym”. Przedmiotowy środek wydawany będzie w ramach „systemu identyfikacji elektronicznej”, rozumianego jako zbiór narzędzi i procedur niezbędnych do prawidłowej obsługi wydawanego środka identyfikacji elektronicznej. Organem zarządzającym wspomnianym wyżej systemem identyfikacji elektronicznej, jak również przeprowadzającym proces uwierzytelnienia w tym systemie z wykorzystaniem „profilu osobistego”, będzie minister właściwy do spraw informatyzacji. Stroną wydającą „profil osobisty”, której zadania będą realizowane w urzędach gmin, będzie minister właściwy do spraw wewnętrznych.

Minister właściwy do spraw informatyzacji, zgodnie z przepisami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570) zarządza już obecnie systemem identyfikacji elektronicznej, w którym wydawany jest środek identyfikacji elektronicznej: „profil zaufany ePUAP”. Działanie wspomnianego wyżej systemu identyfikacji elektronicznej zapewniane jest w ramach systemu

teleinformatycznego przy użyciu którego obsługiwana jest „elektroniczna platforma usług administracji publicznej” (ePUAP). W tym samym systemie teleinformatycznym minister właściwy do spraw informatyzacji zapewnia obywatelom posiadającym „profil zaufany ePUAP” możliwość opatrzenia dokumentu elektronicznego podpisem elektronicznym zwanym „podpisem potwierdzonym profilem zaufanym ePUAP”. Zaznaczyć jednakże należy, że możliwość złożenia takiego podpisu elektronicznego może być udostępniona jako element funkcjonalny usługi online udostępnionej przez podmiot publiczny na ePUAP. Powyższe możliwe jest także do realizacji w innym publicznym systemie teleinformatycznym, o ile podmiot publiczny, odpowiedzialny za ten system, uprawniony jest do jego integracji z systemem teleinformatycznym przy użyciu którego zapewniane jest funkcjonowanie ePUAP. W świetle powyższego po wejściu w życie przepisów regulujących funkcjonowanie „profilu osobistego” minister właściwy do spraw informatyzacji zobowiązany byłby do zarządzania dwoma systemami identyfikacji elektronicznej.

Mając powyższe na uwadze dokonano zmian w ustawie z dnia z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (art. 24) oraz w 45 ustawach w zakresie wskazania rodzaju podpisów i środków identyfikacji elektronicznej. Przyjęto rozwiązanie, w którym zarówno „profil zaufany”, jak i „profil osobisty” będą wydawane w ramach jednego systemu identyfikacji elektronicznej. Funkcjonowanie przedmiotowego systemu identyfikacji elektronicznej zapewnione zostanie przy użyciu dedykowanego systemu teleinformatycznego. Jednocześnie obecnie realizowane zadania związane w wydawaniem i obsługą „profilu zaufanego ePUAP” zostaną pod względem prawnym i technicznym wyłączone ze zbioru zadań realizowanych w ramach ePUAP, a przedmiotowemu środkowi identyfikacji elektronicznej nadana zostanie nazwa „profil zaufany”.

W konsekwencji powyższego, ze zbioru zadań realizowanych w ramach ePUAP wyłączona zostanie pod względem prawnym i technicznym także funkcjonalność pozwalająca na opatrywanie dokumentów elektronicznych „podpisem potwierdzonym profilem zaufanym ePUAP”. Funkcjonalność przedmiotowego podpisu elektronicznego realizowana będzie przez ministra właściwego do spraw informatyzacji przy użyciu wspomnianego wyżej systemu teleinformatycznego zapewniającego funkcjonowanie systemu identyfikacji elektronicznej, w którym wydawany będzie „profil zaufany” i „profil osobisty”. Jednocześnie, mając na uwadze, że przedmiotowy system teleinformatyczny będzie zapewniał możliwość uwierzytelnienia osoby fizycznej przy użyciu „profilu zaufanego” i „profilu osobistego”,

funkcjonalność tego podpisu elektronicznego zostanie rozszerzona o możliwość jego składania po uprzednim uwierzytelnieniu osoby składającej ten podpis jednym z dwóch wyżej wymienionych środków identyfikacji elektronicznej. W związku z powyższymi zmianami przedmiotowemu podpisowi elektronicznemu nadana zostanie nowa uproszczona nazwa „podpis zaufany”.

Stosownie do art. 22 ust. 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579) minister właściwy do spraw informatyzacji zobowiązany jest do zapewnienia funkcjonowania „krajowego węzła identyfikacji”, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 8 rozporządzenia eIDAS. Jednym z zadań przedmiotowego węzła jest zapewnienie możliwości uwierzytelniania osób fizycznych w krajowych (publicznych i niepublicznych) usługach online przy użyciu środków identyfikacji elektronicznej wydanych w ramach notyfikowanych (zgodnie z rozporządzeniem eIDAS) zagranicznych systemów identyfikacji elektronicznej. Zasadnym jest zapewnienie usługodawcom usług online jednego punktu przyłączenia systemów teleinformatycznych, przy użyciu których te usługi są świadczone, do systemu teleinformatycznego, który pozwoli na uwierzytelnienie osoby fizycznej przy użyciu krajowych i zagranicznych środków identyfikacji elektronicznej. Wobec powyższego, wspomniany wyżej system teleinformatyczny, przy użyciu którego realizowane będą zadania związane z obsługą „profilu zaufanego”, „profilu osobistego” oraz „podpisu zaufanego”, zintegrowany zostanie z wspomnianym wyżej „krajowym węzłem identyfikacji” oraz wyposażony w funkcjonalność pozwalającą na uwierzytelnianie użytkowników systemów teleinformatycznych, w ramach których świadczone są usługi online przy użyciu zagranicznych środków identyfikacji elektronicznej.

Podsumowując powyższe, celem proponowanych zmian jest w szczególności zapewnienie podstaw prawnych dla funkcjonowania systemu teleinformatycznego, z którym integrowane będą publiczne i niepubliczne systemy teleinformatyczne, w których świadczone są usługi online. W rezultacie wspomnianej wyżej integracji, możliwe będzie dokonanie uwierzytelnienia użytkowników usług online, świadczonych w ramach tych systemów teleinformatycznych, przy użyciu „profilu zaufanego”, „profilu osobistego” albo zagranicznego środka identyfikacji elektronicznej wydanego w ramach notyfikowanego systemu identyfikacji elektronicznej. Ponadto usługodawca będzie mógł zapewnić użytkownikom świadczonej usługi online możliwość podpisania wykorzystywanych w tej usłudze dokumentów elektronicznych przy użyciu „podpisu zaufanego”, który będzie mógł

być złożony przez osoby uwierzytelnione uprzednio przy użyciu „profilu zaufanego” albo „profilu osobistego”.

Zmiany wprowadzone w poszczególnych przepisach ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

W art. 1 ustawy o informatyzacji ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), zwanej dalej „ustawą o informatyzacji”, dodaje się punkty 9a i 9b, które stanowią, iż ustawa ta określa zasady funkcjonowania publicznego systemu identyfikacji elektronicznej oraz zasady świadczenia usługi „podpisu zaufanego”. Wspomniane wyżej jednostki odnoszą się do zarządzanego przez ministra właściwego do spraw informatyzacji, systemu identyfikacji elektronicznej, w ramach którego wydawane będą dwa środki identyfikacji elektronicznej „profil zaufany” oraz „profil osobisty”. Minister właściwy do spraw informatyzacji będzie zapewniał ponadto usługę elektroniczną pozwalającą na podpisanie dokumentu elektronicznego „podpisem zaufanym”. Kwestie dotyczące wyżej wymienionych narzędzi informatycznych opisano w dalszej części niniejszego uzasadnienia.

Nadaje się nowe brzmienie art. 3 pkt 14 ustawy o informatyzacji. Dotychczas przedmiotowa jednostka zawierała definicję pojęcia „profil zaufany ePUAP”, obecnie zaś wprowadzana jest definicja pojęcia „profil zaufany”. W projektowanym brzmieniu tej jednostki stanowi się, iż „profil zaufany” to „środek identyfikacji elektronicznej” zawierający zestaw danych identyfikujących i opisujących osobę fizyczną. Użyte tu pojęcie „środek identyfikacji elektronicznej” stanowi referencję do art. 3 pkt 2 rozporządzenia eIDAS i w powiązaniu z nowym brzmieniem omawianej jednostki wskazuje, iż „profil zaufany” to niematerialna jednostka zawierająca dane identyfikujące osobę, używane do celów uwierzytelniania dla usługi online. Dotychczas „profil zaufany” był obsługiwany przy użyciu narzędzi informatycznych stanowiących część systemu teleinformatycznego, przy użyciu którego minister właściwy do spraw informatyzacji realizował zbiór zadań związanych z funkcjonowaniem elektronicznej platformy usług administracji publicznej (ePUAP). W efekcie planowanej reorganizacji „profil zaufany” będzie wydawany w ramach wspomnianego już wyżej „publicznego systemu identyfikacji elektronicznej”, obsługiwanego przy użyciu odrębnego systemu teleinformatycznego, stąd też dla porządku zrezygnowano w nazwie tego środka identyfikacji elektronicznej z akronimu „ePUAP”.

W art. 3 dodaje się pkt 14a, który będzie regulował definicję nowego pojęcia „profilu osobistego”. Profil osobisty, podobnie jak wspomniany wyżej „profil zaufany”, stanowił

będzie środek identyfikacji elektronicznej, z tą jednakże istotną różnicą, iż wydawany będzie on obywatelom wraz z dowodem osobistym, o czym stanowiły będą znowelizowane przepisy ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych.

W art. 3 dodaje się ponadto pkt 14b definiujący pojęcie „podpis zaufany”. Podpis zaufany stanowił będzie podpis elektroniczny, w rozumieniu art. 3 pkt 10 rozporządzenia eIDAS. Usługa elektroniczna, pozwalająca na opatrzenie dokumentu elektronicznego „podpisem zaufanym” będzie wymagała uwierzytelnienia sygnatariusza oraz dokonania autoryzacji czynności podpisu dokumentu przy użyciu „profilu zaufanego” albo „profilu osobistego”. Złożony na dokumencie elektronicznym „podpis zaufany” będzie zawierał dane identyfikujące sygnatariusza, czas złożenia tego podpisu oraz identyfikator środka identyfikacji elektronicznej przy użyciu którego uwierzytelniono osobę, która złożyła ten podpis elektroniczny. Autentyczność podpisu elektronicznego, a także integralność tego podpisu elektronicznego i opatrzonego nim dokumentu elektronicznego, będzie zapewniana przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji. Podpis zaufany stanowił będzie narzędzie, które zastąpi dotychczas stosowany w administracji publicznej „podpis potwierdzony profilem zaufanym ePUAP”, stąd też wraz z wprowadzeniem pkt 14b jednocześnie uchyla pkt 15.

W art. 19a uchyla się ust. 2a-2c, a jednocześnie w ust. 3 uchyla się pkt 2-4. Uwierzytelnianie użytkowników ePUAP będzie dokonywane przy użyciu środków identyfikacji elektronicznej obsługiwanych w publicznym systemie identyfikacji elektronicznej. Wobec powyższego nie będzie już konieczności bezpośredniego wykorzystywania w tym celu środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy. Stąd też uchyla się przepisy, które dotychczas stanowiły podstawę prawną do takiego działania.

Nadaje się nowe brzmienie art. 20a ust. 2 pkt 1. Zmiana ma na celu dostosowanie brzmienia obecnego przepisu do terminologii stosowanej w rozporządzeniu eIDAS, zgodnie z którym notyfikacji podlega system identyfikacji elektronicznej, a w procesie tym określa się poziom zaufania wydawanego w tym systemie środka identyfikacji elektronicznej.

W art. 20a ust. 1 w pkt 2 usuwa się akronim „ePUAP”, w związku z uchyleniem przepisów dotyczących stosowanego dotychczas „profilu zaufanego ePUAP” oraz wprowadzanymi regulacjami dotyczącymi „profilu zaufanego”.

W art. 20a w ust. 1 dodaje się pkt 4, który stanowił będzie, iż uwierzytelnienie użytkowników systemu teleinformatycznego korzystających z usług online udostępnianych przez podmioty

określone w art. 2 ustawy o informatyzacji, będzie mogło następować przy użyciu profilu zaufanego, a więc środka identyfikacji elektronicznej, który każdy obywatel otrzyma wraz z nowym dowodem osobistym.

W art. 20a ust. 3 uchyla się pkt 2. Jak już wyżej wspomniano, dotychczas wykorzystywane w administracji publicznej narzędzia takie jak „profil zaufany ePUAP” oraz „podpis potwierdzony profilem zaufanym ePUAP” zostaną pod względem prawnym i funkcjonalnym zastąpione odpowiednio „profilem zaufanym” oraz „podpisem zaufanym”. Wobec powyższego uchyla się część upoważnienia, która zobowiązywała ministra właściwego do spraw informatyzacji do określenia w drodze rozporządzenia zasad i warunków funkcjonowania rozwiązań informacyjnych, które nie będą już wykorzystywane.

Dodaje się art. 20aa zobowiązujący ministra właściwego do spraw informatyzacji do zapewnienia systemu teleinformatycznego przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz świadczona będzie usługa „podpisu zaufanego”. Minister właściwy do spraw informatyzacji zapewni podmiotom świadczącym usługi elektroniczne możliwość przyłączenia do tego systemu teleinformatycznego administrowanych przez te podmioty platform usługowych. Powyższe pozwoli tym podmiotom na uwierzytelnianie użytkowników tych platform przy użyciu środków identyfikacji elektronicznej obsługiwanych przez ten system teleinformatyczny, z zastrzeżeniem że podmioty publiczne będą miały możliwość uwierzytelnienia osoby fizycznej przy użyciu „profilu zaufanego” i „profilu osobistego”, natomiast podmioty niepubliczne będą mogły dokonać uwierzytelnienia przy użyciu „profilu osobistego”. Omawiany system teleinformatyczny będzie zintegrowany z „węzłem krajowym”, o którym mowa w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579), stąd też każdemu podmiotowi, który zintegruje własną platformę usługową z tym systemem teleinformatycznym, zapewniona zostanie możliwość uwierzytelnienia osoby fizycznej także przy użyciu zagranicznego środka identyfikacji elektronicznej, wydanego w notyfikowanym systemie identyfikacji elektronicznej, z zastrzeżeniem że w usługach świadczonych przez podmioty publiczne środek taki będzie musiał spełniać co najmniej średni poziom bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b rozporządzenia eIDAS. Oprócz usługi uwierzytelniania „podmioty publiczne” korzystając z usług świadczonych w opisywanym systemie teleinformatycznym będą miały możliwość zapewnienia użytkownikom własnych platform usługowych możliwości opatrzenia dokumentu elektronicznego „podpisem zaufanym”.

Dodaje się art. 20ab zobowiązujący ministra właściwego do spraw informatyzacji do zarządzania publicznym systemem identyfikacji elektronicznej, o którym mowa w art. 20aa pkt 1, w którym wydawany będzie „profil zaufany” i „profil osobisty”, oraz do gromadzenia i przechowywania informacji związanych z zapewnieniem rozliczalności i niezaprzeczalności działań użytkowników korzystających z wyżej wspomnianych środków identyfikacji.

Dodaje się art. 20ac ustanawiający ministra właściwy do spraw informatyzacji administratorem danych wspomnianego wyżej publicznego systemu identyfikacji elektronicznej oraz określający jakie dane dotyczące osób posługujących się „profilem zaufanym” i „profilem osobistym” będą przetwarzane w tym systemie.

Dodaje się art. 20ad. W ust. 1 określa się zakres danych identyfikujących osobę fizyczną, której uwierzytelnienie w systemach teleinformatycznych będzie dokonywane przy użyciu „profilu zaufanego”. Powyższy zakres danych nie będzie stanowił pełnego zbioru danych zawartych w „profilu zaufanym”, ust. 5 stanowi bowiem, że przedmiotowy środek identyfikacji elektronicznej może zawierać także inne dane niezbędne dla realizacji procesów uwierzytelniania i autoryzacji realizowanych przy użyciu tego środka identyfikacji elektronicznej. Celem zachowania zgodności danych identyfikujących posiadacza „profilu zaufanego” z danymi tej osoby zawartymi w rejestrze PESEL, w ust. 2 wprowadza się obowiązek automatycznej weryfikacji tych danych z rejestrem PESEL w procedurze potwierdzania „profilu zaufanego”, o której mowa w art. 20c ust. 1, a którego brzmienie nowelizowane jest w ramach przedmiotowego projektu. Rejestr PESEL zawiera aktualne dane identyfikujące każdego obywatela. W związku z powyższym, w ust. 3 zobowiązuje się ministra właściwego do spraw informatyzacji, który będzie zarządzał i zapewniał obsługę teleinformatyczną publicznego systemu identyfikacji do zapewnienia funkcjonalności w tym systemie teleinformatycznym, która będzie gwarantowała automatyczną aktualizację danych identyfikujących zawartych w „profilu zaufanym” w przypadku każdej zmiany tych danych w rejestrze PESEL. Jednocześnie w ust. 4, mając na uwadze wiarygodność źródła jakim jest rejestr PESEL, stanowi się, że wyżej wspomniana automatyczna aktualizacja danych identyfikujących nie powoduje unieważnienia „profilu zaufanego”. Powyższy mechanizm prawny ma na celu wykluczyć konieczność ponownego wydawania „profilu zaufanego” między innymi przy zmianie nazwiska związanego z zawarciem związku małżeńskiego.

Dodaje się art. 20ae, w którym w zakresie przedmiotowym ustawy o informatyzacji dokonuje się umocowania prawnego „podpisu zaufanego”, jako wywołującego skutki prawne, o ile został utworzony lub złożony w okresie ważności wykorzystanego w tym celu „profilu

zaufanego” albo „profilu osobistego”. Stanowi się ponadto, że o ile przepisy odrębne nie stanowią inaczej „podpis zaufany” ma skutek prawny równoważny podpisowi własnoręcznemu. W ust. 3 wyklucza się możliwość negacji ważności i skuteczności „podpisu zaufanego” wyłącznie z uwagi na fakt, iż jest to podpis złożony w postaci elektronicznej albo ze względu na zaistnienie zmiany danych innych niż dane służące do wydanie środka identyfikacji elektronicznej, który posłużył do złożenia tego podpisu elektronicznego. Zaznaczyć tu należy, że w brzmieniu dodawanego art. 20ad ust. 3 i 4 reguluje się zmianę danych „profilu zaufanego”, stanowiąc jednocześnie, że zmiana ta nie powoduje unieważniania tego środka identyfikacji elektronicznej, stąd też również „podpis zaufany” złożony przy użyciu „profilu zaufanego” w którym nastąpiła taka zmiana nie może być kwestionowany jako nieważny.

Uchyła się art. 20b w związku z zaprzestaniem obsługi dotychczas stosowanego w administracji publicznej „podpisu potwierdzonego profilem zaufanym ePUAP” oraz jego funkcjonalnym i prawnym zastąpieniem przez „podpis zaufany”.

W art. 20c nadaje się nowe brzmienie ust. 1, w którym określa się cztery sposoby potwierdzenia danych „profilu zaufanego” w procesie wydawania oraz unieważniania tego środka identyfikacji elektronicznej. Profil zaufany będzie zawierał cztery dane identyfikujące osobę fizyczną, określone w brzmieniu wprowadzanego art. 20ad ust. 1, których poprawność będzie weryfikowana z danymi zawartymi w rejestrze PESEL. Data urodzenia zawarta jest w numerze PESEL, o czym stanowi art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2017 r. poz. 657). W związku z powyższym potwierdzenia wymaga: imię (imiona), nazwisko i numer PESEL odpowiednio osoby wnioskującej albo posiadacza „profilu zaufanego”. Potwierdzenie to będzie następowało w punkcie potwierdzającym profil zaufany, którego funkcję pełnić będą podmioty określone w ust. 2 i 3 przedmiotowego artykułu. Potwierdzenie to będzie mogło być także dokonane w systemie teleinformatycznym, o którym mowa w dodawanym art. 20aa ust. 1, na podstawie danych zawartych w użytym w tym procesie przez osobę fizyczną: „profilu osobistym”, środka identyfikacji elektronicznej stosowanym do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy spełniającym warunki określone w ustawie o informatyzacji albo w certyfikacie użytego w tym procesie kwalifikowanego podpisu elektronicznego.

W art. 20c dodaje się ust. 1a stanowiący, że przedłużenie ważności „profilu zaufanego” będzie mogło być dokonane w punkcie potwierdzającym profil zaufany a także w systemie teleinformatycznym, o którym mowa w dodawanym art. 20aa ust. 1, na podstawie danych

zawartych w użytych przez posiadacza tego środka identyfikacji elektronicznej „profilu osobistym” albo certyfikacie użytego kwalifikowanego podpisu elektronicznego.

W art. 20c dodaje się pkt 5 uprawniający spółdzielcze kasy oszczędnościowo-kredytowe, o których mowa w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, z późn. zm.), do wystąpienia do ministra właściwego do spraw informatyzacji z wnioskiem o zgodę na pełnienie funkcji punktu potwierdzającego profil zaufany. Przedstawiciele spółdzielczych kas oszczędnościowo-kredytowe, w kontaktach z Ministrem Cyfryzacji, niejednokrotnie wykazywali gotowość do podjęcia działań pozwalających na świadczenie usług punktu potwierdzającego profil zaufany, stąd też mając na względzie zasadność powiększenia zbioru tego rodzaju placówek, a tym samym dostępności „profilu zaufanego”, dodaje się niniejszy przepis.

W art. 20c nadaje się nowe brzmienie ust. 8. Względem obecnego brzmienia przedmiotowej jednostki usunięciu ulega akronim „ePUAP” z nazwy „profil zaufany ePUAP” w rezultacie czego przepis będzie odnosił się obecnie do nowego, wprowadzanego w niniejszej ustawie, środka identyfikacji elektronicznej. Frazę „do autoryzacji” zastąpiono treścią „do uwierzytelniania i autoryzacji”, co w pełni oddaje przyjęty zakres stosowania „profilu zaufanego”.

W związku z wprowadzeniem do porządku prawnego nowego środka identyfikacji elektronicznej oraz nowego podpisu elektronicznego, dodaje się art. 20d upoważniający ministra właściwego do spraw informatyzacji do określenia w drodze rozporządzenia zasad i warunków wydawania, przedłużania ważności, wykorzystywania i unieważniania „profilu zaufanego”, a także składania „podpisu zaufanego”.

Dodaje się art. 20e dotyczący przyłączania systemów teleinformatycznych, w których świadczone są usługi online, do systemu teleinformatycznego przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz „podpisu zaufanego”. Stanowi się, że przyłączenie realizowane będzie na wniosek. Do wniosku konieczne będzie dołączenie oświadczenia o zapoznaniu się z polityką bezpieczeństwa udostępnioną przez ministra właściwego do spraw informatyzacji na stronie podmiotowej w Biuletynie Informacji Publicznej, co podyktowane jest względami bezpieczeństwa systemu, do którego następuje przyłączenie. Ponadto wymaganym będzie przekazanie listy usług online udostępnianych w przyłączanym systemie teleinformatycznym, w której wnioskodawca określi indywidualnie dla każdej usługi online wymagany poziom

bezpieczeństwa środka identyfikacji elektronicznej, przy użyciu którego może być dokonane uwierzytelnianie usługobiorców. Powyższe konieczne jest do przeprowadzenia prawidłowej integracji z uwagi na fakt, iż system teleinformatyczny administrowany przez ministra właściwego do spraw informatyzacji będzie zapewniał możliwość uwierzytelnienia osoby fizycznej przy użyciu środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej spełniających różne poziomy bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b rozporządzenia eIDAS. Mając na względzie usprawnienie obsługi wniosków stanowi się o konieczności przekazania wniosku w postaci elektronicznej opatrzonego kwalifikowanym podpisem elektronicznym.

Dodaje się art. 20f stanowiący, że minister właściwy do spraw informatyzacji wydaje zgodę na przyłączenie systemu teleinformatycznego, o którym mowa w wyżej wspomnianym art. 20e, po przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym. Testy te potwierdzają interoperacyjność przełączanego systemu teleinformatycznego i systemu teleinformatycznego przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz „podpisu zaufanego”, czyli prawidłowość organizacyjnego i technicznego współdziałania tych systemów teleinformatycznych.

Dodaje się art. 20g zobowiązujący podmioty odpowiedzialne za systemy teleinformatyczne, przyłączone do systemu teleinformatycznego przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz „podpisu zaufanego”, do niezwłocznego informowania ministra właściwego do spraw informatyzacji o każdej zmianie danych zawartych w liście udostępnianych usług online oraz określonych dla tych usług wymaganych poziomów bezpieczeństwa środka identyfikacji elektronicznej przy użyciu którego może być dokonane uwierzytelnianie usługobiorców. Wspomniana wyżej lista przekazywana będzie pierwotnie wraz z wnioskiem o przyłączenie systemu teleinformatycznego, w ramach którego świadczone są usługi online, o czym stanowił będzie dodawany art. 20e ust. 2 pkt 2 ustawy o informatyzacji.

Dodaje się art. 20h zobowiązujący ministra właściwego do spraw informatyzacji do informowania w Biuletynie Informacji Publicznej o systemach teleinformatycznych, w których udostępniane są usługi online, przyłączonych do administrowanego przez tego ministra systemu teleinformatycznego przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz świadczona będzie usługa „podpisu zaufanego”. Powyższa informacja ma na celu umożliwić obywatelom ustalenie w których usługach online możliwe jest potwierdzenie własnej tożsamości przy użyciu „profilu

zaufanego”, „profilu osobistego” albo zagranicznego środka identyfikacji elektronicznej, a także podpisanie dokumentu elektronicznego „podpisem zaufanym”.

W celu umożliwienia użytkownikom usług online udostępnionych na ePUAP potwierdzenia własnej tożsamości przy użyciu „profilu zaufanego”, „profilu osobistego” albo zagranicznego środka identyfikacji elektronicznej, a także podpisania dokumentu elektronicznego „podpisem zaufanym”, dodaje się art. 20i stanowiący, iż system ten przyłącza się z mocy ustawy do systemu teleinformatycznego przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz świadczona będzie usługa „podpisu zaufanego”.

Zmiana ustawy z dnia 24 września 2010 r. o ewidencji ludności:

Projektowana zmiana przewiduje możliwość wykorzystania min. e-Dowodu jako środka identyfikacji elektronicznej, do pobrania z rejestru PESEL informacji o adresie zameldowania. W sytuacji, gdy informacja o aktualnym miejscu zameldowania jest niezbędna do przekazania podmiotom nie mającym dostępu do rejestru PESEL, stworzona przez ministra właściwego do spraw informatyzacji usługa elektroniczna, umożliwi otrzymanie takiej informacji (art. 27).

V. Przepisy przejściowe, dostosowujące i końcowe.

Przepisy przejściowe związane ze zmianą ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne:

Wprowadza się przepis stanowiący o terminach przyłączenia poszczególnych systemów teleinformatycznych, w których świadczone są publiczne usługi online do systemu teleinformatycznego, przy użyciu którego realizowana będzie obsługa publicznego systemu identyfikacji elektronicznej oraz świadczona będzie usługa „podpisu zaufanego”. W ust. 1 określa się zbiór systemów teleinformatycznych, których użytkownicy powinni mieć zapewnioną możliwość potwierdzenia swojej tożsamości przy użyciu „profilu zaufanego” i „profilu osobistego” nie później niż po upływie 1 miesiąca od dnia wejścia w życie niniejszej ustawy. Stosownie do ust. 2, zobowiązuje się właściwe podmioty publiczne do przyłączenia pozostałych systemów teleinformatycznych, działających w dniu ogłoszenia niniejszej ustawy, nie później niż do dnia 31 grudnia 2020 r. Zgodnie zaś z ust. 3, każdy system teleinformatyczny uruchomiony po dniu 31 marca 2018 r. powinien zapewniać możliwość uwierzytelnienia przy użyciu „profilu zaufanego” i „profilu osobistego” w dniu ich udostępnienia użytkownikom.

Wprowadza się przepis, stanowiący, że „profile zaufane ePUAP” potwierdzone zgodnie z dotychczasowymi przepisami ustawy o informatyzacji stają się „profilami zaufanymi” w rozumieniu przepisów niniejszej ustawy. Procedura potwierdzania tożsamości osób fizycznych, którym wydano „profile zaufane ePUAP” spełnia wymogi stawiane analogicznej procedurze przewidzianej dla wydawania „profilu zaufanego”. Wobec powyższego każdy posiadacz „profilu zaufanego ePUAP” stanie się z mocy ustawy posiadaczem „profilu zaufanego”, bez konieczności ponownego potwierdzania swojej tożsamości jako posiadacza tego środka identyfikacji elektronicznej.

W związku z uchyleniem przepisów dotyczących „podpisu potwierdzonego profilem zaufanym ePUAP” i zastąpieniem ich przepisami regulującymi funkcjonowanie podpisu elektronicznego jakim będzie „podpis zaufany”, stanowi się, iż wszędzie tam gdzie przepisy prawa wymagają użycia „podpisu potwierdzonego profilem zaufanym ePUAP” uznaje się, że użycie „podpisu zaufanego” ma równoważny skutek.

Wprowadza się także przepis wskazujący, że zgody udzielone przez ministra właściwego do spraw informatyzacji na art. 20c ust. 3 i ust. 8 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570) pozostają w mocy.

Przepisy przejściowe związane ze zmienianą ustawą o dowodach osobistych:

Wymiana obecnie obowiązujących dowodów osobistych na dowody z warstwą elektroniczną będzie dotyczyła dowodów osobistych z określonym terminem ważności, czyli dowodów osobistych będących w obiegu do końca 2028 roku. Zdecydowano się na wariant naturalnej wymiany dowodów w okresie 10 lat. Proces ten zakończy się w 2029 r. (art. 54). Sprawy wszczęte i niezakończone przed dniem wejścia w życie zmienianej ustawy prowadzi się na podstawie przepisów dotychczasowych (art. 55). Z uwagi na dziesięcioletni okres ważności dowodów osobistych, pierwsze przekazanie dowodów osobistych z warstwą elektroniczną do użycia nastąpi po upływie 10 lat od dnia wejścia w życie ustawy (art. 56).

VI. Termin wejścia w życie ustawy.

Zgodnie ze stanowiskiem KE oraz wytycznymi dotyczącymi zamykania programów operacyjnych z perspektywy 2007-2013, do których należy projekt „pl.ID – polska ID karta”, ostateczny termin zakończenia projektów realizowanych w tej formule to 31 marca 2019 r. Do tego czasu Polska powinna rozpocząć wydawanie elektronicznych dowodów osobistych, dlatego 1 marca 2019 r. wskazano jako termin wejścia w życie niniejszej ustawy. W przypadku niezakończenia projektu w wyznaczonym czasie bądź odstąpienia od jego

realizacji beneficjent będzie zobligowany do zwrotu 85% kwoty wydatków uznanych dotychczas za kwalifikowane tj. 148,4 mln zł. wraz z odsetkami. Wejście w życie przepisów zmieniających ustawę z dnia z dnia 24 września 2010 r. o ewidencji ludności, które są niezależne od realizacji projektu pl.ID, przewidziano na 1 stycznia 2020 r. Jest to czas na przygotowanie usługi umożliwiającej otrzymanie z rejestru PESEL informacji o adresie zameldowania.

Projekt przewiduje wzrost wydatków w związku z wejściem w życie projektowanych rozwiązań. Przyjęto, że dowody osobiste będą podlegały naturalnej wymianie, która zakłada personalizację dokumentów zgodnie z zapotrzebowaniem wynikającym z utraty ważności dokumentów lub też innych przesłanek obligujących do wnioskowania o dowód. Założono 5 % wzrost liczby wydawanych dowodów osobistych w stosunku do obecnie wydawanych uwzględniając potencjalne zainteresowanie obywateli wymianą dowodów osobistych na nowy e – Dowód. Szacując liczbę dowodów wydawanych w najbliższych 10 latach uwzględniono dotychczasową liczbę wydawanych dowodów zwiększając ją o 5 %.

W przypadku ministra właściwego do spraw wewnętrznych wzrost wydatków będzie wynosił 426,582 mln. zł w ciągu 10 lat od wejścia w życie przepisów. Na koszty te składają się zwiększone koszty blankietów dowodów osobistych, które obecnie wynoszą 16,69 zł, a koszt blankietu z warstwą elektroniczną dla interfejsu bezstykowego oszacowano na kwotę – 20,80 zł., koszty personalizacji jednego dokumentu, począwszy od 2019 r. będą wynosić 5,23 zł, aktualny koszt personalizacji to 2,62 zł. oraz koszty utrzymania systemów utrzymywanych przez MSWiA: do personalizacji dowodów osobistych z warstwą elektroniczną w kwocie 3 690 tys. zł. rocznie, a także do zarządzania cyklem życia karty w kwocie 2 214 tys. zł rocznie. Wymienione koszty wymagają zwiększenia limitu na etapie planowania budżetowego 2019 r. w części 42 z przeznaczeniem na wydatki Centrum Personalizacji Dokumentów MSWiA. Na koszty związane z wdrożeniem e – Dowodu składają się także zwiększone koszty utrzymania systemów ministra właściwego do spraw informatyzacji w wysokości 19,626 tys. zł w ciągu 10 lat od wejścia w życie przepisów. Wymienione koszty wymagają zwiększenia limitu na etapie planowania budżetowego 2019 z przeznaczeniem na zwiększenie limitu do części 27.

Z powodu wprowadzenia w urzędach gmin obsługi dowodu z warstwą elektroniczną nie będzie konieczna wymiana sprzętu informatycznego, gdyż obsługa e-Dowodu będzie prowadzona z wykorzystaniem już istniejących systemów informatycznych (aplikacja Źródło). Wydawanie dowodów osobistych przez organy gmin jest zadaniem zleconym z zakresu administracji rządowej, w związku z tym urzędy gmin na wykonywanie tego zadania

otrzymują dotację z budżetu państwa. Od 2015 roku Ministerstwo Finansów wprowadziło zasadę, że dotacja na zadania zlecone jest przyznawana w oparciu o liczbę wykonywanych zadań. W związku z tym wysokość dotacji na wydawanie przez gminy dowodów osobistych obliczana jest jako iloczyn ujednoliconej stawki roboczogodziny (w 2017 roku Ministerstwo Finansów ustaliło stawkę w wysokości 24,44 zł), ujednoliconej czasochłonności zadania (obecnie 0,5 h) oraz liczby wydanych dokumentów (na podstawie liczby przyjętych wniosków). Zakładając 5 % wzrost liczby wydawanych dowodów osobistych w stosunku do obecnie wydawanych przewidziano wzrost kosztów na dotacje dla organów gmin. Przy założeniu, że nie ulegną zmianie zasady przyznawania dotacji i wysokość roboczogodziny koszty te wyniosą 27,330 tys. zł w ciągu 10 lat od wejścia w życie przepisów.

Określając regułę wydatkową dla wydatków na dotacje dla gmin oraz w części 42 z przeznaczeniem na wydatki Centrum Personalizacji Dokumentów MSWiA założono, że w przypadku przekroczenia lub zagrożenia przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, Minister Finansów zapewni dodatkowe środki budżetowe na ten cel. Założenie wynika ze specyfiki realizowanego zadania, które uzależnione jest od liczby wydawanych dowodów osobistych. Liczba ta może być jedynie oszacowana na podstawie prognoz. Nie jest możliwe wprowadzenie mechanizmu ograniczającego liczbę wydawanych dowodów osobistych, ponieważ posiadanie dowodu osobistego przez osoby pełnoletnie jest obowiązkiem. Trudno też ocenić ile osób małoletnich skorzysta z możliwości wystąpienia o dowód osobisty, szczególnie, że będzie to dokument z nowymi funkcjonalnościami.

Ewaluacja efektów projektu będzie prowadzona przez międzyresortowy Komitet Sterujący do spraw Projektu e-Dowód utworzony na podstawie zarządzenia nr 20 Prezesa Rady Ministrów z dnia 26 lutego 2018 r. w sprawie Komitetu Sterującego do spraw Projektu e-Dowód (M.P. poz. 253) w oparciu o liczbę wydawanych dowodów osobistych z warstwą elektroniczną, przyjmując, że do końca 2021 r. zostanie wydanych co najmniej 5 mln. dowodów z warstwą elektroniczną

Projektowane przepisy będą neutralne dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców. Zamówienia i personalizacja blankietów tych dokumentów są realizowane w trybie niekonkurencyjnym zgodnie z art. 4 pkt 5c ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579). Blankiety nowych dowodów osobistych będą, tak jak dotychczas, personalizowane w Centrum Personalizacji Dokumentów MSWiA.

Projekt ustawy podlega notyfikacji zgodnie z trybem przewidzianym w rozporządzeniu 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).

Projekt ustawy nie jest objęty zakresem prawa Unii Europejskiej.