SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Prezes Rady Ministrów
RM-10-110-17

Druk nr 2502

Warszawa, 30 kwietnia 2018 r.

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw z projektami aktów wykonawczych.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Jednocześnie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem

(-) Mateusz Morawiecki

Projekt

U S T A W A

z dnia

o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw[1)]

Art. 1. W ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650) wprowadza się następujące zmiany:

---

1) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, ustawę z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, ustawę z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, ustawę z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym, ustawę z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawę z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, ustawę z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym, ustawę z dnia 15 września 2000 r. – Kodeks spółek handlowych, ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, ustawę z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej, ustawę z dnia 6 września 2001 r. o transporcie drogowym, ustawę z dnia 6 września 2001 r. – Prawo farmaceutyczne, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego, ustawę z dnia 28 lutego 2003 r. – Prawo upadłościowe, ustawę z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, ustawę z dnia 28 listopada 2003 r. o świadczeniach rodzinnych, ustawę z dnia 19 marca 2004 r. – Prawo celne, ustawę z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, ustawę z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawę z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym, ustawę z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów, ustawę z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, ustawę z dnia 24 września 2010 r. o ewidencji ludności, ustawę z dnia 5 stycznia 2011 r. o kierujących pojazdami, ustawę z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3, ustawę z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej, ustawę z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, ustawę z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych, ustawę z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej, ustawę z dnia 14 grudnia 2012 r. o odpadach, ustawę z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw, ustawę z dnia 14 marca 2014 r. o zasadach prowadzenia zbiórek publicznych, ustawę z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014–2020, ustawę z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny, ustawę z dnia 20 lutego 2015 r. o odnawialnych źródłach energii, ustawę z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne, ustawę z dnia 15 maja 2015 r. o substancjach zubożających warstwę ozonową oraz o niektórych fluorowanych gazach cieplarnianych, ustawę z dnia 15 maja 2015 r. o zmianie ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa oraz niektórych innych ustaw, ustawę z dnia 25 czerwca 2015 r. – Prawo konsularne, ustawę z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci, ustawę z dnia 15 grudnia 2016 r. o Prokuratorii Generalnej Rzeczypospolitej Polskiej, ustawę z dnia 24 lutego 2017 r. o uzyskiwaniu tytułu specjalisty w dziedzinach mających zastosowanie w ochronie zdrowia, ustawę z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej, ustawę z dnia 24 listopada 2017 r. o zmianie ustawy o odpadach oraz niektórych innych ustaw oraz ustawę z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy.

1) w art. 1 w ust. 1 w pkt 4 kropkę zastępuje się średnikiem i dodaje się pkt 5 i 6 w brzmieniu:

„5) krajowy schemat identyfikacji elektronicznej;

6) nadzór nad krajowym schematem identyfikacji elektronicznej.”;

2) tytuł rozdziału 4 otrzymuje brzmienie:

„Krajowy schemat identyfikacji elektronicznej”;

3) w rozdziale 4 dodaje się art. 21a–21z w brzmieniu:

„Art. 21a. 1. Krajowy schemat identyfikacji elektronicznej obejmuje:

1) węzeł krajowy identyfikacji elektronicznej, zwany dalej „węzłem krajowym”;

2) przyłączone do węzła krajowego:

a) systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej,

b) systemy teleinformatyczne, w których udostępniane są usługi online;

3) węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, zwany dalej „węzłem transgranicznym”.

2. Węzeł krajowy jest rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego.

3. Wykorzystywanie środka identyfikacji elektronicznej do uwierzytelnienia użytkownika systemu teleinformatycznego w celu realizacji usługi online świadczonej 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 910/2014 jest nieodpłatne.

4. Uwierzytelnienie użytkownika systemu teleinformatycznego w celu realizacji usługi online wymaga użycia środka identyfikacji elektronicznej na poziomie bezpieczeństwa określonym przez podmiot świadczący tę usługę.

5. Funkcjonowanie węzła krajowego zapewnia minister właściwy do spraw informatyzacji.

6. Minister właściwy do spraw informatyzacji przetwarza dane osobowe osób, którym wydano środki identyfikacji elektronicznej, obejmujące:

1) imię (imiona),
2) nazwisko,
3) nazwisko rodowe,
4) numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014,
5) datę urodzenia,
6) miejsce urodzenia,
7) płeć,
8) adres zamieszkania

– w celu uwierzytelnienia z wykorzystaniem węzła krajowego.

Art. 21b. 1. Minister właściwy do spraw informatyzacji wydaje decyzję o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego, podmiotowi odpowiedzialnemu za ten system posiadającemu siedzibę na terenie jednego z państw członkowskich Unii Europejskiej, po:

1) potwierdzeniu spełnienia przez ten system wymagań dla zadeklarowanych poziomów bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie, określonych w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014;
2) przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność systemów identyfikacji elektronicznej, z uwzględnieniem przepisów wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014;
3) zapewnieniu przez podmiot odpowiedzialny za ten system opracowania, ustanawiania, wdrażania, eksploatowania, monitorowania, przeglądania, 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;
4) 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;

5) przedstawieniu przez podmiot odpowiedzialny za ten system oświadczenia o działaniu tego podmiotu zgodnie z przepisami o ochronie danych osobowych.

2. Przyłączenie systemu identyfikacji elektronicznej do węzła krajowego następuje pod warunkiem dostarczenia ministrowi właściwemu do spraw informatyzacji przez podmiot odpowiedzialny za system identyfikacji elektronicznej, w terminie wskazanym przez tego ministra, nie krótszym niż 30 dni, kopii umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej wnioskodawcy.

3. Po spełnieniu warunku, o którym mowa w ust. 2, przyłączenie systemu identyfikacji elektronicznej do węzła krajowego następuje bez zbędnej zwłoki.

Art. 21c. 1. Ubezpieczeniem odpowiedzialności cywilnej, o którym mowa w art. 21b ust. 2, jest objęta odpowiedzialność cywilna podmiotu odpowiedzialnego za system identyfikacji elektronicznej, za szkodę wynikającą z działania lub zaniechania, wyrządzoną w związku z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej, w usłudze online świadczonej 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, lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014, spowodowaną przez awarię, przerwę lub błąd systemu lub przez zaciągnięcie zobowiązania w wyniku nieuprawnionego wykorzystania tego środka identyfikacji elektronicznej.

2. Ubezpieczenie odpowiedzialności cywilnej, o którym mowa w art. 21b ust. 2, nie obejmuje 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 o szkody wynikające ze zdarzeń wskazanych w pkt 1–3.

3. Ubezpieczenie, o którym mowa w art. 21b ust. 2, obejmuje wszystkie szkody w zakresie, o którym mowa w ust. 1, z zastrzeżeniem ust. 2, bez możliwości umownego ograniczenia odpowiedzialności przez zakład ubezpieczeń.

Art. 21d. 1. Minister właściwy do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw informatyzacji, po zasięgnięciu opinii Polskiej Izby Ubezpieczeń, określi, w drodze rozporządzenia, minimalną sumę gwarancyjną ubezpieczenia odpowiedzialności cywilnej, o którym mowa w art. 21b ust. 2, za szkody wynikające z działania lub zaniechania, wyrządzone w związku z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej, w usługach online świadczonych przez podmioty, o których mowa w art. 2 lub art. 19c ust. l ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub podmioty sektora publicznego, o których mowa w art. 3 pkt 7 rozporządzenia 910/2014, spowodowane przez awarie, przerwy lub błędy systemu lub przez zaciągnięcie zobowiązań w wyniku nieuprawnionego wykorzystania środka identyfikacji elektronicznej, uwzględniając specyfikę działalności prowadzonej przez podmioty odpowiedzialne za systemy identyfikacji elektronicznej.

2. Minister właściwy do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, wysokość kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej, za szkody wynikające z działania lub zaniechania wyrządzone, w związku z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej, w usługach online świadczonych przez podmioty, o których mowa w art. 2 lub art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub podmioty sektora publicznego, o których mowa w art. 3 pkt 7 rozporządzenia 910/2014, spowodowane przez awarie, przerwy lub błędy systemu lub za zobowiązanie zaciągnięte w wyniku nieuprawnionego wykorzystania środka identyfikacji elektronicznej, w zależności od poziomu bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie.

Art. 21e. 1. Osoba, której wydano środek identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, jest obowiązana:

1) korzystać ze środka identyfikacji elektronicznej zgodnie z warunkami określonymi przez podmiot odpowiedzialny za system identyfikacji elektronicznej, w którym został wydany ten środek;
2) zgłaszać niezwłocznie podmiotowi odpowiedzialnemu za system identyfikacji elektronicznej, w którym został wydany ten środek, utratę, kradzież, przywłaszczenie środka identyfikacji elektronicznej lub utratę wyłącznej kontroli nad danymi umożliwiającymi identyfikację przy użyciu tego środka albo stwierdzenie nieuprawnione użycia środka identyfikacji elektronicznej.

2. W celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, osoba, której wydano środek identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, z chwilą wydania tego środka, podejmuje niezbędne działania służące zapobieżeniu naruszenia indywidualnych zabezpieczeń tego środka lub danych umożliwiających identyfikację przy użyciu tego środka.

Art. 21f. W przypadku zgłoszenia, o którym mowa w art. 21e ust. 1 pkt 2, osoba, której wydano środek identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, nie ponosi odpowiedzialności za zobowiązanie zaciągnięte po dokonania zgłoszenia z wykorzystaniem środka identyfikacji elektronicznej.

Art. 21g. 1. Przyłączenie systemu identyfikacji elektronicznej do węzła krajowego następuje na wniosek podmiotu odpowiedzialnego za system identyfikacji elektronicznej.

2. Wniosek zawiera:

1) imię i nazwisko lub firmę (nazwę), adres siedziby i miejsca wykonywania działalności, numer w Krajowym Rejestrze Sądowym, 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, podmiotu odpowiedzialnego za system identyfikacji elektronicznej;
2) imię i nazwisko lub firmę (nazwę), adres siedziby i miejsca wykonywania działalności, numer w Krajowym Rejestrze Sądowym, 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, każdego podmiotu:

a) potwierdzającego tożsamość oraz weryfikującego dane identyfikujące osoby ubiegającej się o wydanie środka identyfikacji elektronicznej,

b) wydającego środki identyfikacji elektronicznej,

c) zapewniającego funkcjonalność pozwalającą na uwierzytelnienie osób, którym wydano środek identyfikacji elektronicznej

– w przypadku gdy czynności tych nie wykonuje podmiot odpowiedzialny za system identyfikacji elektronicznej;

3) nazwę i szczegółowy opis systemu identyfikacji elektronicznej, w tym opis środków identyfikacji elektronicznej wydawanych w tym systemie z określeniem ich poziomu bezpieczeństwa, o którym mowa w art. 8 ust. 2 rozporządzenia 910/2014, oraz informacje techniczne i organizacyjne dotyczące wykorzystania tych środków.

3. Do wniosku dołącza się:

1) dokument potwierdzający spełnianie wymagań dla zadeklarowanych poziomów bezpieczeństwa środków identyfikacji elektronicznej, określonych w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014, w szczególności:

a) pozytywny wynik audytu systemu zarządzania bezpieczeństwem informacji obejmujący swym zakresem system identyfikacji elektronicznej, którego dotyczy wniosek, albo

b) pozytywny wynik audytu, o którym mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014

– adekwatnie do poziomu bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie;

2) 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;

3) oświadczenie o zapewnieniu stosowania polityki bezpieczeństwa, o której mowa w art. 39b ust. 1 pkt 3;

4) oświadczenie o działaniu podmiotu zgodnie z przepisami o ochronie danych osobowych.

4. Wniosek oraz dokumenty, o których mowa w ust. 3, składa się w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym.

Art. 21h. Minister właściwy do spraw informatyzacji po dokonaniu oceny wniosku oraz dokumentów załączonych do wniosku wyznacza termin przeprowadzenia testów integracyjnych, o których mowa w art. 21b ust. 1 pkt 2, i przeprowadza testy zgodnie z procedurą udostępnioną w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

Art. 21i. Minister właściwy do spraw informatyzacji informuje podmiot odpowiedzialny za system identyfikacji elektronicznej na piśmie, w postaci papierowej albo elektronicznej o:

1) przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego;
2) każdej zmianie polityki bezpieczeństwa, o której mowa w art. 39b ust. 1 pkt 3.

Art. 21j. W przypadku niespełniania wymagań, o których mowa w art. 21b ust. 1, minister właściwy do spraw informatyzacji wydaje decyzję o odmowie przyłączenia systemu identyfikacji elektronicznej do węzła krajowego.

Art. 21k. Podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego dostarcza ministrowi właściwemu do spraw informatyzacji:

1) dokumenty potwierdzające spełnianie aktualnych wymagań dla wskazanych we wniosku poziomów bezpieczeństwa środków identyfikacji elektronicznej, o których mowa w art. 21g ust. 3 pkt 1, w przypadku zmiany przepisów wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014, w terminie 14 dni od dnia wejścia w życie zmiany tych przepisów;
2) kopię kolejnej umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej wnioskodawcy, w terminie 14 dni od dnia jej zawarcia.

Art. 21l. 1. Ponowne złożenie wniosku, o którym mowa w art. 21g ust. 1, wymagane jest w przypadku:

1) zmiany poziomu bezpieczeństwa środka identyfikacji elektronicznej, wydawanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego;
2) uruchomienia w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego środka identyfikacji elektronicznej nieobjętego zakresem wniosku, na

podstawie którego została wydana decyzja o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego.

2. Umożliwienie korzystania za pośrednictwem węzła krajowego ze środków identyfikacji elektronicznej, o których mowa w ust. 1, następuje po pozytywnym rozpatrzeniu wniosku i przeprowadzeniu testów integracyjnych.

Art. 21m. Do węzła krajowego przyłącza się system teleinformatyczny zapewniający obsługę publicznego systemu identyfikacji elektronicznej, o którym mowa w art. 20aa ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publicznej.

Art. 21n. 1. Minister właściwy do spraw informatyzacji prowadzi rejestr systemów identyfikacji elektronicznej przyłączonych do węzła krajowego, zwany dalej „rejestrem systemów’’.

2. Rejestr systemów jest jawny.

3. Podstawą do wpisania systemu identyfikacji elektronicznej do rejestru systemów jest decyzja, o której mowa w art. 21b ust. 1. Wpis jest czynnością materialno-techniczną.

4. Do rejestru systemów wpisuje się:

1) informacje zawarte we wniosku, o którym mowa w art. 21g ust. 2;
2) datę przyłączenia systemu identyfikacji elektronicznej do węzła krajowego;
3) informacje o zamiarze zaprzestania świadczenia usług związanych ze środkami identyfikacji elektronicznej wydawanymi w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego;
4) informacje o otwarciu likwidacji podmiotu odpowiedzialnego za system identyfikacji elektronicznej oraz datę jego likwidacji;
5) informacje o ogłoszeniu upadłości podmiotu odpowiedzialnego za system identyfikacji elektronicznej lub oddaleniu wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe oraz datę zakończenia postępowania upadłościowego;
6) informacje o zawieszeniu możliwości korzystania z systemu identyfikacji elektronicznej lub uwierzytelniania z wykorzystaniem środków identyfikacji elektronicznych wydanych w tym systemie;

7) informacje o przywróceniu możliwości korzystania z systemu identyfikacji elektronicznej lub uwierzytelniania z wykorzystaniem środków identyfikacji elektronicznej wydanych w tym systemie;
8) informację o tym, czy system identyfikacji elektronicznej został przyłączony do węzła transgranicznego;
9) datę wykreślenia z rejestru systemów podmiotu odpowiedzialnego za system identyfikacji elektronicznej.

Art. 21o. 1. Informacje i dane zawarte w dokumentach potwierdzających spełnianie wymagań, o których mowa w art. 21b ust. 1, których ujawnienie mogłoby narazić na szkodę podmiot odpowiedzialny za system identyfikacji elektronicznej, objęte są tajemnicą.

2. Informacje i dane objęte tajemnicą udostępnia się wyłącznie na żądanie:
1) sądu lub prokuratora – w związku z toczącym się postępowaniem;
2) innych upoważnionych organów – w związku z prowadzonym przez te organy postępowaniem;
3) Szefa Agencji Bezpieczeństwa Wewnętrznego.

Art. 21p. 1. Podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego:
1) zarządza systemem identyfikacji elektronicznej oraz ponosi koszty jego utrzymania i rozwoju;
2) potwierdza tożsamość oraz weryfikuje dane identyfikujące osoby ubiegające się o wydanie środka identyfikacji elektronicznej w sposób adekwatny do poziomu bezpieczeństwa danego środka identyfikacji elektronicznej, zgodnie z wymaganiami określonymi w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014;
3) wydaje, zawiesza i unieważnia środki identyfikacji elektronicznej;
4) zapewnia funkcjonalność pozwalającą na uwierzytelnienie osoby, której wydano środek identyfikacji elektronicznej, z wykorzystaniem tego środka;
5) zapisuje i zachowuje informacje związane z wydawaniem, zawieszaniem i unieważnianiem środków identyfikacji elektronicznej oraz zapewnieniem rozliczalności i niezaprzeczalności działań użytkowników korzystających z tych środków;

6) stosuje politykę bezpieczeństwa węzła krajowego, o której mowa w art. 39b ust. 1 pkt 3.

2. Czynności, o których mowa w ust. 1 pkt 2–5, mogą wykonywać podmioty inne niż podmiot odpowiedzialny za system identyfikacji elektronicznej, spełniające wymogi określone w art. 21b ust. 1 pkt 1, 3 i 5, o ile posiadają siedzibę na terenie jednego z państw członkowskich Unii Europejskiej. Odpowiedzialność za czynności wykonywane przez te podmioty ponosi podmiot odpowiedzialny za system identyfikacji elektronicznej.

3. Podmioty, o których mowa w ust. 2, stosują politykę bezpieczeństwa węzła krajowego, o której mowa w art. 39b ust. 1 pkt 3.

Art. 21q. 1. Podmiot odpowiedzialny za system identyfikacji elektronicznej przetwarza dane osobowe osób, którym w tym systemie wydano środki identyfikacji elektronicznej, obejmujące:

1) imię (imiona),
2) nazwisko,
3) nazwisko rodowe,
4) numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014,
5) datę urodzenia,
6) miejsce urodzenia,
7) płeć,
8) adres zamieszkania

– w celu realizacji zadań, o których mowa w art. 21p ust. 1 pkt 1–5.

2. Podmiot, o którym mowa w art. 21p, inny niż podmiot wskazany 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 910/2014, zapewniając możliwość uwierzytelniania w usługach online nie może pozyskiwać, przechowywać oraz przetwarzać danych dotyczących realizacji tych usług, innych niż dane niezbędne do zrealizowania procesu uwierzytelnienia.

Art. 21r. 1. 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.

2. 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.

Art. 21s. 1. Podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego informuje ministra właściwego do spraw informatyzacji o:

1) każdej zmianie dotyczącej systemu identyfikacji elektronicznej przyłączonego do węzła krajowego mającej wpływ na aktualność danych wpisanych do rejestru systemów – w terminie 14 dni od dnia zmiany tych danych;
2) zamiarze zaprzestania świadczenia usług związanych ze środkami identyfikacji elektronicznej wydawanymi w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego – w terminie 12 miesięcy przed planowanym zaprzestaniem świadczenia tych usług;
3) otwarciu jego likwidacji, ogłoszeniu jego upadłości lub oddaleniu wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe – niezwłocznie;
4) zawieszeniu możliwości uwierzytelniania z powodu naruszenia bezpieczeństwa, o którym mowa w art. 21r ust. 1 oraz przywróceniu możliwości uwierzytelniania po usunięciu naruszenia bezpieczeństwa, o którym mowa w art. 21r ust. 2 – niezwłocznie, nie później niż w ciągu 24 godzin od momentu odpowiednio wykrycia naruszenia bezpieczeństwa oraz usunięcia naruszenia bezpieczeństwa.

2. Minister właściwy do spraw informatyzacji po otrzymaniu danych, o których mowa w ust. 1, 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.

Art. 21t. 1. Minister właściwy do spraw informatyzacji wydaje decyzję o przyłączeniu do węzła krajowego systemu teleinformatycznego, w którym udostępniane są usługi online, po:

1) zapewnieniu przez podmiot odpowiedzialny za ten system opracowania, ustanawiania, wdrażania, eksploatowania, monitorowania, przeglądania, 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;
2) przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność tego systemu z węzłem krajowym;
3) przedstawieniu przez podmiot odpowiedzialny za ten system oświadczenia o działaniu tego podmiotu zgodnie z przepisami o ochronie danych osobowych;
4) wskazaniu interesu faktycznego w uwierzytelnianiu z wykorzystaniem węzła krajowego – w przypadku podmiotu innego niż podmiot wskazany 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 910/2014.

2. Ocena interesu faktycznego dokonywana jest przy uwzględnieniu jego wpływu na bezpieczeństwo i interes publiczny.

Art. 21u. 1. Przyłączenie systemu, o którym mowa w art. 21t ust. 1, do węzła krajowego następuje na wniosek podmiotu odpowiedzialnego za ten system.

2. Wniosek zawiera nazwę podmiotu odpowiedzialnego za system albo jego imię i nazwisko oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania.

3. Do wniosku dołącza się:

1) oświadczenie o zapewnieniu przez podmiot odpowiedzialny za ten system opracowania, ustanawiania, wdrażania, eksploatowania, monitorowania, przeglądania, 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;

2) oświadczenie o zapewnieniu stosowania polityki bezpieczeństwa, o której mowa w art. 39b ust.1 pkt 3;

3) 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;

4) oświadczenie o działaniu podmiotu zgodnie z przepisami o ochronie danych osobowych;

5) uzasadnienie interesu faktycznego w uwierzytelnianiu z wykorzystaniem węzła krajowego – w przypadku podmiotu innego niż podmiot, o których 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 910/2014.

4. Wniosek oraz dokumenty, o których mowa w ust. 3, składa się w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym.

Art. 21v. Minister właściwy do spraw informatyzacji po dokonaniu oceny wniosku oraz dokumentów załączonych do wniosku wyznacza termin przeprowadzenia testów integracyjnych, o których mowa w art. 21t ust. 1 pkt 2, i przeprowadza testy zgodnie z procedurą udostępnioną w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

Art. 21w. Podmiot odpowiedzialny za system teleinformatyczny, w którym udostępniane są usługi online, przyłączony do węzła krajowego, niezwłocznie informuje ministra właściwego do spraw informatyzacji o każdej zmianie danych zawartych w dokumencie, o którym mowa w art. 21u ust. 3 pkt 3.

Art. 21x. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej informację o przyłączonych do węzła krajowego systemach teleinformatycznych, w którym udostępniane są usługi online.

Art. 21y. W przypadku niespełniania wymagań, o których mowa w art. 21t ust. 1, minister właściwy do spraw informatyzacji wydaje decyzję o odmowie przyłączenia

systemu teleinformatycznego, w którym udostępniane są usługi online, do węzła krajowego.

Art. 21z. Do węzła krajowego przyłącza się elektroniczną platformę usług administracji publicznej.”;

4) art. 22 otrzymuje brzmienie:

„Art. 22. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie węzła transgranicznego, zgodnie z rozporządzeniem 910/2014 oraz przepisami wykonawczymi wydanymi na podstawie tego rozporządzenia.

2. Do notyfikacji, o której mowa w art. 9 rozporządzenia 910/2014, mogą być zgłaszane wyłącznie systemy identyfikacji elektronicznej przyłączone do węzła krajowego, jeżeli zostało potwierdzone spełnienie wymagań, o których mowa w art. 7 tego rozporządzenia.

3. Notyfikowany system identyfikacji elektronicznej jest przyłączany do węzła transgranicznego za pośrednictwem węzła krajowego.”;

5) w art. 24:

a) ust. 1 otrzymuje brzmienie:

„1. Wniosek o notyfikowanie systemu identyfikacji elektronicznej w Komisji Europejskiej składa do ministra właściwego do spraw informatyzacji podmiot odpowiedzialny za ten system.”,

b) ust. 3 i 4 otrzymują brzmienie:

„3. 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 910/2014, po pozytywnym zweryfikowaniu wniosku, o którym mowa w ust. 1, biorąc pod uwagę warunki kwalifikowania się systemu do notyfikowania wskazane w art. 7 tego rozporządzenia oraz politykę państwa w zakresie identyfikacji elektronicznej.

4. Minister właściwy do spraw informatyzacji zgłasza system identyfikacji elektronicznej do notyfikacji, o której mowa w art. 9 rozporządzenia 910/2014, biorąc pod uwagę wynik wzajemnej oceny, o której mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 7 tego rozporządzenia.”;

6) art. 25 otrzymuje brzmienie:

„Art. 25. Podmioty odpowiedzialne za systemy teleinformatyczne, w których udostępniane są usługi online, przyłączane do węzła krajowego, określają wymagane

poziomy bezpieczeństwa środków identyfikacji elektronicznej, o których mowa w art. 8 ust. 2 rozporządzenia 910/2014, niezbędne dla realizacji tych usług.”;

7) w art. 26 ust. 2 otrzymuje brzmienie:

„2. Informacje dotyczące naruszenia bezpieczeństwa notyfikowanego systemu identyfikacji elektronicznej albo uwierzytelnienia, o którym mowa w art. 10 rozporządzenia 910/2014, podmiot odpowiedzialny za ten system przekazuje niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia naruszenia, drogą elektroniczną, ministrowi właściwemu do spraw informatyzacji.”;

8) po rozdziale 5 dodaje się rozdział 5a w brzmieniu:

„Rozdział 5a

Nadzór nad krajowym schematem identyfikacji elektronicznej

Art. 39a. Nadzór nad krajowym schematem identyfikacji elektronicznej sprawuje minister właściwy do spraw informatyzacji.

Art. 39b. 1. W ramach nadzoru minister właściwy do spraw informatyzacji:

1) prowadzi kontrole:
   a) spełniania przez systemy identyfikacji elektronicznej przyłączone do węzła krajowego wymagań, o których mowa w art. 21b ust. 1,
   b) spełniania przez systemy teleinformatyczne, w których udostępniane są usługi online, przyłączone do węzła krajowego, wymagań, o których mowa w art. 21t ust. 1;
2) prowadzi działania zapobiegające naruszeniom bezpieczeństwa w krajowym schemacie identyfikacji elektronicznej, w szczególności dokonuje systematycznego szacowania ryzyka wystąpienia incydentów w krajowym schemacie identyfikacji elektronicznej;
3) określa i udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej politykę bezpieczeństwa węzła krajowego;
4) uczestniczy w inicjatywach krajowych i międzynarodowych mających na celu podnoszenie bezpieczeństwa węzła krajowego, węzła transgranicznego oraz systemów identyfikacji elektronicznej;
5) współpracuje z organem właściwym do spraw ochrony danych osobowych.

2. W ramach działań zapobiegających naruszeniom bezpieczeństwa w krajowym schemacie identyfikacji elektronicznej minister właściwy do spraw informatyzacji:

1) prowadzi systematyczne szacowanie ryzyka wystąpienia incydentów, przez które rozumie się każde zdarzenie, które ma lub może mieć niekorzystny wpływ na poufność danych albo rozliczalność działań dokonywanych w ramach świadczonych usług w krajowym schemacie identyfikacji elektronicznej, w tym za pośrednictwem węzła krajowego;
2) wdraża, rozwija i upowszechnia stosowanie środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, odpowiednich i proporcjonalnych do zidentyfikowanych ryzyk, zapewniających bezpieczeństwo systemów teleinformatycznych wykorzystywanych do świadczenia usług za pośrednictwem węzła krajowego;
3) po dostrzeżeniu podatności lub zagrożeń naruszających lub mogących naruszać poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemach teleinformatycznych działających w ramach krajowego schematu identyfikacji elektronicznej niezwłocznie podejmuje działania zaradcze.

Art. 39c. 1. W przypadku naruszenia polityki bezpieczeństwa węzła krajowego lub niespełniania wymagań, o których mowa w art. 21b ust. 1, dotyczących systemu identyfikacji elektronicznej przyłączonego do węzła krajowego, w zakresie mającym wpływ na wiarygodność uwierzytelnienia z wykorzystaniem środków identyfikacji elektronicznej wydanych w tym systemie, minister właściwy do spraw informatyzacji wydaje decyzję o zawieszeniu:

1) możliwości korzystania z tego systemu, jeżeli naruszenie dotyczy całego systemu, albo
2) możliwości korzystania z części środków identyfikacji elektronicznej wydanych w tym systemie, jeżeli naruszenie dotyczy części środków identyfikacji elektronicznej i zawieszenie takie jest możliwe technicznie.

2. Minister właściwy do spraw informatyzacji wydaje decyzję o przywróceniu możliwości korzystania z systemu identyfikacji elektronicznej lub zawieszonej części środków identyfikacji elektronicznej niezwłocznie po otrzymaniu od podmiotu odpowiedzialnego za system identyfikacji elektronicznej potwierdzenia usunięcia naruszenia, które było podstawą do zawieszenia, o którym mowa w ust. 1.

3. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu. Przepisu art. 61 § 2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi nie stosuje się.

Art. 39d. Minister właściwy do spraw informatyzacji wydaje decyzję o odłączeniu systemu identyfikacji elektronicznej od węzła krajowego i odłącza ten system od węzła krajowego, w przypadku:

1) złożenia przez podmiot odpowiedzialny za system identyfikacji elektronicznej wniosku o odłączenie od węzła krajowego;
2) zaprzestania prowadzenia działalności przez podmiot odpowiedzialny za system identyfikacji elektronicznej;
3) nieusunięcia przyczyny zawieszenia możliwości uwierzytelniania, o której mowa w art. 21r ust. 1, lub możliwości korzystania z systemu, o której mowa w art. 39c ust. 1, w terminie trzech miesięcy od dnia jego zawieszenia;
4) nieprzedstawienia kolejnej umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej.

Art. 39e. 1. Decyzja o odłączeniu systemu identyfikacji elektronicznej od węzła krajowego jest podstawą do wykreślenia tego systemu z rejestru systemów.

2. Decyzja podlega natychmiastowemu wykonaniu. Przepisu art. 61 § 2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi nie stosuje się.

Art. 39f. Podmiot odpowiedzialny za system identyfikacji elektronicznej, na żądanie ministra właściwego do spraw informatyzacji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych, jest obowiązany udzielać informacji oraz udostępniać dokumenty, które są bezpośrednio związane z funkcjonowaniem systemu identyfikacji elektronicznej, w tym dotyczą naruszeń, o których mowa w art. 21r ust. 1 lub art. 39c ust. 1.

Art. 39g. 1. W przypadku naruszenia polityki bezpieczeństwa, o której mowa w art. 39b ust. 1 pkt 3, lub niespełniania wymagań, o których mowa w art. 21t ust. 1, dotyczącego 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 zawiesza w tym systemie możliwość uwierzytelniania z wykorzystaniem węzła krajowego.

2. Minister właściwy do spraw informatyzacji przywraca możliwość uwierzytelniania z wykorzystaniem węzła krajowego w systemie teleinformatycznym, w którym udostępniane są usługi online, niezwłocznie po otrzymaniu od podmiotu odpowiedzialnego za ten system potwierdzenia usunięcia naruszenia, które było podstawą do zawieszenia, o którym mowa w ust. 1.

Art. 39h. 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:

1) złożenia przez podmiot odpowiedzialny za ten system wniosku o odłączenie systemu od węzła krajowego;
2) zaprzestania udostępniania usług online w tym systemie;
3) nieusunięcia przyczyny zawieszenia tego systemu, o której mowa w art. 39g ust. 1, w terminie trzech miesięcy od dnia jego zawieszenia.

Art. 39i. Podmiot odpowiedzialny za system teleinformatyczny, w którym udostępniane są usługi online, na żądanie ministra właściwego do spraw informatyzacji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych, jest obowiązany udzielać informacji oraz udostępniać dokumenty, które są bezpośrednio związane z funkcjonowaniem tego systemu, w tym dotyczą naruszeń, o których mowa w art. 39g ust. 1.

Art. 39j. 1. Kontrola, o której mowa w art. 39b ust. 1 pkt 1, jest przeprowadzana przez osoby upoważnione przez ministra właściwego do spraw informatyzacji.

2. Osoby, o których mowa w ust. 1, są uprawnione do:

1) wstępu do obiektów i pomieszczeń podmiotu odpowiedzialnego za system identyfikacji elektronicznej lub podmiotu wydającego środek identyfikacji elektronicznej w tym systemie;
2) wglądu do dokumentów zawierających dane dotyczące funkcjonowania systemu identyfikacji elektronicznej oraz wydanych w tym systemie środków identyfikacji elektronicznej;
3) przetwarzania danych osobowych w zakresie objętym przedmiotem kontroli;

4) 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;
5) 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;
6) zabezpieczania dokumentów i innych materiałów, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

Art. 39k. 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.

Art. 39l. W sprawach nieuregulowanych w ustawie, do przeprowadzenia kontroli, o której mowa w art. 39b ust. 1 pkt 1, stosuje się odpowiednio przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 650).”;

9) tytuł rozdziału 6 otrzymuje brzmienie:

„Przepisy karne i przepisy o karach pieniężnych”;

10) po art. 40 dodaje się art. 40a w brzmieniu:

„Art. 40a. Kto posługuje się cudzym środkiem identyfikacji elektronicznej, wydawanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, w celu uzyskania nieuprawnionego dostępu do usługi online, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.”;

11) po art. 41 dodaje się art. 41a w brzmieniu:

„Art. 41a. Kto bez uprawnienia kopiuje lub przechowuje nieprzyporządkowane do niego dane pozwalające na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej, wydawanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.”;

12) art. 44 otrzymuje brzmienie:

„Art. 44. 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.”;

13) po art. 44 dodaje się art. 44a i art. 44b w brzmieniu:

„Art. 44a. Kto w sposób nieuprawniony gromadzi, przetwarza lub powiela dane dotyczące wykorzystania środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, podlega karze pieniężnej w wysokości do 1 000 000 złotych.

Art. 44b. Podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego, który w wyniku świadomego działania lub zaniechania dopuścił w swoim systemie identyfikacji elektronicznej do uwierzytelnienia z wykorzystaniem środka identyfikacji elektronicznej, co do którego posiada wiedzę, że nie pozostaje on pod wyłączną kontrolą osoby, której ten środek wydano, podlega karze pieniężnej w wysokości do 1 000 000 złotych.”;

14) w art. 96 w pkt 4 uchyla się lit. a;

15) w art. 137 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Dostawcy usług zaufania, producenci oprogramowania oraz podmioty publiczne, zobowiązani są do odpowiedniego dostosowania oprogramowania oraz systemów teleinformatycznych do zmian i terminu określonych w ust. 1.”;

16) art. 142 otrzymuje brzmienie:

„Art. 142. Ustawa wchodzi w życie po upływie 7 dni od dnia ogłoszenia, z wyjątkiem art. 22 oraz art. 24–26, które wchodzą w życie z dniem 29 września 2018 r.”.

Art. 2. W ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650) w art. 33 w § 2a i w § 3a w zdaniu pierwszym, w art. 63 w § 3a w pkt 1, w art. 76a w § 2a w zdaniu pierwszym oraz w art. 220 w § 3, użyte w różnym przypadku wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisem zaufanym”.

Art. 3. W ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155, z późn. zm.[2)]) w art. 126 w § 5 oraz w art. 694^4 w § 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 4. W ustawie z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2018 r. poz. 617, 650 i 697) w art. 3 w ust. 7 w pkt 1 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 5. W ustawie z dnia 20 czerwca 1997 r. − Prawo o ruchu drogowym (Dz. U. z 2017 r. poz. 1260, z późn. zm.[3)]) w art. 80c w ust. 5 w zdaniu pierwszym, w art. 80cc w ust. 2 w zdaniu pierwszym, w art. 80cd w ust. 2 w zdaniu pierwszym, w art. 80ce w ust. 2, w art. 100ah w ust. 4 w zdaniu pierwszym, w art. 100ak w ust. 2 w zdaniu pierwszym, w art. 100al w ust. 2 w zdaniu pierwszym oraz w art. 100am w ust. 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 6. W ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2017 r. poz. 700, z późn. zm.[4)]) w art. 19 w ust. 2b oraz w art. 19e w ust. 2 w zdaniu pierwszym i w zdaniu drugim wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 7. W ustawie z dnia 29 sierpnia 1997 r. − Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201, z późn. zm.[5)]) wprowadza się następujące zmiany:

1) w art. 3f § 1 otrzymuje brzmienie:

„§ 1. Uwierzytelnianie podatników, płatników, inkasentów, ich następców prawnych oraz osób trzecich na portalu podatkowym wymaga użycia danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, profilu zaufanego albo innego środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia

---

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2491 oraz z 2018 r. poz. 5, 138, 398, 416, 650, 730, 756, 770 i 771.

3) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 1926 oraz z 2018 r. poz. 79, 106, 138, 317 i 650.

4) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 1089 i 1133 oraz z 2018 r. poz. 398 i 650.

5) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 648, 768, 935, 1428, 1537, 2169 i 2491 oraz z 2018 r. poz. 106, 138, 398, 650, 723 i 771.

5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w portalu podatkowym.”;

2) w art. 14c w § 4, w art. 138a w § 3 i w § 5 w zdaniu pierwszym, w art. 144b w § 1 i w § 2 w pkt 1, w art. 159 w § 2, w art. 168 w § 3a w pkt 1, w art. 194a w § 2a w zdaniu pierwszym, w art. 210 w § 1 w pkt 8, w art. 217 w § 1 w pkt 7, w art. 282b w § 4 w pkt 6 oraz w art. 306d w § 3, użyte w różnym przypadku wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisem zaufanym”.

Art. 8. W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2018 r. poz. 762) w art. 12a w ust. 1 po pkt 13 dodaje się pkt 13a w brzmieniu:

„13a) identyfikacji elektronicznej;”.

Art. 9. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2017 r. poz. 1778, z późn. zm.[6)]) w art. 39a w ust. 1 we wprowadzeniu do wyliczenia wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 10. W ustawie z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 2017 r. poz. 1368) w art. 54 w ust. 1, w art. 55 w ust. 1, w art. 55a w ust. 7 w zdaniu pierwszym i w ust. 9 w zdaniu drugim, w art. 58a w ust. 1 w części wspólnej i w ust. 2, w art. 59 w ust. 9 w zdaniu pierwszym oraz w art. 61b w ust. 1 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 11. W ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2017 r. poz. 678, z późn. zm.[7)]) w art. 19 w ust. 2c i w ust. 3a wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

---

6) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2018 r. poz. 106, 138, 357, 398, 650, 697, 730 i 771.

7) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 1475 oraz z 2018 r. poz. 106, 138, 398, 431 i 730.

Art. 12. W ustawie z dnia 15 września 2000 r. − Kodeks spółek handlowych (Dz. U. z 2017 r. poz. 1577 oraz z 2018 r. poz. 398 i 650) wprowadza się następujące zmiany:

1) w art. 4 w § 1 uchyla się pkt 13;

2) w art. 10 w § 4 w zdaniu drugim, w art. 23^1 w § 2, w art. 40^1 w § 2 w zdaniu pierwszym, w art. 41 w § 4 w zdaniu pierwszym, w art. 58 w § 2 w zdaniu drugim, w art. 106^1 w § 2, w art. 157^1 w § 2, w art. 167 w § 4 w pkt 1, 2 i 3, w art. 180 w § 2 w zdaniu drugim, w art. 188 w § 4, w art. 208 w § 10 w zdaniu pierwszym, w art. 240^1 w § 2 w zdaniu drugim, w art. 259^1 w zdaniu drugim oraz w art. 270 w pkt 2^1, użyte w różnej liczbie wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 13. W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2018 r. poz. 23, 3, 5, 106, 138 i 771) wprowadza się następujące zmiany:

1) w art. 57 § 5 otrzymuje brzmienie:

„§ 5. Uwierzytelnienie w systemie teleinformatycznym wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, albo otrzymanego w sądzie identyfikatora wskazującego na tożsamość kandydata.”;

2) w art. 57 w § 6 oraz w art. 57aa w § 1 i w § 2 w zdaniu pierwszym wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 14. W ustawie z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej (Dz. U. z 2016 r. poz. 2245 oraz z 2017 r. poz. 1524 i 650) w art. 2a w ust. 3 w pkt 1 oraz w art. 30b w ust. 4 we wprowadzeniu do wyliczenia w zdaniu pierwszym, użyte w różnym przypadku wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisem zaufanym”.

Art. 15. W ustawie z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2017 r. poz. 2200 oraz z 2018 r. poz. 12, 79, 138 i 650) wprowadza się następujące zmiany:

1) w art. 82i ust. 3 i 4 otrzymują brzmienie:

„3. W przypadku przekazywania danych za pośrednictwem elektronicznej skrzynki podawczej Głównego Inspektora Transportu Drogowego przekazywane dane powinny być podpisane przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu zaufanego.

4. Dane przekazywane są do Rejestru przy użyciu formularzy elektronicznych udostępnionych na stronie internetowej Głównego Inspektoratu Transportu Drogowego lub za pośrednictwem elektronicznej platformy usług administracji publicznej.”;

2) w art. 82j ust. 6 otrzymuje brzmienie:

„6. Wniosek, o którym mowa w ust. 3, składany za pośrednictwem elektronicznej skrzynki podawczej Głównego Inspektora Transportu Drogowego powinien być podpisany przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu zaufanego.”.

Art. 16. W ustawie z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2017 r. poz. 2211 oraz z 2018 r. poz. 650 i 697) wprowadza się następujące zmiany:

1) w art. 96a w pkt 3 w lit. e tiret pierwsze otrzymuje brzmienie:

„− w postaci elektronicznej − kwalifikowany podpis elektroniczny, podpis zaufany albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych albo”;

2) w art. 107a w ust. 4 we wprowadzeniu do wyliczenia w zdaniu pierwszym oraz w art. 107f w ust. 5 w pkt 1, użyte w różnym przypadku wyrazy „podpisu potwierdzonego profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisu zaufanego”.

Art. 17. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138, 650, 723 i 730) w art. 35:

1) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Przy wykonywaniu czynności operacyjno-rozpoznawczych funkcjonariusze Agencji mogą posługiwać się środkami identyfikacji elektronicznej zawierającymi dane inne niż dane identyfikujące funkcjonariusza Agencji.”;

2) ust. 3 otrzymuje brzmienie:

„3. Osoby udzielające Agencji pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych mogą posługiwać się dokumentami, o których mowa w ust. 2, oraz odpowiednio środkami identyfikacji elektronicznej, o których mowa w ust. 2a.”;

3) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. ABW prowadzi centralny rejestr środków identyfikacji elektronicznej, o których mowa w ust. 2a.”;

4) w ust. 6:

a) pkt 4 otrzymuje brzmienie:

„4) funkcjonariusz Agencji lub osoba wymieniona w ust. 3, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, o których mowa w ust. 2 i 3, lub środkami identyfikacji elektronicznej, o których mowa w ust. 2a;”,

b) dodaje się pkt 5 w brzmieniu:

„5) kto wydaje środki identyfikacji elektronicznej, o których mowa w ust. 2a, funkcjonariuszowi Agencji albo osobom, o których mowa w ust. 3, lub dopuszcza do uwierzytelnienia z wykorzystaniem takiego środka identyfikacji elektronicznej w swoim systemie identyfikacji elektronicznej.”.

Art. 18. W ustawie z dnia 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego (Dz. U. z 2017 r. poz. 283 oraz z 2018 r. poz. 138, 398 i 650) w art. 25a, w art. 37 w ust. 6, w art. 62ze w ust. 1 w pkt 17, w art. 62zf w ust. 1 w pkt 16 oraz w art. 62zm w ust. 7 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 19. W ustawie z dnia 28 lutego 2003 r. − Prawo upadłościowe (Dz. U. z 2017 r. poz. 2344 i 2491 oraz z 2018 r. poz. 398 i 685) w art. 216a w ust. 1 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 20. W ustawie z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. z 2017 r. poz. 1073 i 1566) w art. 18 w ust. 3 w pkt 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 21. W ustawie z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2017 r. poz. 1952 oraz z 2018 r. poz. 107, 138, 650 i 730) w art. 23:

1) ust. 3b otrzymuje brzmienie:

„3b. Wniosek i załączniki do wniosku określone w ust. 4 w postaci elektronicznej mogą być składane za pomocą:

1) systemu, o którym mowa w ust. 6a, po zastosowaniu zapewnionych w systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych;
2) systemu teleinformatycznego wskazanego w informacji zamieszczonej na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw rodziny po uzgodnieniu z ministrem właściwym do spraw informatyzacji, po opatrzeniu ich kwalifikowanym podpisem elektronicznym albo podpisem zaufanym.”;

2) w ust. 6a zdanie drugie otrzymuje brzmienie:

„Uwierzytelnianie użytkowników w systemie teleinformatycznym wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, albo innych technologii, jeżeli zostaną udostępnione w tym systemie.”.

Art. 22. W ustawie z dnia 19 marca 2004 r. – Prawo celne (Dz. U. z 2018 r. poz. 167) w art. 10b w ust. 1 i 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 23. W ustawie z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2017 r. poz. 1065, z późn. zm.[8)]) wprowadza się następujące zmiany:

1) w art. 4:

a) w ust. 1 pkt 8 otrzymuje brzmienie:

„8) wprowadzanie i rozwijanie w publicznych służbach zatrudnienia systemów teleinformatycznych zapewniających spójny system obsługi rynku pracy, w tym systemu teleinformatycznego umożliwiającego wnoszenie wniosków w postaci elektronicznej do publicznych służb zatrudnienia, oraz prowadzenie i udostępnianie internetowej bazy ofert pracy.”,

b) dodaje się ust. 9 w brzmieniu:

„9. Uwierzytelnianie użytkowników w systemie teleinformatycznym umożliwiającym wnoszenie wniosków w postaci elektronicznej do publicznych służb zatrudnienia wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online albo innych technologii, jeżeli zostaną udostępnione w tym systemie.”;

2) art. 18f otrzymuje brzmienie:

„Art. 18f. Wniosek o wpis do rejestru może być złożony w postaci elektronicznej. Wniosek składany w postaci elektronicznej zawiera dane w ustalonym formacie elektronicznym, zawarte we wzorze wniosku, o którym mowa w art. 19k. Wniosek w postaci elektronicznej składany jest z wykorzystaniem systemu, o którym mowa

---

8) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 1292, 1321, 1428, 1543, 2371 i 2494 oraz z 2018 r. poz. 107, 138, 650 i 730.

w art. 4 ust. 1 pkt 8, po zastosowaniu zapewnionych w systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych.”;

3) w art. 36b ust. 6 otrzymuje brzmienie:

„6. Wniosek o udzielenie akredytacji może być złożony w postaci elektronicznej. Wniosek w postaci elektronicznej składany jest w wykorzystaniem systemu, o którym mowa w art. 4 ust. 1 pkt 8, po zastosowaniu zapewnionych w systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych.”.

Art. 24. W ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2017 r. poz. 1938, z późn. zm.[9)]) w art. 95e w ust. 2, w art. 95g w ust. 2 w pkt 9 oraz w art. 95i w ust. 3 we wprowadzeniu do wyliczenia w zdaniu pierwszym i w ust. 8 w pkt 8, użyte w różnym przypadku wyrazy „podpisem elektronicznym potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisem zaufanym”.

Art. 25. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570) wprowadza się następujące zmiany:

1) w art. 1 po pkt 9 dodaje się pkt 9a i 9b w brzmieniu:

„9a) funkcjonowania publicznego systemu identyfikacji elektronicznej,

9b) świadczenia usługi podpisu zaufanego”;

2) w art. 3:

a) pkt 14 otrzymuje brzmienie:

„14) profil zaufany – środek identyfikacji elektronicznej zawierający zestaw danych identyfikujących i opisujących osobę fizyczną, który został wydany w sposób, o którym mowa w art. 20c;”,

b) po pkt 14 dodaje się pkt 14a w brzmieniu:

„14a) podpis zaufany – podpis elektroniczny, którego autentyczność i integralność jest zapewniana przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający:

a) dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1,

---

[9)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2110, 2217, 2361 i 2434 oraz z 2018 r. poz. 107, 138, 650, 697, 730 i 771.

obejmujące:

– imię (imiona),

– nazwisko,

– numer PESEL,

b) identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony,

c) czas jego złożenia;”,

c) uchyla się pkt 15,

d) pkt 25 i 26 otrzymują brzmienie:

„25) formularz elektroniczny – oprogramowanie służące do przygotowania i wygenerowania dokumentu elektronicznego, zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego, mogące stanowić część usługi udostępnionej na ePUAP lub w innym systemie teleinformatycznym;

26) zakres użytkowy dokumentu elektronicznego – dane zawarte w dokumencie elektronicznym, niezbędne do załatwienia określonego rodzaju spraw, za pośrednictwem usługi udostępnionej na ePUAP lub w innym systemie teleinformatycznym;”;

3) art. 13a otrzymuje brzmienie:

„Art. 13a. Podmioty publiczne, o których mowa w art. 2 ust. 1 pkt 1–7, służby specjalne w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Kancelaria Sejmu, Kancelaria Senatu, Kancelaria Prezydenta Rzeczypospolitej Polskiej, Narodowy Bank Polski, agencje wykonawcze w rozumieniu art. 18 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62) oraz podmioty, o których mowa w art. 2 ust. 4, niewskazane wprost w art. 2 ust. 1, uprawnione do wykonywania praw majątkowych do programu komputerowego stworzonego przez pracowników w ramach wykonywania obowiązków ze stosunku pracy świadczonej na rzecz tych podmiotów, mogą umożliwić sobie wzajemnie nieodpłatne korzystanie z tego programu komputerowego.”;

4) po art. 15 dodaje się art. 15a w brzmieniu:

„Art. 15a. 1. Podmiot publiczny może udostępnić dane gromadzone w prowadzonym rejestrze publicznym lub w systemie teleinformatycznym innemu podmiotowi publicznemu lub podmiotowi, o którym mowa w art. 19c ust. 1,

z uwzględnieniem zasad przewidzianych w przepisach szczególnych dotyczących odpowiednio tego rejestru lub danych gromadzonych w tym systemie teleinformatycznym, wyłącznie na potrzeby usługi online, która jest świadczona na rzecz osoby albo podmiotu przy użyciu systemu teleinformatycznego.

2. Udostępnienie danych, o których mowa w ust. 1, następuje na każdorazowy wniosek osoby albo podmiotu, na rzecz których świadczona jest usługa online, i których te dane dotyczą, po ich uwierzytelnieniu w sposób, o którym mowa w art. 20a ust. 1. Osobie lub podmiotowi, których dane są udostępniane, zapewnia się wgląd do udostępnionych danych.

3. Jeżeli podmiot świadczący usługę online, o której mowa w ust. 1, posiada dostęp do danych osoby albo podmiotu, na rzecz których świadczona jest usługa online, zgromadzonych w rejestrze publicznym lub systemie teleinformatycznym, wynikający:

1) z jawności tych danych, lub

2) z przepisów szczególnych uprawniających ten podmiot do dostępu do tych danych

– a dostęp ten może być realizowany w sposób, o którym mowa w ust. 4, udostępnienie tych danych jest realizowane bez konieczności składania wniosku.

4. Udostępnienie danych, o których mowa w ust. 1, następuje za pośrednictwem usług sieciowych, między systemem teleinformatycznym, z którego udostępniane są dane a systemem teleinformatycznym, przy użyciu którego świadczona jest usługa online.

5. Warunki udostępniania danych, o którym mowa w ust. 1, określa się w porozumieniu, z uwzględnieniem przepisów odrębnych regulujących funkcjonowanie rejestrów lub systemów teleinformatycznych, z których wnioskowane dane pochodzą.

6. Udostępnienie usług sieciowych, o których mowa w ust. 4, następuje w terminie określonym w porozumieniu, nie dłuższym jednak niż 12 miesięcy od zawarcia tego porozumienia.

7. Udostępniane dane, o których mowa w ust. 1, są wykorzystywane wyłącznie do realizacji usługi online świadczonej na rzecz osoby albo podmiotu, o których mowa w ust. 2, w celu:

1) uzupełnienia zakresu użytkowego dokumentu elektronicznego wymaganego w związku ze świadczoną usługą online;

2) potwierdzenia faktów lub stanu prawnego, wymaganego w związku ze świadczoną usługą online.”;

5) w art. 16a:

a) ust. 3–5 otrzymują brzmienie:

„3. Formularz elektroniczny udostępniony na ePUAP lub w innym w systemie teleinformatycznym, którego funkcjonowanie zapewnia minister właściwy do spraw informatyzacji, spełnia standardy dla formularzy elektronicznych określone i opublikowane przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na jego stronie podmiotowej.

4. W przypadku gdy formularz elektroniczny nie spełnia standardów, o których mowa w ust. 3, minister właściwy do spraw informatyzacji może wezwać organ do dostosowania, we wskazanym terminie, formularza elektronicznego do tych standardów.

5. W przypadku niedostosowania we wskazanym terminie formularza elektronicznego do standardów, o których mowa w ust. 3, minister właściwy do spraw informatyzacji może usunąć formularz elektroniczny z systemu, albo po zasięgnięciu opinii organu, który formularz elektroniczny udostępnił, dokonać jego modyfikacji.”,

b) dodaje się ust. 6–8 w brzmieniu:

„6. 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.

7. Jeżeli organ właściwy do określenia wzoru dokumentu nie określił wzoru dokumentu elektronicznego, 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, określić wzór dokumentu elektronicznego.

8. W przypadku określenia wzoru dokumentu elektronicznego przez ministra właściwego do spraw informatyzacji ust. 1 pkt 1–3 stosuje się odpowiednio.”;

6) w art. 16b ust. 1 otrzymuje brzmienie:

„1. 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.”;

7) art. 19c otrzymuje brzmienie:

„Art. 19c. 1. Minister właściwy do spraw informatyzacji może zawrzeć porozumienie w sprawie udostępniania usług na ePUAP lub korzystania z usług sieciowych pozwalających na wykorzystanie profilu zaufanego z:

1) podmiotami, o których mowa w art. 2 ust. 3, realizującymi zadania publiczne,
2) innymi podmiotami realizującymi zadania publiczne lub wspierającymi 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 r. poz. 1376 i 1475)

– jeżeli wykażą interes faktyczny w udostępnianiu usług na ePUAP lub w korzystaniu z usług sieciowych pozwalających na wykorzystanie profilu zaufanego; ocena interesu faktycznego dokonywana jest przy uwzględnieniu jego wpływu na bezpieczeństwo i interes publiczny.

2. W porozumieniu określa się sposób udostępniania usług na ePUAP oraz ich zakres lub warunki korzystania z usług sieciowych pozwalających na wykorzystanie profilu zaufanego.”;

8) po art. 19d dodaje się art. 19e–19j w brzmieniu:

„Art. 19e. 1. Minister właściwy do spraw informatyzacji udostępnia oraz zapewnia rozwój dedykowanego oprogramowania przeznaczonego dla urządzeń mobilnych, zwanego dalej „publiczną aplikacją mobilną”, pozwalającego w szczególności na:

1) pobranie, przechowywanie i prezentację dokumentów elektronicznych, o których mowa w ust. 2, a także przekazywanie tych dokumentów między urządzeniami mobilnymi;

2) weryfikację integralności i pochodzenia dokumentu elektronicznego.

2. Minister właściwy do spraw informatyzacji zapewnia działanie systemu teleinformatycznego, który pozwala, przy użyciu publicznej aplikacji mobilnej na pobranie dokumentu elektronicznego:

1) zawierającego dane osobowe użytkownika publicznej aplikacji mobilnej, pobrane z rejestrów publicznych w zakresie określonym w ust. 3 i 4;
2) zawierającego dane dotyczące sytuacji prawnej lub praw przysługujących użytkownikowi publicznej aplikacji mobilnej;
3) zawierającego dane umożliwiające identyfikację rzeczy związanej z użytkownikiem aplikacji mobilnej;
4) stanowiącego kopię dokumentu urzędowego, który wydawany jest w postaci innej niż postać elektroniczna.

3. Użytkownik publicznej aplikacji mobilnej, po uwierzytelnieniu w sposób określony w art. 20a ust. 1, może pobrać z:

1) Rejestru Dowodów Osobistych aktualne dane, o których mowa w art. 56 pkt 1, 2 i 4 lit. a–c ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2017 r. poz. 1464);
2) rejestru PESEL aktualne dane, o których mowa w art. 8 pkt 1–3, 4–6, 9–11, 14 i 22 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2017 r. poz. 657 i 2286 oraz z 2018 r. poz. 138, 696, 730 i 771).

4. Minister właściwy do spraw informatyzacji zapewnia stosowanie mechanizmów, które pozwalają na potwierdzenie integralności i pochodzenia danych dokumentu elektronicznego.

Art. 19f. 1. Użytkowanie publicznej aplikacji mobilnej:

1) jest bezpłatne i dobrowolne;
2) oznacza wyrażenie zgody na przetwarzanie przez ministra właściwego do spraw informatyzacji danych osobowych użytkownika aplikacji mobilnej w zakresie, o którym mowa w art. 19h.

2. Użytkowanie publicznej aplikacji mobilnej jest możliwe po uprzednim uwierzytelnieniu użytkownika w systemie teleinformatycznym, o którym mowa w art. 19e, w sposób, o którym mowa w art. 20a ust. 1, o ile przepisy szczególne lub porozumienie, o którym mowa w art. 19g, nie stanowią inaczej.

3. Użytkownik aplikacji mobilnej może w każdej chwili zrezygnować z korzystania z publicznej aplikacji mobilnej oraz wycofać zgodę na przetwarzanie danych osobowych.

Art. 19g. 1. Minister właściwy do spraw informatyzacji zawiera porozumienie w sprawie wykorzystywania publicznej aplikacji mobilnej i systemu teleinformatycznego, o których mowa w art. 19e, z podmiotem, o którym mowa w art. 2, na potrzeby zadań realizowanych przez ten podmiot.

2. Minister właściwy do spraw informatyzacji może zawrzeć porozumienie w sprawie wykorzystywania publicznej aplikacji mobilnej i systemu teleinformatycznego, o których mowa w art. 19e, z podmiotem, niebędącym podmiotem publicznym, na potrzeby zadań realizowanych przez ten podmiot.

3. Porozumienie określa warunki wykorzystywania publicznej aplikacji mobilnej oraz systemu teleinformatycznego, o których mowa w art. 19e, a w szczególności zawiera:

1) określenie dokumentu elektronicznego oraz zakres zawartych w nim danych;
2) cel i zakres wykorzystywania publicznej aplikacji mobilnej oraz systemu teleinformatycznego;
3) warunki organizacyjne i techniczne wykorzystania publicznej aplikacji mobilnej oraz systemu teleinformatycznego.

Art. 19h. Minister właściwy do spraw informatyzacji przetwarza w systemie teleinformatycznym, o którym mowa w art. 19e, dane osobowe użytkowników publicznej aplikacji mobilnej w zakresie niezbędnym do obsługi dokumentów elektronicznych, o których mowa w art. 19e, oraz zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.

Art. 19i. Minister właściwy do spraw informatyzacji w Biuletynie Informacji Publicznej na swojej stronie podmiotowej zamieszcza, oraz niezwłocznie aktualizuje, informacje o:

1) aktywnych i nieaktywnych, w tym czasowo zawieszonych, funkcjonalnościach publicznej aplikacji mobilnej;
2) stosowanych mechanizmach zapewniających możliwość potwierdzenia integralności i pochodzenia dokumentów elektronicznych oraz procedurach uzyskania takiego potwierdzenia;

3) adresach elektronicznych, pod którymi są udostępnione:

a) regulamin korzystania z publicznej aplikacji mobilnej,

b) informacja o wymaganiach technicznych dotyczących korzystania z publicznej aplikacji mobilnej.

Art. 19j. Minister właściwy do spraw informatyzacji w uzgodnieniu z ministrem właściwym do spraw wewnętrznych określi, w komunikacie ogłaszanym w Dzienniku Urzędowym „Monitor Polski”, termin uruchomienia rozwiązania, o którym mowa w art. 19e ust. 2 pkt 1, mając na względzie konieczność zapewnienia bezpieczeństwa tego rozwiązania.”;

9) w art. 20a:

a) ust. 1 otrzymuje brzmienie:

„1. Uwierzytelnienie użytkownika systemu teleinformatycznego podmiotu publicznego, w którym udostępniane są usługi online, wymaga użycia:

1) środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), lub

2) środka identyfikacji elektronicznej wydanego w notyfikowanym systemie identyfikacji elektronicznej, lub

3) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online.”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Uwierzytelnianie z wykorzystaniem środków identyfikacji elektronicznej, o których mowa w ust. 1 pkt 1 i 2, zapewnia się adekwatnie do wymaganego poziomu bezpieczeństwa, o którym mowa w art. 25 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.”,

c) ust. 2 otrzymuje brzmienie:

„2. Podmiot publiczny, który używa do realizacji zadań publicznych systemu teleinformatycznego, może umożliwiać użytkownikowi uwierzytelnienie w tym systemie także przez zastosowanie innych technologii.”,

d) w ust. 3 uchyla się pkt 2;

10) po art. 20a dodaje się art. 20aa–20ae w brzmieniu:

„Art. 20aa. Minister właściwy do spraw informatyzacji odpowiada za funkcjonowanie systemu teleinformatycznego, który:

1) zapewnia obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany jest profil zaufany;
2) umożliwia podmiotom publicznym:
   a) uwierzytelnienie osoby fizycznej przy użyciu środka identyfikacji elektronicznej, o którym mowa w pkt 1,
   b) zapewnienie osobie fizycznej możliwości opatrzenia dokumentu elektronicznego podpisem zaufanym.

Art. 20ab. Minister właściwy do spraw informatyzacji:

1) zarządza publicznym systemem identyfikacji elektronicznej;
2) zapisuje i zachowuje informacje związane z zapewnieniem rozliczalności i niezaprzeczalności działań użytkownika korzystającego ze środka identyfikacji elektronicznej wydanego w publicznym systemie identyfikacji elektronicznej.

Art. 20ac. 1. Minister właściwy do spraw informatyzacji jest administratorem danych przetwarzanych w systemie, o którym mowa w art. 20aa.

2. W systemie przetwarza się następujące dane:

1) osoby, której wydano środek identyfikacji elektronicznej, obejmujące:
   a) imię (imiona),
   b) nazwisko,
   c) numer PESEL,
   d) datę urodzenia osoby,
   e) adres poczty elektronicznej,
   f) numer telefonu komórkowego;
2) dane środka identyfikacji elektronicznej obejmujące:
   a) identyfikator,
   b) czas wydania,
   c) termin ważności;
3) dane, o których mowa w art. 20ab pkt 2.

3. Dane przetwarzane są w celu zapewnienia uwierzytelnienia osób fizycznych przy użyciu środków identyfikacji elektronicznej wydawanych w tym systemie oraz możliwości opatrzenia dokumentu elektronicznego podpisem zaufanym.

4. W systemie przetwarza się również dane osób uczestniczących w procesie potwierdzania profilu zaufanego, obejmujące:

1) imię (imiona);

2) nazwisko;

3) numer PESEL.

Art. 20ad. 1. Profil zaufany zawiera dane identyfikujące osobę fizyczną obejmujące:

1) imię (imiona);

2) nazwisko;

3) datę urodzenia;

4) numer PESEL.

2. W procedurze potwierdzania profilu zaufanego dane, o których mowa w ust. 1, są weryfikowane automatycznie z danymi zawartymi w rejestrze PESEL.

3. W przypadku zmiany w rejestrze PESEL danych, o których mowa w ust. 1 pkt 1–3, dokonywana jest automatyczna aktualizacja tych danych zawartych w profilu zaufanym.

4. Aktualizacja danych zawartych w profilu zaufanym, o której mowa w ust. 3, nie powoduje unieważnienia profilu zaufanego.

5. Profil zaufany może zawierać inne dane, niż wymienione w ust. 1, w szczególności identyfikator oraz dane wykorzystywane w procesach uwierzytelniania i autoryzacji realizowanych przy użyciu profilu zaufanego.

Art. 20ae. 1. Podpis zaufany wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności środka identyfikacji elektronicznej, o którym mowa w art. 20aa pkt 1.

2. Dane w postaci elektronicznej opatrzone podpisem zaufanym są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba że przepisy odrębne stanowią inaczej.

3. Nie można odmówić ważności i skuteczności podpisowi zaufanemu tylko na tej podstawie, że istnieje w postaci elektronicznej.”;

11) uchyla się art. 20b;

12) w art. 20c:

a) ust. 1 otrzymuje brzmienie:

„1. Potwierdzenia profilu zaufanego, które polega na weryfikacji zgodności danych zawartych we wniosku o jego wydanie ze stanem faktycznym oraz unieważnienia profilu zaufanego dokonuje:

1) punkt potwierdzający profil zaufany, na podstawie:

a) dowodu osobistego albo paszportu zawierającego:

– imię (imiona),

– nazwisko,

– numer PESEL, albo

b) innego dokumentu tożsamości, jeżeli umożliwia jednoznaczne potwierdzenie tożsamości osoby wnioskującej o potwierdzenie profilu zaufanego posiadającej numer PESEL;

2) samodzielnie osoba fizyczna przy wykorzystaniu kwalifikowanego podpisu elektronicznego, w przypadku gdy kwalifikowany certyfikat podpisu elektronicznego zawiera dane obejmujące co najmniej:

a) imię (imiona),

b) nazwisko,

c) numer PESEL;

3) samodzielnie osoba fizyczna przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy spełniającym warunki, o których mowa w art. 20a ust. 3 pkt 2, o ile środek ten potwierdza dane obejmujące co najmniej:

a) imię (imiona),

b) nazwisko,

c) numer PESEL.”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Przedłużenie ważności profilu zaufanego może nastąpić w sposób, o którym mowa w ust. 1 pkt 1 i 2, albo przy wykorzystaniu profilu zaufanego.”,

c) w ust. 3 w pkt 4 kropkę zastępuje się średnikiem i dodaje się pkt 5 w brzmieniu:

„5) spółdzielcza kasa oszczędnościowo-kredytowa, o której mowa w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, z późn. zm.[10)]).”,

d) ust. 8 otrzymuje brzmienie:

„8. Minister właściwy do spraw informatyzacji, na wniosek banku krajowego lub innego przedsiębiorcy, udziela zgody na nieodpłatne wykorzystywanie środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy do potwierdzania profilu zaufanego w sposób, o którym mowa w ust. 1 pkt 3, oraz do uwierzytelnień i autoryzacji związanych z jego wykorzystaniem, po spełnieniu przez bank krajowy lub innego przedsiębiorcę warunków, o których mowa w przepisach wydanych na podstawie art. 20d pkt 1.”;

13) po art. 20c dodaje się art. 20d–20g w brzmieniu:

„Art. 20d. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, warunki:

1) wydawania, przedłużania ważności, wykorzystywania i unieważniania profilu zaufanego, w tym:

a) okres ważności profilu zaufanego,

b) zbiór danych zawartych w profilu zaufanym, o których mowa w art. 20ad ust. 5,

c) przypadki, w których nie dokonuje się potwierdzenia profilu zaufanego,

d) przypadki, w których profil zaufany traci ważność,

e) warunki przechowywania oraz archiwizowania dokumentów i danych bezpośrednio związanych z potwierdzeniem profilu zaufanego,

f) dane i dokumenty wymagane w procedurze potwierdzania, przedłużania ważności i unieważnienia profilu zaufanego,

g) warunki, które powinien spełniać punkt potwierdzający profil zaufany,

h) warunki organizacyjne i techniczne dla potwierdzenia profilu zaufanego oraz uwierzytelnień i autoryzacji przy nieodpłatnym wykorzystaniu środka

---

[10)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2486 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650 i 723.

identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy,

i) sposób potwierdzania spełniania warunków, o których mowa w lit. h,

2) składania podpisu zaufanego

– biorąc pod uwagę konieczność zapewnienia bezpieczeństwa i pewności w procesie uwierzytelnienia i składania podpisu oraz poufności kluczowych elementarnych czynności.

Art. 20e. 1. Przyłączenie systemu teleinformatycznego, w którym udostępniane są usługi online do systemu, o którym mowa w art. 20aa, w celu wykorzystywania podpisu zaufanego, następuje na wniosek podmiotu odpowiedzialnego za ten system.

2. Do wniosku dołącza się oświadczenie o zapoznaniu się z polityką bezpieczeństwa udostępnioną przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na jego stronie podmiotowej.

3. Wniosek oraz oświadczenie, o których mowa w ust. 2, składa się w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym.

Art. 20f. Minister właściwy do spraw informatyzacji wydaje zgodę na przyłączenie systemu teleinformatycznego podmiotu publicznego, w którym udostępniane są usługi online, do systemu, o którym mowa w art. 20aa, po przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność tego systemu z systemem, o którym mowa w art. 20aa.

Art. 20g. Do systemu, o którym mowa w art. 20aa, przyłącza się elektroniczną platformę usług administracji publicznej.”.

Art. 26. W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2017 r. poz. 1993 i 2405 oraz z 2018 r. poz. 138, 650 i 730) w art. 24:

1) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Przy wykonywaniu czynności operacyjno-rozpoznawczych funkcjonariusze CBA mogą posługiwać się środkami identyfikacji elektronicznej zawierającymi dane inne niż dane identyfikujące funkcjonariusza CBA.”;

2) ust. 3 otrzymuje brzmienie:

„3. Osoby udzielające CBA pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych mogą posługiwać się dokumentami, o których mowa w ust. 2, oraz odpowiednio środkami identyfikacji elektronicznej, o których mowa w ust. 2a.”;

3) w ust. 4:

a) pkt 4 otrzymuje brzmienie:

„4) funkcjonariusz CBA lub osoba wymieniona w ust. 3, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, o których mowa w ust. 2, lub środkami identyfikacji elektronicznej, o których mowa w ust. 2a;”,

b) dodaje się pkt 5 w brzmieniu:

„5) kto wydaje środki identyfikacji elektronicznej, o których mowa w ust. 2a, funkcjonariuszowi CBA albo osobom, o których mowa w ust. 3, lub dopuszcza do uwierzytelnienia z wykorzystaniem takiego środka identyfikacji elektronicznej w swoim systemie identyfikacji elektronicznej.”.

Art. 27. W ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2017 r. poz. 1978 i 2405 oraz z 2018 r. poz. 650) w art. 39:

1) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Przy wykonywaniu czynności operacyjno-rozpoznawczych funkcjonariusze SKW i SWW mogą posługiwać się środkami identyfikacji elektronicznej zawierającymi dane inne niż dane identyfikujące odpowiednio funkcjonariusza SKW albo SWW.”;

2) ust. 3 otrzymuje brzmienie:

„3. Osoby udzielające SKW i SWW pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych mogą posługiwać się dokumentami, o których mowa w ust. 2, oraz odpowiednio środkami identyfikacji elektronicznej, o których mowa w ust. 2a.”;

3) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. SWW prowadzi centralny rejestr środków identyfikacji elektronicznej, o których mowa w ust. 2a.”;

4) w ust. 6:

a) pkt 4 otrzymuje brzmienie:

„4) funkcjonariusz SKW, SWW, żołnierz zawodowy wyznaczony na stanowisko służbowe w SKW albo SWW lub osoba wymieniona w ust. 3, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, o których mowa w ust. 2 i 3, lub środkami identyfikacji elektronicznej, o których mowa w ust. 2a;”,

b) dodaje się pkt 5 w brzmieniu:

„5) kto wydaje środki identyfikacji elektronicznej, o których mowa w ust. 2a, funkcjonariuszowi SKW, SWW albo osobom, o których mowa w ust. 3, lub dopuszcza do uwierzytelnienia z wykorzystaniem takiego środka identyfikacji elektronicznej w swoim systemie identyfikacji elektronicznej.”.

Art. 28. W ustawie z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2017 r. poz. 2195 oraz z 2018 r. poz. 650) w art. 10b w ust. 5 w pkt 1 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 29. W ustawie z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2018 r. poz. 554 i 650) w art. 15:

1) ust. 3b otrzymuje brzmienie:

„3b. Wniosek i załączniki do wniosku określone w ust. 4 w postaci elektronicznej mogą być składane za pomocą:

1) systemu, o którym mowa w ust. 11, po zastosowaniu zapewnionych w systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych;

2) systemu teleinformatycznego wskazanego w informacji zamieszczonej na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw rodziny po uzgodnieniu z ministrem właściwym do spraw informatyzacji, po opatrzeniu ich kwalifikowanym podpisem elektronicznym albo podpisem zaufanym.”;

2) w ust. 11 zdanie drugie otrzymuje brzmienie:

„Uwierzytelnianie użytkowników w systemie teleinformatycznym wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, albo innych technologii jeżeli zostaną udostępnione w tym systemie.”.

Art. 30. W ustawie dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, 2486 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650 i 723) w art. 3 dodaje się ust. 4 w brzmieniu:

„4. Kasy mogą świadczyć na rzecz swoich członków usługi zaufania oraz wydawać swoim członkom środki identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania oraz identyfikacji elektronicznej.”.

Art. 31. W ustawie z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2017 r. poz. 657 i 2286 oraz z 2018 r. poz. 138, 696 i 730) wprowadza się następujące zmiany:

1) w art. 32 w ust. 5 w zdaniu drugim wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”;
2) w art. 46 w ust. 2 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) podmiotom odpowiedzialnym za system identyfikacji elektronicznej oraz podmiotom wydającym środki identyfikacji elektronicznej w systemie identyfikacji elektronicznej zgodnie z ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), w celu wydania środka identyfikacji elektronicznej.”;

3) w art. 49 po ust. 2a dodaje się ust. 2b w brzmieniu:

„2b. Podmiotom, o których mowa w art. 46 ust. 2 pkt 4, udostępnia się, w sposób i na warunkach określonych w ust. 1, dane dotyczące numeru PESEL, daty urodzenia, miejsca urodzenia, płci, imienia (imion), nazwiska, nazwiska rodowego.”;

4) w art. 53 pkt 1 i 2 otrzymują brzmienie:

„1) dla podmiotów, o których mowa w art. 46 ust. 1, art. 46 ust. 2 pkt 4 oraz ministra właściwego do spraw wewnętrznych – nieodpłatnie;

2) dla podmiotów, o których mowa w art. 46 ust. 2 pkt 1–3 – odpłatnie.”.

Art. 32. W ustawie z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2017 r. poz. 978 i 2418 oraz z 2018 r. poz. 138, 650 i 728) w art. 27 w ust. 6 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 33. W ustawie z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3 (Dz. U. z 2018 r. poz. 603 i 650) wprowadza się następujące zmiany:

1) w art. 35b ust. 3 otrzymuje brzmienie:

„3. Wniosek jest składany za pomocą systemu teleinformatycznego, o którym mowa w ust. 62a, po zastosowaniu zapewnionych w tym systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej. Uwierzytelnianie użytkowników w tym systemie wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, albo innych technologii, jeżeli zostaną udostępnione w tym systemie.”;

2) w art. 46b ust. 4 otrzymuje brzmienie:

„4. Wniosek jest składany za pomocą systemu teleinformatycznego, o którym mowa w ust. 62a, po zastosowaniu zapewnionych w tym systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej. Uwierzytelnianie użytkowników w tym systemie wymaga użycia profilu zaufanego, środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, albo innych technologii, jeżeli zostaną udostępnione w tym systemie.”.

Art. 34. W ustawie z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2017 r. poz. 2159 i 2203) w art. 71 w ust. 3 wyrazy „podpisu potwierdzonego profilem zaufanym ePUAP” zastępuje się wyrazami „podpisu zaufanego”.

Art. 35. W ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2017 r. poz. 1845 oraz z 2018 r. poz. 697) wprowadza się następujące zmiany:

1) w art. 2 w ust. 1 w pkt 6 wprowadzenie do wyliczenia otrzymuje brzmienie:
„elektroniczna dokumentacja medyczna − dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych:”;

2) w art. 8 ust. 2 otrzymuje brzmienie:
„2. Do rejestrów medycznych i systemów teleinformatycznych używanych do prowadzenia rejestrów medycznych stosuje się odpowiednio przepisy art. 14 ust. 1 i art. 15–16 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i przepisy wydane na ich podstawie oraz przepisy wydane na podstawie art. 18 tej ustawy.”;

3) w art. 17 w ust. 3 wprowadzenie do wyliczenia otrzymuje brzmienie:
„Pracownik medyczny używa kwalifikowanego podpisu elektronicznego, podpisu zaufanego albo wykorzystuje sposób potwierdzania pochodzenia oraz integralności danych dostępny w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych do podpisywania:”.

Art. 36. W ustawie z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2017 r. poz. 1844 oraz z 2018 r. poz. 650 i 697) w art. 19 w ust. 3, w art. 24 w ust. 6a, w art. 32a w ust. 8, w art. 38 w ust. 5 w pkt 3 w lit. e w tiret pierwszym, w ust. 5a w pkt 9 w lit. a oraz w ust. 6 w pkt 7 w lit. a, użyte w różnym przypadku wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisem zaufanym”.

Art. 37. W ustawie z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2018 r. poz. 123 i 650) w art. 67 w ust. 4d w pkt 1, w art. 76 w ust. 1b w pkt 1 i w art. 80 w ust. 8 w pkt 1 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 38. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2018 r. poz. 21, z 2017 r. poz. 2422 oraz z 2018 r. poz. 650) w art. 65 w ust. 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 39. W ustawie z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. poz. 183, z 2015 r. poz. 1311, z 2016 r. poz. 1579 oraz z 2018 r. poz. 696) w art. 4 w pkt 3 w art. 37 w § 1a, w pkt 4 w art. 37a, w pkt 5 w art. 46 w § 2a, w pkt 7 w art. 48 w § 3a w zdaniu pierwszym i w pkt 12 w art. 74a w § 3 w pkt 2, użyte w różnym przypadku wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiednim przypadku wyrazami „podpisem zaufanym”.

Art. 40. W ustawie z dnia 14 marca 2014 r. o zasadach prowadzenia zbiórek publicznych (Dz. U. z 2017 r. poz. 1223) w art. 9 w ust. 2, w art. 11 w ust. 2 i w art. 18 w ust. 3, użyte w różnej liczbie wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się użytymi w odpowiedniej liczbie wyrazami „podpisem zaufanym”.

Art. 41. W ustawie z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014–2020 (Dz. U. z 2017 r. poz. 1460, 1475 i 2433) art. 70 otrzymuje brzmienie:

„Art. 70. 1. Uwierzytelnianie 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 centralnym systemie teleinformatycznym, wymaga wykorzystania profilu zaufanego, innego środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, albo danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online.

2. W przypadku gdy z powodów technicznych wykorzystanie profilu zaufanego nie jest możliwe, uwierzytelnianie w centralnym systemie teleinformatycznym podmiotu,

o którym mowa w ust. 1, następuje przez wykorzystanie loginu i hasła wygenerowanego przez ten system.”.

Art. 42. W ustawie z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2017 r. poz. 1832 i 2161) w art. 10:

1) ust. 9a otrzymuje brzmienie:

„9a. Wniosek i dokumenty, o których mowa w ust. 4 i 5, mogą być składane drogą elektroniczną wyłącznie za pomocą systemu teleinformatycznego utworzonego przez ministra właściwego do spraw rodziny. Uwierzytelnianie użytkowników w tym systemie wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online, albo innych technologii, jeżeli zostaną udostępnione w tym systemie.”;

2) ust. 10 otrzymuje brzmienie:

„10. Wniosek o przyznanie Karty Dużej Rodziny lub wydanie duplikatu Karty Dużej Rodziny składany jest z wykorzystaniem systemu, o którym mowa w ust. 9a, po zastosowaniu zapewnionych w tym systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej.”.

Art. 43. W ustawie z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz. U. z 2017 r. poz. 1148, 1213 i 1593 oraz z 2018 r. poz. 9 i 650) w art. 79 w ust. 4, w art. 138 w ust. 5 i w art. 147 w ust. 5 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 44. W ustawie z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2017 r. poz. 1508 oraz z 2018 r. poz. 149 i 398) w art. 203 w ust. 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 45. W ustawie z dnia 15 maja 2015 r. o substancjach zubożających warstwę ozonową oraz o niektórych fluorowanych gazach cieplarnianych (Dz. U. z 2017 r. poz. 1951 oraz z 2018 r. poz. 650) w art. 6 w ust. 2 we wprowadzeniu do wyliczenia, w art. 8 w ust. 5

w zdaniu drugim, w art. 9 w ust. 4 i 6, w art. 25 w ust. 4 w zdaniu drugim i w ust. 6 w zdaniu drugim, w art. 27 w ust. 2 w zdaniu drugim i w ust. 4 w zdaniu drugim, w art. 37 w ust. 7 w zdaniu drugim i w ust. 9 w zdaniu drugim oraz w art. 41 w ust. 5 w zdaniu drugim wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 46. W ustawie z dnia 15 maja 2015 r. o zmianie ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa oraz niektórych innych ustaw (Dz. U. poz. 1066, 1735, z 2016 r. poz. 960 oraz z 2017 r. poz. 992) wprowadza się następujące zmiany:

1) w art. 23 w ust. 1 wyrazy „30 czerwca 2018 r.” zastępuje się wyrazami „30 listopada 2018 r.”;
2) w art. 26 pkt 3 otrzymuje brzmienie:

„3) art. 6 pkt 2, który wchodzi w życie z dniem 1 grudnia 2018 r.”.

Art. 47. W ustawie z dnia 25 czerwca 2015 r. – Prawo konsularne (Dz. U. z 2017 r. poz. 1545 i 2361 oraz z 2018 r. poz. 398) w art. 75 w ust. 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 48. W ustawie z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. z 2017 r. poz. 1851 oraz z 2018 r. poz. 107, 138 i 650) w art. 13:

1) w ust. 5 pkt 1 otrzymuje brzmienie:

„1) utworzonego przez ministra właściwego do spraw rodziny; uwierzytelnianie użytkowników w systemie wymaga użycia profilu zaufanego, innego środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 i …), adekwatnie do poziomu bezpieczeństwa środka identyfikacji elektronicznej wymaganego dla usług świadczonych w tym systemie, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online albo innych technologii, jeżeli zostaną udostępnione w tym systemie;”;

2) ust. 7 otrzymuje brzmienie:

„7. Wniosek i załączniki do wniosku określone w ust. 4 składane są w postaci elektronicznej za pomocą:

1) systemu teleinformatycznego, o którym mowa w ust. 5 pkt 1, po zastosowaniu zapewnionych w tym systemie sposobów potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej;

2) systemów teleinformatycznych, o których mowa w ust. 5 pkt 2 i 4, opatruje się kwalifikowanym podpisem elektronicznym albo podpisem zaufanym lub uwierzytelnia w sposób zapewniający możliwość potwierdzenia pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej.”;

3) w ust. 11 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 49. W ustawie z dnia 15 grudnia 2016 r. o Prokuratorii Generalnej Rzeczypospolitej Polskiej (Dz. U. poz. 2261 oraz z 2018 r. poz. 723) w art. 36 w ust. 2 wyrazy „podpisu potwierdzonego profilem zaufanym ePUAP” zastępuje się wyrazami „podpisu zaufanego”.

Art. 50. W ustawie z dnia 24 lutego 2017 r. o uzyskiwaniu tytułu specjalisty w dziedzinach mających zastosowanie w ochronie zdrowia (Dz. U. poz. 599) w art. 6 w ust. 4, w art. 9 w ust. 3 w pkt 1 i w art. 61 w ust. 3 w pkt 1 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 51. W ustawie z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz. U. poz. 2217) w art. 10 w ust. 1 w pkt 2 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 52. W ustawie z dnia 24 listopada 2017 r. o zmianie ustawy o odpadach oraz niektórych innych ustaw (Dz. U. poz. 2422) w art. 1 w pkt 9 w lit. e w ust. 5 wyrazy „podpisu potwierdzonego profilem zaufanym ePUAP” zastępuje się wyrazami „podpisu zaufanego”.

Art. 53. W ustawie z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy (Dz. U. poz. 647) w art. 8 w ust. 4 i w ust. 8 w zdaniu drugim, w art. 10 w ust. 7 i w art. 52 w ust. 4 wyrazy „podpisem potwierdzonym profilem zaufanym ePUAP” zastępuje się wyrazami „podpisem zaufanym”.

Art. 54. 1. Elektroniczna platforma usług administracji publicznej zapewnia możliwość uwierzytelnienia użytkowników z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej z dniem wejścia w życie ustawy.

2. Systemy teleinformatyczne, o których mowa:

1) w art. 23 ust. 3a ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych,
2) w art. 4 ust. 1 pkt 8 ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy,
3) w art. 15 ust. 11 ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów,
4) w art. 62a ustawy z dnia 4 lutego 2011 r. o opiece nad dziećmi do lat 3,
5) w art. 9a ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny,
6) w art. 13 ust. 5 pkt 1 ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci,
7) w art. 2 oraz art. 51 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy

– zapewnią możliwość uwierzytelnienia użytkowników z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej nie później niż w terminie 3 miesięcy od dnia wejścia w życie ustawy.

3. System teleinformatyczny, w którym na dzień 31 grudnia 2017 r. uwierzytelnienie użytkowników odbywało się z wykorzystaniem profilu zaufanego ePUAP, zapewnia możliwość uwierzytelnienia z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej, najpóźniej od dnia 1 stycznia 2020 r.

4. System teleinformatyczny podmiotu publicznego, inny niż systemy wymienione w ust. 1–3, w którym udostępniane są usługi online, funkcjonujący w dniu wejścia w życie ustawy lub uruchomiony przed dniem 1 stycznia 2021 r., zapewnia możliwość uwierzytelnienia użytkowników z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej, najpóźniej od dnia 1 stycznia 2022 r.

5. System teleinformatyczny podmiotu publicznego, w którym udostępniane są usługi online, uruchomiony po dniu 31 grudnia 2020 r., zapewnia możliwość uwierzytelnienia

użytkowników z wykorzystaniem środków identyfikacji elektronicznej wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej, z dniem jego uruchomienia.

Art. 55. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 19a ust. 3, art. 20a ust. 3 pkt 1 i 2 ustawy zmienianej w art. 25, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych odpowiednio na podstawie art. 19a ust. 3, art. 20a ust. 3 pkt 1 i art. 20d ust. 1 ustawy zmienianej w art. 25, w brzmieniu nadanym niniejszą ustawą, jednak nie dłużej niż 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 56. Profil zaufany ePUAP potwierdzony przed dniem wejścia w życie niniejszej ustawy, zgodnie z przepisami ustawy zmienianej w art. 25, w brzmieniu dotychczasowym, staje się profilem zaufanym w rozumieniu art. 3 pkt 14 ustawy zmienianej w art. 25, w brzmieniu nadanym niniejszą ustawą.

Art. 57. Podpis potwierdzony profilem zaufanym ePUAP w rozumieniu art. 3 pkt 15 ustawy zmienianej w art. 25, w brzmieniu dotychczasowym, uznaje się za podpis zaufany w rozumieniu art. 3 pkt 14a ustawy zmienianej w art. 25, w brzmieniu nadanym niniejszą ustawą.

Art. 58. Zgody udzielone przez ministra właściwego do spraw informatyzacji na podstawie art. 20c ust. 3 i 8 ustawy zmienianej w art. 25 pozostają w mocy.

Art. 59. 1. Od dnia 1 marca 2019 r. minister właściwy do spraw wewnętrznych w ramach kompetencji wynikających z ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2017 r. poz. 1464 oraz z 2018 r. poz. 730) wydaje środek identyfikacji elektronicznej w publicznym systemie identyfikacji elektronicznej przyłączonym do węzła krajowego.

2. Dokonanie zakupu w 2018 r. urządzeń służących do obsługi środka identyfikacji elektronicznej wydawanego przez ministra właściwego do spraw wewnętrznych w publicznym systemie identyfikacji elektronicznej przyłączonym do węzła krajowego jest zadaniem zleconym gminy z zakresu administracji rządowej.

3. Środki na zakup przez gminy urządzeń, o których mowa w ust. 2, w 2018 r. pochodzą z rezerwy celowej budżetu państwa. Podziału rezerwy celowej na realizację zadań dokonuje minister właściwy do spraw finansów publicznych w porozumieniu z ministrem właściwym do spraw wewnętrznych.

4. Minister właściwy do spraw wewnętrznych, najpóźniej do dnia 30 września 2018 r., określi i udostępni na swojej stronie podmiotowej w Biuletynie Informacji Publicznej wymagania techniczne dla urządzeń, o których mowa w ust. 2.

5. Organy gmin dokonają zakupu urządzeń, o których mowa w ust. 2, zgodnie z wymaganiami technicznymi określonymi przez ministra właściwego do spraw wewnętrznych.

Art. 60. Publiczny system identyfikacji, o którym mowa w art. 20aa ustawy zmienianej w art. 25, w brzmieniu nadanym niniejszą ustawą, notyfikuje Komisji Europejskiej minister właściwy do spraw informatyzacji.

Art. 61. 1. W latach 2018–2027 maksymalny limit wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy w poszczególnych latach wynosi:

1) 2018 r. – 0 mln zł;
2) 2019 r. – 18,227 mln zł;
3) 2020 r. – 18,443 mln zł;
4) 2021 r. – 16,573 mln zł;
5) 2022 r. – 17,034 mln zł;
6) 2023 r. – 17,854 mln zł;
7) 2024 r. – 17,794 mln zł;
8) 2025 r. – 17,794 mln zł;
9) 2026 r. – 17,794 mln zł;
10) 2027 r. – 17,794 mln zł.

2. Minister właściwy do spraw informatyzacji nadzoruje wykorzystanie limitu wydatków, o których mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku IV kwartału – według stanu na dzień 20 listopada danego roku oraz wdraża mechanizm korygujący, o którym mowa w ust. 3.

3. W przypadku gdy wielkość wydatków, o których mowa w ust. 1, po trzech kwartałach wyniesie łącznie więcej niż 75% limitu przewidzianego na ten rok, wielkość wydatków w czwartym kwartale obniża się o kwotę przekroczenia, określając zakres ograniczeń dla poszczególnych zadań realizowanych na podstawie ustawy.

Art. 62. Ustawa wchodzi w życie po upływie 1 miesiąca od dnia ogłoszenia, z wyjątkiem:

1) art. 1 pkt 4–7 oraz art. 25 w zakresie art. 20a ust. 1 pkt 2, które wchodzą w życie z dniem 29 września 2018 r.;
2) art. 7, art. 13 oraz art. 41, które wchodzą w życie z dniem 1 stycznia 2020 r.;
3) art. 10, art. 21, art. 23, art. 29, art. 33, art. 42 oraz art. 48, które wchodzą w życie po upływie 4 miesięcy od dnia ogłoszenia;
4) art. 46 i art. 59, które wchodzą w życie z dniem następującym po dniu ogłoszenia.

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)] 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

1) link: https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services/at_download/fullReport

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.

Nazwa projektu Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Marek Zagórski, Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Magdalena Witkowska-Krzymowska, Zastępca Dyrektora Departamentu Prawnego, (22) 245 59 15, sekretariat.dp@mc.gov.pl)	**Data sporządzenia:** 16.04.2017 r. **Źródło:** Uchwała Rady Ministrów w sprawie Programu Zintegrowanej Informatyzacji Państwa **Nr w wykazie prac:** UD 244

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Poziom popularyzacji i dostępności usług cyfrowych w Polsce jest nadal niezadowalający. Jednym z powodów tego stanu rzeczy są ograniczenia w zakresie wykorzystywania środków identyfikacji elektronicznej do uwierzytelnienia w systemach publicznych udostępniających e-usługi publiczne.

Gwałtowny rozwój usług online spowodował, że ich dostawcy potrzebują unikatowej identyfikacji elektronicznej w ramach swoich systemów, celem zapewnienia użytkownikom możliwości bezpiecznego korzystania ze świadczonych przez siebie usług.

Obecnie w Polsce nie istnieje narzędzie umożliwiające w sposób ujednolicony, transparentny i bezpieczny dostęp i możliwość łączenia się z jednej strony dostawcy systemu identyfikacji elektronicznej (ang. *Identity Providers*) z systemami udostępniającymi usługi (ang. *Service Providers*). Systemy informatyczne administracji publicznej do identyfikacji elektronicznej swoich użytkowników wykorzystują albo mechanizmy zbudowane wewnątrz administracji, tj. w ramach swoich systemów, albo mechanizm profilu zaufanego ePUAP. Mała liczba użytkowników (ok. 1,5 mln) posiadających profil zaufany ePUAP skutkuje niskim poziomem jego wykorzystania. Powoduje to konieczność dalszego finansowania wewnętrznych systemów identyfikujących użytkowników u każdego usługodawcy. Ponadto, aby system mógł wykorzystywać dostępne mechanizmy identyfikacji, musi zostać każdorazowo integrowany z dostępnymi dostawcami środków identyfikacji elektronicznej oddzielnie.

Świadczenie wygodnych usług online wymaga udostępnienia i przydzielenia użytkownikom odpowiednich uprawnień, co wiąże się z koniecznością założenia konta w systemie świadczącym określone usługi.

W zależności od tego, czego dotyczy usługa online, identyfikacja elektroniczna zabezpiecza przed jej nieuprawnionym przejęciem lub stworzeniem fałszywej tożsamości i co za tym idzie potencjalnego narażenia stron (strony korzystającej z usługi i strony świadczącej usługę) na szkody z tym związane. Z tego powodu banki stosują zabezpieczenia adekwatne dla świadczonych przez siebie usług bankowych, podmioty świadczące usługi telekomunikacyjne zabezpieczenia właściwe dla takich usług, administracja publiczna różne zabezpieczenia właściwe dla świadczonych przez siebie różnych rodzajów usług itd. Inny bowiem powinien być poziom bezpieczeństwa środka identyfikacji elektronicznej dla usług 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.

Powoduje to, że osoba korzystająca z e-usług świadczonych przez różne podmioty zmuszana jest do nauczenia się i zapamiętywania różnych sposobów identyfikowania się w różnych systemach zarządzanych przez różnych dostawców usług. Istnienie wielu systemów identyfikacji elektronicznej staje się dla niego problemem. Efektem tego jest naturalne dążenie użytkowników do posługiwania się podobnym lub identycznym zestawem danych identyfikujących w ramach różnych usług. Obecnie wiele systemów i portali usługowych świadczących usługi online dla obywateli posiada odrębne konta, co zmusza obywatela do założenia indywidualnego, dedykowanego konta do konkretnego systemu, portalu czy serwisu. W konsekwencji obywatel posiada szereg kont i loginów, nie mogąc ich zapamiętać, gdyż systemy świadczące usługi online nie posiadają jednej spójnej polityki bezpieczeństwa np. w zakresie polityki haseł (np. długości hasła, ilości specyficznych znaków np. alfanumerycznych użycia małych lub wielkich liter).

Użytkownicy oczekują takich usług identyfikacji, które będą budowały zaufanie do środowiska online i zarazem nie będą powodowały uciążliwości stosowania różnych środków do różnych usług. Podobnie podmioty świadczące usługi online, gdyby mogły polegać na powszechnym systemie identyfikacji elektronicznej i uwierzytelniania, nie musiałyby same zarządzać takim systemem.

Problemem utrudniającym świadczenie przez podmioty publiczne usług elektronicznych o wyższym poziomie dojrzałości niż obecnie jest często brak możliwości pozyskania danych potrzebnych do realizacji usługi, które mogłyby być pozyskane z rejestru publicznego. Powoduje to, że sposób i zakres udostępnionych usług często nie jest wystarczający z perspektywy oczekiwań obywateli.

Obecne regulacje nie dają także Ministrowi Cyfryzacji, który jest organem administracji rządowej właściwym w sprawach dotyczących świadczenia usług elektronicznych, możliwości odpowiedniego reagowania w przypadkach, gdy e-usługi udostępnione przez inne podmioty publiczne wymagają poprawy ich funkcjonalności, podczas gdy minister

właściwy do spraw informatyzacji, dostarczając rozwiązań centralnych w zakresie świadczenia usług publicznych, ponoszący jednocześnie odpowiedzialność za społeczne postrzeganie usług cyfrowych musi posiadać narzędzia i możliwości służące podnoszeniu poziomu dojrzałości usług cyfrowych.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projekt ustawy ma na celu wdrożenie sprawnie funkcjonującej elektronicznej identyfikacji w Polsce, opartej o powszechnie dostępne, przejrzyste i bezpieczne rozwiązania organizacyjno-techniczne. Planuje się zapewnienie możliwości użycia w publicznych usługach online środków identyfikacji elektronicznej wydawanych przez różne podmioty, w tym także już istniejących środków identyfikacji elektronicznej, sprawdzonych w praktyce w usługach online świadczonych przez podmioty prywatne (np. banki, telekomy). Takie podejście może spowodować szybkie pokonanie bariery braku powszechnego dostępu do środków identyfikacji elektronicznej, jak również umożliwi obywatelom korzystanie z tych samych, przyjaznych dla nich sposobów uwierzytelniania w usługach online.

Projektowana ustawa reguluje funkcjonowanie krajowego schematu identyfikacji elektronicznej. Centralnym elementem przyjętego modelu będzie Krajowy Węzeł Identyfikacji Elektronicznej, który stanowi rozwiązanie techniczno-organizacyjne. Projektowana ustawa wprowadza federacyjny (rozproszony) model identyfikacji elektronicznej istniejący w oparciu o wiele środków identyfikacji elektronicznej wydawanych przez różne podmioty. Zgodnie z przyjętym modelem docelowym w skład publicznego schematu identyfikacji elektronicznej wchodzą również komercyjni dostawcy środków identyfikacji elektronicznej. Węzeł będzie pełnił główną rolę zarządczą w sfederowanym modelu tożsamości w Polsce, w szczególności skupiające systemy identyfikacji elektronicznej, a także będąc pośrednikiem między węzłem transgranicznym i dostawcami usług.

Węzeł adresuje w szczególności poniższe funkcjonalności, dzięki czemu możliwe jest uzyskanie szerokiej interoperacyjności i możliwości modułowego rozszerzania uczestników systemu, bez konieczności przebudowywania istniejących rozwiązań. Węzeł powinien umożliwiać wybór dostawcy środka identyfikacji elektronicznej, przekierowanie do zagranicznych i notyfikowanych dostawców środków identyfikacji elektronicznej, potwierdzenie uwierzytelnienia u dostawcy środka identyfikacji elektronicznej, zarządzanie podłączeniami do Węzła.

Efektem zmian wprowadzanych w drodze ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne ma być 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.

Jednocześnie wskazanym jest wprowadzenie uregulowań prawnych umożliwiających podmiotom świadczącym usługi na rzecz osób fizycznych lub podmiotów, których dane zgromadzone są w z rejestrach bezpośrednio dotyczą, pozyskanie tych danych jako niezbędnych do wykonania usługi.

Podsumowując, projekt wychodzi naprzeciw potrzebom osób korzystających z usługi online, jak i świadczących takie usługi, stwarzając podstawy niezbędne dla budowania zaufania do całego środowiska online, co zostało wskazane jako kluczowe dla rozwoju gospodarczego i społecznego w preambule 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). Zaplanowane zmiany przyczynią się do usprawnienia procesu załatwiania spraw administracyjnych poprzez udoskonalenie wykorzystania stworzonych w tym celu mechanizmów.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Austriacki schemat eID jest systemem scentralizowanym i zamkniętym. Prywatne podmioty nie mogą wydawać tożsamości, a jedynie nośniki tożsamości. Państwo zapewnia kompletną infrastrukturę i ponosi ciężar inwestycji i utrzymania, ale za to usługi są darmowe (przy czym, obok usług identyfikacji i uwierzytelnienia, państwo dostarcza także usługę podpisu elektronicznego). Infrastrukturę, jej techniczną realizację, jak i sposób integracji z systemem dostawców usług, można uznać za skomplikowane i pozostające nieco w tyle za trendami światowymi w tym zakresie. Sposób realizacji wynika jednak ze specyficznych (restrykcyjnych) wymagań prawnych w zakresie identyfikacji obywateli (w tym kwestia ochrony prywatności). Pomimo wydania eID praktycznie każdemu obywatelowi, stopień wykorzystania jest niewysoki (8,5 mln obywateli generuje tylko 650 tys. transakcji rocznie). Stopień aktywacji funkcji eID na kartach jest dość niski, natomiast względny sukces zaczął się dopiero po wprowadzeniu rozwiązania na urządzenia mobilne.

Szwecja jest przykładem rynkowego podejścia do zagadnienia e-identyfikacji obywateli. Państwo wykorzystało w pełni potencjał firm prywatnych. Stworzony model federacyjny umożliwia włączanie się do systemu dowolnych graczy, po spełnieniu określonych wymagań. Szwecja należy do krajów z najlepiej rozwiniętym sektorem e-government, a stopień wykorzystania eID jest wysoki (9,5 mln obywateli generuje ponad 300 mln transakcji rocznie). Technicznie system jest stosunkowo prosty. Usługi identyfikacji na potrzeby e-usług publicznych państwo kupuje od firm prywatnych po cenach rynkowych.

Najważniejsze wnioski, w kontekście uruchomienia polskiego schematu eID, są następujące:

- model szwedzki osiągnął znacznie lepsze rezultaty niż austriacki – pomimo większego nasycenia eID w Austrii, to w Szwecji jest on znacznie częściej używany,
- rozwój rynku eID, a co za tym idzie usług realizowanych drogą elektroniczną, w tym e-gov, jest łatwiej osiągalny

przy modelu federacyjnym, otwartym (jak w Szwecji), gdyż firmy prywatne działają bez uzależnienia od instytucji państwowych w zakresie tworzenia i integracji rozwiązań; w Austrii rozwój jest ograniczony rozwojem centralnej infrastruktury, co z założenia posiada znacznie większą bezwładność,

– infrastruktura techniczna w Austrii jest uznawana za skomplikowaną i ograniczającą rozwój e-usług.

Ze względu na powyższe, a także zbieżne ze szwedzkim rozwiązania stosowane w Polsce w zakresie funkcjonowania prywatnych centrów certyfikacyjnych wydających certyfikaty (kwalifikowane) uznawane w usługach publicznych, przyjęto do realizacji model federacyjny.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Obywatele	32,7 mln	GUS	Będą korzystać z identyfikacji i uwierzytelnienia oraz e-usług.
Dostawcy środków identyfikacji elektronicznej (banki, telekomy, operatorzy pocztowi)	15	Internet	Zapewniają środki identyfikacji elektronicznej.
KPRM i Ministerstwa	21	kprm.gov.pl	Podmioty administracji centralnej są właścicielami biznesowymi udostępnianych usług.
Wojewodowie	16	analiza własna	Podmioty administracji centralnej są właścicielami biznesowymi udostępnianych usług.
Urzędy centralne	58	analiza własna	Podmioty administracji centralnej są właścicielami biznesowymi udostępnianych usług.
Jednostki Samorządu Terytorialnego	2808 (16 województw, 314 powiatów i 2478 gmin (w tym 66 miast na prawach powiatu)	Ministerstwo Spraw Wewnętrznych i Administracji - baza teleadresowa gmin	Usługi udostępniane w kanale cyfrowym realizowane są w dużej mierze przez JST.
Podmioty, którym udostępniane są dane z rejestru PESEL za pomocą urządzeń teletransmisji danych	97	Wykaz użytkowników rejestru PESEL	Przyspieszenie procesu uzyskania poprawnych danych z rejestru PESEL.
Przedsiębiorcy			Będą korzystać z e-usług.
SKOK-i			Będą świadczyć usługi.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projektowana ustawa została zamieszczona w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny", oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach konsultacji publicznych i opiniowania projekt został skierowany na 21 dni do następujących podmiotów:

1. Zakładu Ubezpieczeń Społecznych (ZUS),
2. Generalnego Inspektora Ochrony Danych Osobowych (GIODO),
3. Polskiego Komitetu Normalizacyjnego (PKN),
4. Polskiego Towarzystwa Informatycznego (PTI),
5. Polskiej Izby Informatyki i Telekomunikacji (PIIT);
6. Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (KIGEiT),
7. Stowarzyszenia Instytutu Informatyki Śledczej,
8. Fundacji Panoptykon,
9. Polskiej Izby Komunikacji Elektronicznej,
10. Internet Society Poland,
11. Rady Głównej Instytutów Badawczych (RGIB),
12. Związku Banków Polskich,
13. Izby Gospodarki Elektronicznej,

14. Polskiej Izby Informatyki Medycznej,
15. Ogólnopolskiego Porozumienia Organizacji Samorządowych,
16. Konfederacji Lewiatan.

W ramach konsultacji publicznych i opiniowania uwagi do projektu zgłosili:

1. Zakład Ubezpieczeń Społecznych,
2. Generalny Inspektor Ochrony Danych Osobowych,
3. Polska Izba Informatyki i Telekomunikacji,
4. Polska Izba Komunikacji Elektronicznej,
5. Związek Banków Polskich,
6. Krajowa Izba Rozliczeniowa,
7. Enigma SOI,
8. Śląskie Stowarzyszenie Gmin i Powiatów,
9. Polska Izba Ubezpieczeń,
10. Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa.

Stanowisko do uwag zgłoszonych w ramach konsultacji publicznych oraz opiniowania zostało przedstawione w tabeli, która została opublikowana w BIP RCL oraz przekazana do zainteresowanych podmiotów. Podmioty, które zgłosiły uwagi, zostały zaproszone do udziału w konferencji uzgodnieniowej. W trakcie konferencji omówiono przedmiotowe uwagi. W wyniku konferencji została opracowana nowa wersja projektu ustawy, która została opublikowana w BIP RCL oraz przekazana do zainteresowanych podmiotów.

Do nowej wersji projektu ustawy w ramach konsultacji publicznych i opiniowania uwagi zostały zgłoszone przez podmioty: Polska Izba Ubezpieczeń, Krajowa Izba Rozliczeniowa, Polska Izba Informatyki i Telekomunikacji, Zakład Ubezpieczeń Społecznych, Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa. Wszystkie uwagi zostały rozpatrzone, uwagi, które zostały uznane za uzasadnione, zostały przyjęte.

Projekt został również przekazany Komisji Wspólnej Rządu i Samorządu Terytorialnego i uzyskał pozytywną opinię.

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

6a. Wpływ na sektor finansów publicznych – w zakresie zmian dotyczących publicznego schematu identyfikacji elektronicznej (zmiany w ustawie o usługach zaufania oraz identyfikacji elektronicznej)

(ceny stałe z 2017 r.) Kwoty brutto	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	4,796	8,867	8,713	6,353	6,184	6,184	6,184	6,184	6,184	6,184	6,184	72,017
budżet państwa	4,796	8,867	8,713	6,353	6,184	6,184	6,184	6,184	6,184	6,184	6,184	72,017
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	- 4,796	-8,867	-8,713	-6,353	-6,184	-6,184	-6,184	-6,184	-6,184	-6,184	-6,184	- 72,017
budżet państwa	- 4,796	-8,867	-8,713	-6,353	-6,184	-6,184	-6,184	-6,184	-6,184	-6,184	-6,184	- 72,017
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Sfinansowanie wydatków wynikających z projektu ustawy będzie się odbywało ze środków budżetu państwa będących w dyspozycji podmiotów zobowiązanych do realizacji ustawy (Ministerstwo Cyfryzacji).
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Rok 2018, czyli rok wejścia w życie ustawy, określony w tabeli jako rok „0”, jest pierwszym rokiem wydatkowania środków. Środki przeznaczane na utrzymanie rezultatów projektów będą pochodzić z budżetu państwa cz. 27 (informatyzacja). Wskazane wydatki, które zostaną sfinansowane w ramach corocznie ustalanego w ustawie budżetowej limitu wydatków w części 27, nie będą stanowić podstawy do ubiegania się o dodatkowe środki z budżetu państwa na ten cel w roku bieżącym, jak i w kolejnych latach

	budżetowych. MS poinformował, że przewidywany koszt przyłączenia systemu teleinformatycznego e-KRK do krajowego węzła identyfikacji elektronicznej wyniesie ok. 400 000 zł. Koszt ten został uwzględniony w skutkach finansowych dla roku 2. Środki budżetowe będą pochodziły z części, której dysponentem jest Minister Sprawiedliwości. Środki przeznaczone na utrzymanie rezultatów oraz dostosowanie systemów informatycznych do zmian prawnych, technologicznych i organizacyjnych zachodzących w otoczeniu powinny pochodzić z bieżących wydatków wszystkich zainteresowanych urzędów w ramach corocznego budżetu, bez możliwości ubiegania się o dodatkowe środki na ten cel.

6b. Wpływ na sektor finansów publicznych – w zakresie zmian dotyczących udostępniania, świadczenia i realizacji usług elektronicznych, utrzymania Profilu Zaufanego oraz publicznej aplikacji mobilnej (zmiany w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne)

(ceny stałe z 2017 r.) Kwoty brutto	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	8,65	9,36	9,73	10,22	10,85	11,67	11,61	11,61	11,61	11,61	11,61	118,53
budżet państwa	8,65	9,36	9,73	10,22	10,85	11,67	11,61	11,61	11,61	11,61	11,61	118,53
JST	0,00	0	0	0	0	0	0	0	0	0	0	
pozostałe jednostki (oddzielnie)	0,00	0	0	0	0	0	0	0	0	0	0	
Saldo ogółem	-8,65	-9,36	-9,73	-10,22	-10,85	-11,67	-11,61	-11,61	-11,61	-11,61	-11,61	-118,53
budżet państwa	-8,65	-9,36	-9,73	-10,22	-10,85	-11,67	-11,61	-11,61	-11,61	-11,61	-11,61	-118,53
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Koszty ustawy w zakresie zmian w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne związane z realizacją usług zostaną sfinansowane z budżetu państwa cz. 27 (informatyzacja). Wskazane wydatki w OSR w ramach limitu wydatków części 27 nie będą stanowić podstawy do ubiegania się o dodatkowe środki z budżetu państwa na ten cel w roku bieżącym, jak i w kolejnych latach budżetowych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Rok 2018, czyli rok wejścia w życie ustawy, określony w tabeli jako rok „0", jest pierwszym rokiem wydatkowania środków. Tabela uwzględnia 3 działania Ministerstwa Cyfryzacji: 1) koszty utrzymania profilu zaufanego, którego prawne wyodrębnienie nastąpi w przedmiotowej ustawie; 2) koszty utrzymania systemu publicznej aplikacji mobilnej. W oparciu o obecne dane należy wskazać, że utrzymanie roczne (które rozumie się jako obsługa infrastruktury na ZIR MC, SerwisDesk oraz usuwanie błędów (development) wynosi ok. 80 tyś. miesięcznie. W stosunku rocznym wynosi to zatem 0,96 mln zł. Powyższa kalkulacja uwzględnia koszt utrzymania obecnej funkcjonalności systemu (aplikacji) mDokumenty (zwana dalej publiczną aplikacją mobilną), tj. mObywatel. Każda nowa funkcjonalność w aplikacji w przyszłości będzie zwiększała koszty utrzymania systemu publicznej aplikacji mobilnej. Ministerstwo Cyfryzacji przewiduje, że o ile zaistnieje wola właściwych ministerstw w ramach rozwoju publicznej aplikacji mobilnej, będą uruchomione następujące funkcjonalności np. mLegitymacja Szkolna, Studencka, mKarta Miejska, mKDR, pakiet kierowcy itp. Związane jest to z koniecznością zakupu dodatkowego sprzętu, zwiększenia liczby pracowników odpowiadających za poszczególne linie wsparcia. Szacuje się, że wzrost liczby funkcjonalności uruchamianych w przyszłych latach w systemie publicznej

	aplikacji mobilnej może powodować wzrost kosztów utrzymania ok. 30 procent w danym roku. Jest to uzależnione od tempa rozwoju prac i zakresu działania oraz skali korzystania z funkcjonalności publicznej aplikacji mobilnej. Przyjęto, że największy rozwój funkcjonalności aplikacji nastąpi w latach 2019–2023. W tym zakresie prognozuje się w pkt 1–5 stały zwrot kosztów utrzymania o ok. 30 procent rocznie. Kalkulacja przewiduje także środki na rozwój publicznej aplikacji mobilnej. Jak już wskazano, rozwój publicznej aplikacji mobilnej będzie uzależniony od zapotrzebowania zgłaszanego przez podmioty administracji publicznej. Za prace rozwojowe oraz utrzymanie odpowiedzialny będzie MC. 3) koszt tworzenia, udostępniania, świadczenia i realizacji usług elektronicznych w wysokości 1 mln zł w roku 2018 r. oraz 0,52 mln zł corocznie.

6c. Wpływ na sektor finansów publicznych – podsumowanie tabel 6a-6b

(ceny stałe z 2017 r.) Kwoty brutto	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	13,446	18,227	18,443	16,573	17,034	17,854	17,794	17,794	17,794	17,794	17,794	190,547
budżet państwa	13,446	18,227	18,443	16,573	17,034	17,854	17,794	17,794	17,794	17,794	17,794	190,547
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	-13,446	-18,227	-18,443	-16,573	-17,034	-17,854	-17,794	-17,794	-17,794	-17,794	-17,794	-190,547
budżet państwa	-13,446	-18,227	-18,443	-16,573	-17,034	-17,854	-17,794	-17,794	-17,794	-17,794	-17,794	-190,547
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Łączna kwota wydatków wyniesie ok. 190 mln zł. Środki te będą pochodziły z części 27 budżetu państwa – Informatyzacja. W powyższej kwocie nie została ujęta kwota w wysokości 5 400 tys. zł na zakup czytników dowodów osobistych, która została przewidziana w ustawie budżetowej na rok 2018 w ramach rezerwy celowej poz. 73 pn. Rezerwa na zmiany systemowe i niektóre zmiany organizacyjne, w tym nowe zadania związane z poprawą finansów publicznych, w tym odbudową dochodów budżetu państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Rok 2018, czyli rok wejścia w życie ustawy, określony w tabeli jako rok „0”, jest pierwszym rokiem wydatkowania środków. Wydatki związane z projektowanymi regulacjami będą finansowane w ramach limitu wydatków przewidzianego corocznie w ustawie budżetowej we właściwych częściach budżetowych.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z ... r.)	duże przedsiębiorstwa	brak	brak	brak	brak	brak	brak	
	sektor mikro-, małych i średnich przedsiębiorstw	brak	brak	brak	brak	brak	Brak	
	rodzina, obywatele oraz gospodarstwa domowe	brak	brak	brak	brak	brak	Brak	
W ujęciu	duże przedsiębiorstwa	Możliwość szerszego wykorzystywania ich systemów identyfikacji						

niepieniężnym		elektronicznej.
	sektor mikro-, małych i średnich przedsiębiorstw	Brak bezpośredniego wpływu. Celem zmian jest wykorzystywanie istniejących już systemów identyfikacji elektronicznej. Nie zakłada się, aby mikro- i małe przedsiębiorstwa budowały takie systemy – one będą z nich korzystać.
	rodzina, obywatele oraz gospodarstwa domowe	Ułatwia logowanie do systemów administracji państwowej i samorządowej oraz korzystanie z usług.
	organy administracji publicznej posiadające dostęp do rejestru PESEL	Ułatwienia w zakresie możliwości zgłaszania niezgodności danych w formie dokumentu elektronicznego bezpośrednio do właściwych organów, co przekłada się na skrócenie terminu realizacji spraw.
Niemierzalne		

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☒ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☒ skrócenie czasu na załatwienie sprawy ☒ inne: ułatwienie logowania do systemów administracji państwowej i samorządowej	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

Projektowana ustawa nie ma wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Założenia dla prognoz wykorzystania Węzła Krajowego: – Przyjęto stałą liczbę obywateli RP posiadających zdolność do czynności prawnych jako 85% łącznej liczby obywateli na poziomie 32,7 miliona. – Przyjęto założenie o możliwym dostępie do usług publicznych poprzez banki oferujące narzędzia identyfikacji wykorzystywane do autoryzacji operacji z użyciem PZ. W początkowej fazie zakłada się, że do systemu dołączy ok. 5 banków z łącznym wolumenem klientów bankowości elektronicznej, do których możliwe jest skierowanie rozwiązań eID na poziomie 10 000 000 użytkowników w 2017 roku oraz 20% wzrost tego wskaźnika rok do roku. Integracja ww. podmiotów niepublicznych realizowana będzie poza zakresem niniejszego projektu. – Za liczbę unikalnych użytkowników z wydanymi narzędziami eID rozumiano liczbę obywateli mających udostępnione narzędzia umożliwiające im korzystanie z usług identyfikacji i zaufania w sposób zdalny i zgodnie z przyjętym modelem sfederalizowanym. – Założono stabilny wskaźnik 50% aktywności (tj. wykorzystania usług identyfikacji / zaufania przynajmniej jeden raz w ciągu roku).

	– Przyjęto szacowany procent aktywnych użytkowników logujących się w celu „sprawdzenia" konta miesięcznie. – Szacowany wzrost cyfryzacji społeczeństwa, rozumiany jako skłonność do wykorzystywania dostępnych usług w formule cyfrowej rosnący z 40% w roku 2017 do 65% w roku referencyjnym. – Przyjęto szacowany roczny wzrost wykorzystania usług publicznych w stosunku do wartości bazowej w roku 2016. Założenia dla prognoz wykorzystania ePUAP: – Przyjęto stałą liczbę obywateli RP posiadających zdolność do czynności prawnych jako 85% łącznej liczby obywateli na poziomie 32,7 miliona. – Szacowany wzrost cyfryzacji społeczeństwa, rozumiany jako skłonność do wykorzystywania dostępnych usług w formule cyfrowej rosnący z 40% w roku 2017 do 65% w roku referencyjnym. – Przyjęto szacowany roczny wzrost wykorzystania usług publicznych w stosunku do wartości bazowej w roku 2016.

11. Planowane wykonanie przepisów aktu prawnego

W terminie miesiąca od dnia ogłoszenia ustawy, z zastrzeżeniem terminów dłuższych dla części rozwiązań w celu zapewnienia adekwatnego czasu na wdrożenie nowych rozwiązań.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

W odniesieniu do przepisów dotyczących krajowego schematu identyfikacji elektronicznej planowane jest monitorowanie w cyklach miesięcznych.
Mierniki:
– liczba dostawców środków identyfikacji elektronicznej zintegrowanych z Węzłem Krajowym,
– liczba dostawców usług zintegrowanych z Węzłem Krajowym,
– wypracowanie standardu integracji dostawców usług i dostawców środków identyfikacji elektronicznej z Węzłem Krajowym,
– liczba indywidualnych użytkowników akredytowanych przez Węzeł Krajowy.

W odniesieniu do przepisów dotyczących usług elektronicznych planowane jest monitorowanie w cyklach miesięcznych.
Mierniki:
– wdrażanie e-usług publicznych z zakresu realizacji zadań publicznych drogą elektroniczną,
– upowszechnianie i wspieranie rozwoju e-usług publicznych.

Zwiększenie ilości usług świadczonych za pomocą platformy ePUAP będzie badane poprzez liczbę dokumentów podpisanych oraz przesyłanych za pomocą platformy ePUAP (liczba transakcji). Ułatwienie dostępu do danych i usług społeczeństwa informacyjnego oraz usprawnienie funkcjonowania administracji publicznej poprzez wykorzystanie systemów teleinformatycznych będzie mierzone poprzez liczbę profili zaufanych.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak.

RAPORT Z KONSULTACJI

projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw

Niniejszy raport został sporządzony na podstawie § 51 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin Pracy Rady Ministrów (M.P. z 2016 r. 1006 i 1204). Zawiera on podsumowanie konsultacji publicznych ww. projektu ustawy.

1. Omówienie wyników przeprowadzonych konsultacji publicznych

Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw w dniu 13 kwietnia 2017 r. został skierowany do konsultacji publicznych i opiniowania poprzez udostępnienie w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, w celu zapoznania się z nim przez wszystkie zainteresowane podmioty oraz przesłany niżej wymienionym instytucjom.

W ramach konsultacji publicznych i opiniowania projekt został skierowany na 21 dni do następujących podmiotów:

1. Zakład Ubezpieczeń Społecznych (ZUS),
2. Generalny Inspektor Ochrony Danych Osobowych (GIODO),
3. Polski Komitet Normalizacyjny (PKN),
4. Polskie Towarzystwo Informatyczne (PTI),
5. Polska Izba Informatyki i Telekomunikacji (PIIT);
6. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT),
7. Stowarzyszenie Instytutu Informatyki Śledczej,
8. Fundacja Panoptykon,
9. Polska Izba Komunikacji Elektronicznej,
10. Internet Society Poland,
11. Rada Główna Instytutów Badawczych (RGIB),
12. Związek Banków Polskich,
13. Izba Gospodarki Elektronicznej,
14. Polska Izba Informatyki Medycznej,
15. Ogólnopolskie Porozumienie Organizacji Samorządowych,
16. Konfederacja Lewiatan.

W ramach konsultacji publicznych i opiniowania uwagi do projektu zgłosili:

1. Zakład Ubezpieczeń Społecznych,
2. Generalny Inspektor Ochrony Danych Osobowych,
3. Polska Izba Informatyki i Telekomunikacji,
4. Polska Izba Komunikacji Elektronicznej,
5. Związek Banków Polskich,
6. Krajowa Izba Rozliczeniowa,
7. Enigma SOI,
8. Śląskie Stowarzyszenie Gmin i Powiatów,
9. Polska Izba Ubezpieczeń,
10. Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa.

Wszystkie zgłoszone uwagi zostały rozpatrzone, a w przypadku, gdy były uzasadnione – zostały uwzględnione.

Stanowisko do uwag zgłoszonych w ramach konsultacji publicznych oraz opiniowania zostało przedstawione w tabeli, która została opublikowana w BIP RCL oraz przekazana do zainteresowanych podmiotów. Podmioty, które zgłosiły uwagi zostały zaproszone do udziału w konferencji uzgodnieniowej. W trakcie konferencji omówiono przedmiotowe uwagi. W wyniku

konferencji została opracowana nowa wersja projektu ustawy, która została opublikowana w BIP RCL oraz przekazana do zainteresowanych podmiotów.

Do nowej wersji projektu ustawy w ramach konsultacji publicznych i opiniowania uwagi zostały zgłoszone przez następujące podmioty:

1. Polska Izba Ubezpieczeń, Krajowa Izba Rozliczeniowa,
2. Polska Izba Informatyki i Telekomunikacji,
3. Zakład Ubezpieczeń Społecznych,
4. Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa.

Wszystkie zgłoszone uwagi zostały rozpatrzone, a w przypadku, gdy były uzasadnione – zostały uwzględnione.

2. Przedstawienie wyników konsultacji projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Projekt ustawy nie wymagał przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

3. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa

Zgodnie z przepisami ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej. W toku prac nad projektem żaden podmiot nie zgłosił zainteresowania pracami nad tym projektem w trybie przewidzianym w tej ustawie.

Jednocześnie, zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów, projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny”.

Warszawa, 26 kwietnia 2018 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.649.2017 / 37 / ar

dot.: RM-10-110-17 nowy tekst z dn. 26.04.2018 r.

Pani
Jolanta Rusiniak
Sekretarz Rady Ministrów

Opinia
o zgodności z prawem Unii Europejskiej *projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw*, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowna Pani Minister,

w związku z przedłożonym projektem ustawy pozwalam sobie wyrazić poniższą opinię

Projekt ustawy nie jest sprzeczny z prawem Unii Europejskiej.

Z poważaniem

z up. Ministra Spraw Zagranicznych
Piotr Wawrzyk
Podsekretarz Stanu

Do wiadomości:
Pan Marek Zagórski
Minister Cyfryzacji

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A F I N A N S Ó W

z dnia

w sprawie minimalnej sumy gwarancyjnej obowiązkowego ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej

Na podstawie art. 21d ust. 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa minimalną sumę gwarancyjną obowiązkowego ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej, o którym mowa w art. 21b ust. 2 ustawy, zwanego dalej „ubezpieczeniem OC".

§ 2. 1. Minimalna suma gwarancyjna ubezpieczenia OC wynosi:

1) dla środka identyfikacji o niskim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014", równowartość w złotych 2500 euro w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, w danym roku;
2) dla środka identyfikacji o średnim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b rozporządzenia 910/2014, równowartość w złotych 20 000 euro w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, w danym roku;
3) dla środka identyfikacji o wysokim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b rozporządzenia 910/2014, równowartość w złotych 250 000 euro w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, w danym roku;
4) dla wszystkich zdarzeń w danym roku, w odniesieniu do wszystkich środków identyfikacji elektronicznej, o których mowa w pkt 1–3, równowartość w złotych 1 000 000 euro w danym roku.

2. Kwoty, o których mowa w ust. 1 pkt 1–4 są ustalane przy zastosowaniu kursu średniego euro ogłoszonego przez Narodowy Bank Polski po raz pierwszy w roku, w którym nastąpiło zdarzenie.

§ 3. Rozporządzenie wchodzi w życie z dniem … .

MINISTER FINANSÓW

UZASADNIENIE

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i …) daje możliwość szerokiego wykorzystywania w usługach publicznych środków identyfikacji elektronicznej wydanych w ramach już funkcjonujących systemów identyfikacji elektronicznej, pod warunkiem że systemy te spełniają określone wymagania i zostały przyłączone do węzła krajowego. Podmioty odpowiedzialne za systemy identyfikacji elektronicznej przyłączone do węzła krajowego podlegają obowiązkowi ubezpieczenia odpowiedzialności cywilnej za szkody powstałe w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w tym systemie identyfikacji elektronicznej w usługach publicznych.

Dotąd obowiązkowym ubezpieczeniem odpowiedzialności cywilnej są objęci kwalifikowani dostawcy usług zaufania, co wynika z art. 13 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Podobny wymóg obowiązywał wcześniej także tzw. dostawców usług certyfikacyjnych, o których była mowa w przepisach wydanych na podstawie art. 10 ust. 5 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, z późn. zm.).

Identyfikacja elektroniczna mimo, że podobnie jak usługi zaufania służy zwiększeniu zaufania obywateli przedsiębiorców i podmiotów publicznych do usług świadczonych drogą elektroniczną usługą zaufania nie jest i co za tym idzie nie może jej obejmować ubezpieczenie dotyczące takich usług. Pojęcie identyfikacji elektronicznej nie było formalnie umocowane przed wejściem w życie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS) i co za tym idzie nie ma też doświadczeń w zakresie ubezpieczania uwierzytelniania realizowanego z użyciem środków identyfikacji elektronicznej.

Rozporządzenie określa minimalną sumę gwarancyjną obowiązkowego ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej podmiotu odpowiedzialnego za system identyfikacji elektronicznej, o którym mowa w art. 21b ust. 2 ustawy, różnicując ją w zależności od poziomów bezpieczeństwa środka identyfikacji elektronicznej. Przykładowo Minimalna suma gwarancyjna ubezpieczenia OC wynosi dla środka identyfikacji o niskim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego

dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”, równowartość w złotych 2500 euro w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, w danym roku. Natomiast dla wszystkich zdarzeń w danym roku, w odniesieniu do wszystkich środków identyfikacji elektronicznej niezależnie od poziomów bezpieczeństwa kwota ta wynosi równowartość w złotych 1 000 000 euro w danym roku.

Zgodnie z upoważnieniem ustawowym projekt rozporządzenia zostanie przekazany do zaopiniowania przez Polską Izbę Ubezpieczeń.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Zawarte w projekcie regulacje nie stanowią przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), dlatego też projekt rozporządzenia nie podlega procedurze notyfikacji.

Projekt rozporządzenia nie wymaga przedstawienia właściwym organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji oraz uzgodnienia.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), w związku z art. § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.), projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Nazwa projektu Rozporządzenie Ministra Finansów w sprawie minimalnej sumy gwarancyjnej obowiązkowego ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Finansów i Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** …… **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** 26 kwietnia 2018 r. **Źródło:** Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i ...) **Nr w wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Zasadność podjęcia prac zmierzających do wydania rozporządzenia wynika z wejścia w życie ustawy dnia … o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. …).

Na podstawie art. 21b ust. 1 pkt 4 ustawy, podmiot odpowiedzialny za system identyfikacji elektronicznej, który ma być przyłączony do węzła krajowego będzie zobowiązany przedstawić 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 w usługach publicznych.

Mając na uwadze wskazaną powyżej regulację ustawową powstaje konieczność wydania aktu wykonawczego na podstawie delegacji ustawowej zawartej w art. 21c ustawy o usługach zaufania oraz identyfikacji elektronicznej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Niezbędne jest wydanie aktu wykonawczego na podstawie art. 21c ustawy o usługach zaufania oraz identyfikacji elektronicznej, który będzie określał minimalną sumę gwarancyjną obowiązkowego ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej, który ma być przyłączony do węzła krajowego oraz tego ubezpieczenia. Proponuje się rozwiązanie podobne do tego jakie przyjęto dla obowiązkowego ubezpieczenia OC, jakim jest objęta odpowiedzialność cywilna kwalifikowanych dostawców usług zaufania. Zawężone jednak wyłącznie do usług publicznych, w usługach komercyjnych będzie się to odbywało na zasadach swobody umów.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak informacji.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty odpowiedzialne za system identyfikacji elektronicznej	Obecnie 8 jest podmiotów niepublicznych wydających środki identyfikacji elektronicznej możliwe do wykorzystania w ePUAP	ePUAP.gov.pl	Podmioty niepubliczne wydające środki identyfikacji elektronicznej obecnie możliwe do wykorzystania w ePUAP mogą być potencjalnie zainteresowane przyłączeniem swoich systemów identyfikacji do węzła krajowego

Zakłady ubezpieczeń	30 zakładów ubezpieczeń prowadzących działalność w zakresie ubezpieczeń majątkowych	Komisja Nadzoru Finansowego	Zakłady ubezpieczeń, które będą zawierały umowy przedmiotowego ubezpieczenia OC.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt rozporządzenia zostanie przekazany do konsultacji publicznych i opiniowania. W ramach konsultacji zostanie przesłany m.in. do: Komisji Nadzoru Finansowego, Polskiej Izby Ubezpieczeń, Rzecznika Finansowego.

6. Wpływ na sektor finansów publicznych

(ceny stałe z … r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wydanie rozporządzenia nie będzie miało wpływu na sektor finansów publicznych, w szczególności nie wystąpi skutek w postaci zwiększenia wydatków lub zmniejszenia dochodów jednostek sektora finansów publicznych.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Wejście w życie rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki, przedsiębiorczość i funkcjonowanie przedsiębiorstw.

Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z … r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							

W ujęciu niepieniężnym	duże przedsiębiorstwa	
	sektor mikro-, małych i średnich przedsiębiorstw	
	rodzina, obywatele oraz gospodarstwa domowe	.
Niemierzalne		
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

Wejście w życie rozporządzenia nie spowoduje zmian na rynku pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Projektowane rozporządzenie nie będzie miało wpływu na sytuację i rozwój regionalny oraz pozostałe obszary, o których mowa w pkt 10.

11. Planowane wykonanie przepisów aktu prawnego

Wykonanie przepisów aktu prawnego nastąpi z dniem jego wejścia w życie.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ewaluacja efektów projektu będzie możliwa po okresie co najmniej 1 roku ich funkcjonowania, gdyż umowy ubezpieczenia co do zasady zawierane są na okres 12 miesięcy.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak.

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A F I N A N S Ó W

z dnia

w sprawie wysokości kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej za szkody wyrządzone w związku z wykorzystaniem środków identyfikacji elektronicznej

Na podstawie art. 21d ust. 2 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa wysokość kwot odpowiedzialności podmiotu, odpowiedzialnego za system identyfikacji elektronicznej za szkody wynikające z działania lub zaniechania, wyrządzone w związku z wykorzystaniem środków identyfikacji elektronicznej wydanych w tym systemie identyfikacji elektronicznej, w usługach online świadczonych przez podmioty, o których mowa w art. 2 lub 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 Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”, spowodowane przez awarie, przerwy lub błędy systemu lub przez zaciągnięcie zobowiązań w wyniku nieuprawnionego wykorzystania środka identyfikacji elektronicznej.

§ 2. 1. Wysokość kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej za szkody, o których mowa w art. 21c ust. 1 ustawy, wynosi:

1) dla środka identyfikacji o niskim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. a rozporządzenia 910/2014, – nie więcej niż równowartość w złotych 5000 euro w odniesieniu do jednego zdarzenia, jednak nie więcej niż równowartość w złotych 1 000 000 euro w odniesieniu do wszystkich zdarzeń w danym roku;
2) dla środka identyfikacji o średnim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b rozporządzenia 910/2014, – nie więcej niż równowartość w złotych 40 000

euro w odniesieniu do jednego zdarzenia, jednak nie więcej niż równowartość w złotych 1 000 000 euro w odniesieniu do wszystkich zdarzeń w danym roku;

3) dla środka identyfikacji o wysokim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. b rozporządzenia 910/2014, – nie więcej niż równowartość w złotych 400 000 euro w odniesieniu do jednego zdarzenia, jednak nie więcej niż równowartość w złotych 2 000 000 euro w odniesieniu do wszystkich zdarzeń w danym roku.

2. Kwoty, o których mowa w ust. 1 pkt 1–3, są ustalane przy zastosowaniu kursu średniego euro ogłoszonego przez Narodowy Bank Polski po raz pierwszy w roku, w którym nastąpiło zdarzenie.

§ 3. Rozporządzenie wchodzi w życie z dniem … .

MINISTER FINANSÓW

UZASADNIENIE

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i ...) daje możliwość szerokiego wykorzystywania w usługach publicznych środków identyfikacji elektronicznej wydanych w ramach już funkcjonujących systemów identyfikacji elektronicznej, pod warunkiem że systemy te spełniają określone wymagania i zostały przyłączone do węzła krajowego. Podmioty odpowiedzialne za systemy identyfikacji elektronicznej przyłączone do węzła krajowego odpowiadają za szkody powstałe w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w tym systemie identyfikacji elektronicznej w usługach publicznych.

Zgodnie projektem rozporządzenia podmiot odpowiedzialny za system identyfikacji będzie ponosił odpowiedzialność za szkody wynikające z działania lub zaniechania wyrządzone, w związku z wykorzystaniem środków identyfikacji elektronicznej wydanych w tym systemie identyfikacji elektronicznej, w usługach online świadczonych przez podmioty, o których mowa w art. 2 lub art. 19c 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 Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”, spowodowane przez awarie, przerwy lub błędy systemu lub zaciągnięciem zobowiązania w wyniku nieuprawnionego wykorzystania środka identyfikacji elektronicznej.

W rozporządzeniu określono wysokość kwot odpowiedzialności w zależności od poziomu bezpieczeństwa środka identyfikacji. Przykładowo dla środka identyfikacji o niskim poziomie bezpieczeństwa, o którym mowa w art. 8 ust. 2 lit. a rozporządzenia 910/2014, podmiot poniesie odpowiedzialność do kwoty nie wyższej równowartość w złotych 5000 euro w odniesieniu do jednego zdarzenia, jednak nie wyższej niż równowartość w złotych 1 000 000 euro w odniesieniu do wszystkich zdarzeń w danym roku. Kwoty ubezpieczenia będą ustalane przy zastosowaniu kursu średniego euro ogłoszonego przez Narodowy Bank Polski po raz pierwszy w roku, w którym nastąpiło zdarzenie.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Zawarte w projekcie regulacje nie stanowią przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), dlatego też projekt rozporządzenia nie podlega procedurze notyfikacji.

Projekt zarządzenia nie wymaga przedstawienia właściwym organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji oraz uzgodnienia.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), w związku z art. § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.), projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Nazwa projektu Rozporządzenie Ministra Finansów w sprawie zakresu i wysokości odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej za szkody wyrządzone w związku z wykorzystaniem środków identyfikacji elektronicznej **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Finansów i Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** …… **Kontakt do opiekuna merytorycznego projektu** ...../	**Data sporządzenia** 26 kwietnia 2018 r. **Źródło:** Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 i …) **Nr w wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Zasadność podjęcia prac zmierzających do wydania rozporządzenia wynika z wejścia w życie ustawy dnia … o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. …).

Na podstawie art. 21d ust. 2 ustawy minister właściwy do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw informatyzacji, określi, w drodze rozporządzenia, zakres i wysokość odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej, za szkody wynikające z działania lub zaniechania wyrządzone, w związku z wykorzystaniem środków identyfikacji elektronicznej wydanych w tym systemie identyfikacji elektronicznej, w usługach online świadczonych przez podmioty, o których mowa w art. 2 lub art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub podmioty sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014, spowodowane przez awarie, przerwy lub błędy systemu lub za zobowiązanie zaciągnięte w wyniku nieuprawnionego wykorzystania środka identyfikacji elektronicznej, w zależności od poziomu bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Niezbędne jest wydanie aktu wykonawczego na podstawie art. 21d ust. 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak informacji.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty odpowiedzialne za system identyfikacji elektronicznej	Obecnie jest 8 podmiotów niepublicznych wydających środki identyfikacji elektronicznej możliwe do wykorzystania w usługach publicznych.	ePUAP.gov.pl	Podmioty niepubliczne wydające środki identyfikacji elektronicznej obecnie możliwe do wykorzystania w usługach publicznych mogą być potencjalnie zainteresowane przyłączeniem swoich systemów identyfikacji do węzła krajowego.
Zakłady ubezpieczeń	30 zakładów ubezpieczeń	Komisja Nadzoru Finansowego	Zakłady ubezpieczeń, które będą zawierały

	prowadzących działalność w zakresie ubezpieczeń majątkowych		umowy przedmiotowego ubezpieczenia OC.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt rozporządzenia zostanie przekazany do konsultacji publicznych i opiniowania. W ramach konsultacji zostanie przesłany m.in. do: Komisji Nadzoru Finansowego, Polskiej Izby Ubezpieczeń, Rzecznika Finansowego.

6. Wpływ na sektor finansów publicznych

(ceny stałe z … r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wydanie rozporządzenia nie będzie miało wpływu na sektor finansów publicznych, w szczególności nie wystąpi skutek w postaci zwiększenia wydatków lub zmniejszenia dochodów jednostek sektora finansów publicznych.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Wejście w życie rozporządzenia nie będzie miało wpływu na konkurencyjność gospodarki, przedsiębiorczość i funkcjonowanie przedsiębiorstw.

Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z … r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							

	rodzina, obywatele oraz gospodarstwa domowe	.
Niemierzalne		

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:

9. Wpływ na rynek pracy

Wejście w życie rozporządzenia nie spowoduje zmian na rynku pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Projektowane rozporządzenie nie będzie miało wpływu na sytuację i rozwój regionalny oraz pozostałe obszary, o których mowa w pkt 10.

11. Planowane wykonanie przepisów aktu prawnego

Wykonanie przepisów aktu prawnego nastąpi z dniem jego wejścia w życie.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ewaluacja efektów projektu będzie możliwa po okresie co najmniej 1 roku ich funkcjonowania, gdyż umowy ubezpieczenia co do zasady zawierane są na okres 12 miesięcy.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak.

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I

z dnia

w sprawie profilu zaufanego

Na podstawie art. 20d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 i ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa warunki wydawania przedłużania ważności, wykorzystywania i unieważniania profilu zaufanego oraz składania podpisu zaufanego, w tym:

1) okres ważności profilu zaufanego;
2) zawartość profilu zaufanego;
3) przypadki, w których nie dokonuje się potwierdzenia profilu zaufanego;
4) przypadki, w których profil zaufany traci ważność;
5) warunki przechowywania oraz archiwizowania dokumentów i danych bezpośrednio związanych z potwierdzeniem profilu zaufanego;
6) dane i dokumenty wymagane w procedurze potwierdzania, przedłużania ważności i unieważnienia profilu zaufanego;
7) warunki, które powinien spełniać punkt potwierdzający profil zaufany;
8) warunki organizacyjne i techniczne dla potwierdzenia profilu zaufanego oraz uwierzytelnień i autoryzacji przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy;
9) sposób potwierdzania spełniania warunków, o których mowa w pkt 8;
10) warunki składania podpisu zaufanego.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) identyfikator profilu zaufanego – unikatowy ciąg znaków alfanumerycznych jednoznacznie identyfikujących profil zaufany;
2) identyfikator użytkownika – unikatowy ciąg znaków alfanumerycznych jednoznacznie identyfikujących użytkownika posiadającego konto w systemie profilu zaufanego;

3) system profilu zaufanego – system identyfikacji elektronicznej w ramach którego wydaje się profile zaufane;
4) konto profilu zaufanego – dane opisujące profil zaufany wraz z przyporządkowanymi do nich zasobami systemu profilu zaufanego umożliwiającymi użytkownikowi konta zarządzanie swoim profilem zaufanym i korzystanie z profilu zaufanego;
5) osoba wnioskująca – osobę fizyczna występującą z wnioskiem o potwierdzenie profilu zaufanego.

§ 3. 1. Osoba wnioskująca przesyła w systemie profilu zaufanego wniosek o potwierdzenie profilu zaufanego w postaci elektronicznej przy wykorzystaniu formularza elektronicznego udostępnionego w tym systemie.

2. Jeżeli w okresie 14 dni od daty przesłania wniosku, o którym mowa w ust. 1, osoba wnioskująca nie zgłosi się do punktu potwierdzającego w celu potwierdzenia profilu zaufanego, wniosek ten uważa się za bezskuteczny.

3. Wzór wniosku, o którym mowa w ust. 1, określa załącznik nr 1 do rozporządzenia.

§ 4. 1. W celu potwierdzenia profilu zaufanego osoba wnioskująca zgłasza się do wybranego przez siebie punktu potwierdzającego.

2. W punkcie potwierdzającym osoba upoważniona do potwierdzania profilu zaufanego stwierdza tożsamość osoby wnioskującej na podstawie okazanego dokumentu tożsamości.

3. Osoba upoważniona do potwierdzania profilu zaufanego drukuje wniosek o potwierdzenie profilu zaufanego z systemu profilu zaufanego. Osoba wnioskująca podpisuje wydrukowany wniosek.

4. Osoba upoważniona do potwierdzania profilu zaufanego, po pozytywnej weryfikacji tożsamości osoby wnioskującej, potwierdza profil zaufany i odnotowuje to na wydrukowanym wniosku wraz z podaniem czasu potwierdzenia. W przypadku stwierdzania tożsamości osoby wnioskującej na podstawie dokumentu tożsamości niezawierającego numeru PESEL, o którym mowa w art. 20c ust. pkt 1 lit b. dodatkowo odnotowuje na wydrukowanym wniosku rodzaj i numer okazanego dokumentu tożsamości.

5. Osoba upoważniona do potwierdzania profilu zaufanego podpisuje profil zaufany osoby wnioskującej:

1) podpisem zaufanym albo
2) kwalifikowanym podpisem elektronicznym.

§ 5. Osoba posiadająca ważny profil zaufany w celu jego bezpiecznego wykorzystywania:

1) zapewnia poufność danych, które mogłyby być wykorzystane do identyfikacji i uwierzytelnienia w systemie teleinformatycznym lub złożenia podpisu zaufanego przez osoby trzecie;
2) nie udostępnia konta profilu zaufanego osobom trzecim;
3) niezwłocznie unieważnia profil zaufany w przypadku utraty kontroli nad kontem profilu zaufanego.

§ 6. Potwierdzenia, przedłużenia ważności i unieważnienia profilu zaufanego dokonuje się w systemie profilu zaufanego.

§ 7. 1. Profil zaufany zawiera:

1) dane o których mowa w art. 20ad ust. 1 ustawy;
2) identyfikator użytkownika;
3) identyfikator profilu zaufanego;
4) czas potwierdzenia;
5) termin ważności;
6) adres poczty elektronicznej;
7) numer telefonu komórkowego;
8) wybrane przez użytkownika czynniki uwierzytelniania.

2. W przypadku potwierdzenia profilu zaufanego:

1) w punkcie potwierdzającym – profil zaufany zawiera również oznaczenie punktu potwierdzającego oraz imię i nazwisko osoby upoważnionej do potwierdzania profilu zaufanego;
2) w sposób, o którym mowa w art. 20c ust. 1 pkt 2 ustawy – profil zaufany zawiera również wskazanie, że profil został potwierdzony przy wykorzystaniu kwalifikowanego podpisu elektronicznego;
3) w sposób, o którym mowa w art. 20c ust. 1 pkt 3 ustawy – profil zaufany zawiera również oznaczenie systemu teleinformatycznego banku krajowego lub innego przedsiębiorcy wykorzystanego do potwierdzenia profilu zaufanego.

3. Profil zaufany umożliwia wykorzystywanie co najmniej dwóch czynników uwierzytelnienia należących do najmniej do dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego

i Rady (UE) nr 910/2014 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), przy czym:

1) jednym z tych czynników może być:
   a) hasło dostępu do konta profilu zaufanego, albo
   b) inny czynnik uwierzytelniania wymagający od podmiotu podlegającego uwierzytelnieniu określonej, znanej tylko temu podmiotowi wiedzy, albo
   c) dane posiadacza profilu zaufanego zweryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego;
2) drugi czynnik może stanowić:
   a) hasło jednorazowe przesyłane na wskazany przez użytkownika numer telefonu komórkowego, albo
   b) inny czynnik uwierzytelniania wymagający od posiadacza profilu zaufanego wykazania się posiadaniem ustalonej uprzednio rzeczy lub urządzenia niezbędnego dla wykorzystania tego czynnika.

4. Profil zaufany może wykorzystywać również czynniki uwierzytelniania stosowane w systemie podmiotu niepublicznego pod warunkiem, że należą one co najmniej do dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.

5. Autoryzacja jest dokonywana przy użyciu czynnika uwierzytelniana należącego innej kategorii niż pierwszy czynnik uwierzytelniania, w rozumieniu przepisów wydanych na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.

6. Użytkownik może dokonać zmiany:

1) adresu poczty elektronicznej lub numeru telefonu komórkowego – samodzielnie w systemie profilu zaufanego z zastrzeżeniem że czynność ta wymaga autoryzacji, albo w punkcie potwierdzającym profil zaufany;
2) środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego – samodzielnie w systemie podmiotu niepublicznego;

3) czynnika uwierzytelniania – samodzielnie w systemie profilu zaufanego albo systemie teleinformatycznym podmiotu niepublicznego, o ile system profilu zaufanego albo system teleinformatyczny podmiotu niepublicznego na to pozwala.

7. Komunikaty związane z funkcjonowaniem konta profilu zaufanego przesyłane są na adres poczty elektronicznej, o którym mowa w § 7 ust. 1 pkt 6.

8. Struktura danych profilu zaufanego oraz podpisu potwierdzonego profilem zaufanym są publikowane w przez ministra właściwego do spraw informatyzacji, zwanego dalej „ministrem”.

§ 8. 1. Profil zaufany potwierdza się na okres trzech lat i jego ważność może być przedłużona na taki sam okres.

2. Przedłużenia ważności profilu zaufanego dokonuje w systemie profilu zaufanego samodzielnie osoba posiadająca profil zaufany, potwierdzając to podpisem zaufanym.

§ 9. 1. Nie dokonuje się potwierdzenia profilu zaufanego w przypadku:

1) przedłożenia nieważnego dokumentu, o którym mowa w § 4 ust. 2, lub braku możliwości jednoznacznego potwierdzenia tożsamości osoby wnioskującej na podstawie okazanego dokumentu;
2) niezgodności imienia (imion) lub nazwiska w złożonym wniosku o potwierdzenie profilu zaufanego z tymi danymi w okazanym dokumencie tożsamości;
3) niezgodności numeru PESEL w złożonym wniosku o potwierdzenie profilu zaufanego z numerem PESEL w okazanym dokumencie tożsamości, a w przypadku gdy okazany dokument tożsamości nie zawiera numeru PESEL – niezgodności daty urodzenia zawarte w pierwszych sześciu cyfrach numeru PESEL z datą urodzenia w okazanym dokumencie tożsamości.

2. Niedokonanie potwierdzenia profilu zaufanego osoba upoważniona do potwierdzania profilu zaufanego odnotowuje na wydrukowanym wniosku o potwierdzenie profilu zaufanego wraz z podaniem czasu niedokonania potwierdzenia.

§ 10. 1. Profil zaufany traci ważność w przypadku:

1) usunięcia konta profilu zaufanego;
2) upływu okresu, na jaki został potwierdzony albo przedłużony.

2. W przypadku zmiany adresu poczty elektronicznej, numeru telefonu komórkowego, środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego lub uwierzytelniania użytkownika, profil

zaufany jest unieważniany, a w jego miejsce automatycznie tworzony jest nowy profil zaufany powiązany z dotychczasowym kontem profilu zaufanego.

3. Osoba posiadająca profil zaufany może samodzielnie dokonać unieważnienia swojego profilu zaufanego albo wystąpić z wnioskiem o unieważnienie profilu zaufanego.

4. W celu unieważnienia profilu zaufanego na wniosek osoba posiadająca profil zaufany zgłasza się do wybranego przez siebie punktu potwierdzającego. Osoba upoważniona do potwierdzania profilu zaufanego stwierdza tożsamość osoby wnioskującej na podstawie na podstawie okazanego dokumentu tożsamości.

5. Wzór wniosku o unieważnienie profilu zaufanego określa załącznik nr 2 do rozporządzenia.

§ 11. Profil zaufany potwierdzony na podstawie nieprawdziwych lub nieaktualnych danych jest nieważny od dnia jego potwierdzenia.

§ 12. 1. Złożenie podpisu zaufanego jest możliwe w okresie ważności profilu zaufanego.

2. Złożenie podpisu zaufanego wymaga uprzedniej autoryzacji, o której mowa w § 7 ust. 5, po której następuje opatrzenie podpisywanych danych pieczęcią elektroniczną ministra wykorzystywaną do zapewnienia integralności i autentyczności wykonania operacji złożenia podpisu.

3. Weryfikacja integralności dokumentu lub danych podpisanych przy użyciu podpisu zaufanego oraz autentyczności tego podpisu dokonywana jest za pomocą certyfikatu pieczęci elektronicznej udostępnionego przez ministra.

4. Przed złożeniem podpisu zaufanego osoba posiadająca profil zaufany jest informowana przez interfejs użytkownika oprogramowania umożliwiającego złożenie tego podpisu o tym, że dokonuje czynności złożenia takiego podpisu.

§ 13. 1. Pełnienie funkcji punktu potwierdzającego profil zaufany przez podmioty o których mowa w art. 20c ust. 3 ustawy, jest możliwe po przedłożeniu ministrowi oświadczenia o spełnieniu wymagań określonych w § 3 ust. 2 i 3 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. poz. 1627), w zakresie w jakim dotyczyć to będzie uprawnień osób i czynności realizowanych przez te osoby w związku z potwierdzaniem profilu zaufanego.

2. Punkt potwierdzający stale zapewnia spełnienie wymagań, o których mowa w ust. 1.

3. Punkt potwierdzający, o którym mowa w art. 20c ust. 3 pkt 2–4 ustawy, w przypadku gdy nie posiada instrukcji określającej zasady i tryb postępowania z dokumentacją wydanej na podstawie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r. poz. 217), zapewnia wdrożenie instrukcji określającej zasady i tryb postępowania z dokumentacją związaną z potwierdzaniem, przedłużaniem ważności i unieważnianiem profilu zaufanego oraz przedkłada ministrowi kopię tego dokumentu.

4. Osoby realizujące czynności związane z potwierdzaniem profilu zaufanego, działają zgodnie z procedurami zarządzania profilami zaufanymi oraz nadawania uprawnień do potwierdzania, przedłużania ważności i unieważniania profili zaufanych, zamieszczonymi w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

§ 14. 1. Punkt potwierdzający przechowuje i archiwizuje dokumenty w postaci papierowej w zakresie potwierdzania, przedłużania i unieważniania profilu zaufanego w warunkach zapewniających co najmniej:

1) zachowanie integralności dokumentów;
2) odszukanie i udostępnienie dokumentów;
3) ochronę danych osobowych zawartych w dokumentach;
4) ochronę tych dokumentów przed zniszczeniem.

2. Dokumenty w postaci elektronicznej w zakresie potwierdzania, przedłużania i unieważniania ważności profilu zaufanego, z zachowaniem warunków określonych w ust. 1, przechowuje oraz archiwizuje minister.

3. Obowiązek przechowania dokumentów, o których mowa w ust. 1 i 2, trwa przez okres 20 lat od chwili potwierdzenia albo przedłużenia ważności profilu zaufanego lub od chwili odmowy jego potwierdzenia albo odmowy przedłużenia ważności bądź od chwili jego unieważnienia.

4. Organ lub jednostka organizacyjna przejmująca zadania, funkcje i dokumenty punktu potwierdzającego, którego działalność ustała, zapewnia spełnienie warunków, o których mowa w ust. 1 i 3. W przypadku braku następcy prawnego punktu potwierdzającego spełnienie warunków, o których mowa w ust. 1 i 3, zapewnia minister.

§ 15. Potwierdzenie profilu zaufanego, a także przedłużenie jego ważności lub unieważnienie, w sposób określony w art. 20c ust. 1 pkt 3 ustawy, może być dokonane z wykorzystaniem systemu teleinformatycznego podmiotu niepublicznego.

§ 16. 1. Wykorzystanie środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego do potwierdzania profilu zaufanego oraz autoryzacji wymaga:

1) wdrożenia przez podmiot niepubliczny zabezpieczeń dotyczących co najmniej średniego poziomu zaufania, wymaganych rozporządzeniem wykonawczym Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 7), zwanym dalej „rozporządzeniem wykonawczym 2015/1502”;
2) opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wykonawczych wydanych na podstawie art. 18 ustawy;
3) poddawania się przez podmiot niepubliczny niezależnemu audytowi, o którym mowa w pkt 2.4.7 załącznika do rozporządzenia wykonawczego 2015/1502, sprawdzającemu spełnianie wymagań, o których mowa w pkt 1 i 2, nie rzadziej niż raz na dwa lata;
4) potwierdzenia przez podmiot niepubliczny tożsamości osoby, której udostępniono środki identyfikacji elektronicznej stosowane do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, na podstawie:
   a) okazanego podczas fizycznej obecności dokumentu tożsamości, który zawiera numer PESEL, z zachowaniem należytej staranności w ustaleniu autentyczności dokumentu tożsamości oraz w działaniach zmierzających do zminimalizowania ryzyka, że tożsamość deklarowana przy użyciu okazanego dokumentu tożsamości jest niezgodna z faktyczną tożsamością osoby okazującej ten dokument, albo
   b) danych pochodzących z poprawnie przeprowadzonej weryfikacji kwalifikowanego podpisu elektronicznego, którego certyfikat zawiera numer PESEL, przy użyciu którego osoba ta podpisała dokument elektroniczny, w którym oświadczyła, że świadoma jest warunków i zalecanych zasad korzystania z systemu identyfikacji elektronicznej, oraz wyraziła zgodę na nadanie statusu użytkownika tego systemu

oraz wykorzystywanie udostępnionych środków identyfikacji elektronicznej w systemie;

5) przeprowadzenia testów integracyjnych w zakresie możliwości wykorzystania środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego do potwierdzania profilu zaufanego i autoryzacji, zgodnie z procedurą udostępnioną w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

2. Wymagania, o których mowa w ust. 1 pkt 1–4, uznaje się za spełnione w przypadku przedstawienia przez podmiot niepubliczny:

1) ważnego akredytowanego certyfikatu, obejmującego w swym zakresie stosowanie środków identyfikacji elektronicznej, systemu zarządzania bezpieczeństwem informacji, albo
2) protokołu pokontrolnego kontroli organu nadzoru, potwierdzającego wdrożenie wymogów określonych w przepisach wydanych na podstawie art. 137 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2015 r. poz. 128, z późn. zm.), w zakresie dotyczącym zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, albo
3) pozytywnego wyniku audytu, o którym mowa w ust. 1 pkt 3, przeprowadzonego nie wcześniej niż 15 miesięcy przed dniem złożenia przez podmiot niepubliczny wniosku do ministra o wyrażenie zgody na wykorzystywanie do potwierdzania profilu zaufanego środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, albo
4) innego dokumentu potwierdzającego spełnianie warunków, o których mowa w ust. 1 pkt 1–4.

3. Wymaganie, o którym mowa w ust. 1 pkt 5, uznaje się za spełnione w przypadku przedstawienia pozytywnego wyniku testów integracyjnych.

§ 17. Podmiot niepubliczny przedstawia dokumenty, o których mowa w § 16 ust. 2 i 3, na żądanie ministra.

§ 18. Wnioski o potwierdzenie, przedłużenie ważności i unieważnienie profilu zaufanego ePUAP przesłane przed dniem wejścia w życie rozporządzenia są ważne i traktowane jako wnioski o potwierdzenie profilu zaufanego.

§ 19. Wnioski, o których mowa w art. 20c ust. 4 ustawy, złożone przed dniem wejścia w życie rozporządzenia, rozpatrywane są zgodnie z dotychczasowymi przepisami.

§ 20. Rozporządzenie wchodzi w życie z dniem …

MINISTER CYFRYZACJI

UZASADNIENIE

Potrzeba wydania nowego rozporządzenia w sprawie profilu zaufanego wynika ze zmiany przepisu upoważniającego do wydania tego rozporządzenia a także innych zmian w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570).

Nowe rozporządzenie uwzględnia zmiany w ustawie powodujące formalne oddzielenie profilu zaufany od platformy ePUAP i co z tym idzie dostosowujące nazwę tego środka identyfikacji elektronicznej do powszechnie używanej („profil zaufany" zamiast „profil zaufany ePUAP"). Zgodnie z ustawą, zmianie i uproszczeniu uległa też dotychczasowa „podpisu potwierdzonego profilem zaufanym ePUAP" który zmienił nazwę na „podpis zaufany".

W konsekwencji powyższych zmian wniosek o potwierdzenie profilu zaufanego nie jest już generowany na ePUAP tylko w odrębnym systemie profilu zaufanego.

W stosunku do poprzedniego rozporządzenia z dnia 5 października 2016 r. w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz. U. poz. 1633), nowe rozporządzenie nie zawiera już przepisów wskazujących zakres danych osobowych zawartych w tym profilu gdyż został on określony w ustawie.

Zrezygnowano z dotychczasowej możliwości składania wniosku o potwierdzenie profilu zaufanego bezpośrednio w punkcie potwierdzającym mając na uwadze znikome wykorzystanie tej opcji, jak również ze względu na to, że umiejętność samodzielnego złożenia wniosku online w sposób naturalny weryfikuje umiejętności cyfrowe przyszłego posiadacza profilu zaufanego, co pośrednio wpłynie pozytywnie na bezpieczeństwo przyszłego użytkownika tego profilu. Ponadto w dotychczasowych przepisach, w przypadku gdy wniosek, jest przygotowywany w punkcie potwierdzającym przez osobę upoważnioną do potwierdzania profilu zaufanego ePUAP, wypełniany musi być przez te osobę na podstawie danych już zawartych w ePUAP, co w związku z oddzieleniem platformy ePUAP od systemu profilu zaufanego wyklucza taką możliwość ze względów formalnych.

Mając na uwadze planowaną notyfikację profilu zaufanego w Komisji Europejskiej celem umożliwienia jego posiadaczom uwierzytelniania w publicznych usługach online w całej UE dodano przepisy dostosowujące profil zaufany do tych potrzeb. I tak w § 7 ust. 2 pkt 2 i 3 wskazano na potrzebę odróżniania profili zaufanych potwierdzonych w sposób inny

niż w punkcie potwierdzającym, co da możliwość zawieszenia lub wyłączenia uwierzytelniania tylko dla części profili zaufanych potwierdzonych w określony sposób, a nie dla całego systemu profilu zaufanego, zgodnie z przepisami art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014.

Przepisy § 7 ust. 3–6 mają na celu dostosowanie profilu zaufanego do przepisów Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Obecnie w rozporządzeniu w sprawie profilu zaufanego ePUAP przepisy są tak skonstruowane by wskazać jedynie na drugi czynnik uwierzytelniania zwany w tym rozporządzeniu „autoryzacją" i służący w praktyce do złożenia podpisu potwierdzonego profilem zaufanym. Obecnie rozporządzenie w sprawie profilu w ogóle nie odnosi się do istnienia pierwszego czynnika uwierzytelniania, gdyż ten został zdefiniowany w § 4 ust. 2 rozporządzenia Ministra Cyfryzacji w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (dalej rozporządzenie ePUAP). W związku z tym, że następuje formalne rozdzielenie ePUAP od systemu profilu zaufanego, niezbędne jest takie dostosowanie przepisów w sprawie profilu zaufanego by obejmowały oba składniki uwierzytelniania.

Ponadto zlikwidowano ograniczenia dotyczących użycia konkretnego rozwiązania jak to jest obecnie w § 4 ust. 2 rozporządzenia ePUAP (dla pierwszego składnika uwierzytelniania) i w § 8 ust, 3 rozporządzenia w sprawie profilu zaufanego (dla drugiego składnika uwierzytelniania). Obecnie bowiem przepisy te pozwalają na swobodę wyboru sposobu uwierzytelniania z wykorzystaniem środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, nie wskazując w takim przypadku określonego rozwiązania, ale ustalają z góry dozwolone sposoby uwierzytelniania w przypadku gdy nie odbywa się ono z wykorzystaniem takich środków. Z góry to wyklucza inne technologie np. login/ mobile connect, które potencjalnie użytkownik mógłby mieć do wyboru.

Zrezygnowano też z możliwości przedłużania profilu zaufanego w punkcie potwierdzającym gdyż ta możliwość marginalne wykorzystywana z tego powodu, że można

to samo zrobić online nie wychodząc z domu. Ponadto w przypadku gdy użytkownik nie mogę przedłużyć profilu zaufanego online (bo np. zapomniał hasła) to i tak w punkcie potwierdzającym go nie powinien odzyskać gdyż to zasadniczo zmniejszyłoby bezpieczeństwo profilu zaufanego.

Nazwa projektu Projekt rozporządzenia Ministra Cyfryzacji w sprawie profilu zaufanego **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** …… **Kontakt do opiekuna merytorycznego projektu** ……..	**Data sporządzenia** 6 kwietnia 2018 r. **Źródło:** **Nr w wykazie prac RM: ….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z przewidywanym uchyleniem upoważnienia zawartego w art. 20a ust. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), związanego ze zmianami w projekcie ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UD 244), konieczne jest wydanie nowego rozporządzenia w sprawie profilu zaufanego.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

W związku z powyższym w stosunku do treści rozporządzenia z dnia 5 października 2016 r. w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz.U. poz. 1633) w nowym rozporządzeniu planuje się wprowadzanie następujących zmian:

1. Wprowadzenie zmian terminologicznych wynikających z ustawy (profil zaufany zamiast profil zaufany ePUAP oraz podpis zaufany zamiast podpis potwierdzony profilem zaufanym ePUAP.
2. Dostosowanie do formalnego wyodrębnienia profilu zaufanego z platformy ePUAP, co pozwoli na niezależne od konta na ePUAP wykorzystywanie profilu zaufanego.
3. Formalne wyodrębnienie podpisu zaufanego (usługi zaufania) od środka identyfikacji elektronicznej jakim jest profil zaufany co stworzy podstawy do notyfikacji profilu zaufanego w Komisji Europejskiej jaki systemu identyfikacji elektronicznej (bez podpisu zaufanego), co pozwoli wykorzystywać profil zaufany do uwierzytelniania się w usługach publicznych online w całej UE.
4. Zmiany dostosowujące sposób uwierzytelniania profilem zaufanym do wytycznych wskazanych w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.
5. Zmiany zapewniające możliwość odróżniania profili zaufanych potwierdzonych w sposób inny niż w punkcie potwierdzającym, co da możliwość zawieszenia lub wyłączenia uwierzytelniania tylko dla części profili zaufanych potwierdzonych w określony sposób, a nie dla całego systemu profilu zaufanego, zgodnie z przepisami art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014.
6. Likwidacja ograniczeń wskazujących na konieczność użycia konkretnego czynnika uwierzytelniania jak to jest obecnie w § 4 ust. 2 rozporządzenia Ministra Cyfryzacji w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (dla pierwszego składnika uwierzytelniania) i w § 8 ust. 3 aktualnie obowiązującego rozporządzenia w sprawie profilu zaufanego ePUAP (dla drugiego składnika uwierzytelniania), co da możliwość szybkiego wykorzystywania nowych technologii dla uwierzytelniania profilem zaufanym w jednoczesnym uwzględnieniem wytycznych wskazanych w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

W innych krajach członkowskich OECD/UE nie funkcjonuje rozwiązanie podobne jak w przypadku profilu zaufanego, który jest środkiem identyfikacji elektronicznej jednocześnie pozwalającym na złożenie podpisu elektronicznego zrównanego w określonych warunkach z podpisem własnoręcznym.

Środki identyfikacji elektronicznej wydawane w ramach systemów identyfikacji elektronicznej notyfikowanych przez państwa członkowskie UE w Komisji Europejskiej (Niemcy) oraz w ramach systemów dla których proces notyfikacji trwa (Chorwacja, Estonia, Luksemburg, Hiszpania) są przeważnie oparte o dowód tożsamości z warstwą elektroniczną. Wyjątkiem są Włochy gdzie co do zasady występują środki identyfikacji elektronicznej inne niż oparte o dowód osobisty i Estonia gdzie oprócz dowodu osobistego można wykorzystać też identyfikację wykorzystującą karty SIM. W żadnym

z tych ww. krajów nie istnieje możliwość wykorzystania środka identyfikacji do złożenia podpisu elektronicznego potwierdzonego tym środkiem w sposób podobnie zorganizowany jak w Polsce.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Potencjalni posiadacze profilu zaufanego. Pełnoletnie osoby fizyczne posiadające nadany nr PESEL korzystające z Internetu i niemające profilu zaufanego.	Około 20 milionów (67% dorosłych Polaków deklarujących umiejętności cyfrowe)	Komunikat CBOS nr 49/2017, Korzystanie z Internetu, Warszawa, kwiecień 2017. ISSN 2353-5822	Łatwiejszy dostęp do profilu zaufanego
Osoby fizyczne posiadające profili zaufany.	Ok. 1,5 miliona	Statystyki ePUAP (źródło własne)	Oddzielenie możliwości uwierzytelniania od składania podpisu elektronicznego.
Podmioty publiczne utrzymujące usługi online umożliwiające skorzystanie z profili zaufanego	Ok. 60 podmiotów świadczących łącznie ok. 2000 usług	Na podstawie ilości zidentyfikowanej dla potrzeb zmian profilu zaufanego w 2016 r.	Możliwość dostosowania usług wymagających tylko uwierzytelniania, tak by nie wymagały składania podpisu elektronicznego opartego o profil zaufany.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt ustawy zostanie zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny", oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Projekt ustawy zostanie skierowany do konsultacji publicznych i opiniowania z terminem 21 dni na zgłaszanie uwag. W ramach konsultacji publicznych i opiniowania projekt otrzymają:

1. Generalny Inspektor Ochrony Danych Osobowych (GIODO);
2. Prokuratoria Generalna Rzeczypospolitej Polskiej;
3. Zakład Ubezpieczeń Społecznych (ZUS);
4. Polski Komitet Normalizacyjny (PKN);
5. Polskie Towarzystwo Informatyczne (PTI);
6. Polska Izba Informatyki i Telekomunikacji (PIIT);
7. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT);
8. Stowarzyszenie Instytutu Informatyki Śledczej;
9. Fundacja Panoptykon;
10. Polska Izba Komunikacji Elektronicznej;
11. Internet Society Poland;
12. Związek Pracodawców Branży Internetowej IAB Polska;
13. Instytut Logistyki i Magazynowania (ILiM;
14. Rada Główna Instytutów Badawczych (RGIB);
15. Izba Gospodarki Elektronicznej;
16. Polska Izba Informatyki Medycznej;
17. Ogólnopolskie Porozumienie Organizacji Samorządowych;
18. Konfederacja Lewiatan;
19. Federacja Przedsiębiorców Polskich;
20. Poczta Polska S. A.;
21. Stowarzyszenie Archiwizjoner.

6. Wpływ na sektor finansów publicznych												
(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	60,9
budżet państwa	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	60,9
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	6,09	60,9
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Budżet państwa
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projektowane zmiany rozporządzenia mają charakter techniczny i będą służyć dostosowaniu jego przepisów do rozwiązań wynikających z projektowanej ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UD 244). Bieżące utrzymanie profilu zaufanego wymaga zapewnienie funkcjonowania dwóch podsystemów: 1) tzw. podsystemu DT dającego możliwość założenia konta o wybranym przez użytkownika sposobie logowania, na stronie pz.gov.pl lub epuap.gov.pl (pierwszy składnik uwierzytelniania); 2) tzw. podsystemu PZ dającego możliwość potwierdzenia tożsamości dla konta w systemie DT oraz dodanie numeru telefonu komórkowego, na który będą przesyłane smsami jednorazowe kody (drugi składnik uwierzytelniania). Podsystemy te muszą ponadto skutecznie i bezpiecznie komunikować się z systemami przedsiębiorców, którzy uzyskali zgody na nieodpłatne wykorzystywanie do identyfikacji i uwierzytelniania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w ich systemach na podstawie art. 19a ust. 2a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. W ramach umowy utrzymaniowej zawartej 27 grudnia 2017 r. pomiędzy MC i COI na okres trzech lat, przewidziano stała kwotę na bieżące utrzymanie ww. systemu 10 034 431,17 brutto oraz kwotę na rozwój systemu 8 236 610,95 zł brutto, co łącznie oznacza, że roczne utrzymanie i zapewnienie możliwości rozwoju profilu zaufanego wynosić będzie do 6,09 mln zł. Prace dostosowawcze wynikające ze zmian w stosunku do obecnie obowiązującego rozporządzenia polegające między innymi na wyodrębnieniu podpisu zaufanego (usługi zaufania) od środka identyfikacji elektronicznej jakim jest profil zaufany pozwalające wykorzystywać profil zaufany do uwierzytelniania bez potrzeby podpisywania będą realizowane w ramach środków rozwojowych. Koszty utrzymania Profilu Zaufanego zostały określone w OSR do ustawy o zmianie ustawy o o usługach zaufania oraz identyfikacji elektronicznej.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	budżet państwa	Systemy teleinformatyczne zapewniające możliwość skorzystania z usług online, w których wymaga się uwierzytelnienia profilem zaufanym ePUAP będą mogły być dostosowane w taki sposób by nie wymagały w tym celu złożenia podpisu zaufanego (obecnie podpis potwierdzony profilem zaufanym ePUAP). Dostosowanie odbędzie się w ramach prac mających na celu przyłączenie tych systemów do węzła krajowego. Zakres takich działań będzie zależny od możliwości systemów teleinformatycznych użytkowanych przez dany podmiot, dotychczas stosowanych sposobów wykorzystywania profilu zaufanego oraz możliwości organizacyjno-technicznych po stronie tych systemów.						
	duże przedsiębiorstwa	Brak wpływu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Brak wpływu.						
	rodzina, obywatele oraz gospodarstwa domowe	Brak wpływu.						
Niemierzalne	odbiorcy usług	Brak wpływu.						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		Umowa na świadczenie usług utrzymania oraz usług rozwoju z dnia 27.12.2017 r. zawarta pomiędzy Ministrem Cyfryzacji a Centralnym Ośrodkiem Informatyki. Koncepcja notyfikacji Profilu Zaufanego (ekspertyza z dnia 17.02.2017 r. wykonana na zamówienie Centralnego Ośrodka Informatyki).						

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: audyty na koszt kwalifikowanego dostawcy usług zaufania raz na dwa lata, obowiązek raportowania incydentów
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

Komentarz:
9. Wpływ na rynek pracy
0
10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	

11. Planowane wykonanie przepisów aktu prawnego
1.8.2018 r.
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
Nie dotyczy.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)