UZASADNIENIE

Wspieranie rozwoju społecznego i gospodarczego poprzez zapewnienie obywatelom, a w tym także przedsiębiorcom, efektywnych e-usług publicznych jest jednym z celów strategicznych wskazanych w „Programie Zintegrowanej Informatyzacji Państwa”. Zgodnie z przyjętymi w programie założeniami, wysokiej jakości usługi elektroniczne będą dostarczane przy użyciu nowoczesnych rozwiązań informatycznych wspierających spójny system informacyjny państwa, zbudowany i utrzymywany przy współpracy wszystkich resortów. Sprawne państwo, aby mogło efektywnie spełniać swoje funkcje, powinno dysponować szerokim spektrum informacji, które pozwoli na świadczenie usług wymagających minimum zaangażowania ze strony obywateli przy jednoczesnym skróceniu czasu realizacji oraz maksymalizacji ich efektywności.

Poziom dostępności publicznych usług elektronicznych w Polsce jest nadal niezadowalający. Jednym z powodów takiego stanu rzeczy są ograniczenia w zakresie możliwych do wykorzystania środków identyfikacji elektronicznej, co prowadzi do problemu odpowiedniego uwierzytelnienia użytkowników systemów teleinformatycznych, w których udostępniane są e-usługi online. Narastające oczekiwania społeczne dotyczące możliwości nawiązywania kontaktów z organami administracji publicznej za pośrednictwem usług online powodują, że podmioty publiczne coraz częściej dostrzegają potrzebę dostępu do mechanizmów bezpiecznej i wiarygodnej identyfikacji elektronicznej pozwalających na zapewnienie warunków bezpiecznego świadczenia usług elektronicznych zarówno dla usługodawcy, jak i dla usługobiorcy. Aktualnie organy administracji publicznej wykorzystują do uwierzytelniania użytkowników systemów teleinformatycznych głównie mechanizmy opracowane i wykorzystywane wewnątrz administracji, w szczególności rozwiązania funkcjonujące w ramach własnych systemów albo profil zaufany ePUAP (udostępniany przez Ministra Cyfryzacji), który w zakresie usług publicznych stanowi jedyny powszechnie używany publiczny środek identyfikacji elektronicznej. Dostępność i skala użycia profilu zaufanego ePUAP jest jednakże nadal ograniczona mimo zmian prawnych i organizacyjnych wprowadzonych w ostatnim kwartale 2016 roku pozwalających na potwierdzanie profilu zaufanego ePUAP i autoryzacji z nim związanych między innymi za pomocą poświadczeń bankowych.

Warto wskazać, że aby w ramach publicznych systemów teleinformatycznych możliwe było wykorzystywanie zewnętrznych mechanizmów identyfikacji elektronicznej, każdy z tych systemów musi zostać zintegrowany z systemami dostawców środków identyfikacji elektronicznej. Także wspomniani wyżej dostawcy muszą podejmować działania mające na celu indywidualną integrację własnych systemów z systemami teleinformatycznymi odbiorców swoich usług świadczonych w zakresie identyfikacji elektronicznej. Uproszczeniem współpracy wyżej wspomnianych stron mógłby być system teleinformatyczny pełniący rolę „węzła”, czyli pośrednika w wymianie danych, do którego jednokrotne przyłączenie własnego systemu teleinformatycznego pozwoliłoby podmiotom publicznym korzystać z usług szerokiego wachlarza dostawców środków identyfikacji elektronicznej, zaś dostawcom tym świadczyć usługi na rzecz całej administracji publicznej.

Świadczenie bezpiecznych usług wymaga przydzielenia użytkownikom systemu teleinformatycznego odpowiednich uprawnień. Odpowiednie uwierzytelnienie użytkownika zabezpiecza zaś przed nieuprawnionym dostępem do danych stanowiących elementy świadczonej usługi, a co za tym idzie pozwala zapobiec narażeniu stron (strony korzystającej z usługi i strony świadczącej usługę) na szkody z tym związane. Warto jednakże wskazać, iż w ramach świadczonych usług mogą być stosowane różne poziomy uwierzytelniania zapewniające różne poziomy bezpieczeństwa. Inny bowiem powinien być poziom bezpieczeństwa środka identyfikacji elektronicznej użytego w usługach zdrowotnych, gdzie przetwarzane mogą być dane szczególnie wrażliwe, czy dla usług bankowych, a inny w sklepie internetowym – w każdym przypadku jednak niezbędna jest identyfikacja elektroniczna. Dlatego dążąc do wprowadzenia zasad i mechanizmów powszechnego stosowania środków identyfikacji elektronicznej należy wziąć pod uwagę ich zróżnicowanie pod względem zapewnianego poziomu bezpieczeństwa.

Obecnie większość dostawców usług, zarówno publicznych jak i niepublicznych, korzysta z procedur uwierzytelniania realizowanych głównie w ramach wewnętrznych mechanizmów systemów teleinformatycznych, w których udostępniane są usługi. Taki stan rzeczy powoduje, że osoba korzystająca z usług online świadczonych przez różne podmioty zmuszana jest do uczenia się i zapamiętywania różnych procedur identyfikowania się w różnych systemach teleinformatycznych, zarządzanych przez różnych dostawców usług. Istnienie wielu systemów identyfikacji elektronicznej staje się dla obywateli narastającym problemem, w związku z czym pojawia się naturalne dążenie do posługiwania się podobnym lub identycznym zestawem danych wykorzystywanych do identyfikacji w ramach różnych usług, co negatywnie wpływa na ich bezpieczeństwo. Obywatele oczekują więc stosowania w ramach świadczonych usług takich metod identyfikacji i uwierzytelniania, które nie będą uciążliwe dla użytkownika, a jednocześnie będą zapewniały odpowiedni poziom bezpieczeństwa, co w rezultacie przyczyni się do wzrostu popularności i zaufania do usług świadczonych przez administrację publiczną.

Umożliwienie uwierzytelniania użytkowników usług online z wykorzystaniem różnych środków identyfikacji elektronicznej dostarczanych, zarówno przez podmioty publiczne, jak i podmioty komercyjne, na zasadach federacyjnych (czyli otwartości i równorzędności) powinno w znacznym stopniu przyczynić się do upowszechnienia wykorzystania usług e-administracji. Zastosowanie bowiem mechanizmów identyfikacji, które są znane obywatelom, co ważne także w zakresie zasad bezpiecznego posługiwania się posiadanymi środkami identyfikacji elektronicznej (np. środki identyfikacji elektronicznej umożliwiające dostęp do usług banku lub operatora telekomunikacyjnego), znacznie uprości dostęp do usług online.

Zapewnienie powszechności stosowania oraz bezpieczeństwa wyżej wspomnianych rozwiązań osiągnięte zostanie przez ustanowienie w drodze ustawy porządku instytucjonalnego krajowego schematu identyfikacji elektronicznej oraz określenie praw i obowiązków podmiotów, przed którymi stoją następujące cele:

* szybkie osiągnięcie znacznej liczby użytkowników posługujących się środkami identyfikacji elektronicznej, co będzie sprzyjać udostępnianiu nowych usług elektronicznych;
* rozwój otwartej na sektor prywatny i innowacje architektury zapewniającej bezpieczne i wiarygodne mechanizmy uwierzytelniania, która przyczyni się do pozytywnego wizerunku e-administracji;
* zapewnienie odpowiedniej dywersyfikacji środków identyfikacji elektronicznej, a docelowo zapewnienie publicznych środków identyfikacji elektronicznej na wszystkich poziomach bezpieczeństwa przy jednoczesnej klarowności systemu i oferowanych przez niego metod identyfikacji dla obywateli;
* popularyzacja środków identyfikacji elektronicznej, które zapewnią powszechny dostęp do istniejących (oraz pośrednio przyczynią się do powstania nowych) usług cyfrowych administracji publicznej;
* zapewnienie wysokiej elastyczności i potencjału wzrostu dla rynku usług publicznych;
* stworzenie warunków dla zapewnienia wysokiego poziomu bezpieczeństwa danych obywateli.

Realizacja powyższych celów dokonana zostanie na gruncie projektowanej ustawy, która przewiduje nowelizację przepisów ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650), polegającą na uzupełnieniu przepisów rozdziału 4 „Identyfikacja elektroniczna”, który otrzymał nowy tytuł „Krajowy schemat identyfikacji elektronicznej” oraz dodaniu nowego rozdziału 5a. „Nadzór nad krajowym schematem identyfikacji elektronicznej”. Proponowane zmiany mają na celu stworzenie podstaw prawnych dla funkcjonowania krajowego schematu identyfikacji elektronicznej. Schemat ten, jako rozwiązanie o charakterze instytucjonalnym, ma na celu w szczególności umożliwienie realizacji usług online udostępnianych w publicznych systemach teleinformatycznych, dla których czynnikiem krytycznym jest zapewnienie odpowiedniego uwierzytelnienia usługobiorców.

Krajowy schemat identyfikacji elektronicznej obejmował będzie „węzeł krajowy”, czyli system teleinformatyczny pośredniczący w wymianie danych, do którego przyłączone będą systemy identyfikacji elektronicznej, w ramach których wydawane będą środki identyfikacji elektronicznej (systemy tzw. dostawców tożsamości) oraz systemy teleinformatyczne, w których udostępniane są usługi online (systemy tzw. dostawców usług). W skład krajowego schematu identyfikacji elektronicznej wchodził będzie także „węzeł transgraniczny”, czyli system teleinformatyczny pośredniczący w wymianie danych, wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 8 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 eIDAS”.

Węzeł transgraniczny będzie połączony z węzłem krajowym, za pośrednictwem którego będzie umożliwiał uwierzytelnianie użytkowników usług online z wykorzystaniem środków wydanych w systemach identyfikacji elektronicznej podmiotów działających na terenie państw członkowskich Unii Europejskiej. Zgodnie z definicją zawartą w rozporządzeniu eIDAS system identyfikacji elektronicznej to system, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne. Każdy system identyfikacji elektronicznej podlega wymaganiom technicznym, organizacyjnym oraz proceduralnym, które powinien spełniać dostawca środka identyfikacji elektronicznej, odpowiednio do poziomu bezpieczeństwa, jaki zapewniają wydawane w tym systemie środki. Środek identyfikacji elektronicznej został zdefiniowany w art. 3 pkt 2 rozporządzenia eIDAS jako: „materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online”. W świecie cyfrowym środek identyfikacji elektronicznej pełni więc rolę podobną do tej jaką spełnia dokument tożsamości w świecie realnym, jego głównym celem jest bowiem umożliwienie wiarygodnego potwierdzenia tożsamości posługującej się nim osoby, występującej w imieniu swoim lub określonego podmiotu.

Stosowanie środków identyfikacji elektronicznej powinno być adekwatne do potrzeb usługodawców, którzy na podstawie analizy ryzyka określają wystarczające środki potrzebne do zapewnienia bezpieczeństwa świadczonych usług. W art. 8 pkt 2 rozporządzenia eIDAS określone zostały trzy poziomy bezpieczeństwa:

* niski poziom bezpieczeństwa,
* średni poziom bezpieczeństwa,
* wysoki poziom bezpieczeństwa.

Poziomy te odnoszą się do środka identyfikacji elektronicznej, a konkretnie do stopnia zaufania względem podawanej lub zgłaszanej tożsamości uwierzytelnionej przy użyciu tego środka. Wyżej wymienione poziomy stanowią referencję odpowiednio do ograniczonego, średniego (podstawowego) oraz wyższego stopnia zaufania. Należy wskazać, iż zapewnienie każdego z tych poziomów wymaga od dostawcy środka identyfikacji elektronicznej dostosowania systemu identyfikacji elektronicznej do odpowiednich specyfikacji i standardów technicznych, a także podporządkowania się ustalonym procedurom, których celem jest odpowiednie do deklarowanego poziomu obniżenie ryzyka podszycia się lub modyfikacji potwierdzanej tożsamości. Stąd też poziom bezpieczeństwa należy odnieść do środka identyfikacji elektronicznej w kontekście systemu identyfikacji elektronicznej, w którym ten środek jest wydawany.

Przyjęto, że na poziomie krajowym funkcjonowały będą trzy poziomy bezpieczeństwa odpowiadające wyżej wspomnianym poziomom bezpieczeństwa, o których mowa rozporządzeniu eIDAS. Zakłada się, że średni poziom bezpieczeństwa jest poziomem bazowym (podstawowym), który będzie miał zastosowanie do większości usług publicznych świadczonych drogą elektroniczną. Szczegółowe wymagania dotyczące stosowanych zabezpieczeń dla poziomów wiarygodności (bezpieczeństwa) zostały określone w Rozporządzeniu Wykonawczym Komisji (UE) Nr 2015/1502. Uwierzytelnienie użytkownika systemu teleinformatycznego w celu realizacji usługi online będzie wymagało użycia środka identyfikacji elektronicznej na poziomie bezpieczeństwa określonym przez podmiot udostępniający tę usługę.

Zgodnie z projektowaną ustawą zakłada się nieodpłatność wykorzystywania środków identyfikacji elektronicznej do uwierzytelnienia w celu realizacji elektronicznych usług publicznych, zdefiniowanych przez pryzmat podmiotu świadczącego taką usługę, czyli usług online świadczonych przez podmiot, o którym mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570) lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia eIDAS. Stosownie do brzmienia wyżej wskazanego rozporządzenia, przez „podmioty sektora publicznego” należy rozumieć każdy „organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez jeden lub kilka takich organów lub jeden lub kilka takich podmiotów prawa publicznego, lub jednostkę prywatną, której co najmniej jeden z tych organów, podmiotów lub jedno z takich stowarzyszeń udzieliły upoważnienia do świadczenia usług publicznych, gdy działa ona na podstawie takiego upoważnienia”.

Węzeł krajowy umożliwiał będzie uwierzytelnienie użytkowników systemów teleinformatycznych korzystających z usług online podmiotów publicznych, z wykorzystaniem środka identyfikacji elektronicznej wydanego w krajowym systemie identyfikacji elektronicznej przyłączonym do tego węzła albo środka identyfikacji elektronicznej wydanego w zagranicznym systemie identyfikacji elektronicznej, do którego dostęp będzie możliwy za pośrednictwem węzła transgranicznego. Został on przewidziany jako rozwiązanie organizacyjno-techniczne, łączące z jednej strony platformy, na których udostępniane są usługi publiczne i niepubliczne, a z drugiej systemy identyfikacji elektronicznej, w ramach których wydawane będą środki identyfikacji elektronicznej oraz węzeł transgraniczny. Funkcjonowanie węzła krajowego zapewniał będzie minister właściwy do spraw informatyzacji.

W celu zapewnienia zgodności z przepisami 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 4.05.2016, str. 1); przewidziano przepis dotyczący przetwarzania przez ministra właściwego do spraw informatyzacji, jako organu zapewniającego funkcjonowanie węzła krajowego, danych osobowych użytkowników środków identyfikacji elektronicznej, w celu uwierzytelnienia z wykorzystaniem węzła krajowego.

W celu zapewnienia bezpieczeństwa i pewności obrotu, w którym jako podmioty odpowiedzialne za systemy identyfikacji elektronicznej uczestniczyć będą podmioty niepubliczne przewidziano, że zgoda na przyłączenie do węzła krajowego systemu identyfikacji elektronicznej wydawana będzie przez ministra właściwego do spraw informatyzacji w drodze decyzji administracyjnej. Minister będzie mógł wydać decyzję o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego po:

* potwierdzeniu spełniania przez system wymagań dla zadeklarowanych poziomów bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie,
* przeprowadzeniu testów integracyjnych, których termin minister właściwy do spraw informatyzacji wyznaczy po dokonaniu oceny wniosku (o którym mowa w dalszej części uzasadnienia) i dokumentów załączonych do tego wniosku, oraz które przeprowadzone zostaną zgodnie z procedurą udostępnioną w Biuletynie Informacji Publicznej na stronie podmiotowej tego ministra,
* zapewnieniu przez podmiot odpowiedzialny za ten system opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
* przedstawieniu przez podmiot odpowiedzialny za ten system dokumentu zawierającego przyrzeczenie zakładu ubezpieczeń zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej wnioskodawcy,
* zapewnieniu działania zgodnie z przepisami o ochronie danych osobowych.

Niespełnianie powyższych wymogów skutkować będzie wydaniem decyzji o odmowie przyłączenia systemu identyfikacji elektronicznej do węzła krajowego.

Podmiot odpowiedzialny za system identyfikacji elektronicznej będzie obowiązany zawrzeć, przed dniem faktycznego przyłączenia systemu identyfikacji elektronicznej do węzła krajowego, umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w tym systemie. Stąd też decyzja o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego będzie miała charakter warunkowy, bowiem przyłączenie systemu identyfikacji elektronicznej do węzła krajowego będzie następowało dopiero po dostarczeniu ministrowi właściwemu do spraw informatyzacji przez podmiot odpowiedzialny za system identyfikacji elektronicznej kopii wspomnianej wyżej umowy ubezpieczenia. W projektowanym akcie normatywnym wskazuje się termin 30 dni na dostarczenie przedmiotowego dokumentu.

Wspomnianym wyżej ubezpieczeniem odpowiedzialności cywilnej będzie objęta odpowiedzialność cywilna podmiotu odpowiedzialnego za system identyfikacji elektronicznej przyłączony do węzła krajowego, za szkody wynikające z działania lub zaniechania wyrządzone w okresie przyłączenia tego systemu do węzła krajowego użytkownikom usług online wykorzystującym środki identyfikacji elektronicznej wydane w tym systemie identyfikacji elektronicznej, niezależnie od tego, czy ich użycie nastąpiło za pośrednictwem węzła krajowego, spowodowane przez awarie, przerwy lub błędy systemu albo za zobowiązanie zaciągnięte w wyniku nieuprawnionego wykorzystania środka identyfikacji elektronicznej. Ubezpieczenie to nie będzie obejmowało szkód:

1. wyrządzonych przez ubezpieczonego po dniu wydania ostatecznej decyzji o odłączeniu systemu identyfikacji elektronicznej od węzła krajowego, chyba że szkoda jest następstwem działania lub zaniechania, które miało miejsce w okresie przyłączenia węzła krajowego,
2. polegających na zapłacie kar umownych,
3. powstałych wskutek siły wyższej,

chyba że w umowie ubezpieczenia zakres ochrony ubezpieczeniowej zostanie rozszerzony również na szkody wynikające ze zdarzeń wskazanych w pkt 1–3. Za niedopuszczalne przyjmuje się natomiast zawężanie wyżej opisanego zakresu ubezpieczenia w drodze umownego ograniczenia odpowiedzialności przez zakład ubezpieczeń.

W projektowanej ustawie zawarto upoważnienie dla ministra właściwego do spraw instytucji finansowych, który w porozumieniu z ministrem właściwym do spraw informatyzacji, po zasięgnięciu opinii Polskiej Izby Ubezpieczeń, określi, w drodze rozporządzenia, minimalną sumę gwarancyjną, uwzględniając specyfikę działalności prowadzonej przez podmioty odpowiedzialne za systemy identyfikacji elektronicznej.

Dążąc do zachowania wiarygodności uwierzytelnień osób fizycznych dokonywanych w usługach online, dokonywanych za pośrednictwem węzła krajowego, rekomenduje się uregulowanie w niniejszej ustawie także wymogów skierowanych do osób, którym wydano środki identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do tego węzła. Głównym, proponowanym wymogiem jest zobowiązanie takich osób aby korzystały z wydanego środka identyfikacji elektronicznej zgodnie z warunkami określonymi przez podmiot odpowiedzialny za system identyfikacji elektronicznej, w którym został wydany ten środek. Jednym z kluczowych celów niniejszych przepisów jest uniknięcie sytuacji, w której osoba nieuprawniona mogłaby zostać uwierzytelniona w usłudze online przy danych osobowych innej osoby fizycznej. Stąd też rekomenduje się wprowadzenie wymogu niezwłocznego zgłoszenia podmiotowi odpowiedzialnemu za system identyfikacji elektronicznej, w którym został wydany środek identyfikacji elektronicznej, stwierdzenia utraty, kradzieży, przywłaszczenia środka identyfikacji elektronicznej lub utraty wyłącznej kontroli nad danymi umożliwiającymi identyfikację przy użyciu tego środka, albo nieuprawnionego użycia środka identyfikacji elektronicznej. Przepis ten ma na celu zapewnienie podmiotom odpowiedzialnym za systemy identyfikacji elektronicznej, przyłączone do węzła krajowego, możliwości niezwłocznego zawieszenia lub unieważnienia środków identyfikacji elektronicznej, których użycie mogłoby potencjalnie nastąpić poza wyłączną kontrolą osoby, której te środki wydano. Proponuje się ponadto zobowiązać osoby, którym wydano środki identyfikacji elektronicznej, aby podejmowały niezbędne działania służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń tego środka lub danych umożliwiających identyfikację przy użyciu tego środka. Powyższe ma na celu wykluczenie sytuacji w których osoby nie obniżały bezpieczeństwa wykorzystywanych środków identyfikacji elektronicznej na skutek swoich własnych nieodpowiedzialnych działań.

Zasadnym jest zabezpieczenie obywateli przed negatywnymi skutkami, jakie mogą wyniknąć w sytuacji gdy w sposób niezawiniony utracą oni wyłączną kontrolę nad posiadanym środkiem identyfikacji elektronicznej, wydanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego. Dlatego też rekomenduje się uregulowanie, iż jeżeli posiadacz takiego środka niezwłocznie poinformuje podmiot odpowiedzialny za system identyfikacji elektronicznej, w którym wydano ten środek, o fakcie utraty wyłącznej kontroli nad tym środkiem, nie będzie ponosił odpowiedzialności za zobowiązania zaciągnięte z wykorzystaniem wydanego mu środka identyfikacji elektronicznej zaistniałe od momentu dokonania zgłoszenia.

Minister będzie wydawał decyzję o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego na wniosek podmiotu odpowiedzialnego za system identyfikacji elektronicznej. Wniosek zawierał będzie nazwę i szczegółowy opis systemu identyfikacji elektronicznej, wraz z wskazaniem środków wydawanych w ramach tego systemu i określeniem poziomu bezpieczeństwa tych środków oraz dane dotyczące podmiotu odpowiedzialnego za system (takie jak imię i nazwisko lub firma, adres siedziby i miejsca wykonywania działalności, nr KRS, a w przypadku, gdy podmiot nie posiada numeru w Krajowym Rejestrze Sądowym, wskazanie organu, któremu działalność podmiotu została zgłoszona lub właściwego rejestru oraz podanie numeru identyfikacyjnego, jeżeli został on nadany). W przypadku gdy czynności tych nie wykonuje podmiot odpowiedzialny za system identyfikacji elektronicznej konieczne jest przekazanie danych identyfikacyjnych, w tym imienia i nazwiska lub firmy, adresu siedziby i miejsca wykonywania działalności, nr KRS (a w przypadku, gdy podmioty te nie posiadają numeru w Krajowym Rejestrze Sądowym, wskazanie organu, któremu działalność podmiotu została zgłoszona lub właściwego rejestru oraz podanie numeru identyfikacyjnego, jeżeli został on nadany) podmiotów:

* potwierdzających tożsamość oraz weryfikujących dane identyfikujące osoby ubiegające się o wydanie środka identyfikacji elektronicznej,
* wydających środki identyfikacji elektronicznej, lub
* zapewniających funkcjonalność uwierzytelnienia osób, którym wydano środek identyfikacji elektronicznej.

Do wniosku dołączane będą dokumenty potwierdzające spełnienie przez system identyfikacji elektronicznej wymagań dla wskazanych we wniosku poziomów bezpieczeństwa środków identyfikacji elektronicznej (w szczególności pozytywny wynik audytu systemu zarządzania bezpieczeństwem informacji, obejmujący w swym zakresie system identyfikacji elektronicznej, którego dotyczy wniosek, albo pozytywny wynik audytu, o którym mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia eIDAS), dokument zawierający przyrzeczenie zakładu ubezpieczeń zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej wnioskodawcy, a także oświadczenie o zapewnieniu stosowania polityki bezpieczeństwa węzła krajowego i oświadczenie o działaniu podmiotu zgodnie z przepisami o ochronie danych osobowych. Wymaganym będzie, aby wniosek wraz z wymaganymi załącznikami składany był w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.

Proponuje się zobowiązanie ministra właściwego do spraw informatyzacji do poinformowania podmiotu odpowiedzialnego za system identyfikacji elektronicznej na piśmie, w postaci papierowej albo elektronicznej, o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego oraz o każdej zmianie polityki bezpieczeństwa węzła krajowego.

Mając na uwadze konieczność zapewnienia poziomu bezpieczeństwa środków identyfikacji elektronicznych, do których dostęp zapewniany jest za pośrednictwem węzła krajowego, odpowiadającego aktualnym wymogom prawnym UE, zobowiązuje się podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego do przekazania ministrowi właściwemu do spraw informatyzacji, w terminie 14 dni o dnia wejścia w życie nowych przepisów prawa UE, aktualnych dokumentów potwierdzających spełnianie wymagań dla zadeklarowanych we wniosku poziomów bezpieczeństwa środków identyfikacji elektronicznej w przypadku zmiany przepisów wydanych na podstawie art. 8 ust. 3 rozporządzenia eIDAS.

Wymaganym jest, aby podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego posiadał przez cały okres swojej działalności ubezpieczenie odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w tym systemie identyfikacji elektronicznej. W związku z powyższym zobowiązuje się ten podmiot do dostarczenia ministrowi właściwemu do spraw informatyzacji kopii każdej kolejnej umowy ubezpieczenia, w terminie 14 dni od jej zawarcia.

W projekcie ustawy określono, że ponowne złożenie wniosku wymagane będzie w przypadku zmiany poziomu bezpieczeństwa środka identyfikacji elektronicznej, wydawanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, albo w przypadku uruchomienia w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego środka identyfikacji elektronicznej, nie objętego zakresem uprzednio złożonego wniosku, na podstawie którego została wydana decyzja o przyłączenie systemu identyfikacji elektronicznej do węzła krajowego. Reguluje się przy tym, że umożliwienie korzystania za pośrednictwem węzła krajowego z wyżej wspomnianych środków identyfikacji elektronicznej, stanowiących przedmiot dokonanej zmiany, będzie następowało po pozytywnym rozpatrzeniu wniosku i przeprowadzeniu testów integracyjnych.

Przewidziano, że system teleinformatyczny zapewniający obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany będzie w szczególności „profil zaufany” (kwestie dotyczące przedmiotowego środka identyfikacji elektronicznej zostały rozwinięte w dalszej części uzasadnienia), zostanie z mocy prawa przyłączony do węzła krajowego.

Systemy identyfikacji elektronicznej przyłączone do węzła krajowego będą wpisywane do prowadzonego przez ministra właściwego do spraw informatyzacji rejestru. Zakres danych podlegających wpisowi do rejestru został wskazany w ustawie. Rejestr będzie jawny.

Informacje zawarte w dokumentach potwierdzających spełnianie przez system identyfikacji elektronicznej niezbędnych wymagań, których ujawnienie mogłoby narazić na szkodę podmiot odpowiedzialny za system identyfikacji elektronicznej, stanowić będą tajemnicę. Informacje te będą mogły być udzielone wyłącznie na żądanie: sądu lub prokuratora – w związku z toczącym się postępowaniem, innych upoważnionych organów – w związku z prowadzonym przez te organy postępowaniem, albo Szefa Agencji Bezpieczeństwa Wewnętrznego.

W projekcie uregulowano również kwestię obowiązków podmiotów odpowiedzialnych za systemy identyfikacji elektronicznej przyłączone do węzła krajowego, do których należy zarządzanie systemem identyfikacji elektronicznej oraz ponoszenie kosztów jego utrzymania i rozwoju, potwierdzanie tożsamości oraz weryfikowanie danych identyfikujących osoby ubiegające się o wydanie środka identyfikacji elektronicznej, wydawanie (zawieszanie, unieważnianie) środków identyfikacji elektronicznej, zapewnianie funkcjonalności pozwalającej na uwierzytelnienie osób, którym wydano środek identyfikacji elektronicznej, zapisywanie i zachowywanie informacji związanych z wydawaniem środków identyfikacji elektronicznej oraz zapewnieniem rozliczalności i niezaprzeczalności działań użytkowników korzystających z tych środków, a także stosowanie polityki bezpieczeństwa węzła krajowego.

Jednym z ww. obowiązków jest potwierdzanie tożsamości osoby ubiegającej się o wydanie środka identyfikacji elektronicznej. Należy zaznaczyć, że chodzi o potwierdzenie tożsamości osoby w świecie rzeczywistym, tj. o zweryfikowanie z dokumentem tożsamości, czy osoba ubiegająca się o wydanie środka identyfikacji elektronicznej nie podaje się za kogoś innego.

Podmiot odpowiedzialny za system identyfikacji elektronicznej musi posiadać siedzibę w jednym z państw członkowskich Unii Europejskiej.

Projekt zakłada, że obowiązki dotyczące potwierdzania tożsamości oraz weryfikowania danych identyfikujących osoby ubiegające się o wydanie środka identyfikacji elektronicznej, wydawania, zawieszania i unieważniania środków identyfikacji elektronicznej, zapewniania funkcjonalności pozwalającej na uwierzytelnienie osób, którym wydano środek identyfikacji elektronicznej, a także gromadzenie informacji związanych z wydawaniem środków identyfikacji elektronicznej oraz zapewnieniem rozliczalności i niezaprzeczalności działań użytkowników korzystających z tych środków, mogą wykonywać podmioty inne niż podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego, spełniające wymogi określone w art. 21b ust. 1 pkt 1 i 3, o ile posiadają siedzibę w jednym z państw członkowskich Unii Europejskiej. Podmioty te zobowiązane będą do stosowania polityki bezpieczeństwa węzła krajowego. Podkreślenia wymaga, iż odpowiedzialność za czynności wykonywane przez wyżej wspomniane inne podmioty ponosił będzie podmiot odpowiedzialny za system identyfikacji elektronicznej.

Podmioty odpowiedzialne za systemy identyfikacji elektronicznej przyłączone do węzła krajowego przetwarzają dane osobowe posiadaczy środków identyfikacji elektronicznej wydanych w ramach tego systemu, w zakresie niezbędnym dla realizacji wyżej opisanych zadań. Bez takiej możliwości podmioty odpowiedzialne za system identyfikacji nie mogłyby w pełni zapewnić rozliczalności, a co za tym idzie także bezpieczeństwa działań realizowanych z wykorzystaniem środków identyfikacji elektronicznej wydanych w ramach systemu, w szczególności uwierzytelniania. Mając na uwadze, że zapewnienie rozliczalności jest cechą systemu identyfikacji jako określonej całości oznacza to, że każdy podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego przetwarza dane osobowe posiadaczy środków identyfikacji elektronicznej wydanych w ramach tego systemu bez względu na to, czy uwierzytelnianie następuje za pośrednictwem węzła czy nie. To, że w węźle krajowym będą przetwarzane dane ograniczone do uwierzytelniania w ramach określonych usług nie może powodować takiego ograniczenia w samym systemie identyfikacji elektronicznej przyłączonym do węzła.

W tym kontekście warto zauważyć podobne podejście do tzw. notyfikowanych systemów identyfikacji elektronicznej jakie przewidziano w przepisach rozporządzenia eIDAS, co zostało wyraźnie wyartykułowane w sekcji 4.2.3 Decyzji wykonawczej Komisji (UE) 2015/1984 z dnia 3 listopada 2015 r. w sprawie określenia okoliczności, formatów i procedur notyfikacji zgodnie z art. 9 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnetrznym. Mając na uwadze, że nie jest wykluczone osiągnięcie w przyszłości przez system przyłączony do węzła krajowego statusu systemu notyfikowanego już teraz ten przepis należy rozumieć jako odnoszący się do całości systemu.

Wprowadzono regulację o charakterze ogólnym ustalającą, że podmiot zapewniający możliwość uwierzytelniania w usługach online, niebędący „podmiotem publicznym” zdefiniowanym jako podmiot, o którym mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub podmiot sektora publicznego, o których mowa w art. 3 pkt 7 rozporządzenia eIDAS, nie może pozyskiwać, przechowywać oraz przetwarzać danych dotyczących realizacji tych usług, innych niż dane niezbędne do zrealizowania procesu uwierzytelnienia. Celem regulacji jest ustanowienie wprost zakazu przetwarzania danych przez ww. podmiot przeprowadzający procedurę uwierzytelniania, innych niż te niezbędne dla realizacji usługi online. Mając na uwadze bardzo szybki rozwój usług online realizowanych drogą elektroniczną, jak również zmieniające się technologie wspomagające proces uwierzytelniania w takich usługach, przepis będzie jednoznaczną wytyczną dla przyszłych rozwiązań techniczno-organizacyjnych.

Przewidziano także rozwiązania dotyczące sposobu postępowania w przypadku naruszenia bezpieczeństwa systemu identyfikacji elektronicznej, polegające na tym, że w przypadku gdy nastąpi naruszenie bezpieczeństwa systemu identyfikacji elektronicznej przyłączonego do węzła krajowego lub części środków identyfikacji elektronicznej wydanych w tym systemie, mogące mieć wpływ na rozliczalność i niezaprzeczalność działań wykonywanych z wykorzystaniem tego systemu lub części środków identyfikacji elektronicznej wydanych w tym systemie, podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego niezwłocznie zawiesza możliwość uwierzytelniania z wykorzystaniem środków identyfikacji elektronicznej, których dotyczy naruszenie bezpieczeństwa. Po usunięciu naruszenia bezpieczeństwa systemu identyfikacji elektronicznej lub zawieszonej części środków identyfikacji elektronicznej podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego przywraca możliwość uwierzytelniania za pomocą środków identyfikacji elektronicznej, których dotyczyło zawieszenie.

Projekt nakłada na podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego obowiązki informacyjne wobec ministra właściwego do spraw informatyzacji określając przy tym zakres przekazywanych danych. Reguluje się nadto, że minister właściwy do spraw informatyzacji po otrzymaniu wyżej wspomnianych danych, przekazuje je Szefowi Agencji Bezpieczeństwa Wewnętrznego, jeżeli istnieją uzasadnione przesłanki pozwalające wnioskować, iż zmiany tych danych mogą mieć wpływ na bezpieczeństwo publiczne, bezpieczeństwo państwa lub zagrażają w sposób bezpośredni bezpieczeństwu systemów teleinformatycznych państwa.

W projekcie wskazano, że system, w którym udostępniane są publiczne lub niepubliczne usługi online będzie mógł być przyłączony do węzła krajowego po zapewnieniu przez podmiot odpowiedzialny za ten system opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, po przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność tych systemów z węzłem krajowym, oraz po złożeniu przez podmiot wnioskujący oświadczenia, że będzie on działał zgodnie z przepisami o ochronie danych osobowych. Minister właściwy do spraw informatyzacji przed wydaniem decyzji o przyłączeniu tych systemów może sprawdzać spełnianie wyżej wspomnianych wymagań. W przypadku niespełniania wyżej wspomnianych wymagań wydaje decyzję o odmowie przyłączenia do węzła krajowego systemu, w którym udostępniane są usługi online, nie zostanie udzielona.

Decyzja o przyłączeniu do węzła krajowego systemu teleinformatycznego, w którym udostępniane są usługi online, wydawana jest na wniosek podmiotu odpowiedzialnego za ten system. Wniosek powinien zawierać nazwę podmiotu odpowiedzialnego za system albo jego imię i nazwisko oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania. Celem wykluczenia nieuzasadnionego obciążania systemu teleinformatycznego, przy użyciu którego obsługiwany będzie węzeł krajowy, wymagane będzie, aby podmiot niepubliczny, rozumiany jako podmiot inny niż podmiot, o którym mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia eIDAS, wskazał i uzasadnił interes faktyczny wykorzystywania uwierzytelnienia z wykorzystaniem węzła. Do wniosku dołącza się: oświadczenie dotyczące wspomnianego wyżej systemu zarządzania bezpieczeństwem informacji, oświadczenie o zapewnieniu stosowania polityki bezpieczeństwa węzła krajowego, listę usług online udostępnianych w tym systemie wraz z określeniem dla każdej z tych usług wymaganych poziomów bezpieczeństwa środków identyfikacji elektronicznej, o których mowa w art. 8 ust. 2 rozporządzenia 910/2014, niezbędnych dla realizacji tych usług, a także oświadczenie o zapewnieniu działania podmiotu zgodnie z przepisami o ochronie danych osobowych. Wymaganym będzie, aby wniosek wraz z wymaganymi załącznikami złożony został w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.

Minister właściwy do spraw informatyzacji po dokonaniu oceny wniosku i dokumentów załączonych do wniosku wyznaczy termin przeprowadzenia testów integracyjnych oraz przeprowadzi te testy zgodnie z procedurą udostępnioną w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.

Podmiot odpowiedzialny za system teleinformatyczny, w którym udostępniane są usługi online, przyłączony do węzła krajowego, obowiązany jest do niezwłocznego informowania ministra właściwego do spraw informatyzacji o każdej zmianie danych zawartych w przekazanej, w załączeniu do wniosku, liście usług udostępnianych w tym systemie, zawierającej wskazanie dla każdej z tych usług wymaganego poziomu bezpieczeństwa środków identyfikacji elektronicznej niezbędnych dla realizacji tych usług.

Minister właściwy do spraw informatyzacji udostępni na stronie podmiotowej Biuletynu Informacji Publicznej informację o przyłączonych do węzła krajowego systemach teleinformatycznych, w których są udostępniane usługi online.

Do węzła krajowego zostanie z mocy prawa przyłączona elektroniczna platforma usług administracji publicznej.

Należy także podkreślić, że minister właściwy do spraw informatyzacji na podstawie art. 22 ust. 1 pkt 2 ustawy z dnia … 2018 r. o krajowym systemie cyberbezpieczeństwa, jako podmiot publiczny realizujący zadanie publiczne zależne od systemów informacyjnych będzie miał obowiązek zgłaszania incydentu w podmiocie publicznym (incydentu, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego) niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia do CSIRT GOV (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym, prowadzonego przez Szefa Agencji Bezpieczeństwa Wewnętrznego). Ponadto, będzie zobowiązany do zarządzanie incydentem, jak również w wypadku takiej potrzeby współpracy w jego obsłudze z zespołami CSIRT. W rozumieniu wymienionej ustawy incydentem jest każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Zakłada się też nowelizację art. 22 ustawy z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej, dotyczącego w obecnym stanie prawnym węzła krajowego w rozumieniu art. 12 ust. 8 rozporządzenia eIDAS. Mając na uwadze, że w projekcie przewidziano węzeł krajowy jako element krajowego schematu identyfikacji elektronicznej, zasadne jest dokonanie zmiany nazwy węzła krajowego w rozumieniu przepisów rozporządzenia eIDAS. W konsekwencji w art. 22 ustawy wskazuje się, że do realizacji usług transgranicznych wykorzystywany będzie węzeł transgraniczny, którego funkcjonowanie zapewni minister właściwy do spraw informatyzacji, zgodnie z przepisami rozporządzenia eIDAS oraz przepisami wykonawczymi wydanymi na podstawie tego rozporządzenia. Do węzła transgranicznego podłączone będą notyfikowane Komisji Europejskiej systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej, i tylko te środki identyfikacji elektronicznej będą służyły do realizacji usług w innym kraju UE. Zmiana art. 22 ma na celu zatem doprecyzowanie terminologiczne obowiązującej ustawy oraz wskazanie, że ww. systemy identyfikacji elektronicznej są podłączone do węzła transgranicznego za pośrednictwem węzła krajowego.

W art. 22 doprecyzowano również, że do notyfikacji, o której mowa w art. 9 rozporządzenia eIDAS mogą być zgłaszane tylko systemy identyfikacji elektronicznej przyłączone do węzła krajowego, dla których potwierdzone zostało spełnienie wymagań, o których mowa w art. 7 tego rozporządzenia eIDAS, a notyfikowany system identyfikacji elektronicznej przyłączany będzie do węzła transgranicznego za pośrednictwem węzła krajowego.

Doprecyzowane zostało również brzmienie art. 25 poprzez wskazanie, że podmioty przyłączające do węzła krajowego systemy teleinformatyczne, w których udostępniane są publiczne lub niepubliczne usługi online, określają wymagane poziomy bezpieczeństwa, o których mowa w art. 8 rozporządzenia eIDAS, środków identyfikacji elektronicznej, niezbędne dla realizacji tych usług.

Wprowadzono zmiany terminologiczne o charakterze dostosowującym w art. 24 i art. 26. Doprecyzowano brzmienie art. 24 ust. 3, podkreślając, że minister właściwy do spraw informatyzacji może zgłosić system identyfikacji elektronicznej do przeprowadzenia wzajemnej oceny, o której mowa w art. 12 ust. 6 lit. c rozporządzenia eIDAS, po pozytywnym zweryfikowaniu wniosku o notyfikowanie systemu identyfikacji elektronicznej w Komisji, biorąc pod uwagę warunki kwalifikowania się systemu do notyfikowania wskazane w art. 7 rozporządzenia eIDAS oraz politykę państwa w zakresie identyfikacji elektronicznej. Ponadto skorygowano brzmienie art. 26 ust. 2, który odnosił się do naruszenia bezpieczeństwa notyfikowanego „systemu identyfikacji elektronicznej albo systemu uwierzytelnienia”, podczas gdy w art. 10 ust. 1 rozporządzenia eIDAS, do którego odwołuje się przedmiotowy przepis, odnosi się do naruszenia bezpieczeństwa „systemu identyfikacji elektronicznej (…) albo uwierzytelnienia”. W przedmiotowej jednostce uzupełniono ponadto że informacje dotyczące naruszenia bezpieczeństwa notyfikowanego systemu identyfikacji elektronicznej albo uwierzytelnienia przekazuje niezwłocznie, jednak nie później niż w ciągu 24 godzin od naruszenia.

Nowoprojektowany rozdział 5a zawiera przepisy regulujące zagadnienia związane z nadzorem ministra właściwego do spraw informatyzacji nad krajowym schematem identyfikacji elektronicznej. W ramach nadzoru minister właściwy do spraw informatyzacji będzie prowadził kontrole spełniania przez system identyfikacji elektronicznej oraz systemy teleinformatyczne, w których udostępniane są usługi online, wymagań dla systemów elektronicznych, przyłączanych do węzła krajowego. Zadaniem realizowanym przez ministra właściwego do spraw informatyzacji, w ramach nadzoru nad funkcjonowaniem krajowego schematu identyfikacji elektronicznej, będzie również określenie polityki bezpieczeństwa dla węzła krajowego, oraz jej udostępnienie na stronie podmiotowej w Biuletynie Informacji Publicznej, a także prowadzenie działań zapobiegających naruszeniom bezpieczeństwa.

Celem zapewnienia niezakłóconego funkcjonowania krajowego schematu identyfikacji elektronicznej zobowiązuje się ministra właściwego do spraw informatyzacji do podejmowania w przedmiotowym zakresie działań o charakterze prewencyjnym, w szczególności systematycznego prowadzenia analiz ryzyka wystąpienia incydentów bezpieczeństwa, czego następstwem będzie wdrożenie i upowszechnienie środków technicznych i organizacyjnych, uwzględniających aktualny stan wiedzy (w tym uznane w obrocie profesjonalnym standardy i metodyki), adekwatnych do wykrytych podatności oraz przewidywanych zagrożeń.

Wspomniane wyżej kontrole przeprowadzane będą przez osoby upoważnione przez ministra właściwego do spraw informatyzacji. Osoby te uprawnione będą do:

* wstępu do obiektów i pomieszczeń podmiotu odpowiedzialnego za system identyfikacji elektronicznej lub podmiotu wydającego środek identyfikacji elektronicznej w tym systemie;
* wglądu do dokumentów zawierających dane dotyczące funkcjonowania systemu identyfikacji elektronicznej oraz wydanych w tym systemie środków identyfikacji elektronicznej;
* przetwarzania danych osobowych w zakresie objętym przedmiotem kontroli;
* przeprowadzania oględzin obiektów oraz innych składników majątkowych związanych z funkcjonowaniem systemu identyfikacji elektronicznej, a także sprawdzenia przebiegu czynności związanych z wydawaniem środków identyfikacji elektronicznej oraz oceny technicznej środków identyfikacji elektronicznej;
* żądania udzielenia ustnych lub pisemnych wyjaśnień od pracowników podmiotu odpowiedzialnego za system identyfikacji elektronicznej, podmiotu wydającego środek identyfikacji elektronicznej oraz przeprowadzającego procedurę uwierzytelniania w tym systemie;
* zabezpieczania dokumentów i innych materiałów, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

W projekcie przewidziano możliwość zawieszenia przez ministra właściwego do spraw informatyzacji, w drodze decyzji, systemu identyfikacji elektronicznej przyłączonego do węzła krajowego albo możliwości korzystania z części środków identyfikacji elektronicznej wydanych w tym systemie, jeżeli naruszenie dotyczy części środków identyfikacji elektronicznej i zawieszenie takie jest możliwe technicznie. Decyzja taka będzie wydawana przez ministra właściwego do spraw informatyzacji w przypadku naruszenia polityki bezpieczeństwa węzła krajowego lub wymagań dla systemów identyfikacji elektronicznych, przyłączanych do węzła krajowego. Decyzja o zawieszeniu systemu będzie podlegała natychmiastowemu wykonaniu tak, aby chronić dane obywateli korzystających z tego środka lub systemu.

Projekt zawiera również przepisy regulujące kwestię wydania przez ministra właściwego do spraw informatyzacji decyzji o odłączeniu systemu identyfikacji elektronicznej od węzła krajowego. Decyzja ta będzie wydawana na uzasadniony wniosek dostawcy systemu identyfikacji elektronicznej, w przypadku zaprzestania prowadzenia działalności przez podmiot odpowiedzialny za system, w przypadku gdy w terminie 3 miesięcy od dnia zawieszenia danego systemu podmiot odpowiedzialny za system nie usunął przyczyny zawieszenia systemu identyfikacji elektronicznej, a także w przypadku nieprzedstawienia kolejnej umowy ubezpieczenia odpowiedzialności cywilnej.

Podmiot odpowiedzialny za system identyfikacji elektronicznej zobowiązany zostanie do udzielania informacji oraz udostępniania dokumentów, które są bezpośrednio związane z funkcjonowaniem systemu identyfikacji elektronicznej, w tym dotyczą naruszeń polityki bezpieczeństwa węzła krajowego, na żądanie ministra właściwego do spraw informatyzacji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego. Powyższy obowiązek uwzględniać ma zachowanie przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

W przypadku naruszenia polityki bezpieczeństwa węzła krajowego lub niespełniania wymagań, określonych dla systemu teleinformatycznego, w którym udostępniane są usługi online, przyłączonego do węzła krajowego, w zakresie mającym wpływ na bezpieczeństwo uwierzytelnienia z wykorzystaniem węzła krajowego, minister właściwy do spraw informatyzacji zawiesi możliwość korzystania tego systemu z uwierzytelniania użytkowników z wykorzystaniem węzła krajowego. Jednocześnie minister właściwy do spraw informatyzacji przywróci możliwość korzystania z systemu, w którym udostępniane są usługi online z uwierzytelniania użytkowników z wykorzystaniem węzła krajowego, niezwłocznie po otrzymaniu od podmiotu odpowiedzialnego za ten system potwierdzenia usunięcia naruszenia, które było podstawą do zawieszenia.

Minister właściwy do spraw informatyzacji wydaje decyzję o odłączeniu systemu teleinformatycznego, w którym udostępniane są usługi online, i odłącza ten system od węzła krajowego w przypadku: złożenia przez podmiot odpowiedzialny za ten system wniosku o odłączenie od węzła krajowego, zaprzestania prowadzenia działalności przez podmiot odpowiedzialny za ten system, nieusunięcia przyczyny zawieszenia tego systemu w terminie trzech miesięcy od dnia jego zawieszenia.

Podmiot odpowiedzialny za system teleinformatyczny, w którym udostępniane są usługi online, zobowiązany zostanie do udzielania informacji oraz udostępniania dokumentów, które są bezpośrednio związane z funkcjonowaniem tego systemu, w tym dotyczą naruszeń polityki bezpieczeństwa węzła krajowego, na żądanie ministra właściwego do spraw informatyzacji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego. Powyższy obowiązek uwzględniać ma zachowanie przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

Zgodnie z projektowaną ustawą w przypadku gdy wyniki kontroli wykażą niezgodność z przepisami ustawy, minister właściwy do spraw informatyzacji, po zapoznaniu się z zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez podmiot kontrolowany, może wydać decyzję nakładającą obowiązek usunięcia stwierdzonych niezgodności w terminie nie krótszym niż 14 dni. W sprawach nieuregulowanych w projektowanej ustawie, do przeprowadzenia wyżej wspomnianych kontroli zastosowanie będą miały odpowiednio przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646).

Tytułowi rozdziału nr 6 proponuje się nadanie brzmienia „Przepisy karne i przepisy o karach pieniężnych”.

Do nowelizowanej ustawy wprowadza się przepisy nakładające sankcje karne za identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej zawierającego dane innej osoby oraz za kopiowanie lub przechowywanie bez uprawnienia danych pozwalających na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej. Wspomniane wyżej przepisy karne dotyczą środków identyfikacji elektronicznej wydawanych w ramach systemów identyfikacji elektronicznej przyłączonych do węzła krajowego. Jednocześnie przyjmuje się, iż w przypadku działań, analogicznych do wyżej wymienionych, dotyczących środków identyfikacji elektronicznej wydawanych w ramach innych systemów identyfikacji elektronicznej, ewentualne sankcje karne wynikały wprost z przepisów ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204, z późn. zm.), w szczególności art. 267 § 2 tej ustawy.

Pojęcie „identyfikacja” jest tu rozumiane zgodnie z terminologią jaką zastosowano w rozporządzeniu eIDAS, a więc jako zbiór czynności dokonywanych przez osobę posiadającą środek identyfikacji elektronicznej, których celem jest zadeklarowanie swojej tożsamości w systemie informatycznym. Mając na uwadze, iż w brzmieniu projektowanego przepisu jest mowa o posłużeniu się środkiem identyfikacji elektronicznej zawierającym dane innej osoby, należy wskazać, iż przepis ten odnosi się do sytuacji w której określona osoba wykorzystuje środek identyfikacji elektronicznej, wydany innej osobie, w celu podszycia się pod tożsamość tej innej osoby. Należy wskazać, iż działanie takie powinno być penalizowane niezależnie od wyniku procesu uwierzytelniania, a więc czynności dokonywanych przez stronę ufającą (np. dostawcę e–usług), które zmierzają do potwierdzenia tożsamości jaką określona osoba (np. użytkownik systemu teleinformatycznego, w którym udostępniane są e-usługi) zadeklarowała przy użyciu posiadanych danych w procesie identyfikacji.

W projektowanym brzmieniu art. 41a proponuje się nałożenie sankcji karnych na każdego kto bez uprawnienia kopiuje lub przechowuje nieprzyporządkowane do niego dane pozwalające na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej w systemie identyfikacji elektronicznej, przyłączonym do węzła krajowego. Zaznaczyć należy, iż powyższe nie odnosi się do podmiotów wydających środki identyfikacji elektronicznej, które mogą posiadać takie dane na potrzeby przeprowadzenia procesów uwierzytelniania osób, którym środki te zostały wydane, co wynika ze specyfiki działalności w zakresie tego typu usług. Ponadto, w zamierzeniu projektodawcy przepis odnosić się ma do posiadania kompletnych danych pozwalających na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej. Przepis ten nie będzie zatem dotyczył sytuacji, w której osoba nieupoważniona będzie w posiadaniu części danych pozwalających na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej, na przykład wyłącznie identyfikatora użytkownika (loginu) innej osoby, w szczególności w przypadku gdy takie dane są jawne lub łatwe do ustalenia. Przepis ten odnosi się do przechowywania wspomnianych danych w dowolnej formie i postaci, na dowolnym nośniku danych, zapisanych w sposób jawny i nieujawniony (np. zaszyfrowane).

Aktualizuje się nadto brzmienie art. 44 nadając przedmiotowemu przepisowi brzmienie, zgodnie z którym „Kto wydaje środek identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego osobie nieuprawnionej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.”

Proponuje się dodanie art. 44a i art. 44b. Pierwszy z nich stanowiłby, że karze pieniężnej w wysokości do 1 000 000 złotych podlega nieuprawnione gromadzenie, przetwarzanie lub powielanie danych dotyczących wykorzystania środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego. Zgodnie zaś z proponowanym brzmieniem art. 44b podmiot odpowiedzialny za system identyfikacji elektronicznej, przyłączony do węzła krajowego, który w wyniku świadomego działania lub zaniechania dopuściłby się w swoim systemie identyfikacji elektronicznej do uwierzytelnienia z wykorzystaniem środka identyfikacji elektronicznej, co do którego posiadał wiedzę, że nie pozostaje on pod wyłączną kontrolą osoby, której ten środek wydano, podlegałby karze pieniężnej w wysokości do 1 000 000 złotych.

Celem przedmiotowych przepisów jest napiętnowanie działań godzących w wiarygodność środków identyfikacji elektronicznej, a tym samym podważających zaufanie do tych środków jako narzędzi pozwalających na potwierdzenie tożsamości identyfikujących się przy ich użyciu osób.

W brzmieniu art. 3f § 1 ustawy z dnia 29 sierpnia 1997 r. ̶ Ordynacja podatkowa dokonuje się zmiany mającej na celu dopuszczenie możliwości stosowania środków identyfikacji elektronicznej, wydanych w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w portalu podatkowym, w celu uwierzytelniania podatników, płatników, inkasentów, ich następców prawnych oraz osób trzecich.

W ustawie z dnia 4 września 1997 r. o działach administracji rządowej do zakresu spraw właściwych dla działu „informatyzacja” dodaje się sprawy dotyczące „identyfikacji elektronicznej”.

W brzmieniu art. 57 § 5 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych dokonuje się zmiany mającej na celu dopuszczenie możliwości stosowania środków identyfikacji elektronicznej, wydanych w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w systemie teleinformatycznym obsługującym postępowanie w sprawie powołania do pełnienia urzędu na stanowisku sędziowskim w celu uwierzytelniania użytkowników tego systemu.

W ustawie z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy wprowadza się zmianę doprecyzowującą brzmienie przepisów mającą na celu wskazanie, iż w ramach zadań realizowanych na rzecz rynku przez ministra właściwego do spraw pracy mieści się wprowadzenie i rozwijanie w publicznych służbach zatrudnienia systemu teleinformatycznego umożliwiającego wnoszenie wniosków w postaci elektronicznej do jednostek publicznych służb zatrudnienia. Określa się nadto metody uwierzytelnienia użytkowników wyżej wspomnianego systemu teleinformatycznego, Dodaje się także przepisy stanowiące, iż wniosek o wpis do rejestru podmiotów prowadzących agencje zatrudnienia oraz wniosek o udzielenie akredytacji, o której mowa w art. 36b ust. 1 przedmiotowej ustawy, może być złożony przy wykorzystaniu wyżej wspomnianego systemu po zastosowaniu zapewnionych w tym systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych.

Projekt przewiduje wprowadzenie zmian w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Zmiany te mają między innymi na celu stworzenie podstaw prawnych dla rozwiązań informatycznych pozwalających organom administracji publicznej na świadczenie usług elektronicznych o wyższym niż dotychczas poziomie dojrzałości. Działanie takie wpisuje się w oczekiwania obywateli, iż korzystanie z usług świadczonych przez administrację publiczną będzie odbywało się w możliwie najprostszy sposób i bez konieczności osobistego stawiennictwa w urzędzie. Powyższy cel może być osiągnięty poprzez szersze wykorzystanie gromadzonych przez administrację zasobów publicznych, ukierunkowane na uproszczenie usług elektronicznych pozwalających obywatelom na załatwianie ich spraw urzędowych przez Internet.

Minister właściwy do spraw informatyzacji, zgodnie z przepisami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne zarządza obecnie systemem identyfikacji elektronicznej, w którym wydawany jest środek identyfikacji elektronicznej „profil zaufany ePUAP”. Działanie wspominanego 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”.

Środek identyfikacji elektronicznej, jakim jest „profil zaufany ePUAP”, w świetle pierwotnych założeń służyć miał do uwierzytelniania osób korzystających z usług online udostępnianych na ePUAP. Obecnie profil zaufany ePUAP wykorzystywany jest także na potrzeby usług świadczonych w ramach innych dziedzinowych systemów teleinformatycznych administrowanych przez podmioty publiczne. Przedmiotowy projekt zakłada, że węzeł krajowy stanowił będzie narzędzie integrujące systemy teleinformatyczne, w których świadczone są usługi online z systemami teleinformatycznymi pozwalającymi na uwierzytelnienie usługobiorców przy użyciu środków identyfikacji elektronicznej. W związku z powyższym, jak również ze względów organizacyjnych i technicznych, rekomendowanym jest aby zadania związane z wydawaniem i obsługą „profilu zaufanego ePUAP” zostały pod względem prawnym wyłączone ze zbioru zadań realizowanych w ramach ePUAP, a przedmiotowemu środkowi identyfikacji elektronicznej nadana została nazwa „profil zaufany” oraz wydawany był w ramach określonego w niniejszym projekcie „publicznego systemu identyfikacji elektronicznej”. Jednocześnie w nawiązaniu do powyższego rekomenduje się aby, ze zbioru zadań realizowanych w ramach ePUAP wyłączona została pod względem prawnym także funkcjonalność opatrywania dokumentów elektronicznych „podpisem potwierdzonym profilem zaufanym ePUAP”. Przedmiotowemu podpisowi elektronicznemu, którego złożenie będzie możliwe po uprzednim uwierzytelnieniu „profilem zaufanym”, proponuje się nadanie nowej uproszczonej nazwy „podpis zaufany”. Niezależnie od powyższych zmian, działanie wyżej wspomnianych narzędzi powinno być nadal zapewniane przez ministra właściwego do spraw informatyzacji przy użyciu systemów teleinformatycznych.

Stosownie do art. 3 pkt 2 rozporządzenia eIDAS, „środek identyfikacji elektronicznej” oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online. Minimalnym zestawem danych, który służy identyfikacji osoby fizycznej przez polskich dostawców w usługach publicznych i niepublicznych, jest co do zasady: imię, nazwisko oraz numer PESEL stanowiący unikalny identyfikator osoby fizycznej w państwowym systemie ewidencji ludności. Stąd też, podobnie jak obecnie w „profilu zaufanym ePUAP”, wspomniany wyżej zbiór danych stanowił będzie zestaw „danych identyfikujących osobę” stanowiący trzon nowego środka identyfikacji elektronicznej, czyli „profilu zaufanego”.

Należy w tym miejscu podkreślić, że w art. 3 rozporządzenia eIDAS zdefiniowano trzy kategorie podpisów, odpowiednio w punktach:

* 10) „podpis elektroniczny”, który oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis;
* 11) „zaawansowany podpis elektroniczny”, który oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26;
* 12) „kwalifikowany podpis elektroniczny”, który oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Podpis zaufany (wg aktualnej nomenklatury „podpis potwierdzony profilem zaufanym ePUAP”) nie stanowi zaawansowanego podpisu elektronicznego, należy bowiem wskazać, iż nie spełnia on wymagania art. 26 lit. c rozporządzenia eIDAS. Dostrzeżono to między innymi w raporcie ENISA z grudnia 2017 r.[[1]](#footnote-1)) gdzie na str. 16 wskazuje się podpis potwierdzony profilem zaufanym jako przykład „innego podpisu krajowego”.

Ponadto należy także podkreślić, że przepisy art. 27 rozporządzenia eIDAS w wersji angielskiej (pierwotnej) nie wymagają wzajemnego uznawania podpisów zaawansowanych tylko ich rozpoznawania.

Nadaje się nowe brzmienie art. 13a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne celem uwzględnienia państwowych lub samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu realizacji zadań publicznych w zbiorze podmiotów, które będąc uprawnionymi do wykonywania praw majątkowych do programu komputerowego opracowanego przez pracowników w ramach wykonywania obowiązków ze stosunku pracy świadczonej na rzecz tych podmiotów, mogą umożliwić sobie wzajemnie nieodpłatne korzystanie z tego programu komputerowego. Jednocześnie, w brzmieniu przedmiotowego przepisu zastępuje się wyraz „opracowanego” na „stworzonego”. Jest to wyłącznie zmiana redakcyjna mająca na celu doprecyzowanie zastosowanej terminologii do prawa autorskiego, która nie zmienia dotychczasowego rozumienia przedmiotowej jednostki redakcyjnej.

Zgodnie z obowiązującym art. 220 § 1 pkt 2 lit. b ustawy z dnia 14 czerwca 1960 r. – Kodeksu postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650) organ administracji publicznej nie może żądać zaświadczenia ani oświadczenia na potwierdzenie faktów lub stanu prawnego, jeżeli możliwe są do ustalenia przez ten organ na podstawie rejestrów publicznych posiadanych przez inne podmioty publiczne, do których organ ten ma dostęp w drodze elektronicznej, na zasadach określonych w przepisach ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Analogiczna regulacja zawarta została w art. 306d § 1 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa   
(Dz. U. z 2017 r. poz. 201, z późn. zm).

Niestety aktualna rzeczywistość stosowania tych przepisów nie jest zadowalająca. W wielu sprawach organy administracji publicznej, zamiast ustalić w rejestrach publicznych innych podmiotów publicznych informacje potrzebne do załatwienia sprawy, wymagają od obywateli dostarczenia zaświadczeń. Niestosowanie w praktyce wyżej przytoczonego przepisu jest wynikiem braku mechanizmów prawnych pozwalających na zapewnienie organom, świadczącym usługi na rzecz obywateli, szybkiego dostępu do danych zgromadzonych w rejestrach publicznych prowadzonych przez inne podmioty publiczne.

Nawiązując do powyższego problemu w ramach art. 25 pkt 3 projektu dodaje się do ustawy o informatyzacji art. 15a.

Artykuł 15a stanowić ma dla podmiotów publicznych podstawę prawną zapewniającą możliwość udostępniania danych gromadzonych w prowadzonych rejestrach publicznych lub w systemach teleinformatycznych innym podmiotom na potrzeby usług online, które są świadczone na rzecz osób albo podmiotów przy użyciu systemu teleinformatycznego. Udostępnienie to ma następować z uwzględnieniem zasad przewidzianych w przepisach szczególnych dotyczących rejestru publicznego lub systemu teleinformatycznego, z którego te dane są udostępniane. Udostępnione dane usługodawca będzie mógł wykorzystać wyłącznie do uzupełnienia zakresu użytkowego dokumentu elektronicznego, wymaganego w związku ze świadczoną usługą online, lub potwierdzenia faktów lub stanu prawnego, wymaganego w związku ze świadczoną usługą online.

Przyjęto, że dane będą udostępniane na wniosek osoby lub przedstawiciela podmiotu, na rzecz których świadczona jest usługa online, w ramach której dane te zostaną w dalszej kolejności przekazane przez wnioskodawcę podmiotowi świadczącemu tę usługę. Celem zapewnienia możliwości uwierzytelnienia osoby lub podmiotu wnioskującego o dostęp do danych wskazano na wymóg stosowania w przedmiotowym zakresie mechanizmów określonych w art. 20a ust. 1 ustawy o informatyzacji.

Udostępnienie danych będzie następowało w drodze bezpośredniej wymiany danych pomiędzy systemem teleinformatycznym, z którego udostępniane są dane a systemem teleinformatycznym, przy użyciu którego świadczona jest usługa online. Wymiana danych będzie realizowana z wykorzystaniem usług sieciowych, a warunki udostępnienia danych określane będą w porozumieniu, zawartym pomiędzy dysponentami wyżej wspominanych systemów teleinformatycznych, uwzględniającym przepisy odrębne regulujących funkcjonowanie rejestrów lub systemów teleinformatycznych, z których wnioskowane dane pochodzą. Przyjęto że udostępnienie wyżej wspomnianych usług sieciowych nastąpi w terminie określonym w porozumieniu, jednakże nie dłuższym niż 12 miesięcy od dnia zawarcia tego porozumienia. Wskazany wyżej okres czasu wynika z uwzględnienia czasu potrzebnego na przeprowadzenie niezbędnych prac, których celem będzie odpowiednie dostosowanie systemu teleinformatycznego z którego udostępniane będą dane, a także uwzględnienie w budżecie organu zobowiązanego do udostępnienia danych środków finansowych niezbędnych dla przeprowadzenia tych prac.

W art. 3 w pkt 25 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne proponuje się zdefiniowanie formularza elektronicznego wprost jako oprogramowania służącego do przygotowania i wygenerowania dokumentu elektronicznego, zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego, mogącego stanowić część usługi publicznej udostępnionej na ePUAP lub w innym systemie teleinformatycznym. Powyższy zabieg ma na celu uwypuklenie tego, iż formularz elektroniczny służący do załatwienia sprawy elektronicznie ma nie być odzwierciedleniem procedury papierowego załatwienia sprawy, a podmiot udostępniający formularz elektroniczny ma zaprojektować z jego wykorzystaniem proces realizacji usługi elektronicznej w taki sposób, aby dokument elektroniczny, który zostanie wygenerowany z użyciem tego oprogramowania zawierał wszystkie dane konieczne do załatwienia sprawy.

W związku z powyższym proponuje się doprecyzować definicję zakresu użytkowego dokumentu elektronicznego o wskazanie, iż są to dane zawarte w dokumencie elektronicznym, niezbędne do załatwienia określonego rodzaju spraw, w szczególności za pośrednictwem usługi publicznej udostępnionej na ePUAP lub w innym systemie teleinformatycznym. Szczególnie ważne jest podkreślenie obowiązku zamieszczenia w tym zakresie wszystkich danych i informacji niezbędnych do załatwienia konkretnej sprawy. Inaczej mówiąc, zakres użytkowy dokumentu elektronicznego ma odzwierciedlać nie tylko sam wniosek papierowy, który zapoczątkowuje sprawę, ale też konieczne wszystkie inne dane i informacje, które mają być dołączone do tego wniosku, aby był kompletny i mógł służyć załatwieniu sprawy skutecznie.

Zgodnie z ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne „elektroniczna platforma usług administracji publicznej” (ePUAP) to system teleinformatyczny, w którym instytucje publiczne udostępniają usługi publiczne przez pojedynczy punkt dostępowy w sieci Internet. Usługi te zgodnie z przepisami ustawy są realizowane z wykorzystaniem formularzy elektronicznych, jako narzędzia umożliwiającego załatwienie sprawy elektronicznie. Oceniając poziom elektronizacji usług aktualnie należy uznać, iż jest on niezadowalający, gdyż nie wszystkie sprawy wynikające dziś z obowiązujących przepisów można załatwiać elektronicznie. W celu poprawienia funkcjonalności usług oferowanych na ePUAP lub w innych systemach teleinformatycznych, których funkcjonowanie zapewnia minister właściwy do spraw informatyzacji, proponuje się umożliwienie ministrowi właściwemu do spraw informatyzacji dokonania modyfikacji zamieszczonych w tych systemach formularzy elektronicznych. Dodatkowo, w celu poprawienia funkcjonalności usługi minister właściwy do spraw informatyzacji może, po zasięgnięciu opinii organu właściwego do określenia wzoru dokumentu oraz w uzasadnionych przypadkach organów, w których właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentu elektronicznego, udostępnić na ePUAP lub w innym w systemie teleinformatycznym formularz elektroniczny stworzony przez siebie, który będzie oprogramowaniem służącym do załatwienia sprawy przez obywatela czy przedsiębiorcę. Z analizy zamieszczonych dziś na ePUAP usług wynika, że nie wszystkie podmioty odpowiedzialne za określenie wzorów dokumentów elektronicznych zamieszczają te wzory na ePUAP. Tym samym nie wszystkie sprawy, które mogłyby być realizowane elektronicznie są możliwe do realizacji tą drogą. W związku z powyższym projekt przepisów przygotowanych przewiduje, że minister właściwy do spraw informatyzacji, po konsultacji z odpowiedzialnym właściwym organem, będzie mógł udostępniać na ePUAP formularze elektroniczne, za pomocą których możliwe będzie załatwianie kolejnych spraw elektronicznie.

Analogiczną zmianę w zakresie kompetencji ministra właściwego do spraw informatyzacji przewidziano w art. 16b ustawy, czyli w przypadku gdy w przepisach prawa nie został wskazany organ właściwy do określenia wzoru dokumentu, wzór dokumentu elektronicznego może przekazać do centralnego repozytorium wzorów dokumentów elektronicznych organ, w którego właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentów elektronicznych lub minister właściwy do spraw informatyzacji po zasięgnięciu w uzasadnionych przypadkach opinii organów, w których właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentu elektronicznego.

Nadaje się nowe brzmienie art. 19c ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne określające podmioty, z którymi minister może zawrzeć porozumienie w sprawie udostępniania usług na ePUAP lub korzystania z usług sieciowych. Do podmiotów tych należeć będą podmioty, o których mowa w art. 2 ust. 3, realizujące zadania publiczne oraz inne podmioty wykonujące zadania publiczne lub wspierające świadczenie tych zadań w celu realizacji strategii i programów przyjętych przez Radę Ministrów lub strategii rozwoju, programów i dokumentów programowych w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2017 poz. 1376). Podmioty te zobowiązane są do wskazania interesu faktycznego udostępniania usług na ePUAP lub korzystania z usług sieciowych pozwalających na wykorzystanie profilu zaufanego. Ocena interesu faktycznego dokonywana jest przy uwzględnieniu jego wpływu na bezpieczeństwo i interes publiczny.

Do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne dodaje się art. 19e–19j, które stanowiły będą podstawę prawną dla funkcjonowania „mDokumentów”, czyli dokumentów elektronicznych przechowywanych na urządzeniach mobilnych, których użycie ma pozwolić obywatelowi na potwierdzenie swojej tożsamości oraz posiadanych uprawnień, co w powyższym zakresie ma pozwolić na zastąpienie użycia odpowiednich dla tych czynności dokumentów nieelektronicznych.

Zgodnie z projektowanymi przepisami minister właściwy do spraw informatyzacji zapewni możliwość korzystania z „mDokumentów” przy użyciu systemu teleinformatycznego oraz dedykowanego do tego celu oprogramowania przeznaczonego dla urządzeń mobilnych, nazwanego „publiczną aplikacją mobilną”. System teleinformatyczny będzie pozwalał na pobranie dokumentu elektronicznego, który zależnie od celu jego utworzenia będzie zawierał: dane osobowe użytkownika publicznej aplikacji mobilnej pobrane z rejestrów publicznych w zakresie określonym w niniejszej ustawie, dane dotyczące sytuacji prawnej lub praw przysługujących użytkownikowi aplikacji mobilnej, dane umożliwiające identyfikację rzeczy związanej z użytkownikiem aplikacji mobilnej albo będzie stanowił kopię dokumentu urzędowego, który wydawany jest w postaci nieelektronicznej. Wspomniany wyżej dokument elektroniczny będzie mógł być pobrany na urządzenie mobilne przy użyciu publicznej aplikacji mobilnej. Aplikacja ta będzie pozwalała na przechowywanie i prezentację takich dokumentów, a także ich przekazywanie pomiędzy urządzeniami mobilnymi oraz weryfikację ich integralności i pochodzenia.

Zastrzec należy, że udostępnienie funkcjonalności „mDokumentu” zawierającego dane osobowe użytkownika publicznej aplikacji mobilnej, pobrane z rejestrów publicznych (PESEL, RDO), może być dokonane przez ministra właściwego do spraw informatyzacji wyłącznie w uzgodnieniu z ministrem spraw wewnętrznych. Powyższe dokonane będzie w drodze komunikatu ogłaszanego w Dzienniku Urzędowym Monitor Polski, w którym określony będzie termin uruchomienia takiego rozwiązania.

Kluczowym warunkiem użyteczności przedmiotowego rozwiązania jest zapewnienie wiarygodności, prezentowanego lub przekazywanego przez obywatela przy użyciu urządzenia mobilnego, dokumentu elektronicznego. Dlatego też, wprowadza się przepis zobowiązujący ministra właściwego do spraw informatyzacji do stosowania w przedmiotowym zakresie mechanizmów, które pozwolą na potwierdzenie integralności i pochodzenia danych dokumentu elektronicznego. Zgodnie z przyjętymi założeniami, mechanizmy takie będą pozwalały co najmniej na potwierdzenie: że dokument elektroniczny został utworzony w systemie teleinformatycznym ministra właściwego do spraw informatyzacji, czas utworzenia takiego dokumentu, a także niezmienność tego dokumentu oraz zawartych w nim danych od momentu jego utworzenia.

Zbiór dostępnych dokumentów elektronicznych, którymi będzie można posługiwać się przy użyciu publicznej aplikacji mobilnej, będzie zależał od potrzeb, wynikających z realizowanych zadań, zgłaszanych przez podmioty, o których mowa w art. 2 i art. 19c zmienianej ustawy. Zapewnienie w publicznej aplikacji mobilnej możliwości korzystania z nowego dokumentu elektronicznego, będzie następowało na podstawie porozumienia pomiędzy ministrem właściwym do spraw informatyzacji a podmiotem wnioskującym o udostępnienie takiej funkcjonalności. Zawarcie wspomnianego wyżej porozumienia będzie dla ministra właściwego do spraw informatyzacji obowiązkowe tylko w przypadku podmiotów, o których mowa w art. 2 zmienianej ustawy.

Użytkowanie publicznej aplikacji mobilnej będzie bezpłatne i dobrowolne. Pobieranie publicznej aplikacji mobilnej będzie traktowane jako zgoda użytkownika tej aplikacji na przetwarzanie przez ministra właściwego do spraw informatyzacji jego danych osobowych w zakresie niezbędnym do obsługi udostępnianych w tej aplikacji dokumentów elektronicznych, zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego. Korzystanie z dokumentu elektronicznego, obsługiwanego w publicznej aplikacji mobilnej, będzie możliwe po uprzednim uwierzytelnieniu użytkownika tej aplikacji, w systemie teleinformatycznym ministra właściwego do spraw informatyzacji, w sposób, o którym mowa w art. 20a ust. 1 zmienianej ustawy, o ile przepisy szczególne lub porozumienie, o którym mowa powyżej, nie będą stanowiły inaczej. Wyjątek od powyższego, będzie mógł wynikać z przepisów szczególnych lub porozumienia, na podstawie których określony dokument elektroniczny udostępniany będzie w publicznej aplikacji mobilnej. Minister właściwy do spraw informatyzacji zobowiązany zostanie do publikowania i aktualizacji, na swojej stronie podmiotowej w Biuletynie Informacji Publicznej, zamieszcza informacje o:

* aktywnych i nieaktywnych, w tym czasowo zawieszonych, funkcjonalnościach publicznej aplikacji mobilnej,
* stosowanych mechanizmach zapewniających możliwość potwierdzenia integralności i pochodzenia dokumentów elektronicznych oraz procedurach uzyskania takiego potwierdzenia,
* adresach elektronicznych, pod którymi udostępniony jest regulamin korzystania oraz informacja o wymaganiach technicznych dotyczących korzystania z publicznej aplikacji mobilnej.

Na potrzeby świadczenia usług przy użyciu dokumentów elektronicznych przechowywanych w publicznej aplikacji mobilnej dodaje się przepis stanowiący, że dane i wizerunek użytkownika tej aplikacji będą mogły być pobrane z Rejestru Dowodów Osobistych, na podstawie art. 63 ust. 4 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, oraz z rejestru PESEL na podstawie art. 45 ust. 1 a ustawy z dnia 24 września 2010 r. o ewidencji ludności. Jednocześnie, w wyżej wymienionych ustawach dodaje się przepisy uprawniające każdą osobę do pobrania dotyczących jej danych odpowiednio z Rejestru Dowodów Osobistych oraz z rejestru PESEL.

W przepisie art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, dotyczącym uwierzytelnienia użytkownika systemów teleinformatycznych udostępnianych przez podmioty publiczne, rozszerzono katalog wskazanych dotychczas środków identyfikacji elektronicznej służących temu celowi o środek identyfikacji elektronicznej, wydany w przyłączonym do węzła krajowego systemie identyfikacji elektronicznej. Doprecyzowano nadto, że uwierzytelnianie z wykorzystaniem środków identyfikacji elektronicznej zapewnia się adekwatnie do wymaganego poziomu bezpieczeństwa, niezbędnego dla realizacji usług, określonego przez podmioty odpowiedzialne za systemy teleinformatyczne, w których udostępniane są usługi online, przyłączane do węzła krajowego. Dostosowano brzmienie art. 20a ust. 1 zastępując pojęcie „identyfikacja” pojęciem „uwierzytelnienie”. Doprecyzowano ponadto obecne brzmienie art. 20a ust. 1 pkt 3 wskazując, że uwierzytelnienie użytkownika systemu teleinformatycznego może nastąpić jak dotychczas przy użyciu „danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego”, jednakże wyłącznie w przypadku gdy dane zawarte w przedmiotowym certyfikacie „pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi publicznej”. Należy bowiem wskazać, iż zgodnie z brzmieniem lit. c załącznika I do rozporządzenia eIDAS, kwalifikowany certyfikat podpisu elektronicznego może zawierać wyłącznie „imię i nazwisko podpisującego lub jego pseudonim”. Certyfikat taki może więc zawierać zbiór danych, który nie będzie wystarczający do ustalenia tożsamości użytkownika usługi publicznej. Podkreślenia wymaga, iż art. 20a ust. 1 posługuje się pojęciem „uwierzytelnianie”, w rozumieniu art. 3 pkt 5 rozporządzenia eIDAS, czyli w odniesieniu do procesu elektronicznego, który umożliwia ustalenie tożsamości (w tym przypadku) osoby fizycznej. Należy więc wskazać, że projektowane brzmienie art. 20a ust. 1 pkt 3 nie odnosi się do sytuacji w której przepisy prawa wymagają zastosowania podpisu elektronicznego, nie jest więc przedmiotem tego przepisu zastosowanie kwalifikowanego certyfikatu podpisu elektronicznego w celu opatrzenia dokumentu elektronicznego kwalifikowanym podpisem elektronicznym. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne dodaje się także 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 publicznym świadczącym usługi elektroniczne możliwość uwierzytelniania użytkowników tych platform przy użyciu „profilu zaufanego”. Omawiany system teleinformatyczny będzie zintegrowany z węzłem krajowym. 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”. Ponadto, dodaje się art. 20ab zobowiązujący ministra właściwego do spraw informatyzacji do zarządzania publicznym systemem identyfikacji elektronicznej, o którym mowa w art. 20aa pkt 1, oraz do gromadzenia i przechowywania informacji związanych z zapewnieniem rozliczalności i niezaprzeczalności działań użytkowników korzystających z „profilu zaufanego”. Dodaje się art. 20ac ustanawiający ministra właściwego do spraw informatyzacji administratorem danych wspomnianego wyżej publicznego systemu identyfikacji elektronicznej oraz określający jakie dane dotyczące osób posługujących się „profilem zaufanym”, oraz uczestniczących w procesach potwierdzania tego środka identyfikacji elektronicznej, będą przetwarzane w tym systemie.

Dodaje się art. 20ad, w którego 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”. 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.

Uchyla 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, z późn. zm.). 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 środku 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 użytym przez posiadacza tego środka identyfikacji elektronicznej 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-kredytowych, 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 powiększania 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 „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. 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. 20aa, po przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym. Testy te potwierdzają interoperacyjność przyłączanego systemu teleinformatycznego i systemu teleinformatycznego, przy użyciu którego realizowana będzie obsługa „podpisu zaufanego”, czyli prawidłowość organizacyjnego i technicznego współdziałania tych systemów teleinformatycznych.

W celu umożliwienia użytkownikom usług online udostępnionych na ePUAP podpisania dokumentu elektronicznego „podpisem zaufanym”, dodaje się art. 20g stanowiący, iż system ten przyłącza się z mocy ustawy do systemu teleinformatycznego, przy użyciu którego świadczona będzie usługa „podpisu zaufanego”.

Efektem zmian wprowadzanych ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne ma być głównie zwiększenie liczby i jakości usług świadczonych drogą elektroniczną, a także ich dostępności dla zainteresowanych podmiotów, jak również przyśpieszenie realizacji niektórych czynności w ramach prowadzonych postępowań, zaoszczędzenie czasu oraz oszczędności finansowe dla obywatela, wynikające z załatwiania spraw drogą elektroniczną.

Skuteczne działanie służb takich jak Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego może wymagać posługiwania się środkami identyfikacji elektronicznej na szczególnych zasadach. Stąd też w ustawach regulujących funkcjonowanie tych służb dodaje się odpowiednio przepisy stanowiące, iż funkcjonariusze tych służb, a także osoby udzielające pomocy tym służbom, mogą posługiwać się, w ramach wykonywania czynności operacyjno-rozpoznawczych, środkami identyfikacji elektronicznej zawierającymi dane inne niż dane identyfikujące odpowiednio tych funkcjonariuszy lub wspomniane wyżej osoby. Jednocześnie dodaje się przepisy wyłączające odpowiedzialność karną za wydawanie takich środków identyfikacji elektronicznej wspomnianym wyżej funkcjonariuszom lub osobom, a także za dopuszczenie do uwierzytelnienia osoby fizycznej z wykorzystaniem takiego środka identyfikacji elektronicznej w systemie identyfikacji elektronicznej, w którym taki środek został wydany.

Ze względu na brak jednoznacznego uregulowania w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych możliwości świadczenia przez spółdzielcze kasy oszczędnościowo-kredytowe usług zaufania dla swoich członków i wydawania im środków identyfikacji elektronicznej, mając na uwadze istniejące przepisy w art. 20c w ust. 3 dodano pkt 5, stanowiący że spółdzielcze kasy oszczędnościowo-kredytowe, mogą świadczyć na rzecz swoich członków usługi zaufania oraz wydawać swoim członkom środki identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania. Nowy przepis rozwieje ewentualne wątpliwości dotyczące podstawy prawnej dla wydawanych już przez SKOK-i środków identyfikacji elektronicznej w ramach usług świadczonych dla swoich członków i w sposób jednoznaczny pozwoli na wykorzystanie zarówno tych środków jak i usług zaufania także poza obszarem określonym wprost w ustawie o spółdzielczych kasach oszczędnościowo-kredytowych.

W ustawie o ewidencji ludności dodaje się także przepisy stanowiące o udostępnianiu podmiotom odpowiedzialnym za system identyfikacji elektronicznej oraz podmiotom wydającym środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej, danych z rejestru PESEL, rejestrów mieszkańców oraz rejestrów zamieszkania cudzoziemców, w zakresie niezbędnym do realizacji zadań, jakie te podmioty realizują zgodnie z ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Wspomnianym wyżej podmiotom udostępniane będą, w sposób i na warunkach określonych w art. 49 ust. 1 tej ustawy, dane dotyczące numeru PESEL, daty urodzenia, miejsca urodzenia, płci, imienia (imion), nazwiska, oraz nazwiska rodowego. Udostępnienie przedmiotowych danych realizowane będzie nieodpłatnie.

Projekt przewiduje wprowadzenie zmian w następujących ustawach dotyczących obszaru „rodzina”, które wprowadzają usługi publiczne elektronicznego wnioskowania: ustawa z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2017 r. poz. 1952, z późn. zm.), ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2017 r. poz. 1065, z późn. zm.), ustawa z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2018 r. poz. 554 i 650), ustawa z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3 (Dz. U. z 2018 r. poz. 603 i 650), ustawa z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2017 r. poz. 1832), ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. z 2017 r. poz. 1851, z późn. zm.). Ustawy dotyczące obszaru „rodzina” określają sposób podpisywania się pod wnioskiem składanym w postaci elektronicznej (podpis kwalifikowany lub podpis zaufany). W celu ujednolicenia poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w systemach regulowanych przez ww. ustawy, powinno się uspójnić przepisy tych ustaw. Zmiany te pozwolą na ujednolicenie przepisów związanych z rozwiązaniem informatycznym pozwalającym organom obszarowej administracji publicznej na świadczenie usług elektronicznych. Wprowadzenie spójnych przepisów ułatwi obywatelowi wykorzystanie umocowanych prawnie rozwiązań teleinformatycznych w sprawnej komunikacji z urzędami, a pracownikom obszarowej administracji samorządowej zapewni jednolity sposób postępowania przy obsłudze elektronicznego kanału komunikacji.

W brzmieniu art. 70 ust. ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014–2020 dokonuje się zmiany mającej na celu dopuszczenie możliwości stosowania środków identyfikacji elektronicznej, wydanych w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w „centralnym systemie teleinformatycznym”, w rozumieniu tej ustawy, w celu uwierzytelnienia beneficjenta lub osoby fizycznej, która zgodnie z postanowieniami umowy o dofinansowanie projektu lub decyzji o dofinansowaniu projektu jest upoważniona do reprezentowania beneficjenta w zakresie czynności związanych z realizacją projektu w tym systemie.

Zgodnie z projektem ustawy elektroniczna platforma usług administracji publicznej zapewni możliwość uwierzytelnienia użytkowników z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego z dniem wejścia w życie ustawy. Jednocześnie określa się końcowe terminy, w których analogiczne zapewnienie zostanie odpowiednio dokonane we wskazanych w ustawie publicznych systemach teleinformatycznych, w ramach których świadczone są usługi publiczne.

Ustawa wejdzie w życie po upływie 1 miesiąca od dnia ogłoszenia. Część przepisów wejdzie w życie w innych terminach, przy czym zróżnicowanie terminu wejścia w życie części przepisów jest niezbędne dla ich prawidłowej realizacji, w tym w związku z potrzebą dostosowania systemów.

Wspomniane już wyżej zastąpienie odpowiednio „profilu zaufanego ePUAP” środkiem identyfikacji elektronicznej nazwanym „profil zaufany” oraz „podpisu potwierdzonego profilem zaufanym ePUAP” podpisem elektronicznym nazwanym „podpis zaufany” pociąga za sobą konieczność dokonania adekwatnych zmian w ustawach, w których te pojęcia występują. Stąd też projekt uwzględnia dokonanie w powyższym zakresie odpowiednich zmian w szeregu obowiązujących obecnie aktów normatywnych.

Art. 56 projektu stanowi, że „profile zaufane ePUAP” potwierdzone zgodnie z przepisami ustawy zmienianej w art. 25 w brzmieniu dotychczasowym stają się „profilami zaufanymi” w rozumieniu art. 3 pkt 14 ustawy zmienianej w art. 25 w brzmieniu nadanym niniejszą ustawą. 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”, w art. 57 stanowi się, iż wszędzie tam gdzie przepisy prawa wymagają użycia „podpisu potwierdzonego profilem zaufanym ePUAP” uznaje się, że użycie „podpisu zaufanego” ma równoważny skutek.

W art. 58 projektu stanowi się, że zgody udzielone przez ministra właściwego do spraw informatyzacji na podstawie 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.

Art. 59 projektu zobowiązuje do podziału przez ministra właściwego do spraw finansów publicznych w porozumieniu z ministrem właściwym do spraw wewnętrznych – środków z rezerwy celowej na zakup przez gminy urządzeń służących do obsługi środka identyfikacji elektronicznej, wydawanego przez ministra właściwego do spraw wewnętrznych w publicznym systemie identyfikacji elektronicznej przyłączonym do węzła krajowego. W marcu 2019 r. planowane jest wdrożenie dowodu osobistego z warstwą elektroniczną. W warstwie elektronicznej tego dowodu będzie umieszczony m.in. certyfikat identyfikacji i uwierzytelnienia. Certyfikat ten będzie wydawany przez ministra właściwego do spraw wewnętrznych. Założono, że przed wdrożeniem dowodu osobistego jako nośnika środka identyfikacji elektronicznej, niezbędne będzie wyposażenie w urządzenia służące do obsługi środka identyfikacji elektronicznej, tj. czytniki nowego dokumentu, stanowisk w gminach zajmujących się wydawaniem dowodów osobistych. Koszt zakupu czytników w wysokości 5 400 tys. zł. zostanie pokryty z rezerwy celowej zaplanowanej na 2018 r. Uwzględniając konieczność zapewnienia wystandaryzowanych urządzeń, minister właściwy do spraw wewnętrznych przekaże wymagania techniczne dla tych urządzeń.

Art. 60 zobowiązywał będzie ministra właściwego do spraw informatyzacji do notyfikacji Komisji Europejskiej wspomnianego wyżej publicznego systemu identyfikacji.

Projekt ustawy nie ma bezpośredniego wpływu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Projekt ustawy nie jest sprzeczny z prawem Unii Europejskiej oraz nie zawiera norm technicznych 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, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowana ustawa nie wymaga przedstawienia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu.

Projekt został umieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz w BIP na stronie podmiotowej Ministerstwa Cyfryzacji.

Żaden podmiot nie zgłosił zainteresowania pracami nad projektem ustawy w trybie przepisów ustawy o działalności lobbingowej w procesie stanowienia prawa.

1. ) link: https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services/at\_download/fullReport [↑](#footnote-ref-1)