

U S T A W A

z dnia

o usługach zaufania oraz identyfikacji elektronicznej^{1), 2)}

¹⁾ Niniejsza ustawa służy stosowaniu 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 253 z 28.08.2014, str. 73).

²⁾ 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 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, ustawę z dnia 26 maja 1982 r. – Prawo o adwokaturze, ustawę z dnia 6 lipca 1982 r. o radcach prawnych, ustawę z dnia 15 listopada 1984 r. o podatku rolnym, ustawę z dnia 8 marca 1990 r. o samorządzie gminnym, ustawę z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych, ustawę z dnia 6 grudnia 1996 r. o zastawie rejestrowym i rejestrze zastawów, ustawę z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, ustawę z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 5 czerwca 1998 r. o samorządzie powiatowym, 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 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, ustawę z dnia 15 września 2000 r. – Kodeks spółek handlowych, ustawę z dnia 29 listopada 2000 r. – Prawo atomowe, ustawę z dnia 11 kwietnia 2001 r. o rzecznikach patentowych, ustawę z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym, 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 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego, ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, ustawę z dnia 30 października 2002 r. o podatku leśnym, 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 28 listopada 2003 r. o wspieraniu rozwoju obszarów wiejskich ze środków pochodzących z Sekcji Gwarancji Europejskiego Funduszu Orientacji i Gwarancji Rolnej, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 11 marca 2004 r. o podatku od towarów i usług, ustawę z dnia 20 kwietnia 2004 r. o organizacji rynku mleka i przetworów mlecznych, ustawę z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, ustawę z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, ustawę z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 8 lipca 2005 r. o Prokuraturii Generalnej Skarbu Państwa, ustawę z dnia 29 lipca 2005 r. o systemie tachografów cyfrowych, ustawę z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia, ustawę z dnia 7 marca 2007 r. o wspieraniu rozwoju obszarów wiejskich z udziałem środków Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich w ramach Programu Rozwoju Obszarów Wiejskich na lata 2007–2013, ustawę z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów, ustawę z dnia 10 lipca 2008 r. o odpadach wydobywczych, ustawę z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko, ustawę z dnia 25 czerwca 2009 r. o rolnictwie ekologicznym, ustawę z dnia 20 maja 2010 r. o wyrobach medycznych, ustawę z dnia 6 sierpnia 2010 r. o dowodach osobistych, ustawę z dnia 5 stycznia 2011 r. o kierujących

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa:

- 1) krajową infrastrukturę zaufania;
- 2) działalność dostawców usług zaufania, w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych;
- 3) tryb notyfikacji krajowego systemu identyfikacji elektronicznej;
- 4) nadzór nad dostawcami usług zaufania.

2. Przepisów ustawy nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników.

Art. 2. Ilekroć w ustawie jest mowa o:

- 1) dostawcy usług zaufania – należy przez to rozumieć osobę fizyczną lub osobę prawną, o której mowa w art. 3 pkt 19 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 uchylającej dyrektywę 1999/93/WE (Dz. Urz. UE L 253 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”;

pojazdami, 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 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 zbiorów 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 11 lipca 2014 r. o petycjach, ustawę z dnia 28 listopada 2014 r. – Prawo o aktach stanu cywilnego, ustawę z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny, ustawę z dnia 5 lutego 2015 r. o płatnościach w ramach systemów wsparcia bezpośredniego, ustawę z dnia 20 lutego 2015 r. o wspieraniu rozwoju obszarów wiejskich z udziałem środków Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich w ramach Programu Rozwoju Obszarów Wiejskich na lata 2014–2020, ustawę z dnia 20 lutego 2015 r. o odnawialnych źródłach energii, 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. – Prawo restrukturyzacyjne, ustawę z dnia 12 czerwca 2015 r. o systemie handlu uprawnieniami do emisji gazów cieplarnianych, ustawę z dnia 25 czerwca 2015 r. – Prawo konsularne, ustawę z dnia 10 lipca 2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, ustawę z dnia 9 października 2015 r. o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, ustawę z dnia 9 października 2015 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw, ustawę z dnia 28 stycznia 2016 r. – Prawo o prokuraturze, ustawę z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci oraz ustawę z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.

- 2) elektronicznym znaczniku czasu – należy przez to rozumieć znacznik, o którym mowa w art. 3 pkt 33 rozporządzenia 910/2014;
- 3) identyfikacji elektronicznej – należy przez to rozumieć proces, o którym mowa w art. 3 pkt 1 rozporządzenia 910/2014;
- 4) jednostkę oceniającą zgodność – należy przez to rozumieć jednostkę, o której mowa w art. 3 pkt 18 rozporządzenia 910/2014;
- 5) kwalifikowanym dostawcy usług zaufania – należy przez to rozumieć dostawcę usług zaufania, o którym mowa w art. 3 pkt 20 rozporządzenia 910/2014;
- 6) kwalifikowanym podpisie elektronicznym – należy przez to rozumieć zaawansowany podpis elektroniczny, o którym mowa w art. 3 pkt 12 rozporządzenia 910/2014;
- 7) kwalifikowanej pieczęci elektronicznej – należy przez to rozumieć zaawansowaną pieczęć elektroniczną, o której mowa w art. 3 pkt 27 rozporządzenia 910/2014;
- 8) kwalifikowanej usłudze zaufania – należy przez to rozumieć usługę zaufania, o której mowa w art. 3 pkt 17 rozporządzenia 910/2014;
- 9) niekwalifikowanym dostawcy usług zaufania – należy przez to rozumieć dostawcę usług zaufania, który nie jest kwalifikowanym dostawcą usług zaufania, w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014;
- 10) niekwalifikowanej usłudze zaufania – należy przez to rozumieć usługę zaufania, która nie jest kwalifikowaną usługą zaufania w rozumieniu art. 3 pkt 17 rozporządzenia 910/2014;
- 11) pieczęci elektronicznej – należy przez to rozumieć pieczęć, o której mowa w art. 3 pkt 25 rozporządzenia 910/2014;
- 12) podpisie elektronicznym – należy przez to rozumieć podpis w rozumieniu art. 3 pkt 10 rozporządzenia 910/2014;
- 13) systemie identyfikacji elektronicznej – należy przez to rozumieć system, o którym mowa w art. 3 pkt 4 rozporządzenia 910/2014;
- 14) środka identyfikacji elektronicznej – należy przez to rozumieć środek, o którym mowa w art. 3 pkt 2 rozporządzenia 910/2014;
- 15) usłudze zaufania – należy przez to rozumieć usługę, o której mowa w art. 3 pkt 16 rozporządzenia 910/2014;
- 16) uwierzytelnianiu – należy przez to rozumieć proces, o którym mowa w art. 3 pkt 5 rozporządzenia 910/2014;

- 17) zaawansowanej pieczęci elektronicznej – należy przez to rozumieć pieczęć elektroniczną, o której mowa w art. 3 pkt 26 rozporządzenia 910/2014;
- 18) zaawansowanym podpisie elektronicznym – należy przez to rozumieć podpis elektroniczny, o którym mowa w art. 3 pkt 11 rozporządzenia 910/2014;
- 19) zaufanej liście – należy przez to rozumieć listę kwalifikowanych dostawców usług zaufania, o której mowa w art. 22 ust. 1 rozporządzenia 910/2014.

Rozdział 2

Krajowa infrastruktura zaufania

Art. 3. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje:

- 1) rejestr dostawców usług zaufania, zwany dalej „rejestr”;
- 2) zaufaną listę;
- 3) narodowe centrum certyfikacji.

Art. 4. 1. Rejestr jest prowadzony w postaci elektronicznej.

2. Rejestr jest jawny. Każdy ma prawo dostępu do danych zawartych w rejestrze.

3. Do rejestru wpisuje się dostawców usług zaufania, którzy mają siedzibę lub oddział na terytorium Rzeczypospolitej Polskiej, oraz usługi zaufania świadczone przez tych dostawców.

4. Do rejestru wpisuje się:

- 1) imię i nazwisko lub firmę (nazwę) dostawcy usług zaufania;
- 2) adres siedziby i miejsca wykonywania działalności;
- 3) numer w Krajowym Rejestrze Sądowym – w przypadku dostawców usług zaufania podlegających wpisowi do tego rejestru;
- 4) numer identyfikacji podatkowej;
- 5) nazwę polityki świadczenia usług;
- 6) rodzaj świadczonych usług zaufania;
- 7) datę rozpoczęcia świadczenia usługi zaufania;
- 8) datę zakończenia świadczenia usługi zaufania;
- 9) informację o wystawionych certyfikatach, o których mowa w art. 11 pkt 1;
- 10) nazwę i adres zakładu ubezpieczeń, z którym dostawca usług zaufania zawarł umowę ubezpieczenia, okres, na jaki umowa ta została zawarta, oraz sumę ubezpieczenia;

- 11) informacje o zamiarze zaprzestania prowadzenia działalności w zakresie świadczenia usług zaufania lub zamiarze ograniczenia zakresu świadczonych usług zaufania;
- 12) informacje o otwarciu likwidacji dostawcy usług zaufania oraz datę jego likwidacji;
- 13) informacje o ogłoszeniu upadłości dostawcy usług zaufania lub oddaleniu wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, z późn. zm.³⁾) oraz datę zakończenia postępowania upadłościowego;
- 14) datę wykreślenia z rejestru dostawcy usług zaufania.

Art. 5. 1. Wpis do rejestru:

- 1) dostawcy usług zaufania, który zamierza świadczyć kwalifikowane usługi zaufania, lub
 - 2) kwalifikowanej usługi zaufania
- następuje na wniosek dostawcy usług zaufania.

2. Wniosek o wpis, o którym mowa w ust. 1, zawiera dane i informacje, o których mowa w art. 4 ust. 4 pkt 1–7.

3. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej formularz elektroniczny wniosku o wpis, o którym mowa w ust. 1.

4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej, dokumenty lub ich kopie:

- 1) raport z oceny zgodności, o którym mowa w art. 21 rozporządzenia 910/2014, wydany przez jednostkę oceniającą zgodność;
- 2) politykę świadczenia usług objętych wnioskiem, zgodnie z którą mają być świadczone usługi zaufania;
- 3) plan zakończenia działalności, o którym mowa w art. 24 ust. 2 lit. i rozporządzenia 910/2014;
- 4) dane niezbędne do wystawienia certyfikatu, o którym mowa w art. 11 pkt 1.

5. Minister właściwy do spraw informatyzacji, po rozpatrzeniu wniosku, o którym mowa w ust. 1, wydaje decyzję o wpisie:

- 1) dostawcy usług zaufania i świadczonych przez niego usług zaufania do rejestru, jeżeli spełniają wymagania określone w przepisach o usługach zaufania;

³⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 978, 1259 i 1844 oraz z 2016 r. poz. 615.

2) kwalifikowanej usługi zaufania do rejestru, w przypadku gdy usługa spełnia wymagania określone w przepisach o usługach zaufania.

6. Decyzja o wpisie, o którym mowa w ust. 5, zawiera informacje podlegające wpisowi do rejestru.

Art. 6. 1. Decyzja, o której mowa w art. 5 ust. 5, jest podstawą do wydania certyfikatu, o którym mowa w art. 11 pkt 1, oraz dokonania wpisu na zaufaną listę i oznacza nadanie statusu kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego usłudze.

2. Minister właściwy do spraw informatyzacji prowadzi zaufaną listę.

Art. 7. 1. Wpis do rejestru:

1) dostawcy usług zaufania świadczącego co najmniej jedną niekwalifikowaną usługę zaufania lub

2) niekwalifikowanej usługi zaufania

– następuje na podstawie zgłoszenia przesłanego w postaci elektronicznej przez dostawcę usług zaufania.

2. Niekwalifikowany dostawca usług zaufania w zgłoszeniu, o którym mowa w ust. 1, zgłasza co najmniej informacje, o których mowa w art. 4 ust. 4 pkt 1–6 i 10.

Art. 8. Dostawca usług zaufania wpisany do rejestru jest obowiązany informować ministra właściwego do spraw informatyzacji o:

1) każdej zmianie danych wpisanych do rejestru – w terminie 14 dni od zmiany tych danych;

2) zamiarze zaprzestania świadczenia kwalifikowanych usług zaufania, 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.

Art. 9. 1. Minister właściwy do spraw informatyzacji wykreśla dostawcę kwalifikowanych usług zaufania lub świadczoną przez niego usługę zaufania z rejestru w drodze decyzji.

2. Decyzja o wykreśleniu z rejestru kwalifikowanego dostawcy usług zaufania oznacza odebranie statusu kwalifikowanego temu dostawcy.

3. Decyzja o wykreśleniu z rejestru kwalifikowanej usługi zaufania oznacza odebranie tej usłudze statusu kwalifikowanego.

4. Minister właściwy do spraw informatyzacji wydaje decyzję o wykreśleniu z rejestru kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego kwalifikowanej usługi zaufania w przypadku:

- 1) złożenia przez tego dostawcę wniosku o wykreślenie z rejestru;
- 2) wykorzystywania certyfikatów, o których mowa w art. 11 pkt 1, w sposób wykraczający poza zakres ich stosowania;
- 3) o którym mowa w art. 20 ust. 3 rozporządzenia 910/2014;
- 4) zaprzestania działalności przez dostawcę kwalifikowanych usług zaufania.

5. Decyzja o wykreśleniu, o której mowa w ust. 1, jest podstawą wykreślenia dostawcy usług zaufania z listy zaufania oraz może być podstawą do unieważnienia certyfikatów, o których mowa w art. 11 pkt 1.

6. Minister właściwy do spraw informatyzacji wykreśla dostawcę świadczącego niekwalifikowane usługi zaufania z rejestru w przypadku ustalenia, że zaprzestał on świadczenia usług zaufania.

Art. 10. 1. Decyzja o wykreśleniu kwalifikowanego dostawcy usług zaufania z rejestru oraz decyzja o wykreśleniu wpisu kwalifikowanej usługi zaufania z rejestru podlega natychmiastowemu wykonaniu. Przepisu art. 61 § 2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2016 r. poz. 718 i 846) nie stosuje się.

2. W przypadku wykreślenia dostawcy usług zaufania z rejestru w rejestrze pozostawia się informacje o dostawcy i świadczonych przez niego usługach.

Art. 11. 1. Narodowe centrum certyfikacji:

- 1) tworzy i wydaje kwalifikowanym dostawcom usług zaufania certyfikaty służące do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa w załączniku I lit. g, załączniku III lit. g i załączniku IV lit. h do rozporządzenia 910/2014, oraz certyfikatów służących do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców, zwanych dalej „certyfikatami dostawcy usługi zaufania”;
- 2) publikuje certyfikaty, o których mowa w pkt 1;
- 3) publikuje listy unieważnionych certyfikatów, o których mowa w pkt 1;

4) tworzy dane do opatrywania pieczęcią elektroniczną certyfikatów, o których mowa w pkt 1, oraz certyfikatów do weryfikacji tych pieczęci, zwanych dalej „certyfikatami narodowego centrum certyfikacji”.

2. Narodowe centrum certyfikacji realizuje zadania, o których mowa w ust. 1, zgodnie z polityką certyfikacji.

Art. 12. 1. Na wniosek Prezesa Narodowego Banku Polskiego, minister właściwy do spraw informatyzacji może upoważnić Narodowy Bank Polski do realizacji zadań, o których mowa w art. 11, jak również do prowadzenia rejestru i zaufanej listy.

2. W przypadku upoważnienia do realizacji zadań, o których mowa w art. 11, polityka certyfikacji narodowego centrum certyfikacji podlega uzgodnieniu z ministrem właściwym do spraw informatyzacji.

3. W przypadku upoważnienia do realizacji zadań, o których mowa w art. 11, minister właściwy do spraw informatyzacji przekazuje do Narodowego Banku Polskiego kopie dokumentów stanowiących podstawę wpisu do rejestru lub wykreślenia z rejestru albo zmian wpisów w rejestrze.

Art. 13. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia:

- 1) wymagania organizacyjno-techniczne krajowej infrastruktury zaufania,
- 2) szczegółową treść wpisów w rejestrze oraz sposób ich dokonywania,
- 3) tryb wydawania i unieważniania certyfikatów dostawcy usługi zaufania oraz certyfikatów narodowego centrum certyfikacji,
- 4) wymagania dla polityki certyfikacji narodowego centrum certyfikacji,
- 5) wymagania bezpieczeństwa krajowej infrastruktury zaufania

– uwzględniając konieczność zapewnienia ochrony tajemnicy przedsiębiorstwa i interesów odbiorców usług zaufania oraz interoperacyjność systemów stosowanych przez dostawców usług zaufania oraz krajową infrastrukturę zaufania.

Rozdział 3

Działalność dostawców usług zaufania

Art. 14. 1. Kwalifikowany dostawca usług zaufania jest obowiązany posiadać zawartą umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania.

2. Kwalifikowany dostawca usług zaufania jest obowiązany zawrzeć umowę, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania wpisu kwalifikowanej usługi zaufania

do rejestru, nie później jednak niż jeden dzień przed dniem rozpoczęcia świadczenia tej usługi.

3. Kwalifikowany dostawca usług zaufania jest obowiązany, w terminie 30 dni od dnia doręczenia decyzji o wpisie do rejestru, przekazać ministrowi właściwemu do spraw informatyzacji, drogą elektroniczną, kopię umowy, o której mowa w ust. 1.

4. Kwalifikowany dostawca usług zaufania jest obowiązany, w terminie 7 dni od dnia upływu okresu ubezpieczenia, przekazać ministrowi do spraw informatyzacji, drogą elektroniczną, kopię kolejnej umowy ubezpieczenia.

5. Minister właściwy do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw informatyzacji, po zasięgnięciu opinii Polskiej Izby Ubezpieczeń, określi, w drodze rozporządzenia, szczegółowy zakres ubezpieczenia, o którym mowa w ust. 1, oraz minimalną sumę gwarancyjną, uwzględniając specyfikę działalności prowadzonej przez kwalifikowanych dostawców usług zaufania.

Art. 15. Kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie.

Art. 16. 1. Informacje i dane związane ze świadczeniem usług zaufania, których ujawnienie mogłoby narazić na szkodę dostawcę usług zaufania lub odbiorcę usług zaufania, w szczególności dane do składania podpisów elektronicznych lub pieczęci elektronicznych, są objęte tajemnicą.

2. Tajemnicą, o której mowa w ust. 1, nie są objęte informacje o naruszeniach przepisów o usługach zaufania przez dostawcę usług zaufania oraz informacje o naruszeniach bezpieczeństwa i utracie integralności, o których mowa w art. 19 ust. 2 rozporządzenia 910/2014.

3. Do zachowania tajemnicy, o której mowa w ust. 1, są obowiązane:

- 1) osoby pozostające z dostawcą usług zaufania w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze;
- 2) osoby pozostające z podmiotami świadczącymi usługi na rzecz dostawcy usług zaufania w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze.

4. Osoby, o których mowa w ust. 3, mają obowiązek udzielenia informacji i danych, o których mowa w ust. 1, z wyjątkiem danych do składania podpisów elektronicznych lub pieczęci elektronicznych, wyłącznie na żądanie:

- 1) sądu lub prokuratora – w związku z toczącym się postępowaniem;
- 2) ministra właściwego do spraw informatyzacji – w związku ze sprawowaniem przez niego nadzoru nad działalnością dostawców usług zaufania;
- 3) innych upoważnionych organów – w związku z prowadzonym przez te organy postępowaniem.

5. Obowiązek zachowania tajemnicy, o której mowa w ust. 1, trwa przez 10 lat od dnia ustania stosunku prawnego, o którym mowa w ust. 3.

6. Obowiązek zachowania w tajemnicy danych do składania podpisu elektronicznego lub pieczęci elektronicznej jest nieograniczony w czasie.

Art. 17. Zaawansowany podpis elektroniczny lub zaawansowana pieczęć elektroniczna weryfikowane za pomocą certyfikatu dostawcy usług zaufania służą do opatrywania podpisem elektronicznym lub pieczęcią elektroniczną:

- 1) certyfikatów kwalifikowanych, o których mowa w załączniku I lit. g, załączniku III lit. g oraz załączniku IV lit. h do rozporządzenia 910/2014;
- 2) informacji o statusie certyfikatów kwalifikowanych, w tym listy zawieszonych lub unieważnionych certyfikatów;
- 3) innych certyfikatów związanych ze świadczeniem kwalifikowanych usług zaufania.

Art. 18. 1. Kwalifikowany dostawca usług zaufania przechowuje następujące dokumenty i dane związane ze świadczeniem usług zaufania:

- 1) potwierdzenie, o którym mowa w art. 15,
- 2) listy zawieszonych i unieważnionych kwalifikowanych certyfikatów,
- 3) politykę świadczenia usługi,
- 4) żądania unieważnienia kwalifikowanego certyfikatu,
- 5) inne dokumenty, o ile polityka świadczenia usługi wymagała ich utworzenia i przechowywania

– w sposób umożliwiający odczytanie oraz zapewniający bezpieczeństwo przechowywanych dokumentów i danych.

2. Kwalifikowany dostawca usług zaufania jest obowiązany przechowywać dokumenty i dane, o których mowa w ust. 1, z wyłączeniem danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej, przez 20 lat od dnia ich wytworzenia.

Art. 19. 1. Podpis elektroniczny lub pieczęć elektroniczna weryfikowane za pomocą certyfikatu wywołują skutki prawne, jeżeli zostały złożone w okresie ważności tego certyfikatu.

2. Podpis elektroniczny lub pieczęć elektroniczna złożone w okresie zawieszenia certyfikatu wykorzystywanego do jego weryfikacji nie wywołują skutków prawnych. Informacja o zawieszeniu certyfikatu jest udostępniana w ramach usługi informowania o statusie certyfikatu.

3. Po uchyleniu zawieszenia certyfikatu, skutek prawny podpisu elektronicznego lub pieczęci weryfikowanych tym certyfikatem złożonych w trakcie zawieszenia następuje z chwilą uchylenia tego zawieszenia.

Art. 20. 1. Dostawca usług zaufania jest obowiązany posiadać politykę świadczenia usługi.

2. Polityka świadczenia usługi stanowi nazwany zestaw reguł, w szczególności takich jak polityka certyfikacji, określający zasady świadczenia usługi, odpowiedzialność stron, zasady postępowania z danymi i mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa, opracowywany na podstawie norm lub standardów określających wymagania dla polityk świadczenia usług.

3. Kwalifikowany dostawca usług zaufania jest obowiązany posiadać plan zakończenia działalności oraz zastosować ten plan do zakończenia działalności.

Art. 21. 1. W przypadku gdy kwalifikowany dostawca usług zaufania utracił status kwalifikowany i żaden inny podmiot kwalifikowany nie przejął jego działalności w zakresie świadczenia usług zaufania, przekazuje on dokumenty i dane, o których mowa w art. 18 ust. 1, ministrowi właściwemu do spraw informatyzacji w terminie 30 dni od dnia utraty statusu kwalifikowanego.

2. Minister właściwy do spraw informatyzacji przechowuje dokumenty i dane, o których mowa w art. 18 ust. 1, do końca okresu, o którym mowa w art. 18 ust. 2.

3. Kwalifikowany dostawca usług zaufania niszczy niezwłocznie dane do składania przez niego zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej weryfikowanych za pomocą certyfikatu dostawcy usług zaufania, w przypadku

gdy polityka świadczenia usługi nie przewiduje dalszego wykorzystania tych danych lub w przypadku unieważnienia certyfikatu dostawcy usług zaufania powiązanego z tymi danymi.

4. Kwalifikowany dostawca usług zaufania z czynności, o których mowa w ust. 3, sporządza protokół zniszczenia danych i przekazuje go ministrowi właściwemu do spraw informatyzacji w terminie 7 dni od wykonania tych czynności.

Art. 22. Dostawca usług zaufania nie odpowiada za szkody wynikające z nieprzestrzegania przez odbiorcę usług zaufania zasad określonych w polityce świadczenia usługi, w szczególności za szkody wynikające z:

- 1) użycia certyfikatu niezgodnie z zakresem określonym w polityce świadczenia usługi wskazanej w certyfikacie, w tym za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została wskazana w certyfikacie;
- 2) nieprawdziwości danych zawartych w certyfikacie, podanych przez odbiorcę usług zaufania używającego tego certyfikatu, chyba że szkoda była wynikiem niedołożenia należytej staranności przez dostawcę usług zaufania;
- 3) przechowywania lub używania przez odbiorców usług zaufania danych do składania podpisu elektronicznego, pieczęci elektronicznej lub uwierzytelniania witryn internetowych w sposób niezapewniający ich ochrony przed nieuprawnionym wykorzystaniem.

Rozdział 4

Identyfikacja elektroniczna

Art. 23. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowego węzła identyfikacji, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014.

2. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, warunki organizacyjno-techniczne udostępniania krajowego węzła identyfikacji, mając na uwadze potrzebę zapewnienia interoperacyjności systemów identyfikacji elektronicznej, wykorzystywanych do uwierzytelniania osób w usługach online.

Art. 24. Minister właściwy do spraw informatyzacji koordynuje działania na poziomie krajowym na rzecz współpracy z państwami członkowskimi Unii Europejskiej w sprawach dotyczących systemów identyfikacji elektronicznej, prowadzonej zgodnie z art. 12 ust. 5 i 6 rozporządzenia 910/2014, w szczególności zapewniając obsługę pojedynczego punktu

kontaktowego, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 7 tego rozporządzenia.

Art. 25. 1. Wniosek o notyfikowanie krajowego systemu identyfikacji elektronicznej w Komisji Europejskiej składa do ministra właściwego do spraw informatyzacji podmiot odpowiedzialny za ten system.

2. Do wniosku, o którym mowa w ust. 1, załącza się formularz notyfikacji systemu identyfikacji elektronicznej zgodny ze wzorem określonym w przepisach wykonawczych wydanych na podstawie art. 9 ust. 5 rozporządzenia 910/2014.

3. Minister właściwy do spraw informatyzacji zgłasza krajowy 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.

4. Minister właściwy do spraw informatyzacji zgłasza krajowy 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.

5. Minister właściwy do spraw informatyzacji może powierzyć wykonywanie zadań, o których mowa w ust. 3 i 4, podmiotowi publicznemu w rozumieniu art. 2 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352).

Art. 26. Podmiot udostępniający usługę publiczną online określa wymagane poziomy bezpieczeństwa, o których mowa w art. 8 rozporządzenia 910/2014, dla środków identyfikacji elektronicznej, niezbędne dla realizacji tej usługi, oraz udostępnia informację o tych wymaganiach.

Art. 27. 1. Obowiązki, o których mowa w art. 10 rozporządzenia 910/2014, wykonuje minister właściwy do spraw informatyzacji.

2. Informacje dotyczące naruszenia bezpieczeństwa notyfikowanego krajowego systemu identyfikacji elektronicznej albo systemu uwierzytelnienia, o którym mowa w art. 10 rozporządzenia 910/2014, zarządzający tymi systemami przekazują niezwłocznie, drogą elektroniczną, ministrowi właściwemu do spraw informatyzacji.

Rozdział 5

Nadzór nad dostawcami usług zaufania

Art. 28. 1. Nadzór nad dostawcami usług zaufania sprawuje minister właściwy do spraw informatyzacji.

2. W zakresie nadzoru, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji:

- 1) wykonuje zadania określone w przepisach rozporządzenia 910/2014;
- 2) wydaje certyfikaty dostawców usług zaufania;
- 3) tworzy certyfikaty narodowego centrum certyfikacji;
- 4) może unieważniać certyfikaty, o których mowa w pkt 2 i 3;
- 5) może żądać niezwłocznego unieważnienia kwalifikowanego certyfikatu przez kwalifikowanego dostawcę usług zaufania;
- 6) bada zgodność polityki świadczenia usługi z przepisami o usługach zaufania;
- 7) prowadzi rejestr dostawców usług zaufania;
- 8) nakłada kary pieniężne;
- 9) wykonuje inne zadania określone w przepisach prawa.

Art. 29. Dostawca usługi zaufania, na żądanie ministra właściwego do spraw informatyzacji, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych, jest obowiązany udzielać informacji lub udostępniać dokumenty, które są bezpośrednio związane ze świadczonymi usługami zaufania lub mają wpływ na świadczone usługi zaufania, w tym dotyczą zarządzania incydentami związanymi z usługą zaufania.

Art. 30. 1. W przypadku odebrania kwalifikowanemu dostawcy usługi zaufania statusu kwalifikowanego lub statusu kwalifikowanego świadczonej przez niego usłudze zaufania minister właściwy do spraw informatyzacji, w drodze decyzji, może unieważnić odpowiednie certyfikaty dostawcy usługi zaufania, wydane temu dostawcy.

2. Unieważniając certyfikaty dostawcy usługi zaufania, minister właściwy do spraw informatyzacji bierze pod uwagę stopień zagrożenia bezpieczeństwa świadczenia usług zaufania, możliwość usunięcia tego zagrożenia w inny sposób oraz pewność obrotu.

Art. 31. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że kwalifikowany dostawca usługi zaufania prowadzi działalność niezgodnie z przepisami o usługach zaufania, może:

- 1) wezwać kwalifikowanego dostawcę usług zaufania, aby w wyznaczonym terminie:
 - a) usunął stwierdzone nieprawidłowości i doprowadził swoją działalność do stanu zgodnego z przepisami o usługach zaufania,
 - b) zmienił politykę świadczenia usług lub inne dokumenty związane ze świadczeniem usług zaufania,
 - c) unieważnił kwalifikowane certyfikaty wydane z naruszeniem polityki świadczenia usług;
- 2) wydać decyzję o odebraniu kwalifikowanemu dostawcy usług zaufania statusu kwalifikowanego lub statusu kwalifikowanego świadczonej przez niego usłudze zaufania.

Art. 32. Audyt, o którym mowa w art. 20:

- 1) ust. 2 rozporządzenia 910/2014 – jest przeprowadzany przez osoby upoważnione przez ministra właściwego do spraw informatyzacji, zwane dalej „audytorami organu nadzoru”;
- 2) ust. 1 lub 2 rozporządzenia 910/2014 – może być przeprowadzany przy udziale osób upoważnionych przez ministra właściwego do spraw informatyzacji, zwanych dalej „obserwatorami organu nadzoru”, w przypadku gdy jest przeprowadzany przez jednostkę przeprowadzającą zgodność.

Art. 33. 1. Audytorzy organu nadzoru oraz obserwatorzy organu nadzoru odpowiednio przeprowadzają audyt albo biorą udział w przeprowadzeniu audytu na podstawie imiennego upoważnienia wydanego przez ministra właściwego do spraw informatyzacji.

2. Audytorzy organu nadzoru i obserwatorzy organu nadzoru nie mogą prowadzić działalności gospodarczej w zakresie świadczenia usług zaufania, świadczyć usług zaufania, być współnikami albo akcjonariuszami dostawcy usług zaufania ani wykonywać obowiązków osoby reprezentującej lub członka rady nadzorczej albo komisji rewizyjnej tego dostawcy, a także pozostawać z tym dostawcą w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze.

Art. 34. 1. Audytorzy organu nadzoru są uprawnieni do:

- 1) wstępu do obiektów i pomieszczeń kwalifikowanych dostawców usług zaufania;

- 2) wglądu do dokumentów i danych, z wyjątkiem danych do składania podpisów elektronicznych lub pieczęci elektronicznych dostawców usług zaufania i innych informacji, które mogą służyć do odtworzenia tych danych, związanych z działalnością w zakresie usług zaufania;
- 3) przetwarzania danych osobowych w zakresie objętym przedmiotem audytu;
- 4) przeprowadzania oględzin obiektów oraz innych składników majątkowych związanych ze świadczeniem usług zaufania, a także sprawdzenia przebiegu czynności związanych ze świadczeniem tych usług;
- 5) żądania udzielenia ustnych lub pisemnych wyjaśnień od pracowników kwalifikowanych dostawców usług zaufania;
- 6) zabezpieczania dokumentów i innych materiałów, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

2. Upoważniony przedstawiciel audytowanego kwalifikowanego dostawcy usług zaufania udziela wyjaśnień lub przedkłada, na żądanie audytora organu nadzoru, dokumenty i inne materiały niezbędne do przeprowadzenia audytu.

3. Przepisy ust. 1 pkt 1–4 stosuje się do obserwatorów organu nadzoru.

Art. 35. W przypadku gdy wyniki audytu przeprowadzanego na podstawie art. 20 ust. 2 rozporządzenia 910/2014 wykażą niezgodność z przepisami o usługach zaufania, minister właściwy do spraw informatyzacji, po zapoznaniu się z zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez dostawcę usług zaufania, może wydać decyzję nakładającą na tego dostawcę obowiązek usunięcia stwierdzonych niezgodności w terminie nie krótszym niż 14 dni.

Art. 36. Audytorzy organu nadzoru i obserwatorzy organu nadzoru są obowiązani do bezterminowego zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzaniem audytu, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

Art. 37. W sprawach nieuregulowanych w ustawie, do przeprowadzenia audytu dostawców usług zaufania przez audytorów organu nadzoru stosuje się odpowiednio przepisy

rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 584, z późn. zm.⁴⁾), z wyłączeniem przepisu art. 83 ust. 1.

Art. 38. 1. Minister właściwy do spraw informatyzacji może wyznaczyć podmiot badający zgodność kwalifikowanych urządzeń do składania podpisu elektronicznego lub pieczęci elektronicznej z wymogami, o których mowa w załączniku II do rozporządzenia 910/2014.

2. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej nazwę i adres wyznaczonego podmiotu, o którym mowa w ust. 1.

Art. 39. Minister właściwy do spraw informatyzacji może zawierać porozumienia z organami nadzoru innych państw członkowskich Unii Europejskiej w celu prowadzenia wspólnych postępowań, o których mowa w art. 18 ust. 3 rozporządzenia 910/2014.

Art. 40. Minister właściwy do spraw informatyzacji, w porozumieniu z innymi organami określonymi w art. 19 ust. 2 rozporządzenia 910/2014, ustala sposób zgłaszania drogą elektroniczną przypadków naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe.

Rozdział 6

Przepisy o karach administracyjnych

Art. 41. Karze pieniężnej podlega kwalifikowany dostawca usług zaufania, który:

- 1) nie wykonuje obowiązku wynikającego z art. 24 ust. 1 rozporządzenia 910/2014;
- 2) nie usunął w terminie określonym w wezwaniu, o którym mowa w art. 31 pkt 1 lit. a, stwierdzonych nieprawidłowości w prowadzonej przez siebie działalności;
- 3) stosuje politykę świadczenia usługi lub przyjmuje inne dokumenty związane ze świadczeniem usługi zaufania niezgodne z tymi przepisami;
- 4) nie unieważnia kwalifikowanych certyfikatów mimo wezwania ministra właściwego do spraw informatyzacji, o którym mowa w art. 31 pkt 1 lit. c;
- 5) wydaje certyfikaty niezgodnie z polityką świadczenia usługi;

⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 i 1893 oraz z 2016 r. poz. 65, 352, 615, 780 i 868.

- 6) nie udziela informacji lub nie udostępnia dokumentów w przypadku, o którym mowa w art. 29;
- 7) nie poinformował ministra właściwego do spraw informatyzacji o zmianie danych podlegających wpisowi do rejestru lub danych dotyczących technicznych możliwości prowadzenia działalności w zakresie świadczenia usług zaufania wskazanych we wniosku o wpis do rejestru;
- 8) nie wykonuje obowiązków informacyjnych, o których mowa w art. 19 ust. 2 rozporządzenia 910/2014;
- 9) uniemożliwia lub utrudnia audytorowi organu nadzoru wykonywanie czynności audytowych;
- 10) nie posiada planu zakończenia działalności lub nie stosuje go do zakończenia działalności;
- 11) nie wykona obowiązku, o którym mowa w art. 21 ust. 3 lub 4;
- 12) nie wykona obowiązku, o którym mowa w art. 14 ust. 1.

Art. 42. 1. Karę pieniężną, o której mowa w art. 41, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

2. Wysokość kary pieniężnej, o której mowa w art. 41:

- 1) pkt 1–9 i 12, wynosi do 50 000 zł;
- 2) pkt 10, wynosi do 10 000 zł;
- 3) pkt 11, wynosi do 100 000 zł.

Art. 43. Przy ustalaniu wysokości kary pieniężnej, o której mowa w art. 41, minister właściwy do spraw informatyzacji uwzględnia zakres, czas trwania i skutki naruszenia wymagań, o których mowa w przepisach o usługach zaufania.

Art. 44. Do kar pieniężnych stosuje się odpowiednio przepisy działu III i IV ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2015 r. poz. 613, z późn. zm.⁵⁾).

⁵⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 699, 978, 1197, 1269, 1311, 1649, 1923, 1932 i 2184 oraz z 2016 r. poz. 615 i 846.

Rozdział 7

Przepisy karne

Art. 45. 1. Kto składa kwalifikowany podpis elektroniczny lub zaawansowany podpis elektroniczny z wykorzystaniem danych do składania podpisu elektronicznego przyporządkowanych do innej osoby,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

2. Tej samej karze podlega ten, kto składa kwalifikowaną pieczęć elektroniczną lub zaawansowaną pieczęć elektroniczną, nie będąc do tego uprawnionym.

3. Tej samej karze podlega ten, kto składa zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną kwalifikowanego dostawcy usług zaufania za pomocą danych przyporządkowanych do tego podmiotu, nie będąc uprawnionym.

Art. 46. Kto bez uprawnienia kopiuje lub przechowuje nieprzyporządkowane do niego dane do składania zaawansowanego podpisu elektronicznego lub pieczęci elektronicznej lub inne dane, które mogłyby służyć do ich odtworzenia,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 47. 1. Kto, świadcząc usługi zaufania, wydaje certyfikat zawierający nieprawdziwe dane w celu popełnienia czynu zabronionego,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

2. Tej samej karze podlega ten, kto składa podpis elektroniczny lub pieczęć elektroniczną weryfikowane certyfikatem, o którym mowa w ust. 1.

Art. 48. Kto, świadcząc usługi zaufania, wbrew obowiązkowi, o którym mowa w art. 31 pkt 1 lit. c, celowo zaniecha unieważnienia certyfikatu,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 49. 1. Kto, będąc obowiązany do zachowania tajemnicy związanej ze świadczeniem usług zaufania, ujawnia lub wykorzystuje, wbrew warunkom określonym w przepisach o usługach zaufania, informacje objęte tą tajemnicą,

podlega grzywnie.

2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 jako kwalifikowany dostawca usług zaufania albo w celu osiągnięcia korzyści majątkowej lub osobistej,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 50. Kto, wydając środek identyfikacji elektronicznej w ramach notyfikowanego systemu identyfikacji elektronicznej, wydaje taki środek osobie nieuprawnionej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 51. Karom określonym w art. 45–50 podlega także ten, kto dopuszcza się czynów, o których mowa w tych przepisach, działając w imieniu lub w interesie innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Rozdział 8

Zmiany w przepisach

Art. 52. W ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23 i 868) wprowadza się następujące zmiany:

1) w art. 33:

a) § 2a otrzymuje brzmienie:

„§ 2a. Pełnomocnictwo w formie dokumentu elektronicznego powinno być opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”,

b) § 3a otrzymuje brzmienie:

„§ 3a. Jeżeli odpis pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie zostały sporządzone w formie dokumentu elektronicznego, ich uwierzytelnienia, o którym mowa w § 3, dokonuje się, opatrując odpisy kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Odpisy pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie uwierzytelniane elektronicznie są sporządzane w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;

2) w art. 46 w § 4 pkt 3 otrzymuje brzmienie:

„3) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym organu administracji publicznej, oraz informację o wymogu podpisania urzędowego poświadczenia odbioru w określony sposób.”;

3) w art. 54 § 2 otrzymuje brzmienie:

„§ 2. Wezwanie powinno być opatrzone podpisem pracownika organu wzywającego, z podaniem imienia, nazwiska i stanowiska służbowego podpisującego lub, jeżeli dokonywane jest z użyciem dokumentu elektronicznego, powinno być opatrzone kwalifikowanym podpisem elektronicznym.”;

4) w art. 63 w § 3a pkt 1 otrzymuje brzmienie:

„1) być opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, lub uwierzytelniane w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej.”;

5) w art. 73 § 3 otrzymuje brzmienie:

„§ 3. Organ administracji publicznej może zapewnić stronie dokonanie czynności, o których mowa w § 1, w swoim systemie teleinformatycznym, po uwierzytelnieniu strony w sposób określony w art. 20a ust. 1 albo 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;

6) w art. 76a § 2a otrzymuje brzmienie:

„§ 2a. Jeżeli odpis dokumentu został sporządzony w formie dokumentu elektronicznego, poświadczenie jego zgodności z oryginałem, o którym mowa w § 2, dokonuje się przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP. Odpisy dokumentów poświadczone elektronicznie sporządzane są w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;

7) w art. 107 § 1 otrzymuje brzmienie:

„§ 1. Decyzja powinna zawierać: oznaczenie organu administracji publicznej, datę wydania, oznaczenie strony lub stron, powołanie podstawy prawnej, rozstrzygnięcie, uzasadnienie faktyczne i prawne, pouczenie, czy i w jakim trybie służy od niej odwołanie, podpis z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do wydania decyzji lub, jeżeli decyzja wydana została w formie dokumentu elektronicznego, powinna być opatrzona kwalifikowanym podpisem elektronicznym. Decyzja, w stosunku do której może być wniesione powództwo do sądu powszechnego lub skarga do sądu administracyjnego, powinna zawierać ponadto pouczenie o dopuszczalności wniesienia powództwa lub skargi.”;

8) w art. 124 § 1 otrzymuje brzmienie:

„§ 1. Postanowienie powinno zawierać: oznaczenie organu administracji publicznej, datę jego wydania, oznaczenie strony lub stron albo innych osób biorących udział w postępowaniu, powołanie podstawy prawnej, rozstrzygnięcie, pouczenie, czy i w jakim trybie służy na nie zażalenie lub skarga do sądu administracyjnego, oraz podpis z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do jego wydania lub, jeżeli postanowienie wydane zostało w formie dokumentu elektronicznego, powinno być opatrzone kwalifikowanym podpisem elektronicznym.”;

9) w art. 217 § 4 otrzymuje brzmienie:

„§ 4. Zaświadczenie wydaje się w formie dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym, jeżeli zażąda tego osoba ubiegająca się o zaświadczenie.”;

10) w art. 220 § 3 otrzymuje brzmienie:

„§ 3. Jeżeli strona lub inny uczestnik postępowania nie może uzyskać w formie dokumentu elektronicznego zaświadczenia wymaganego do potwierdzenia faktów lub stanu prawnego lub innego dokumentu wydanego przez podmiot publiczny w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jak również potwierdzenia uiszczenia opłat i kosztów postępowania, strona lub inny uczestnik postępowania może złożyć elektroniczną kopię takiego dokumentu, po uwierzytelnieniu jej przez wnoszącego, przy użyciu kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP.”;

11) w art. 238 § 1 otrzymuje brzmienie:

„§ 1. Zawiadomienie o sposobie załatwienia skargi powinno zawierać: oznaczenie organu, od którego pochodzi, wskazanie, w jaki sposób skarga została załatwiona, oraz podpis z podaniem imienia, nazwiska i stanowiska służbowego osoby upoważnionej do załatwienia skargi lub, jeżeli zawiadomienie sporządzone zostało w formie dokumentu elektronicznego, powinno być opatrzone kwalifikowanym podpisem elektronicznym. Zawiadomienie o odmownym załatwieniu skargi powinno zawierać ponadto uzasadnienie faktyczne i prawne oraz pouczenie o treści art. 239.”.

Art. 53. W ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2014 r. poz. 101, z późn. zm.⁶⁾) wprowadza się następujące zmiany:

1) w art. 126 § 5 otrzymuje brzmienie:

„§ 5. Pismo procesowe wniesione za pośrednictwem systemu teleinformatycznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

2) w art. 505³⁰ § 2 otrzymuje brzmienie:

„§ 2. Czynności sądu, referendarza i przewodniczącego utrwalane są wyłącznie w systemie teleinformatycznym, a wytworzone w ich wyniku dane w postaci elektronicznej opatrywane są kwalifikowanym podpisem elektronicznym.”;

3) w art. 626⁴ § 1 otrzymuje brzmienie:

„§ 1. Notariusz, komornik oraz naczelnik urzędu skarbowego działający jako administracyjny organ egzekucyjny składa wnioski o wpis wyłącznie za pośrednictwem systemu teleinformatycznego. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

4) w art. 694³ § 3 otrzymuje brzmienie:

„§ 3. Wniosek złożony do sądu rejestrowego drogą elektroniczną opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

5) w art. 694⁴:

a) § 2 otrzymuje brzmienie:

„§ 2. Dokumenty, o których mowa w § 1, składane drogą elektroniczną, opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

b) § 3 otrzymuje brzmienie:

„§ 3. Wypisy aktów notarialnych, wyciągi, odpisy i poświadczenia dokumentów mogą być przesłane do sądu drogą elektroniczną, jeżeli notariusz opatrzył je kwalifikowanym podpisem elektronicznym.”;

⁶⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 293, 379, 435, 567, 616, 945, 1091, 1161, 1296, 1585, 1626, 1741 i 1924, z 2015 r. poz. 2, 4, 218, 539, 978, 1062, 1137, 1199, 1311, 1418, 1419, 1505, 1527, 1567, 1587, 1595, 1634 i 1854 oraz z 2016 r. poz. 868.

6) art. 816¹ otrzymuje brzmienie:

„Art. 816¹. Dane w postaci elektronicznej wytworzone w wyniku czynności komornika wymienionych w art. 797 § 4 i art. 816 § 2 opatrywane są kwalifikowanym podpisem elektronicznym.”.

Art. 54. W ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2016 r. poz. 599 i 868) w art. 27 § 4 otrzymuje brzmienie:

„§ 4. Tytuł wykonawczy przekazywany do organu egzekucyjnego przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej zawiera kwalifikowany podpis elektroniczny.”.

Art. 55. W ustawie z dnia 26 maja 1982 r. – Prawo o adwokaturze (Dz. U. z 2015 r. poz. 615, z późn.zm.⁷⁾) w art. 37b ust. 2 otrzymuje brzmienie:

„2. Dopuszcza się również komunikowanie się adwokata z sądem w elektronicznym postępowaniu upominawczym przy wykorzystaniu kwalifikowanego podpisu elektronicznego.”.

Art. 56. W ustawie z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. z 2016 r. poz. 233) w art. 229 ust. 2 otrzymuje brzmienie:

„2. Dopuszcza się również komunikowanie się radcy prawnego z sądem w elektronicznym postępowaniu upominawczym przy wykorzystaniu kwalifikowanego podpisu elektronicznego.”.

Art. 57. W ustawie z dnia 15 listopada 1984 r. o podatku rolnym (Dz. U. z 2016 r. poz. 617) w art. 6a w ust. 13 pkt 3 otrzymuje brzmienie:

„3) limity wysokości zobowiązania podatkowego, kwoty nadpłaty lub zwrotu podatku wynikające z deklaracji na podatek rolny, a także wymagania dla poszczególnych rodzajów podpisu elektronicznego, w szczególności dotyczące weryfikacji podpisu elektronicznego i wykorzystania elektronicznych znaczników czasu.”.

Art. 58. W ustawie z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2016 r. poz. 446) w art. 68 ust. 1d otrzymuje brzmienie:

„1d. Zgłoszenie, o którym mowa w ust. 1a, opatruje się kwalifikowanym podpisem elektronicznym.”.

⁷⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 1064, 1224, 1255 i 1311.

Art. 59. W ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2016 r. poz. 716) w art. 6 w ust. 15 pkt 3 otrzymuje brzmienie:

„3) limity wysokości zobowiązania podatkowego, kwoty nadpłaty lub zwrotu podatku wynikające z deklaracji na podatek od nieruchomości, a także wymagania dla poszczególnych rodzajów podpisu elektronicznego, w szczególności dotyczące weryfikacji podpisu elektronicznego i wykorzystania elektronicznych znaczników czasu.”.

Art. 60. W ustawie z dnia 6 grudnia 1996 r. o zastawie rejestrowym i rejestrze zastawów (Dz. U. z 2016 r. poz. 297) wprowadza się następujące zmiany:

1) w art. 39 ust. 2a otrzymuje brzmienie:

„2a. Wnioski składane drogą elektroniczną opatruje się kwalifikowanym podpisem elektronicznym. W aktach przechowuje się wydruk tych wniosków i załączniki dokumentów wraz ze wskazaniem osób, które je podpisały.”;

2) w art. 42 ust. 3a otrzymuje brzmienie:

„3a. Odpisy i zaświadczenia wydane drogą elektroniczną przez centralną informację o zastawach rejestrowych opatrzone kwalifikowanym podpisem elektronicznym, mają moc dokumentów urzędowych.”.

Art. 61. W ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2016 r. poz. 687) w art. 19 w ust. 2b zdanie pierwsze otrzymuje brzmienie:

„Wnioski składane drogą elektroniczną opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 62. W ustawie z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2015 r. poz. 1774 i 1777 oraz z 2016 r. poz. 65) w art. 158 ust. 2 otrzymuje brzmienie:

„2. W terminie nie dłuższym niż 2 miesiące od dnia sporządzenia operatu szacunkowego rzeczoznawca majątkowy przekazuje, z uwzględnieniem art. 175 ust. 3, wyciąg z wykonanego przez siebie operatu szacunkowego, zawierający dane, o których mowa w ust. 1, organom prowadzącym kataster nieruchomości za pośrednictwem elektronicznej platformy usług administracji publicznej, o której mowa w art. 3 pkt 13 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352), opatrując go

podpisem potwierdzonym profilem zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym.”.

Art. 63. W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2015 r. poz. 613, z późn. zm.⁸⁾) wprowadza się następujące zmiany:

- 1) w art. 3b w § 3 pkt 2 otrzymuje brzmienie:
 - „2) limity wysokości zobowiązania podatkowego, kwoty nadpłaty lub zwrotu podatku wynikających z deklaracji i rodzaj podatku, którego dotyczy deklaracja, a także wymagania dla poszczególnych rodzajów podpisu elektronicznego, w szczególności dotyczące weryfikacji podpisu i kwalifikowanych elektronicznych znaczników czasu.”;
- 2) 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 albo profilu zaufanego ePUAP w rozumieniu art. 3 pkt 15 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;
- 3) w art. 14c § 4 otrzymuje brzmienie:

„§ 4. Interpretację indywidualną wydaną w formie dokumentu elektronicznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;
- 4) w art. 138a:
 - a) § 3 otrzymuje brzmienie:

„§ 3. Pełnomocnictwo w formie dokumentu elektronicznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”,
 - b) § 5 otrzymuje brzmienie:

„§ 5. Jeżeli odpis pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie zostały sporządzone w formie dokumentu elektronicznego, ich uwierzytelnienia, o którym mowa w § 4, dokonuje się, opatrując odpisy kwalifikowanym podpisem elektronicznym albo podpisem

⁸⁾ Patrz odnośnik nr 5.

potwierdzonym profilem zaufanym ePUAP. Odpisy pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie uwierzytelniane elektronicznie są sporządzane w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;

5) w art. 143 § 1a otrzymuje brzmienie:

„§ 1a. Upoważnienie może obejmować podpisywanie pism w formie dokumentu elektronicznego kwalifikowanym podpisem elektronicznym.”;

6) w art. 144b § 1 i 2 otrzymują brzmienie:

„§ 1. W przypadku pism wydanych w formie dokumentu elektronicznego przy wykorzystaniu systemu teleinformatycznego ministra właściwego do spraw finansów publicznych, które zostały opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, doręczenie może polegać na doręczeniu wydruku pisma uzyskanego z tego systemu odzwierciedlającego treść tego pisma, jeżeli strona nie wносиła o doręczanie pism za pomocą środków komunikacji elektronicznej lub nie wyraziła zgody na doręczanie pism w taki sposób.

§ 2. Wydruk pisma, o którym mowa w § 1, zawiera:

- 1) informację, że pismo zostało wydane w formie dokumentu elektronicznego przy wykorzystaniu systemu teleinformatycznego ministra właściwego do spraw finansów publicznych i podpisane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, ze wskazaniem imienia i nazwiska oraz stanowiska służbowego osoby, która je podpisała;
- 2) identyfikator tego pisma, nadawany przez system teleinformatyczny ministra właściwego do spraw finansów publicznych.”;

7) w art. 152a w § 1 pkt 3 otrzymuje brzmienie:

„3) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym organu podatkowego, oraz informację o wymogu podpisania urzędowego poświadczenia odbioru w określony sposób.”;

8) w art. 159 § 2 otrzymuje brzmienie:

„§ 2. Wezwanie powinno być podpisane przez pracownika organu podatkowego, z podaniem jego imienia, nazwiska i stanowiska służbowego, a jeżeli jest sporządzone

w formie dokumentu elektronicznego, powinno być opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

9) w art. 168 w § 3a pkt 1 otrzymuje brzmienie:

„1) być podpisane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

10) w art. 194a § 2a otrzymuje brzmienie:

„§ 2a. Jeżeli odpis dokumentu został sporządzony w formie dokumentu elektronicznego, poświadczenia jego zgodności z oryginałem, o którym mowa w § 2, dokonuje się przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP. Odpisy dokumentów poświadczone elektronicznie są sporządzane w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;

11) w art. 210 w § 1 pkt 8 otrzymuje brzmienie:

„8) podpis osoby upoważnionej, z podaniem jej imienia i nazwiska oraz stanowiska służbowego, a jeżeli decyzja została wydana w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”;

12) w art. 217 w § 1 pkt 7 otrzymuje brzmienie:

„7) podpis osoby upoważnionej, z podaniem jej imienia i nazwiska oraz stanowiska służbowego, a jeżeli postanowienie zostało wydane w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”;

13) w art. 282b w § 4 pkt 6 otrzymuje brzmienie:

„6) podpis osoby upoważnionej do zawiadomienia, a jeżeli zawiadomienie zostało wydane w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”;

14) w art. 306d § 3 otrzymuje brzmienie:

„§ 3. Jeżeli strona lub inny uczestnik postępowania nie może uzyskać w formie dokumentu elektronicznego zaświadczenia wymaganego na potwierdzenie faktów lub stanu prawnego lub innego dokumentu wydanego przez podmiot publiczny w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jak również potwierdzenia uiszczenia opłat i kosztów

postępowania, strona lub inny uczestnik postępowania może złożyć elektroniczną kopię takiego dokumentu, po uwierzytelnieniu jej przez wnoszącego, przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP.”.

Art. 64. W ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2015 r. poz. 128, z późn. zm.⁹⁾) wprowadza się następujące zmiany:

1) w art. 6 w ust. 1 pkt 6a otrzymuje brzmienie:

„6a) świadczyć usługi zaufania oraz wydawać środki identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania;”;

2) po art. 7a dodaje się art. 7b w brzmieniu:

„Art. 7b. Oświadczenia woli związane z dokonywaniem czynności, o których mowa w art. 6 ust. 1 pkt 6a, mogą być składane w postaci elektronicznej.”.

Art. 65. W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2016 r. poz. 543 i 749) wprowadza się następujące zmiany:

1) w art. 9 w ust. 2 uchyla się pkt 6;

2) w art. 12a w ust. 1 w pkt 12 kropkę zastępuje się średnikiem i dodaje się pkt 13 w brzmieniu:

„13) nadzoru nad świadczeniem usług zaufania w rozumieniu przepisów o usługach zaufania.”.

Art. 66. W ustawie z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2016 r. poz. 814) w art. 68 ust. 5 otrzymuje brzmienie:

„5. Zgłoszenie, o którym mowa w ust. 2, opatruje się kwalifikowanym podpisem elektronicznym.”.

Art. 67. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2016 r. poz. 963) wprowadza się następujące zmiany:

1) w art. 39a w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Począwszy od 2016 r., co cztery lata, w okresie od dnia 1 kwietnia do dnia 31 lipca, członek otwartego funduszu emerytalnego lub osoba, której Zakład ewidencjonuje składkę na subkoncie, o którym mowa w art. 40a, zgodnie z art. 22 ust. 3 pkt 2, może

⁹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 559, 978, 1166, 1223, 1260, 1311, 1348, 1357, 1513, 1634, 1830, 1854, 1864 i 2281 oraz z 2016 r. poz. 615 i 904.

złożyć do Zakładu pisemnie lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym, podpisem potwierdzonym profilem zaufanym ePUAP albo wykorzystując sposób potwierdzania pochodzenia oraz integralności danych udostępniony bezpłatnie przez Zakład w systemie teleinformatycznym, zgodne ze wzorem oświadczenie o:";

- 2) w art. 47a ust. 2a otrzymuje brzmienie:

„2a. Dokumenty elektroniczne, o których mowa w ust. 1 oraz w art. 41 ust. 8, opatruje się kwalifikowanym podpisem elektronicznym osoby odpowiedzialnej za przekazanie tych dokumentów.”.

Art. 68. W ustawie z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 2016 r. poz. 372 i 960) wprowadza się następujące zmiany:

- 1) w art. 54 ust. 1 otrzymuje brzmienie:

„1. Zakład Ubezpieczeń Społecznych upoważnia do wystawiania zaświadczeń lekarskich o czasowej niezdolności do pracy z powodu choroby, pobytu w szpitalu albo innym przedsiębiorstwie podmiotu leczniczego wykonującego działalność leczniczą w rodzaju stacjonarne i całodobowe świadczenia zdrowotne albo o konieczności osobistego sprawowania opieki nad chorym członkiem rodziny, zwanych dalej „zaświadczeniem lekarskim”, lekarza, lekarza dentystę, felczera lub starszego felczera, zwanych dalej „wystawiającym zaświadczenie lekarskie”, po złożeniu, w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP przekazanego na elektroniczną skrzynkę podawczą Zakładu Ubezpieczeń Społecznych utworzoną zgodnie z przepisami wydanymi na podstawie art. 16 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwaną dalej „elektroniczną skrzynką podawczą Zakładu Ubezpieczeń Społecznych”, oświadczenia, że zobowiązuje się do przestrzegania zasad orzekania o czasowej niezdolności do pracy i wykonywania obowiązków wynikających z przepisów ustawy i przepisów o ochronie danych osobowych.”;

- 2) w art. 55 ust. 1 otrzymuje brzmienie:

„1. Zaświadczenie lekarskie jest wystawiane w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, zgodnie ze wzorem ustalonym przez Zakład Ubezpieczeń

Społecznych, za pośrednictwem systemu teleinformatycznego udostępnionego bezpłatnie przez Zakład Ubezpieczeń Społecznych.”;

3) w art. 55a:

a) w ust. 7 zdanie pierwsze otrzymuje brzmienie:

„W przypadku gdy wystawienie zaświadczenia lekarskiego w formie dokumentu elektronicznego, o którym mowa w art. 55 ust. 1, nie jest możliwe, w szczególności w przypadku braku możliwości dostępu do Internetu lub braku możliwości opatrzenia zaświadczenia lekarskiego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, wystawiający zaświadczenie lekarskie w dniu badania przekazuje ubezpieczonemu zaświadczenie lekarskie wystawione na formularzu zaświadczenia lekarskiego wydrukowanym z systemu teleinformatycznego, o którym mowa w art. 55 ust. 1, zawierające dane i informacje, o których mowa w art. 55 ust. 3 pkt 1–8 i 10, opatrzone jego podpisem i pieczętą.”,

b) w ust. 9 zdanie drugie otrzymuje brzmienie:

„Jeżeli przekazanie zaświadczenia lekarskiego w tym terminie nie jest możliwe, w szczególności w przypadku braku możliwości dostępu do Internetu lub braku możliwości opatrzenia zaświadczenia lekarskiego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, wystawiający zaświadczenie lekarskie przekazuje zaświadczenie lekarskie nie później niż w terminie 3 dni roboczych od ustania przyczyn uniemożliwiających przekazanie zaświadczenia lekarskiego.”;

4) w art. 58a ust. 1 i 2 otrzymują brzmienie:

„1. W przypadku gdy w zaświadczeniu lekarskim został popełniony błąd, wystawiający zaświadczenie lekarskie, który wystawił zaświadczenie lekarskie, w którym został popełniony błąd, albo inny wystawiający zaświadczenie lekarskie, w terminie 3 dni roboczych od dnia stwierdzenia błędu lub otrzymania informacji o stwierdzeniu błędu, w szczególności od płatnika składek, ubezpieczonego lub Zakładu Ubezpieczeń Społecznych, przekazuje na elektroniczną skrzynkę podawczą Zakładu Ubezpieczeń Społecznych, o której mowa w art. 55 ust. 2, odpowiednio:

1) informację o stwierdzeniu nieważności zaświadczenia lekarskiego, w którym został popełniony błąd, albo

2) informację, o której mowa w pkt 1, oraz nowe zaświadczenie lekarskie, zawierające identyfikator i datę jego wystawienia oraz dane i informacje, o których mowa w art. 55 ust. 3 pkt 2–10, zawarte w zaświadczeniu lekarskim, w którym został popełniony błąd, po sprostowaniu tego błędu

– opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP; przepisu art. 55 ust. 4 pkt 1 nie stosuje się.

2. Jeżeli przekazanie informacji o stwierdzeniu nieważności zaświadczenia lekarskiego, w którym został popełniony błąd, lub nowego zaświadczenia lekarskiego w terminie, o którym mowa w ust. 1, nie jest możliwe, w szczególności w przypadku braku możliwości dostępu do Internetu lub braku możliwości opatrzenia zaświadczenia lekarskiego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, wystawiający zaświadczenie lekarskie przekazuje informację lub zaświadczenie lekarskie nie później niż w terminie 3 dni roboczych od ustania przyczyn uniemożliwiających przekazanie informacji lub zaświadczenia lekarskiego.”;

5) w art. 59 ust. 9 otrzymuje brzmienie:

„9. Zaświadczenie, o którym mowa w ust. 8, lekarz orzecznik Zakładu Ubezpieczeń Społecznych wystawia w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, zgodnie ze wzorem ustalonym przez Zakład Ubezpieczeń Społecznych, za pośrednictwem systemu teleinformatycznego udostępnionego bezpłatnie przez Zakład Ubezpieczeń Społecznych. Przepisy art. 55 ust. 2 i art. 55a ust. 7–9 stosuje się odpowiednio.”;

6) w art. 61b ust. 1 otrzymuje brzmienie:

„1. Postępowanie w sprawie przyznania i wypłaty zasiłku wszczyna się na wniosek złożony w formie pisemnej lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP przekazanego na elektroniczną skrzynkę podawczą Zakładu Ubezpieczeń Społecznych.”.

Art. 69. W ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2015 r. poz. 1036 i 1629 oraz z 2016 r. poz. 862) wprowadza się następujące zmiany:

1) w art. 12:

a) ust. 1b otrzymuje brzmienie:

„1b. Karty rejestracyjne przekazywane za pośrednictwem systemu teleinformatycznego opatruje się zaawansowanym podpisem elektronicznym weryfikowanym certyfikatem wystawianym przez Ministra Sprawiedliwości.”,

b) ust. 2d otrzymuje brzmienie:

„2d. Zawiadomienia, o których mowa w art. 11 ust. 1 pkt 2 i 3, przekazywane za pośrednictwem systemu teleinformatycznego opatruje się zaawansowanym podpisem elektronicznym weryfikowanym certyfikatem wystawianym przez Ministra Sprawiedliwości.”,

c) uchyla się ust. 2e;

2) w art. 19:

a) ust. 2c otrzymuje brzmienie:

„2c. Zapytanie o udzielenie informacji o osobie oraz zapytanie o udzielenie informacji o podmiocie zbiorowym składane za pośrednictwem systemu teleinformatycznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”,

b) ust. 3a otrzymuje brzmienie:

„3a. Wniosek osoby, o której mowa w art. 7 ust. 1, o udzielenie informacji z Rejestru oraz wniosek podmiotu zbiorowego, o którym mowa w art. 7 ust. 2, składany za pośrednictwem systemu teleinformatycznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

3) w art. 20 ust. 3 otrzymuje brzmienie:

„3. Informację o osobie oraz informację o podmiocie zbiorowym doręczane za pośrednictwem systemu teleinformatycznego opatruje się kwalifikowanym podpisem elektronicznym osoby upoważnionej do ich wydania.”.

Art. 70. W ustawie z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2016 r. poz. 296) w art. 15:

1) ust. 1 otrzymuje brzmienie:

„1. Podstawą do ogłoszenia aktu normatywnego lub innego aktu prawnego jest akt w formie dokumentu elektronicznego opatrzony kwalifikowanym podpisem elektronicznym przez upoważniony do wydania aktu organ.”;

2) ust. 4 otrzymuje brzmienie:

„4. Podstawą do ogłoszenia orzeczenia jest jego odpis w formie dokumentu elektronicznego, który w swojej treści zawiera poświadczenie zgodności z oryginałem oraz jest opatrzony przez osobę upoważnioną do sporządzenia odpisu orzeczenia kwalifikowanym podpisem elektronicznym, a także odpis tego orzeczenia w postaci papierowej.”;

3) ust. 7 otrzymuje brzmienie:

„7. W przypadku ogłoszenia aktu normatywnego lub innego aktu prawnego w formie dokumentu elektronicznego wiza organu wydającego dziennik urzędowy nadawana przy skierowaniu aktu do ogłoszenia jest opatrzona kwalifikowanym podpisem elektronicznym organu wydającego dziennik urzędowy.”.

Art. 71. W ustawie z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz. U. z 2013 r. poz. 1030, z późn. zm.¹⁰⁾) wprowadza się następujące zmiany:

1) w art. 10 w § 4 zdanie drugie otrzymuje brzmienie:

„Oświadczenia zbywcy i nabywcy wymagają w takiej sytuacji opatrzenia kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

2) w art. 23¹ § 2 otrzymuje brzmienie:

„§ 2. Zawarcie umowy spółki jawnej przy wykorzystaniu wzorca umowy wymaga wypełnienia formularza umowy udostępnionego w systemie teleinformatycznym i opatrzenia umowy kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

¹⁰⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 1161, z 2015 r. poz. 4, 978, 1333 i 1830 oraz z 2016 r. poz. 615.

3) w art. 40¹ § 2 otrzymuje brzmienie:

„§ 2. Podjęcie uchwały przy wykorzystaniu wzorca uchwały wymaga wypełnienia formularza uchwały udostępnionego w systemie teleinformatycznym i opatrzenia uchwały kwalifikowanymi podpisami elektronicznymi albo podpisami potwierdzonymi profilem zaufanym ePUAP. Uchwała taka jest równoważna z uchwałą w formie pisemnej.”;

4) w art. 41 § 4 otrzymuje brzmienie:

„§ 4. Uchwałę, o której mowa w § 3, opatruje się kwalifikowanymi podpisami elektronicznymi albo podpisami potwierdzonymi profilem zaufanym ePUAP. Uchwała taka jest równoważna z uchwałą w formie pisemnej.”;

5) w art. 58 w § 2 zdanie drugie otrzymuje brzmienie:

„Podjęcie uchwały przy wykorzystaniu wzorca uchwały wymaga wypełnienia formularza uchwały udostępnionego w systemie teleinformatycznym i opatrzenia uchwały kwalifikowanymi podpisami elektronicznymi albo podpisami potwierdzonymi profilem zaufanym ePUAP.”;

6) w art. 106¹ § 2 otrzymuje brzmienie:

„§ 2. Zawarcie umowy spółki komandytowej przy wykorzystaniu wzorca umowy wymaga wypełnienia formularza umowy udostępnionego w systemie teleinformatycznym i opatrzenia umowy kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

7) w art. 180 w § 2 zdanie drugie otrzymuje brzmienie:

„Oświadczenia zbywcy i nabywcy opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

8) w art. 188 § 4 otrzymuje brzmienie:

„§ 4. Jeżeli zmiana wspólników następuje na podstawie umowy, o której mowa w art. 180 § 2, albo jest skutkiem uchwały podjętej przy wykorzystaniu wzorca uchwały udostępnionego w systemie teleinformatycznym, lista wspólników powinna być sporządzona przy wykorzystaniu wzorca udostępnionego w systemie teleinformatycznym i opatrzona kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

9) w art. 208 § 10 otrzymuje brzmienie:

„§ 10. Uchwałę, o której mowa w § 9, opatruje się kwalifikowanymi podpisami elektronicznymi albo podpisami potwierdzonymi profilem zaufanym ePUAP. Uchwała taka jest równoważna z uchwałą w formie pisemnej.”;

10) w art. 240¹ w § 2 zdanie drugie otrzymuje brzmienie:

„Prawo głosu wykonuje się przez oświadczenie złożone w systemie teleinformatycznym, opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

11) w art. 259¹ zdanie drugie otrzymuje brzmienie:

„Oświadczenia wymagają złożenia ich w systemie teleinformatycznym i opatrzenia kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

12) w art. 270 pkt 2¹ otrzymuje brzmienie:

„2¹) w przypadku spółki, której umowa została zawarta przy wykorzystaniu wzorca umowy, również uchwała wspólników o rozwiązaniu spółki opatrzona przez wszystkich wspólników kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.”;

13) w art. 412¹ w § 2 zdanie drugie otrzymuje brzmienie:

„Udzielenie pełnomocnictwa w postaci elektronicznej nie wymaga opatrzenia kwalifikowanym podpisem elektronicznym.”.

Art. 72. W ustawie z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2014 r. poz. 1512, z 2015 r. poz. 1505 i 1893 oraz z 2016 r. poz. 266) wprowadza się następujące zmiany:

1) w art. 39d w ust. 2 pkt 3 otrzymuje brzmienie:

„3) za pomocą środków komunikacji elektronicznej, bez konieczności opatrywania ich kwalifikowanym podpisem elektronicznym.”;

2) w art. 55n w ust. 2 pkt 3 otrzymuje brzmienie:

„3) za pomocą środków komunikacji elektronicznej, bez konieczności opatrywania ich kwalifikowanym podpisem elektronicznym.”.

Art. 73. W ustawie z dnia 11 kwietnia 2001 r. o rzecznikach patentowych (Dz. U. z 2016 r. poz. 221) w art. 17a ust. 2 i 3 otrzymują brzmienie:

„2. Dopuszcza się również komunikowanie się rzecznika patentowego z sądem w elektronicznym postępowaniu upominawczym przy wykorzystaniu kwalifikowanego podpisu elektronicznego.

3. Wnioski rzeczników patentowych o udzielenie danych wskazanych w ust. 1 złożone do właściwego okręgowego zgromadzenia rzeczników patentowych będą przesyłane właściwemu sądowi wraz z potwierdzeniem udziału (zrzeszenia) rzecznika we właściwym zgromadzeniu. Osoby zamierzające komunikować się z sądem w sposób wskazany w ust. 2 zawiadamiają o tym sąd za pośrednictwem właściwego okręgowego zgromadzenia rzeczników patentowych.”.

Art. 74. W ustawie z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2012 r. poz. 1017, z 2013 r. poz. 1650, z 2015 r. poz. 1893 oraz z 2016 r. poz. 554) w art. 30 ust. 4 otrzymuje brzmienie:

„4. Dopuszcza się przeprowadzanie transakcji dotyczących broni i amunicji za pośrednictwem sieci teleinformatycznej. Strony transakcji opatrują dokumenty dotyczące obrotu bronią i amunicją kwalifikowanym podpisem elektronicznym.”.

Art. 75. W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133, z późn. zm.¹¹⁾) wprowadza się następujące zmiany:

1) w art. 57 § 5 i 6 otrzymują brzmienie:

„§ 5. Uwierzytelnienie w systemie teleinformatycznym wymaga użycia profilu zaufanego ePUAP, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego albo otrzymanego w sądzie identyfikatora wskazującego na tożsamość kandydata.

§ 6. Zgłaszający swoją kandydaturę wypełnia w systemie teleinformatycznym kartę zgłoszenia kandydata na wolne stanowisko sędziowskie, opatruje ją podpisem elektronicznym nadanym przez ten system, podpisem potwierdzonym profilem

¹¹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 509, 694, 1066, 1224, 1309, 1311, 1418, 1595 i 1781 oraz 2016 r. poz. 147, 437, 663 i 960.

zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym, a następnie wnosi za pośrednictwem systemu do prezesa właściwego sądu.”;

2) w art. 57aa § 1–3 otrzymują brzmienie:

„§ 1. Dokumenty dołączane do karty zgłoszenia kandydat tworzy w systemie teleinformatycznym i wnosi za pośrednictwem tego systemu, opatrując je podpisem elektronicznym nadanym przez ten system, podpisem potwierdzonym profilem zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym.

§ 2. Dokumenty mające w oryginale postać papierową kandydat zamieszcza w systemie teleinformatycznym w postaci elektronicznych kopii, opatrując je podpisem elektronicznym nadanym przez ten system, podpisem potwierdzonym profilem zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym, co jednocześnie stanowi oświadczenie o zgodności elektronicznej kopii dokumentu z oryginałem w postaci papierowej. Oświadczenie to jest składane pod rygorem odpowiedzialności karnej za fałszywe zeznania. Prezes właściwego sądu, któremu zgłoszono kandydaturę na wolne stanowisko sędziowskie, w uzasadnionych przypadkach może wezwać kandydata do doręczenia w terminie trzech dni oryginałów dokumentów. Obowiązek zamieszczenia w systemie teleinformatycznym elektronicznej kopii dokumentu nie dotyczy oświadczenia, o którym mowa w art. 7 ust. 1 ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990, oraz treści tych dokumentów, a także informacji, o której mowa w art. 7 ust. 3a tej ustawy.

§ 3. Prezes właściwego sądu, któremu zgłoszono kandydaturę na wolne stanowisko sędziowskie, zamieszcza w systemie teleinformatycznym elektroniczne kopie dokumentów innych niż zamieszczone przez kandydata, mających w oryginale postać papierową, wymaganych w tym postępowaniu, opatrując je podpisem elektronicznym nadanym przez ten system. Obowiązek zamieszczenia w systemie teleinformatycznym elektronicznej kopii dokumentu nie dotyczy oświadczenia, o którym mowa w art. 7 ust. 1 ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990, oraz treści tych dokumentów, a także informacji, o której mowa w art. 7 ust. 3a tej ustawy.”.

Art. 76. W ustawie z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej (Dz. U. z 2014 r. poz. 1384, z późn. zm.¹²⁾) wprowadza się następujące zmiany:

1) w art. 2a ust. 2 i 3 otrzymują brzmienie:

„2. Warunkiem dokonywania przez osoby określone w ust. 1 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

3. Potwierdzenia, o którym mowa w ust. 2, dokonuje się na podstawie wniosku o nadanie uprawnień:

1) opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352) lub

2) potwierdzonego przez Krajową Izbę Diagnostów Laboratoryjnych w zakresie tożsamości osoby, która konto założyła.”;

2) w art. 30b w ust. 4 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podstawowa jednostka organizacyjna uczelni zamierzająca prowadzić szkolenie specjalizacyjne składa do dyrektora CMKP za pomocą SMK wnioski o udzielenie akredytacji w postaci elektronicznej, podpisany przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Wniosek zawiera następujące dane:”.

Art. 77. W ustawie z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2013 r. poz. 1414, z późn. zm.¹³⁾) w art. 39e ust. 4 otrzymuje brzmienie:

„4. Wojewoda, o którym mowa w ust. 2 pkt 1, może umożliwić przekazywanie informacji oraz danych, o których mowa w ust. 2 pkt 1 i 3 oraz ust. 3, w postaci elektronicznej z wykorzystaniem kwalifikowanego podpisu elektronicznego.”.

¹²⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 1491, z 2015 r. poz. 1087, 1893 i 1991 oraz z 2016 r. poz. 65 i 960.

¹³⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 486, 805, 915 i 1310 oraz z 2015 r. poz. 211, 390, 978, 1269, 1273 i 1893.

Art. 78. W ustawie z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2008 r. poz. 271, z późn. zm.¹⁴⁾) wprowadza się następujące zmiany:

1) w art. 39 ust. 4 otrzymuje brzmienie:

„4. Główny Inspektor Farmaceutyczny zapewnia możliwość złożenia wniosku o wydanie albo zmianę zezwolenia na wytwarzanie lub import produktu leczniczego, w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

2) w art. 41 ust. 4a otrzymuje brzmienie:

„4a. Główny Inspektor Farmaceutyczny zapewnia możliwość złożenia wniosków, o których mowa w ust. 1 i 3, w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

3) w art. 47a ust. 5 otrzymuje brzmienie:

„5. Główny Inspektor Farmaceutyczny zapewnia możliwość złożenia wniosku, o którym mowa w ust. 1, w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

4) w art. 51b ust. 12 otrzymuje brzmienie:

„12. Główny Inspektor Farmaceutyczny zapewnia możliwość złożenia wniosku, o którym mowa w ust. 4, w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

5) w art. 51i ust. 7 otrzymuje brzmienie:

„7. Główny Inspektor Farmaceutyczny zapewnia możliwość złożenia wniosków, o których mowa w ust. 1–3, w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

¹⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2008 r. poz. 1505 i 1570, z 2009 r. poz. 97, 206, 753, 788 i 817, z 2010 r. poz. 513 i 679, z 2011 r. poz. 322, 451, 622, 654, 657 i 696, z 2012 r. poz. 1342 i 1544, z 2013 r. poz. 1245, z 2014 r. poz. 822 i 1491, z 2015 r. poz. 28, 277, 788, 875, 1771, 1830, 1918, 1926 i 1991 oraz z 2016 r. poz. 823.

6) w art. 73b ust. 2 otrzymuje brzmienie:

„2. Główny Inspektor Farmaceutyczny zapewnia możliwość złożenia wniosku, o którym mowa w ust. 1, w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej. Wniosek opatruje się kwalifikowanym podpisem elektronicznym.”;

7) w art. 96a w ust. 1 w pkt 3 lit. e otrzymuje brzmienie:

„e) podpis, w przypadku recepty:

- w postaci elektronicznej – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP albo
- w postaci papierowej – podpis własnoręczny;”;

8) w art. 107a w ust. 4 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podstawowa jednostka organizacyjna uczelni zamierzająca prowadzić szkolenie specjalizacyjne składa do dyrektora CMKP za pomocą Systemu Monitorowania Kształcenia Pracowników Medycznych, o którym mowa w art. 30 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, zwanego dalej „SMK”, wniosek o udzielenie akredytacji w postaci elektronicznej, podpisany przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Wniosek zawiera następujące dane:”;

9) w art. 107f ust. 4 i 5 otrzymują brzmienie:

„4. Warunkiem dokonywania przez osoby określone w ust. 3 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

5. Potwierdzenia, o którym mowa w ust. 4, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą okręgową izbę aptekarską lub Naczelną Izbę Aptekarską w zakresie tożsamości osoby, która konto założyła.”.

Art. 79. W ustawie z dnia 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego (Dz. U. z 2015 r. poz. 1100 i 1893 oraz z 2016 r. poz. 544) wprowadza się następujące zmiany:

1) art. 25a otrzymuje brzmienie:

„Art. 25a. Wniosek, o którym mowa w art. 24 ust. 2, wraz załącznikami może być złożony za pośrednictwem środków komunikacji elektronicznej, po opatrzeniu kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, z tym że dokument wewnątrzspółnotowego przemieszczania materiałów wybuchowych składa się wyłącznie w postaci papierowej.”;

2) w art. 37 ust. 6 otrzymuje brzmienie:

„6. Wniosek, o którym mowa w ust. 3, wraz z załącznikami może być złożony za pośrednictwem środków komunikacji elektronicznej, po opatrzeniu kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

3) w art. 62ze w ust. 1 pkt 17 otrzymuje brzmienie:

„17) przekazania rejestru, o którym mowa w pkt 14, ministrowi właściwemu do spraw gospodarki w przypadku zakończenia działalności gospodarczej za pośrednictwem środków komunikacji elektronicznej, w formacie ustalonym z ministrem właściwym do spraw gospodarki po opatrzeniu kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

4) w art. 62zf w ust. 1 pkt 16 otrzymuje brzmienie:

„16) przekazania rejestru, o którym mowa w pkt 13, ministrowi właściwemu do spraw gospodarki w przypadku zakończenia działalności gospodarczej za pośrednictwem środków komunikacji elektronicznej, w formacie ustalonym z ministrem właściwym do spraw gospodarki po opatrzeniu kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

5) w art. 62zm ust. 7 otrzymuje brzmienie:

„7. Przekazanie rejestru w przypadku, o którym mowa w ust. 6, następuje za pośrednictwem środków komunikacji elektronicznej, w formacie ustalonym z jednostką notyfikowaną lub ministrem właściwym do spraw gospodarki, które przejmą rejestr, po opatrzeniu kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 80. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z 2015 r. poz. 1884 oraz z 2016 r. poz. 147 i 615) w art. 7 w pkt 1 lit. b otrzymuje brzmienie:

„b) jednoznaczłą identyfikację stron usługi świadczonej drogą elektroniczną oraz potwierdzenie faktu złożenia oświadczeń woli i ich treści, niezbędnych do zawarcia drogą elektroniczną umowy o świadczenie tej usługi, w szczególności przy wykorzystaniu kwalifikowanego podpisu elektronicznego;”.

Art. 81. W ustawie z dnia 30 października 2002 r. o podatku leśnym (Dz. U. z 2016 r. poz. 374) w art. 6 w ust. 11 pkt 3 otrzymuje brzmienie:

„3) limity wysokości zobowiązania podatkowego, kwoty nadpłaty lub zwrotu podatku wynikające z deklaracji na podatek leśny, a także wymagania dla poszczególnych rodzajów podpisu elektronicznego, w szczególności dotyczące weryfikacji podpisu elektronicznego i wykorzystania elektronicznych znaczników czasu.”.

Art. 82. W ustawie z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, z późn. zm.¹⁵⁾) w art. 216a ust. 1 otrzymuje brzmienie:

„1. Jeżeli ustawa przewiduje złożenie dokumentu w postaci elektronicznej, dokument składa się za pośrednictwem Rejestru i opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 83. W ustawie z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. z 2016 r. poz. 778) w art. 18 ust. 3 otrzymuje brzmienie:

„3. Jako wniesione na piśmie uznaje się również uwagi wniesione za pomocą elektronicznej skrzynki podawczej w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne:

- 1) opatrzone kwalifikowanym podpisem elektronicznym albo
- 2) opatrzone podpisem potwierdzonym profilem zaufanym ePUAP.”.

¹⁵⁾ Patrz odnośnik nr 3.

Art. 84. W ustawie z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2015 r. poz. 114, z późn. zm.¹⁶⁾) w art. 23:

1) ust. 3b otrzymuje brzmienie:

„3b. Wniosek i załączniki do wniosku określone w ust. 4 składane w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. W przypadku gdy wniosek i załączniki składane są z wykorzystaniem systemu, o którym mowa w ust. 6a, w systemie tym może być zapewniony inny sposób potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej.”;

2) ust. 3d otrzymuje brzmienie:

„3d. W przypadku wniosku składanego w postaci elektronicznej, po wpisaniu do formularza wniosku numerów PESEL wnioskodawcy i członków jego rodziny, formularz wniosku może być uzupełniony o dane zgromadzone w rejestrze PESEL w zakresie imion, nazwiska, miejsca urodzenia, daty urodzenia, stanu cywilnego, obywatelstwa i płci osoby występującej o przyznanie świadczeń rodzinnych i dzieci pozostających na utrzymaniu tej osoby.”;

3) ust. 6a otrzymuje brzmienie:

„6a. Minister właściwy do spraw rodziny jest obowiązany do utworzenia i prowadzenia systemu teleinformatycznego umożliwiającego ubieganie się o świadczenia rodzinne drogą elektroniczną oraz zapewnienia funkcjonowania tego systemu. Uwierzytelnianie użytkowników w systemie teleinformatycznym wymaga użycia profilu zaufanego ePUAP, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego lub innych technologii, jeżeli zostaną udostępnione w tym systemie.”.

Art. 85. W ustawie z dnia 28 listopada 2003 r. o wspieraniu rozwoju obszarów wiejskich ze środków pochodzących z Sekcji Gwarancji Europejskiego Funduszu Orientacji i Gwarancji Rolnej (Dz. U. z 2014 r. poz. 1613) w art. 5 ust. 4c otrzymuje brzmienie:

„4c. Do złożenia wniosków, o których mowa w ust. 4a, za pomocą formularza umieszczonego na stronie internetowej Agencji nie jest wymagany zaawansowany podpis elektroniczny.”.

¹⁶⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 693, 995, 1217, 1240, 1268, 1302, 1359 i 1830 oraz z 2016 r. poz. 195 i 972.

Art. 86. W ustawie z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 oraz z 2016 r. poz. 831) wprowadza się następujące zmiany:

1) w art. 10a ust. 5 otrzymuje brzmienie:

„5. Oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenia, w tym jednolity dokument, sporządza się, pod rygorem nieważności, w postaci elektronicznej, i opatruje się kwalifikowanym podpisem elektronicznym.”;

2) w art. 91c ust. 2 otrzymuje brzmienie:

„2. Postąpienia, pod rygorem nieważności, składa się opatrzone kwalifikowanym podpisem elektronicznym.”;

3) w art. 131bc ust. 5 otrzymuje brzmienie:

„5. Ofertę składa się, pod rygorem nieważności, w formie pisemnej w postaci papierowej albo, za zgodą zamawiającego, w postaci elektronicznej, opatrzoną przez wykonawcę odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.”;

4) w art. 180 ust. 4 otrzymuje brzmienie:

„4. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.”;

5) w art. 183 ust. 6 otrzymuje brzmienie:

„6. Wniosek, o którym mowa w ust. 2, zamawiający może złożyć za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe, osobiście, za pośrednictwem posłańca albo w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym.”;

6) w art. 185 ust. 2 otrzymuje brzmienie:

„2. Wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje, i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje. Zgłoszenie przystąpienia doręcza się Prezesowi Izby w postaci papierowej albo elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, a jego kopię przesyła się zamawiającemu oraz wykonawcy wnoszącemu odwołanie.”.

Art. 87. W ustawie z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2016 r. poz. 710, 846 i 960) w art.106m w ust. 5 pkt 1 otrzymuje brzmienie:

„1) kwalifikowanego podpisu elektronicznego lub”.

Art. 88. W ustawie z dnia 20 kwietnia 2004 r. o organizacji rynku mleka i przetworów mlecznych (Dz. U. z 2016 r. poz. 155) w art. 48a ust. 4 otrzymuje brzmienie:

„4. Wniosek, o którym mowa w ust. 3, składany w postaci elektronicznej, opatruje się kwalifikowanym podpisem elektronicznym.”.

Art. 89. W ustawie z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2016 r. poz. 645, 691 i 868) wprowadza się następujące zmiany:

- 1) w art. 18f pkt 1 i 2 otrzymują brzmienie:
 - „1) kwalifikowanym podpisem elektronicznym albo
 - 2) podpisem potwierdzonym profilem zaufanym ePUAP.”;
- 2) w art. 36b w ust. 6 pkt 1 i 2 otrzymują brzmienie:
 - „1) kwalifikowanym podpisem elektronicznym albo
 - 2) podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 90. W ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 584, z późn. zm.¹⁷⁾) wprowadza się następujące zmiany:

- 1) w art. 22b po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Jeżeli przepisy odrębne wymagają podpisania dokumentów, o których mowa w ust. 1, dokumenty te są podpisywane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, albo wykorzystując sposób potwierdzania pochodzenia i integralności danych udostępniony bezpłatnie przez pojedynczy punkt kontaktowy.”;
- 2) art. 22g otrzymuje brzmienie:

„Art. 22g. Minister właściwy do spraw gospodarki określi, w drodze rozporządzenia, szczegółowy zakres i warunki korzystania z pojedynczego punktu kontaktowego, w tym w szczególności sposób potwierdzania pochodzenia i integralności danych udostępniony bezpłatnie przez pojedynczy punkt kontaktowy, o którym mowa w art. 22b ust. 2a, z uwzględnieniem roli punktu kontaktowego w realizacji procedur związanych z podejmowaniem, wykonywaniem i zakończeniem działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, uznawaniem kwalifikacji zawodowych nabytych w państwach członkowskich Unii Europejskiej,

¹⁷⁾ Patrz odnośnik nr 4.

świadczeniem usług transgranicznych i ubieganiem się o wydanie europejskiej legitymacji zawodowej oraz zasad przetwarzania i ochrony danych osobowych.”;

3) w art. 26 ust. 4 otrzymuje brzmienie:

„4. Organ gminy przekształca wnioski, o którym mowa w ust. 2, na formę dokumentu elektronicznego, podpisuje go kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, albo podpisuje w inny sposób akceptowany przez system CEIDG umożliwiający jednoznaczną identyfikację osoby podpisującej przekształcony wniosek i przesyła go do CEIDG nie później niż następnego dnia roboczego od dnia jego otrzymania.”;

4) w art. 27 ust. 7 otrzymuje brzmienie:

„7. Wniosek o wpis do CEIDG składany w sposób określony w art. 26 ust. 1 podpisany jest kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, albo podpisany w inny sposób akceptowany przez system CEIDG umożliwiający jednoznaczną identyfikację osoby składającej wniosek.”.

Art. 91. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.¹⁸⁾) w art. 60b w ust. 3 w pkt 2 lit. b otrzymuje brzmienie:

„b) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego,”.

Art. 92. W ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2015 r. poz. 581, z późn. zm.¹⁹⁾) w art. 56 w ust. 1 pkt 2 otrzymuje brzmienie:

„2) elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP w rozumieniu przepisów o informatyzacji działalności podmiotów realizujących zadania publiczne.”.

¹⁸⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 827 i 1198, z 2015 r. poz. 1069, 1893 i 2281 oraz z 2016 r. poz. 147 i 542.

¹⁹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 1240, 1269, 1365, 1569, 1692, 1735, 1830, 1844, 1893, 1991, 1916 i 1994 oraz z 2016 r. poz. 65 i 652.

Art. 93. W ustawie z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego (Dz. U. z 2015 r. poz. 487 i 1505 oraz z 2016 r. poz. 65) w art. 18 ust. 1a otrzymuje brzmienie:

„1a. Tłumacz przysięgły może, za pomocą kwalifikowanego podpisu elektronicznego, poświadczyć tłumaczenie lub odpis pisma w postaci elektronicznej. Poświadczenie odpisu pisma w postaci elektronicznej może być dokonane tylko na podstawie oryginału, tłumaczenia lub odpisu dokumentu w formie pisemnej.”.

Art. 94. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352) wprowadza się następujące zmiany:

1) w art. 3:

a) pkt 15 otrzymuje brzmienie:

„15) podpis potwierdzony profilem zaufanym ePUAP – podpis elektroniczny złożony przez użytkownika konta ePUAP, do którego zostały dołączone informacje identyfikujące zawarte w profilu zaufanym ePUAP, a także:

- a) jednoznacznie wskazujący profil zaufany ePUAP osoby, która wykonała podpis,
- b) zawierający czas wykonania podpisu,
- c) jednoznacznie identyfikujący konto ePUAP osoby, która wykonała podpis,
- d) autoryzowany przez użytkownika konta ePUAP,
- e) opatrzony i chroniony pieczęcią elektroniczną wykorzystywaną w ePUAP w celu zapewnienia integralności i autentyczności wykonania operacji przez system ePUAP;”.

b) uchyla się pkt 16,

c) w pkt 26 kropkę zastępuje się średnikiem i dodaje się pkt 27 w brzmieniu:

„27) autoryzacja – przydzielenie osobie fizycznej lub prawnej, uprawnień w systemie teleinformatycznym po jej pozytywnym uwierzytelnieniu lub potwierdzenie woli realizacji czynności w postaci elektronicznej przez uwierzytelnionego użytkownika za pomocą dodatkowych danych.”;

2) w art. 19a ust. 3 otrzymuje brzmienie:

„3. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, zakres i warunki korzystania z ePUAP, w tym warunki organizacyjne i techniczne

nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, z uwzględnieniem roli ePUAP w procesie realizacji zadań publicznych drogą elektroniczną oraz zasad przetwarzania i ochrony danych osobowych.”;

3) w art. 19b ust. 3 otrzymuje brzmienie:

„3. Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.”;

4) w art. 20a:

a) ust. 1 otrzymuje brzmienie:

„1. Uwierzytelnienie użytkowników systemu teleinformatycznego korzystających z usług online udostępnianych przez podmioty określone w art. 2 wymaga:

- 1) użycia notyfikowanego środka identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa wymaganego dla usług świadczonych w ramach tych systemów, lub
- 2) profilu zaufanego ePUAP, lub
- 3) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego.”,

b) w ust. 3 w pkt 2:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„zasady i warunki potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego ePUAP, w tym:”,

– lit. f otrzymuje brzmienie:

„f) warunki składania podpisu elektronicznego potwierdzonego profilem zaufanym ePUAP,”,

– w lit. i dodaje się przecinek i dodaje się lit. j w brzmieniu:

„j) warunki organizacyjne i techniczne dla potwierdzania profilu zaufanego ePUAP przy nieodpłatnym wykorzystaniu środka identyfikacji

elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy”;

5) art. 20b otrzymuje brzmienie:

„Art. 20b. 1. Podpis potwierdzony profilem zaufanym ePUAP wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności tego profilu.

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

3. Nie można odmówić ważności i skuteczności podpisowi elektronicznemu potwierdzonemu profilem zaufanym ePUAP tylko na tej podstawie, że istnieje w postaci elektronicznej lub zmianie uległy dane inne niż służące do potwierdzenia profilu zaufanego.”;

6) w art. 20c:

a) ust. 1 otrzymuje brzmienie:

„1. Potwierdzenia profilu zaufanego ePUAP, które polega na weryfikacji zgodności danych zawartych w profilu użytkownika ze stanem faktycznym oraz nadaniu uprawnień wynikających z posiadania profilu zaufanego ePUAP, jak również przedłużenia ważności i unieważnienia profilu zaufanego ePUAP dokonuje:

- 1) punkt potwierdzający profil zaufany ePUAP;
- 2) samodzielnie osoba fizyczna występująca z wnioskiem o potwierdzenie, podpisanym kwalifikowanym podpisem elektronicznym, w przypadku gdy kwalifikowany certyfikat podpisu elektronicznego zawiera dane obejmujące co najmniej:
 - a) imię,
 - b) nazwisko,
 - c) numer PESEL;
- 3) samodzielnie osoba fizyczna występująca z wnioskiem o potwierdzenie, 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,

- b) nazwisko,
 - c) numer PESEL.”,
- b) dodaje się ust. 8–10 w brzmieniu:

„8. Minister właściwy do spraw informatyzacji, na wniosek banku krajowego lub innego przedsiębiorcy, wydaje zgodę na wykorzystywanie środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy do potwierdzania profilu zaufanego ePUAP w sposób, o którym mowa w ust. 1 pkt 3, po złożeniu przez bank krajowy lub innego przedsiębiorcę oświadczenia o spełnieniu przez bank krajowy lub innego przedsiębiorcę warunków, o których mowa w przepisach wydanych na podstawie art. 20a ust. 3 pkt 2.

9. Minister właściwy do spraw informatyzacji może sprawdzać, czy bank krajowy lub inny przedsiębiorca w przypadku, o którym mowa w ust. 8, spełnia warunki, o których mowa w przepisach wydanych na podstawie art. 20a ust. 3 pkt 2.

10. Minister właściwy do spraw informatyzacji cofa zgodę, o której mowa w ust. 8, w przypadku gdy bank krajowy lub inny przedsiębiorca nie spełnia warunków określonych w przepisach wydanych na podstawie art. 20a ust. 3 pkt 2.”.

Art. 95. W ustawie z dnia 8 lipca 2005 r. o Prokuraturii Generalnej Skarbu Państwa (Dz. U. z 2013 r. poz. 1150, z późn. zm.²⁰⁾) w art. 17a ust. 2 i 3 otrzymują brzmienie:

„2. Dopuszcza się również komunikowanie się radcy Prokuraturii Generalnej z sądem w elektronicznym postępowaniu upominawczym przy wykorzystaniu kwalifikowanego podpisu elektronicznego.

3. Wnioski radców Prokuraturii Generalnej o udzielenie danych wskazanych w ust.1 złożone odpowiednio do dyrektora właściwego oddziału Prokuraturii Generalnej lub Prezesa Prokuraturii Generalnej będą przesyłane właściwemu sądowi wraz z potwierdzeniem zatrudnienia radcy Prokuraturii Generalnej odpowiednio we właściwym oddziale Prokuraturii Generalnej lub w Głównym Urzędzie Prokuraturii Generalnej. Osoby zamierzające komunikować się z sądem w sposób wskazany w ust. 2

²⁰⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2013 r. poz. 1247 oraz z 2015 r. poz. 1064, 1224, 1311, 1595 i 1635.

zawiadamiają o tym sąd za pośrednictwem odpowiednio dyrektora właściwego oddziału Prokuraturii Generalnej lub Prezesa Prokuraturii Generalnej.”.

Art. 96. W ustawie z dnia 29 lipca 2005 r. o systemie tachografów cyfrowych (Dz. U. poz. 1494, z późn. zm.²¹⁾) w art. 21 ust. 2 otrzymuje brzmienie:

„2. Wnioski wraz z załącznikami, o których mowa w ust. 1, składane są w formie pisemnej w postaci papierowej lub elektronicznej. Wniosek w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym.”.

Art. 97. W ustawie z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (Dz. U. z 2015 r. poz. 594 i 1893 oraz z 2016 r. poz. 65) w art. 29 ust. 5 i 6 otrzymują brzmienie:

„5. Jeżeli dokument elektroniczny, o którym mowa w ust. 4, nie został opatrzony kwalifikowanym podpisem elektronicznym, powiadomienia, o którym mowa w ust. 1, należy dokonać również w formie pisemnej na formularzu według wzoru, o którym mowa w ust. 4.

6. Za dzień złożenia powiadomienia, o którym mowa w ust. 1, uznaje się dzień otrzymania przez Głównego Inspektora Sanitarnego powiadomienia opatrzonego kwalifikowanym podpisem elektronicznym lub własnoręcznym podpisem.”.

Art. 98. W ustawie z dnia 7 marca 2007 r. o wspieraniu rozwoju obszarów wiejskich z udziałem środków Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich w ramach Programu Rozwoju Obszarów Wiejskich na lata 2007–2013 (Dz. U. z 2013 r. poz. 173, z 2015 r. poz. 349 oraz z 2016 r. poz. 337) w art. 24 ust. 3 otrzymuje brzmienie:

„3. Do złożenia wniosków, o których mowa w ust. 1, za pomocą formularza umieszczonego na stronie internetowej podmiotu wdrażającego nie jest wymagany zaawansowany podpis elektroniczny.”.

²¹⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2007 r. poz. 661, z 2011 r. poz. 622 i 1016 oraz z 2015 r. poz. 1893.

Art. 99. W ustawie z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2016 r. poz. 169 i 195) w art. 15:

1) ust. 3b otrzymuje brzmienie:

„3b. Wniosek i załączniki do wniosku określone w ust. 4 składane w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. W przypadku gdy wniosek i załączniki składane są z wykorzystaniem systemu, o którym mowa w ust. 11, w systemie tym może być zapewniony inny sposób potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej.”;

2) ust. 3d otrzymuje brzmienie:

„3d. W przypadku wniosku składanego w postaci elektronicznej, po wpisaniu do formularza wniosku numerów PESEL wnioskodawcy i członków jego rodziny, formularz wniosku może być uzupełniony o dane zgromadzone w rejestrze PESEL w zakresie imion, nazwiska, miejsca urodzenia, daty urodzenia, stanu cywilnego, obywatelstwa i płci wnioskodawcy i członków jego rodziny.”;

3) ust. 11 otrzymuje brzmienie:

„11. Minister właściwy do spraw rodziny jest obowiązany do utworzenia i prowadzenia systemu teleinformatycznego umożliwiającego ubieganie się o świadczenia z funduszu alimentacyjnego drogą elektroniczną oraz zapewnienia funkcjonowania tego systemu. Uwierzytelnianie użytkowników w systemie teleinformatycznym wymaga użycia profilu zaufanego ePUAP, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego lub innych technologii jeżeli zostaną udostępnione w tym systemie.”.

Art. 100. W ustawie z dnia 10 lipca 2008 r. o odpadach wydobywczych (Dz. U. z 2013 r. poz. 1136 oraz z 2014 r. poz. 1101) w art. 15a w ust. 3 pkt 3 otrzymuje brzmienie:

„3) za pomocą środków komunikacji elektronicznej bez konieczności opatrywania ich kwalifikowanym podpisem elektronicznym.”.

Art. 101. W ustawie z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz. U. z 2016 r. poz. 353) w art. 34 pkt 3 otrzymuje brzmienie:

„3) za pomocą środków komunikacji elektronicznej bez konieczności opatrywania ich kwalifikowanym podpisem elektronicznym.”.

Art. 102. W ustawie z dnia 25 czerwca 2009 r. o rolnictwie ekologicznym (Dz. U. z 2015 r. poz. 497) w art. 17 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) ministrowi właściwemu do spraw rolnictwa, Głównemu Inspektorowi oraz Prezesowi Agencji Restrukturyzacji i Modernizacji Rolnictwa, za pośrednictwem środków komunikacji elektronicznej w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym, do dnia 30 listopada każdego roku, wykaz producentów, o których mowa w ustawie z dnia 18 grudnia 2003 r. o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności (Dz. U. z 2015 r. poz. 807 i 1419), którzy spełnili określone wymagania dotyczące produkcji ekologicznej zgodnie z przepisami dotyczącymi rolnictwa ekologicznego, według stanu na dzień 15 listopada tego roku;”.

Art. 103. W ustawie z dnia 20 maja 2010 r. o wyrobach medycznych (Dz. U. z 2015 r. poz. 876 i 1918 oraz z 2016 r. poz. 542) wprowadza się następujące zmiany:

1) w art. 51 w ust. 2 zdanie drugie otrzymuje brzmienie:

„Informację tę sponsor może sporządzać w języku angielskim oraz przekazywać ją drogą elektroniczną bez konieczności stosowania kwalifikowanego podpisu elektronicznego.”;

2) w art. 68 ust. 9 otrzymuje brzmienie:

„9. Prezes Urzędu w wykonywaniu ustawy współpracuje i wymienia informacje z właściwymi organami państw trzecich oraz instytucjami Unii Europejskiej, także w formie elektronicznej, bez konieczności stosowania kwalifikowanego podpisu elektronicznego.”;

3) w art. 73a ust. 1 otrzymuje brzmienie:

„1. W postępowaniach w sprawach nadzoru nad wyrobami, o ile ustawa nie stanowi inaczej, korespondencja z podmiotami może być prowadzona w języku

angielskim i może być przekazywana drogą elektroniczną bez konieczności stosowania kwalifikowanego podpisu elektronicznego.”;

4) w art. 84 ust. 1 otrzymuje brzmienie:

„1. W postępowaniach w sprawach incydentów medycznych i bezpieczeństwa wyrobów, o ile ustawa nie stanowi inaczej, korespondencja z podmiotami może być prowadzona w języku angielskim i może być przekazywana drogą elektroniczną bez konieczności stosowania kwalifikowanego podpisu elektronicznego.”.

Art. 104. W ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2016 r. poz. 391 i 862) wprowadza się następujące zmiany:

1) w art. 28 pkt 11 otrzymuje brzmienie:

„11) własnoręczny czytelny podpis wnioskodawcy, a w przypadku wniosku złożonego w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP;”;

2) w art. 48 w ust. 2 pkt 2 otrzymuje brzmienie:

„2) własnoręczny czytelny podpis zgłaszającego, a w przypadku formularza złożonego w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”.

Art. 105. W ustawie z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2015 r. poz. 155, z późn. zm.²²⁾) w art. 27 ust. 6 otrzymuje brzmienie:

„6. Starosta, o którym mowa w ust. 1 pkt 1, może umożliwić przekazywanie informacji oraz danych, o których mowa w ust. 1 pkt 1 oraz ust. 2 pkt 1, w formie elektronicznej z wykorzystaniem kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP.”.

Art. 106. W ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2015 r. poz. 636, z późn. zm.²³⁾) w art. 17 w ust. 3 wprowadzenie do wyczerpania otrzymuje brzmienie:

„Pracownik medyczny używa kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP do podpisywania:”.

²²⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 541, 1045, 1273, 1327, 2183 i 2281 oraz z 2016 r. poz. 27.

²³⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 788, 855, 1066, 1918, 1991, 1994 i 2281.

Art. 107. W ustawie z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2015 r. poz. 345, 1893 i 1991) w art. 38:

1) w ust. 5 w pkt 3 lit. e otrzymuje brzmienie:

„e) podpis, w przypadku zlecenia:

- w postaci elektronicznej – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP albo
- w postaci papierowej – podpis własnoręczny;”;

2) w ust. 5a w pkt 9 lit. a otrzymuje brzmienie:

„a) kwalifikowany podpis elektroniczny albo zaawansowany podpis elektroniczny weryfikowany przy pomocy wydawanego przez Fundusz ważnego certyfikatu, albo podpis potwierdzony profilem zaufanym ePUAP – w przypadku zlecenia w postaci elektronicznej, albo”;

3) w ust. 6 w pkt 7 lit. a otrzymuje brzmienie:

„a) w postaci elektronicznej – kwalifikowany podpis elektroniczny albo zaawansowany podpis elektroniczny weryfikowany przy pomocy wydawanego przez Fundusz ważnego certyfikatu, albo podpis potwierdzony profilem zaufanym ePUAP, albo”.

Art. 108. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2013 r. poz. 21, z późn. zm.²⁴⁾) w art. 65 ust. 2 otrzymuje brzmienie:

„2. Formę pisemną wniosku o wpis do rejestru, wniosku o zmianę wpisu w rejestrze oraz wniosku o wykreślenie z rejestru stanowi wydruk wypełnionego formularza opatrzony podpisem wnioskodawcy albo wypełniony formularz w postaci elektronicznej opatrzony kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 109. 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 oraz z 2015 r. poz. 1311) wprowadza się następujące zmiany:

1) w art. 4:

a) pkt 3–5 otrzymują brzmienie:

„3) w art. 37 po § 1 dodaje się § 1a w brzmieniu:

²⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2013 r. 888 i 1238, z 2014 r. poz. 695, 1101 i 1322 oraz z 2015 r. poz. 87, 122, 933, 1045, 1688, 1936 i 2281.

„§ 1a. Jeżeli odpis pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie zostały sporządzone w formie dokumentu elektronicznego, ich uwierzytelnienia, o którym mowa w § 1, dokonuje się z wykorzystaniem kwalifikowanego podpisu elektronicznego, podpisu potwierdzonego profilem zaufanym ePUAP lub przez zastosowanie innych mechanizmów, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jeżeli takie mechanizmy zostały wprowadzone przez sąd administracyjny. Odpisy pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie uwierzytelniane elektronicznie sporządzane są w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 tej ustawy.”;

- 4) po art. 37 dodaje się art. 37a w brzmieniu:

„Art. 37a. Pełnomocnictwo udzielone w formie dokumentu elektronicznego powinno być podpisane kwalifikowanym podpisem elektronicznym, podpisem potwierdzonym profilem zaufanym ePUAP lub przez zastosowanie innych mechanizmów, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jeżeli takie mechanizmy zostały wprowadzone przez sąd administracyjny.”;

- 5) w art. 46 po § 2 dodaje się § 2a–2d w brzmieniu:

„§ 2a. Gdy pismo strony jest wnoszone w formie dokumentu elektronicznego, powinno ponadto zawierać adres elektroniczny oraz zostać podpisane przez stronę albo jej przedstawiciela ustawowego lub pełnomocnika kwalifikowanym podpisem elektronicznym, podpisem potwierdzonym profilem zaufanym ePUAP lub przez zastosowanie innych mechanizmów, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jeżeli takie mechanizmy zostały wprowadzone przez sąd administracyjny.

§ 2b. Zasady podpisywania przewidziane w § 2a dotyczą także załączników wnoszonych w formie dokumentu elektronicznego.

§ 2c. Pismo wnoszone w innej formie niż forma dokumentu elektronicznego, zawierające żądanie doręczania pism sądu za pomocą środków komunikacji elektronicznej, powinno zawierać oznaczenie adresu elektronicznego.

§ 2d. Jeżeli pismo, o którym mowa w § 2a, nie zawiera adresu elektronicznego, sąd przyjmuje, że właściwym jest adres elektroniczny, z którego nadano pismo wniesione w formie dokumentu elektronicznego, a gdy wniesiono je w innej formie i zawiera ono żądanie, o którym mowa w § 2c, doręczenie pism przez sąd następuje na adres wskazany zgodnie z § 2, przy czym w pierwszym piśmie sąd poucza o warunku podania adresu elektronicznego w żądaniu doręczania pism środkami komunikacji elektronicznej.”;

b) pkt 7 otrzymuje brzmienie:

„7) w art. 48 po § 3 dodaje się § 3a w brzmieniu:

„§ 3a. Jeżeli odpis dokumentu został sporządzony w formie dokumentu elektronicznego, poświadczenie jego zgodności z oryginałem, o którym mowa w § 3, dokonuje się z wykorzystaniem kwalifikowanego podpisu elektronicznego, podpisu potwierdzonego profilem zaufanym ePUAP lub przez zastosowanie innych mechanizmów, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jeżeli takie mechanizmy zostały wprowadzone przez sąd administracyjny. Odpisy dokumentów poświadczane elektronicznie sporządzane są w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 tej ustawy.”;

c) pkt 12 otrzymuje brzmienie:

„12) po art. 74 dodaje się art. 74a w brzmieniu:

„Art. 74a. § 1. Doręczenie pism przez sąd następuje za pomocą środków komunikacji elektronicznej, jeżeli strona spełniła jeden z następujących warunków:

1) wniosła pismo w formie dokumentu elektronicznego przez elektroniczną skrzynkę podawczą sądu lub organu, za pośrednictwem którego składane jest pismo;

- 2) wystąpiła do sądu o takie doręczenie i wskazała sądowi adres elektroniczny;
- 3) wyraziła zgodę na doręczanie pism za pomocą tych środków i wskazała sądowi adres elektroniczny.

§ 2. Jeżeli strona zrezygnuje z doręczania pism za pomocą środków komunikacji elektronicznej, sąd doręcza pismo w sposób określony dla pisma w formie innej niż forma dokumentu elektronicznego.

§ 3. W celu doręczenia pisma w formie dokumentu elektronicznego sąd przesyła na adres elektroniczny adresata zawiadomienie zawierające:

- 1) informację, że adresat może odebrać pismo w formie dokumentu elektronicznego, wraz ze wskazaniem adresu elektronicznego, z którego adresat może pobrać dokument i pod którym powinien dokonać potwierdzenia doręczenia dokumentu;
- 2) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu identyfikacji adresata pod wskazanym adresem elektronicznym w systemie teleinformatycznym sądu, oraz informację o wymogu podpisania urzędowego poświadczenia odbioru kwalifikowanym podpisem elektronicznym, podpisem potwierdzonym profilem zaufanym ePUAP lub przez zastosowanie innych mechanizmów, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jeżeli takie mechanizmy zostały wprowadzone przez sąd administracyjny.

§ 4. Zawiadomienie, o którym mowa w § 3, może być automatycznie tworzone i przesyłane przez system teleinformatyczny sądu, a odbioru tego zawiadomienia nie potwierdza się.

§ 5. Datą doręczenia pisma jest data podpisania przez adresata pisma urzędowego poświadczenia odbioru w sposób, o którym mowa w § 3 pkt 2.

§ 6. W przypadku nieodebrania pisma w formie dokumentu elektronicznego sąd, po upływie siedmiu dni, licząc od dnia wysłania zawiadomienia, przesyła powtórne zawiadomienie o możliwości odebrania tego pisma.

§ 7. Do powtórnego zawiadomienia stosuje się przepisy § 3 i 4.

§ 8. W przypadku nieodebrania pisma, doręczenie uważa się za dokonane po upływie czternastu dni, licząc od dnia przesłania pierwszego zawiadomienia.

§ 9. W przypadku uznania pisma w formie dokumentu elektronicznego za doręczone sąd umożliwia adresatowi pisma w swoim systemie teleinformatycznym dostęp do treści pisma w formie dokumentu elektronicznego oraz do informacji o dacie uznania pisma za doręczone oraz o datach wysłania zawiadomień, o których mowa w § 3 i 6.

§ 10. W przypadku pism doręczanych uczestniczącym w postępowaniu przed sądem prokuratorowi, Rzecznikowi Praw Obywatelskich i Rzecznikowi Praw Dziecka oraz organowi, którego działanie, bezczynność lub przewlekłe prowadzenie postępowania zaskarżono, sąd przesyła pismo bezpośrednio do elektronicznej skrzynki podawczej podmiotu publicznego w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, za urzędowym poświadczeniem odbioru.

§ 11. Datą doręczenia pism, o których mowa w § 10, jest data określona w urzędowym poświadczeniu odbioru.

§ 12. Pisma sądu, odpisy pism i załączników w postępowaniu sądowym oraz orzeczeń, doręczane przez sąd w formie dokumentu elektronicznego opatrzone są kwalifikowanym podpisem elektronicznym.”;”;

2) w art. 11 pkt 3 otrzymuje brzmienie:

„3) art. 4, który wchodzi w życie z dniem 15 maja 2018 r.”.

Art. 110. W ustawie z dnia 14 marca 2014 r. o zasadach prowadzenia zbiorów publicznych (Dz. U. poz. 498) wprowadza się następujące zmiany:

1) w art. 9 ust. 2 otrzymuje brzmienie:

„2. Zgłoszenie zbiórki publicznej dokonywane w postaci elektronicznej osoba uprawniona do reprezentowania organizatora zbiórki opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

2) w art. 11 ust. 2 otrzymuje brzmienie:

„2. Akt założycielski sporządzony w postaci elektronicznej członkowie komitetu społecznego opatrzą kwalifikowanymi podpisami elektronicznymi lub podpisami potwierdzonymi profilem zaufanym ePUAP.”;

3) w art. 18 ust. 3 otrzymuje brzmienie:

„3. Sprawozdania sporządzone w postaci elektronicznej osoba uprawniona do reprezentowania organizatora zbiórki opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 111. 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 2016 r. poz. 217) w art. 70 ust. 1 otrzymuje brzmienie:

„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 ePUAP albo danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego.”.

Art. 112. W ustawie z dnia 11 lipca 2014 r. o petycjach (Dz. U. poz. 1195) w art. 4 ust. 5 otrzymuje brzmienie:

„5. Petycja składana za pomocą środków komunikacji elektronicznej może być opatrzona kwalifikowanym podpisem elektronicznym oraz powinna zawierać także adres poczty elektronicznej podmiotu wnoszącego petycję.”.

Art. 113. W ustawie z dnia 28 listopada 2014 r. – Prawo o aktach stanu cywilnego (Dz. U. poz. 1741, z późn. zm.²⁵⁾) wprowadza się następujące zmiany:

1) w art. 44 ust. 6 otrzymuje brzmienie:

„6. Odpis aktu stanu cywilnego, zaświadczenie o stanie cywilnym lub zaświadczenie o zamieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczących wskazanej osoby mogą zostać wydane, na wniosek, w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym.”;

²⁵⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 1888 oraz z 2015 r. poz. 262, 1087, 1274 i 2281.

2) w art. 54 ust. 4 otrzymuje brzmienie:

„4. Karta urodzenia i karta martwego urodzenia są przekazywane kierownikowi urzędu stanu cywilnego w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym.”;

3) w art. 144 ust. 5 otrzymuje brzmienie:

„5. Do dnia 1 stycznia 2018 r. karta urodzenia i karta martwego urodzenia mogą zostać przekazane kierownikowi urzędu stanu cywilnego w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym.”.

Art. 114. W ustawie z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2016 r. poz. 785) w art. 10:

1) ust. 10 otrzymuje brzmienie:

„10. Wniosek o przyznanie karty lub wydanie jej duplikatu składany w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. W przypadku gdy wniosek ten składany jest z wykorzystaniem systemu, o którym mowa w ust. 9a, w systemie tym może być zapewniony inny sposób potwierdzenia pochodzenia oraz integralności przesłanych danych w postaci elektronicznej.”;

2) ust. 12 otrzymuje brzmienie:

„12. W przypadku wniosku składanego w postaci elektronicznej, po wpisaniu do formularza wniosku numerów PESEL wnioskodawcy i członków rodziny wielodzietnej, formularz wniosku może być uzupełniony o dane zgromadzone w rejestrze PESEL w zakresie imion, nazwiska, daty urodzenia, stanu cywilnego, obywatelstwa wnioskodawcy i członków rodziny wielodzietnej.”.

Art. 115. W ustawie z dnia 5 lutego 2015 r. o płatnościach w ramach systemów wsparcia bezpośredniego (Dz. U. poz. 1551 oraz z 2016 r. poz. 337) wprowadza się następujące zmiany:

1) w art. 22:

a) w ust. 7 w pkt 1 lit. b otrzymuje brzmienie:

„b) te dokumenty w postaci elektronicznej opatrzone zaawansowanym podpisem elektronicznym;”;

b) ust. 9 otrzymuje brzmienie:

„9. Do złożenia wniosków, o których mowa w ust. 1, za pomocą formularza umieszczonego na stronie internetowej Agencji nie jest wymagany zaawansowany podpis elektroniczny.”;

2) w art. 33 ust. 4 otrzymuje brzmienie:

„4. Organ właściwy w sprawach, o których mowa w ust. 1 i 2, albo osoba przez niego upoważniona potwierdza kwalifikowanym podpisem elektronicznym zgodność z oryginałem cyfrowej kopii dokumentów, o których mowa w ust. 1 i 2.”.

Art. 116. W ustawie z dnia 20 lutego 2015 r. o wspieraniu rozwoju obszarów wiejskich z udziałem środków Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich w ramach Programu Rozwoju Obszarów Wiejskich na lata 2014–2020 (Dz. U. poz. 349 i 1888 oraz z 2016 r. poz. 337) wprowadza się następujące zmiany:

1) w art. 33 ust. 4 otrzymuje brzmienie:

„4. Organ właściwy w sprawie, o której mowa w ust. 1 lub 2, lub osoba przez niego upoważniona potwierdza kwalifikowanym podpisem elektronicznym zgodność z oryginałem cyfrowej kopii dokumentów, o których mowa w ust. 1 i 2.”;

2) w art. 42 ust. 5 otrzymuje brzmienie:

„5. Do złożenia wniosków, o których mowa w ust. 1, za pomocą formularza, o którym mowa w ust. 4, nie jest wymagany zaawansowany podpis elektroniczny.”.

Art. 117. W ustawie z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz. U. poz. 478 i 2365 oraz z 2016 r. poz. 925) wprowadza się następujące zmiany:

1) w art. 79 ust. 4 otrzymuje brzmienie:

„4. Oferty opatruje się, pod rygorem nieważności, kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;

2) w art. 138 w ust. 5 pkt 1 i 2 otrzymują brzmienie:

„1) opatruje się kwalifikowanym podpisem elektronicznym albo
2) podpisem potwierdzonym profilem zaufanym ePUAP.”;

3) w art. 147 w ust. 5 pkt 1 i 2 otrzymują brzmienie:

„1) opatruje się kwalifikowanym podpisem elektronicznym albo
2) podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 118. W ustawie z dnia 15 maja 2015 r. o substancjach zubożających warstwę ozonową oraz o niektórych fluorowanych gazach cieplarnianych (Dz. U. poz. 881) wprowadza się następujące zmiany:

1) w art. 6 ust. 2 otrzymuje brzmienie:

„2. Wnioski sporządza się w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, na formularzu według wzoru określonego w przepisach wydanych na podstawie ust. 12, w języku polskim wraz z tłumaczeniem wniosku na język angielski.”;

2) w art. 8 ust. 5 otrzymuje brzmienie:

„5. Wniosek o udzielenie autoryzacji oraz oświadczenia dołączane do niego składa się w formie pisemnej w postaci papierowej albo elektronicznej. Wniosek w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP. Dokumenty potwierdzające spełnienie wymagań, o których mowa w ust. 2 pkt 1 i 2, składa się w kopii lub elektronicznej kopii. Minister właściwy do spraw środowiska może żądać od przedsiębiorstwa lub operatora przedstawienia oryginałów dokumentów potwierdzających spełnienie wymagań, o których mowa w ust. 2 pkt 1 i 2.”;

3) w art. 9:

a) ust. 4 otrzymuje brzmienie:

„4. Wnioski sporządza się w postaci elektronicznej na formularzu według wzoru określonego w przepisach wydanych na podstawie ust. 8 i opatruje kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.”;

b) ust. 6 otrzymuje brzmienie:

„6. Przedsiębiorstwa, które uzyskały wpis do rejestru, o którym mowa w art. 7 ust. 1, i zaprzestały prowadzenia działalności, o której mowa w ust. 1, są obowiązane poinformować o tym fakcie ministra właściwego do spraw środowiska, pismem w postaci elektronicznej opatrzonym kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, w terminie 60 dni od dnia zaprzestania prowadzenia takiej działalności.”;

4) w art. 25:

a) ust. 4 otrzymuje brzmienie:

„4. Podmiot zamierzający pełnić funkcję jednostki oceniającej personel zgłasza taki zamiar w formie pisemnej w postaci papierowej albo elektronicznej do jednostki certyfikującej personel. Zgłoszenie w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.”,

b) ust. 6 otrzymuje brzmienie:

„6. Do zgłoszenia dołącza się, w formie pisemnej w postaci papierowej albo elektronicznej, oświadczenie o dysponowaniu odpowiednim wyposażeniem technicznym niezbędnym do przeprowadzania egzaminów oraz zatrudnianiu osób posiadających odpowiednią wiedzę teoretyczną i doświadczenie praktyczne. Oświadczenie w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP. Oświadczenie składane jest pod rygorem odpowiedzialności karnej za składanie fałszywych zeznań. Oświadczenie zawiera klauzulę następującej treści: „Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.”. Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za składanie fałszywych zeznań.”;

5) w art. 27:

a) ust. 2 otrzymuje brzmienie:

„2. Podmiot zamierzający pełnić funkcję jednostki prowadzącej szkolenia zgłasza taki zamiar w formie pisemnej w postaci papierowej albo elektronicznej do jednostki certyfikującej personel. Zgłoszenie w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.”,

b) ust. 4 otrzymuje brzmienie:

„4. Do zgłoszenia dołącza się, w formie pisemnej w postaci papierowej albo elektronicznej, oświadczenie o spełnieniu wymagań określonych w ust. 1 pkt 1–3, składane pod rygorem odpowiedzialności karnej za składanie fałszywych zeznań. Oświadczenie w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP. Oświadczenie zawiera klauzulę następującej treści: „Jestem świadomy

odpowiedzialności karnej za złożenie fałszywego oświadczenia.”. Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za składanie fałszywych zeznań.”;

6) w art. 37:

a) ust. 7 otrzymuje brzmienie:

„7. Podmiot zamierzający pełnić funkcję jednostki, o której mowa w ust. 2, jest obowiązany zgłosić do jednostki certyfikującej personel zamiar rozpoczęcia prowadzenia szkoleń i wydawania zaświadczeń o odbytym szkoleniu, w formie pisemnej w postaci papierowej albo elektronicznej. Zgłoszenie w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.”,

b) ust. 9 otrzymuje brzmienie:

„9. Do zgłoszenia dołącza się, w formie pisemnej w postaci papierowej albo elektronicznej, oświadczenie o spełnieniu wymagań określonych w ust. 2 pkt 1–3, składane pod rygorem odpowiedzialności karnej za składanie fałszywych zeznań. Oświadczenie w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP. Oświadczenie zawiera klauzulę następującej treści: „Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.”. Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za składanie fałszywych zeznań.”;

7) w art. 41 ust. 5 otrzymuje brzmienie:

„5. Podmioty użytkujące systemy ochrony przeciwpożarowej i gaśnice zawierające halony i przeznaczone do zastosowań krytycznych, zgodnie z rozporządzeniem (WE) nr 1005/2009, będące na wyposażeniu jednostek organizacyjnych Sił Zbrojnych Rzeczypospolitej Polskiej, przekazują do Ministra Obrony Narodowej sprawozdania, o których mowa w ust. 4, w formie pisemnej w postaci papierowej albo elektronicznej, w terminie do dnia 28 lutego za rok poprzedni. Sprawozdania w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP. Minister Obrony Narodowej przygotowuje zbiorcze zestawienie sprawozdań i przekazuje je do wyspecjalizowanej jednostki, w postaci elektronicznej, do dnia 31 marca za rok poprzedni.”.

Art. 119. W ustawie z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. poz. 978, z późn. zm.²⁶⁾) w art. 203 ust. 2 otrzymuje brzmienie:

„2. Jeżeli ustawa przewiduje złożenie dokumentu w postaci elektronicznej, dokument składa się za pośrednictwem Rejestru i opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”.

Art. 120. W ustawie z dnia 12 czerwca 2015 r. o systemie handlu uprawnieniami do emisji gazów cieplarnianych (Dz. U. poz. 1223 oraz z 2016 r. poz. 266 i 542) wprowadza się następujące zmiany:

1) w art. 10 w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Krajowy ośrodek informuje niezwłocznie, pismem w postaci elektronicznej opatrzonym kwalifikowanym podpisem elektronicznym albo pismem w postaci papierowej, podmiot ubiegający się o otwarcie rachunku w rejestrze Unii albo posiadacza rachunku w tym rejestrze o”;

2) w art. 32 ust. 7 otrzymuje brzmienie:

„7. Wniosek, o którym mowa w ust. 4, sporządza się w postaci papierowej albo elektronicznej, za pomocą formularza, według wzoru określonego w przepisach wydanych na podstawie art. 36 ust. 6 pkt 1. Wniosek w postaci elektronicznej opatruje się kwalifikowanym podpisem elektronicznym.”;

3) w art. 38 ust. 5 otrzymuje brzmienie:

„5. Podmiot realizujący zadanie inwestycyjne jest obowiązany poinformować, pismem w postaci elektronicznej opatrzonym kwalifikowanym podpisem elektronicznym albo pismem w postaci papierowej, ministra właściwego do spraw środowiska o terminie zaprzestania realizacji tego zadania, nie później niż po upływie 21 dni od dnia zaprzestania realizacji zadania inwestycyjnego.”;

4) w art. 58 ust. 2 otrzymuje brzmienie:

„2. Prowadzący instalację jest obowiązany poinformować, pismem w postaci elektronicznej opatrzonym kwalifikowanym podpisem elektronicznym albo pismem w postaci papierowej, organ właściwy do wydania zezwolenia i Krajowy ośrodek o wystąpieniu przypadku, o którym mowa w ust. 1, w terminie 21 dni od dnia jego wystąpienia.”.

²⁶⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615.

Art. 121. W ustawie z dnia 25 czerwca 2015 r. – Prawo konsularne (Dz. U. poz. 1274) wprowadza się następujące zmiany:

- 1) w art. 68 w ust. 2 pkt 3 otrzymuje brzmienie:

„3) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym konsula służącym do obsługi doręczeń, oraz informację o wymogu podpisania urzędowego poświadczenia odbioru w określony sposób.”;
- 2) w art. 75 ust. 2 otrzymuje brzmienie:

„2. Wniosek w formie dokumentu elektronicznego wniesiony za pomocą elektronicznej skrzynki podawczej opatruje się podpisem potwierdzonym profilem zaufanym ePUAP lub kwalifikowanym podpisem elektronicznym.”;
- 3) w art. 81 ust. 1 otrzymuje brzmienie:

„1. Decyzja zawiera oznaczenie konsula, datę wydania, oznaczenie strony, powołanie podstawy prawnej, rozstrzygnięcie, uzasadnienie prawne i faktyczne, pouczenie o możliwości i trybie wniesienia odwołania od decyzji oraz podpis urzędnika konsularnego z podaniem imienia i nazwiska oraz zajmowanego stanowiska; jeżeli decyzja została wydana w formie dokumentu elektronicznego, urzędnik konsularny opatruje decyzję kwalifikowanym podpisem elektronicznym.”.

Art. 122. W ustawie z dnia 10 lipca 2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. poz. 1311, z późn. zm.²⁷⁾) wprowadza się następujące zmiany:

- 1) w art. 1:
 - a) pkt 9 otrzymuje brzmienie:

„9) po art. 78 dodaje się art. 78¹ w brzmieniu:

„Art. 78¹. § 1. Do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym.

§ 2. Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej.”;
 - b) pkt 11 otrzymuje brzmienie:

²⁷⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 1513 oraz z 2016 r. poz. 178, 394 i 615.

„11) w art. 81 w § 2 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu:

„3) w razie opatrzenia kwalifikowanym elektronicznym znacznikiem czasu dokumentu w postaci elektronicznej – od daty opatrzenia kwalifikowanym elektronicznym znacznikiem czasu.”;

2) w art. 2:

a) pkt 33 otrzymuje brzmienie:

„33) w art. 324 dodaje się § 4 w brzmieniu:

„§ 4. W postępowaniu wszczętym za pośrednictwem systemu teleinformatycznego wyrok może być utrwalony w systemie teleinformatycznym i opatrzony kwalifikowanym podpisem elektronicznym.”;

b) w pkt 74 lit. a w zakresie dodawanego § 3¹ otrzymuje brzmienie:

„§ 3¹. Postanowienie o nadaniu klauzuli wykonalności tytułom egzekucyjnym, o których mowa w art. 777 § 1 pkt 1 i 1¹, wydanym w postaci elektronicznej, jest wydawane bez spisania odrębnej sentencji, poprzez umieszczenie klauzuli wykonalności w systemie teleinformatycznym i opatrzenie jej kwalifikowanym podpisem elektronicznym, sędziego albo referendarza sądowego, który wydaje postanowienie.”;

3) w art. 3 w pkt 10 lit. b w zakresie dodawanego § 2a otrzymuje brzmienie:

„§ 2a. Jeżeli zawiadomienie o zajęciu prawa majątkowego doręcza się dłużnikowi zajętej wierzytelności przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej:

1) w zawiadomieniu o zajęciu nie umieszcza się podpisu z podaniem imienia, nazwiska i stanowiska służbowego podpisującego oraz odcisku pieczęci organu egzekucyjnego;

2) zawiadomienie o zajęciu zawiera numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub numer identyfikacji podatkowej (NIP) zobowiązanego, o ile są znane organowi egzekucyjnemu;

3) zawiadomienie o zajęciu opatruje się kwalifikowanym podpisem elektronicznym.”;

4) w art. 7:

a) pkt 2 w zakresie zmienianego art. 95h § 1 otrzymuje brzmienie:

„§ 1. Notariusz niezwłocznie po sporządzeniu aktu poświadczenia dziedziczenia dokonuje jego wpisu do Rejestru Spadkowego przez wprowadzenie za pośrednictwem systemu teleinformatycznego danych wynikających z tego aktu, o których mowa w art. 95ha pkt 3–7. Notariusz opatruje wpis kwalifikowanym podpisem elektronicznym.”,

b) pkt 4 w zakresie zmienianego art. 95i § 1 otrzymuje brzmienie:

„§ 1. Krajowa Rada Notarialna tworzy system teleinformatyczny w celu prowadzenia Rejestru Spadkowego, zapewnia notariuszom i sądom dostęp do tego systemu w celu dokonywania wpisów oraz ochronę danych zgromadzonych w Rejestrze Spadkowym przed nieuprawnionym dostępem, przetwarzaniem oraz zmianą lub utratą. Dane weryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego zapewniają notariuszowi oraz prezesowi sądu lub osobie przez niego wyznaczonej dostęp do Rejestru Spadkowego.”,

c) pkt 6 otrzymuje brzmienie:

„6) w art. 97 dotychczasową treść oznacza się jako § 1 i dodaje się § 2 w brzmieniu:

„§ 2. Elektroniczne poświadczenie zgodności odpisu, wyciągu lub kopii z okazanym dokumentem notariusz opatruje kwalifikowanym podpisem elektronicznym.”.

Art. 123. W ustawie z dnia 9 października 2015 r. o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA (Dz. U. poz. 1712) w art. 8 w ust. 11 pkt 9 otrzymuje brzmienie:

„9) podpis osoby upoważnionej, z podaniem jej imienia i nazwiska oraz stanowiska służbowego, a jeżeli wynik kontroli został wydany w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny.”.

Art. 124. W ustawie z dnia 9 października 2015 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (Dz. U. poz. 1991, z późn. zm.²⁸⁾) wprowadza się następujące zmiany:

1) w art. 4 w pkt 2 lit. b w zakresie dodawanego ust. 6 i 7 otrzymuje brzmienie:

„6. Warunkiem dokonywania przez osoby określone w ust. 5 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

7. Potwierdzenia, o którym mowa w ust. 6, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą uczelnię medyczną w zakresie tożsamości osoby, która konto założyła, lub
- 3) potwierdzonego przez właściwą okręgową izbę lekarską lub Naczelną Izbę Lekarską w zakresie tożsamości osoby, która konto założyła.”;

2) w art. 9 pkt 2 w zakresie dodawanego art. 10b ust. 4 i 5 otrzymuje brzmienie:

„4. Warunkiem dokonywania przez osoby określone w ust. 3 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

5. Potwierdzenia, o którym mowa w ust. 4, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą uczelnię lub wojewodę właściwego ze względu na miejsce zamieszkania, a w przypadku gdy nie jest możliwe ustalenie właściwego wojewody, Wojewodę Mazowieckiego, w zakresie tożsamości osoby, która konto założyła.”;

3) w art. 13:

a) w pkt 3 lit. b otrzymuje brzmienie:

„b) dodaje się ust. 3 w brzmieniu:

²⁸⁾ Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2016 r. poz. 65, 580, 652 i 832.

„3. Wynikiem negocjacji jest dokument sporządzony w postaci elektronicznej w trakcie negocjacji podpisany przez przewodniczącego zespołu negocjacyjnego oraz wnioskodawcę za pomocą podpisu potwierdzonego profilem zaufanym ePUAP lub kwalifikowanym podpisem elektronicznym, przekazywany następnie Komisji w celu podjęcia uchwały.”;

b) w pkt 4 lit. c w zakresie dodawanego ust. 6a otrzymuje brzmienie:

„6a. Wnioski, o których mowa w ust. 1, oraz dokumenty, o których mowa w ust. 2, opatruje się podpisem potwierdzonym profilem zaufanym ePUAP lub kwalifikowanym podpisem elektronicznym.”;

c) pkt 8 w zakresie dodawanego art. 32a ust. 8 otrzymuje brzmienie:

„8. Wniosek o założenie konta w SOLR złożony w postaci elektronicznej opatruje się podpisem potwierdzonym profilem zaufanym ePUAP lub kwalifikowanym podpisem elektronicznym.”;

4) w art. 15:

a) w pkt 8 lit. b w zakresie dodawanego ust. 4c i 4d otrzymuje brzmienie:

„4c. Warunkiem dokonywania przez osoby określone w ust. 4b czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

4d. Potwierdzenia, o którym mowa w ust. 4c, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwego organizatora kształcenia pielęgniarek i położnych w zakresie tożsamości osoby, która konto założyła, lub
- 3) potwierdzonego przez właściwą okręgową izbę pielęgniarek i położnych lub Naczelną Izbę Pielęgniarek i Położnych w zakresie tożsamości osoby, która konto założyła.”;

b) w pkt 12 lit. b w zakresie dodawanego ust. 1a i 1b otrzymuje brzmienie:

„1a. Warunkiem dokonywania określonych ustawą czynności za pomocą SMK jest założenie konta w sposób umożliwiający potwierdzenie danych podmiotu zamierzającego wykonywać działalność w zakresie kształcenia podyplomowego, o którym mowa w ust. 1, do dokonywania tych czynności.

1b. Potwierdzenia, o którym mowa w ust. 1a, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą okręgową izbę pielęgniarek i położnych lub Naczelną Izbę Pielęgniarek i Położnych w zakresie danych podmiotu zamierzającego wykonywać działalność w zakresie kształcenia podyplomowego, o którym mowa w ust. 1.”,

c) w pkt 16 lit. c w zakresie dodawanego ust. 7 i 8 otrzymuje brzmienie:

„7. Warunkiem dokonywania określonych ustawą czynności za pomocą SMK jest założenie konta w sposób umożliwiający potwierdzenie danych podmiotu zamierzającego wykonywać działalność w zakresie kształcenia podyplomowego, o którym mowa w ust. 1, do dokonywania tych czynności.

8. Potwierdzenia, o którym mowa w ust. 7, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą okręgową izbę pielęgniarek i położnych lub Naczelną Izbę Pielęgniarek i Położnych w zakresie danych podmiotu zamierzającego wykonywać działalność w zakresie kształcenia podyplomowego, o którym mowa w ust. 1.”;

5) w art. 28 ust. 2 i 3 otrzymują brzmienie:

„2. Warunkiem dokonywania przez osoby określone w art. 20–27 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

3. Potwierdzenia, o którym mowa w ust. 2, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą okręgową izbę lekarską lub Naczelną Izbę Lekarską w zakresie tożsamości osoby, która konto założyła.”;

6) w art. 35 ust. 2 i 3 otrzymują brzmienie:

„2. Warunkiem dokonywania przez osoby określone w art. 31, art. 33 i art. 34 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

3. Potwierdzenia, o którym mowa w ust. 2, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez Krajową Izbę Diagnostów Laboratoryjnych w zakresie tożsamości osoby, która konto założyła.”;

7) w art. 43 ust. 2 i 3 otrzymują brzmienie:

„2. Warunkiem dokonywania przez osoby określone w art. 39, art. 41 i art. 42 czynności za pomocą SMK jest potwierdzenie tożsamości osoby, która konto założyła, i weryfikacja uprawnień tej osoby.

3. Potwierdzenia, o którym mowa w ust. 2, dokonuje się na podstawie wniosku o nadanie uprawnień:

- 1) podpisanego kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP lub
- 2) potwierdzonego przez właściwą okręgową izbę aptekarską lub Naczelną Izbę Aptekarską w zakresie tożsamości osoby, która konto założyła.”.

Art. 125. W ustawie z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2016 r. poz. 177) w art. 68 § 2 otrzymuje brzmienie:

„§ 2. Dopuszcza się również komunikowanie się prokuratora z sądem w elektronicznym postępowaniu upominawczym przy wykorzystaniu kwalifikowanego podpisu elektronicznego.”.

Art. 126. W ustawie z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. poz. 195) w art. 13:

1) ust. 7 otrzymuje brzmienie:

„7. Wniosek i załączniki do wniosku określone w ust. 4 składane w postaci elektronicznej za pomocą systemów teleinformatycznych, o których mowa w ust. 5 pkt 1, 2 i 4, opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP lub uwierzytelnia w sposób zapewniający

możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej.”;

2) ust. 11 otrzymuje brzmienie:

„11. W przypadku wniosku składanego w postaci elektronicznej opatrzonego kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP lub uwierzytelnionego w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej, po wpisaniu do formularza wniosku numerów PESEL osoby występującej o przyznanie świadczenia wychowawczego i dzieci pozostających na utrzymaniu tej osoby, formularz wniosku może być uzupełniony o dane zgromadzone w rejestrze PESEL w zakresie imion, nazwiska, daty urodzenia, stanu cywilnego, obywatelstwa i płci osoby występującej o przyznanie świadczenia wychowawczego i dzieci pozostających na utrzymaniu tej osoby.”.

Art. 127. W ustawie z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. poz. 542) w art. 23 ust. 4 otrzymuje brzmienie:

„4. Wniosek złożony za pomocą środków komunikacji elektronicznej opatruje się kwalifikowanym podpisem elektronicznym.”.

Rozdział 9

Przepisy przejściowe

Art. 128. Bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, z 2014 r. poz. 1662 oraz z 2015 r. poz. 1893) jest kwalifikowanym podpisem elektronicznym w rozumieniu niniejszej ustawy.

Art. 129. 1. Zaświadczenia certyfikacyjne, poświadczenia elektroniczne i certyfikaty wydane zgodnie z przepisami ustawy z dnia 18 września 2001 r. o podpisie elektronicznym zachowują ważność przez okres w nich wskazany, o ile nie zostaną unieważnione.

2. Do zaświadczeń certyfikacyjnych, poświadczeń elektronicznych i certyfikatów, o których mowa w ust. 1, stosuje się odpowiednio przepisy dotyczące certyfikatów krajowych dostawców usług zaufania oraz narodowego centrum certyfikacji.

Art. 130. 1. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne, o którym mowa w art. 23 ust. 1 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, staje się rejestrem dostawców usług zaufania w rozumieniu niniejszej ustawy.

2. Usługę znakowania czasem, o której mowa w art. 3 pkt 16 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, wpisaną do rejestru, o którym mowa w art. 23 ust. 1 tej ustawy, uznaje się za usługę elektronicznego znacznika czasu.

3. Elektroniczny znacznik czasu, o którym mowa w ust. 2, wywołuje skutki prawne określone w art. 7 ust. 2 i 3 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.

Art. 131. Upoważnienie udzielone Narodowemu Bankowi Polskiemu przez ministra właściwego do spraw gospodarki na podstawie art. 23 ust. 5 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym zachowuje moc do chwili odwołania przez ministra właściwego do spraw informatyzacji.

Art. 132. 1. Postępowania wszczęte i prowadzone przed dniem wejścia w życie niniejszej ustawy przed ministrem właściwym do spraw gospodarki w sprawach, w których właściwy na mocy przepisów niniejszej ustawy staje się minister właściwy do spraw informatyzacji, są prowadzone na podstawie przepisów dotychczasowych przez ministra właściwego do spraw informatyzacji.

2. Minister właściwy do spraw gospodarki, w terminie 14 dni od dnia wejścia w życie niniejszej ustawy, przekaze ministrowi właściwemu do spraw informatyzacji dokumentację w zakresie przejętych przez niego spraw.

3. Z dniem wejścia w życie niniejszej ustawy stroną udzielonych upoważnień lub umów zawartych przez ministra właściwego do spraw gospodarki w zakresie spraw przekazanych na podstawie niniejszej ustawy staje się minister właściwy do spraw informatyzacji.

Art. 133. Banki wykonujące czynności, o których mowa w art. 6 ust. 1 pkt 6a ustawy zmienianej w art. 64, w brzmieniu dotychczasowym, są obowiązane dostosować statuty do przepisów ustawy zmienianej w art. 64, w brzmieniu nadanym niniejszą ustawą, w terminie 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 134. Do dnia 1 lipca 2018 r. do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych można stosować funkcję skrótu SHA-1, chyba że wymagania techniczne wynikające z aktów wykonawczych wydanych na podstawie rozporządzenia 910/2014 wyłączą możliwość stosowania tej funkcji skrótu.

Art. 135. Do umów ubezpieczenia odpowiedzialności cywilnej zawartych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

Art. 136. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 10 ust. 5 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 14 ust. 5, jednak nie dłużej niż 3 miesiące od dnia wejścia w życie niniejszej ustawy.

Art. 137. Prezes Rady Ministrów dokona, w drodze rozporządzenia, przeniesienia planowanych dochodów i wydatków budżetowych, w tym wynagrodzeń oraz limitów zatrudnienia, między częścią budżetu państwa, której dysponentem jest minister właściwy do spraw gospodarki, a częścią, której dysponentem jest minister właściwy do spraw informatyzacji, z zachowaniem przeznaczenia środków publicznych wynikających z ustawy budżetowej.

Rozdział 10

Przepisy końcowe

Art. 138. Traci moc ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, z 2014 r. poz. 1662 oraz z 2015 r. poz. 1893).

Art. 139. Ustawa wchodzi w życie po upływie 7 dni od dnia ogłoszenia, z wyjątkiem art. 23, art. 25–27 i art. 94 pkt 4 w zakresie zmienianego art. 20a ust. 1 pkt 1, które wchodzi w życie z dniem 29 września 2018 r.

UZASADNIENIE

1. Potrzeba i cel wydania aktu

Wejście w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania publicznego w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (eIDAS) implikuje nowy porządek prawny w obszarze usług zaufania, co rodzi konieczność dostosowania prawa krajowego do nowych uwarunkowań. Celem regulacji zawartych w ustawie o usługach zaufania oraz identyfikacji elektronicznej jest wydanie przepisów w odniesieniu do kwestii wskazanych przez eIDAS jako pozostające w kompetencji państw członkowskich oraz dokonanie koniecznych do prawidłowej realizacji rozporządzenia eIDAS zmian w aktach rangi ustawowej. Obecne rozwiązania w polskim porządku prawnym nie przystają do rozporządzenia eIDAS, w związku z czym niezbędne jest uchylenie ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, oraz powstrzymanie się, co do zasady, od regulowania tej materii przepisami prawa krajowego. Rozporządzenie eIDAS wraz z systemem aktów wykonawczych będzie obowiązywać bezpośrednio w krajowym porządku prawnym.

W prawie polskim regulowana była dotychczas w sposób pełny jedynie instytucja podpisu elektronicznego (w tym zwłaszcza bezpiecznego podpisu elektronicznego) oraz znakowanie czasem. Rozporządzenie eIDAS poszerza gamę dostępnych usług oraz nakłada na państwa członkowskie obowiązek ustanowienia nadzoru. Kwestie dotyczące nadzoru usług zaufania oraz notyfikacji systemów elektronicznej identyfikacji stanowią najważniejszą treść nowej krajowej regulacji.

Ważną funkcją ustawy jest usunięcie istniejących w krajowych przepisach odwołań do ustawy o podpisie elektronicznym, która zostanie uchylona, dostosowanie terminologii oraz wprowadzenie niezbędnych odwołań do rozporządzenia eIDAS, w tym stworzenie warunków dla zapewnienia zgodności usługodawców z wymaganiami określonymi przez rozporządzenie eIDAS oraz raportowania i zgłaszania incydentów w zakresie usług zaufania.

Regulacje zawarte w rozporządzeniu eIDAS dotyczące usług zaufania pozostawiają w kilku obszarach swobodę dla prawa krajowego. Niezbędne jest m.in. określenie na poziomie ustawy porządku instytucjonalnego w sposób określający role poszczególnych instytucji, których pełnienie jest przewidziane rozporządzeniem eIDAS. Rozporządzenie nakłada na państwa członkowskie wymóg ustanowienia

i notyfikowania nadzoru nad usługami zaufania. Ustawa zakłada, że organem nadzoru nad usługami zaufania będzie minister właściwy do spraw informatyzacji. Nadzór dotyczył będzie zarówno usług kwalifikowanych, jak i niekwalifikowanych. W niezbędnym zakresie celem zapewnienia efektywności sprawowanego nadzoru ustawa wprowadza kary. Określenie czynów niedozwolonych z punktu widzenia zapewnienia bezpieczeństwa rynku usług zaufania jest analogiczne do zapisów istniejących w dotychczasowej (uchylanej) ustawie o podpisie elektronicznym.

Rozporządzenie eIDAS odsyła do prawa krajowego w zakresie zasad odpowiedzialności cywilnoprawnej dostawców usług zaufania. Co do zasady, odpowiedzialność ta jest uregulowana w Kodeksie Cywilnym, stąd wprowadzenie kompleksowej regulacji w tym zakresie jest bezprzedmiotowe.

Rozporządzenie eIDAS powoduje wprowadzenie do obrotu prawnego nowych usług zaufania, a przez to również nowych pojęć. Zmiany wymaga zatem siatka pojęciowa funkcjonująca dotychczas w wielu aktach prawnych w Polsce, a także niezbędne jest wprowadzenie w polskim systemie prawnym zmian porządkujących oraz zapewniających spójność systemu prawa. Dotyczy to w szczególności zastąpienia bezpiecznego podpisu elektronicznego weryfikowanego ważnym certyfikatem kwalifikowanym przez kwalifikowany podpis elektroniczny oraz znakowania czasem przez kwalifikowany znacznik czasu.

2. Stan faktyczny do uregulowania

Celem ustawy jest stworzenie warunków do realizacji rozporządzenia eIDAS przez:

- 1) dostosowanie krajowego porządku prawnego do uwarunkowań rozporządzenia eIDAS przez wyeliminowanie wszelkich przepisów niezgodnych z rozporządzeniem eIDAS, np. wyeliminowanie pojęć nieznanymi rozporządzeniu eIDAS, dostosowanie terminologii w krajowych aktach do terminów występujących w rozporządzeniu eIDAS, tj. dokonanie swoistego „czyszczenia” systemu prawa. Należy przy tym zaznaczyć, że ustawa o usługach zaufania może wprowadzić określone zmiany w innych ustawach, ale nie może i nie wprowadza zmian w aktach niższego rzędu, w tym w rozporządzeniach i aktach prawa lokalnego;

- 2) uregulowanie tych obszarów, które niezbędne są do umożliwienia stosowania rozporządzenia eIDAS na gruncie prawa polskiego, tj. m.in. przyporządkowanie ról odpowiednim organom w zakresie kompetencji nadzorczych;
- 3) terminologia rozporządzenia eIDAS została ujednolicona na poziomie europejskim i z tego względu krajowy porządek prawny powinien być do niej dostosowany. Zmiany wymagają pojęcia, które nie będą dłużej funkcjonowały w krajowym systemie prawnym, ale same narzędzia zostaną utrzymane. Należy dokonać nowelizacji szeregu aktów prawnych, wprowadzając terminologię zgodną z eIDAS.

Na potrzeby opracowania niniejszej ustawy dokonano analizy krajowego porządku prawnego pod kątem wymaganych zmian w związku z wejściem w życie rozporządzenia eIDAS. Analiza ta doprowadziła do poniższych wniosków.

Po pierwsze, w krajowym porządku prawnym istnieje wiele aktów prawnych, których przepisy odsyłają do ustawy o podpisie elektronicznym. Są to najczęściej odesłania do pojęć stosowanych w tej ustawie.

Drugą grupą aktów prawnych, które analizowano na potrzeby niniejszej ustawy są akty, które zawierają w swojej treści pojęcia odnoszące się do usług zaufania.

Samo uchylene ustawy o podpisie elektronicznym doprowadziłoby do pojawienia się w polskim porządku prawnym pustych odesłań i pustych definicji w wielu aktach prawnych dotyczących rozmaitych dziedzin. W związku z tym ustawa zawiera nowelizację wszystkich aktów prawnych, które wymagają zmiany w związku z uchycieniem ustawy o podpisie elektronicznym.

Ustawa o podpisie elektronicznym regulowała usługę podpisu elektronicznego, znakowanie czasem oraz przewidywała inne usługi certyfikacyjne (tzw. usługi nienazwane). W rozporządzeniu eIDAS mowa jest o podpisie elektronicznym, zaawansowanym podpisie elektronicznym oraz kwalifikowanym podpisie elektronicznym, podczas gdy w ustawie o podpisie elektronicznym użyte zostały analogiczne pojęcia podpisu elektronicznego, bezpiecznego podpisu elektronicznego oraz bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu. Ponadto rozporządzenie eIDAS wprowadza do europejskiego porządku prawnego zamknięty katalog unijnych usług zaufania, których ewentualne doregulowanie (wyłącznie w zakresie niezharmonizowanym) zostało pozostawione krajowym porządkom prawnym. Należy zwrócić uwagę na fakt, że rozporządzenie eIDAS wprowadziło wprost skutek prawny

kwalifikowanego podpisu elektronicznego, wskazując, że jest on równoważny względem podpisu własnoręcznego bez względu na to, w którym z państw członkowskich został wydany kwalifikowany certyfikat.

3. Różnice i podobieństwa między dotychczasowym a projektowanym stanem prawnym

Określając zakres przedmiotowy ustawy uwzględniono fakt, że rozporządzenie eIDAS odsyła w bardzo wielu kwestiach do obligatoryjnych, lub – w większej liczbie – fakultatywnych aktów wykonawczych, które mają być wydane przez Komisję Europejską. Dotyczy to przede wszystkim określenia norm, formatów referencyjnych odnoszących się do poszczególnych usług zaufania czy też określonych procedur. Rozporządzenie eIDAS zawiera regulacje dotyczące zarówno samego podpisu elektronicznego, jak też innych usług zaufania takich jak: pieczęć elektroniczna, elektroniczny znacznik czasu, usługa rejestrowanego doręczenia elektronicznego, uwierzytelnianie witryn internetowych. Prawodawca unijny zdecydował się na wydanie jednej regulacji, która obejmuje kilka rozwijających się usług zaufania. Niektóre z nich są jednak regulowane w sposób cząstkowy, co przemawia za wydaniem krajowych aktów prawnych. Prace w tym zakresie będą prowadzone etapowo, gdyż obecnie nie są znane szczegółowe wymagania techniczne dla niektórych nowych usług. Wprowadzenie krajowo specyficznych uregulowań w zakresie kwalifikowanych lub niekwalifikowanych usług zaufania wymagałoby skierowania aktu do notyfikacji przepisów prawa technicznego, co nie jest możliwe w okresie bezpośrednio poprzedzającym wydanie regulacji. Wprowadzenie do stosowania narzędzi takich jak e-doręczenia czy e-konserwacja będzie wymagać innej ustawy oraz szerokich konsultacji z interesariuszami.

Ustawa zawiera podstawę prawną do wydania niezbędnych aktów wykonawczych, które doregulują w sposób szczegółowy zagadnienia ubezpieczenia odpowiedzialności cywilnej oraz krajowej infrastruktury zaufania – podobnie jak miało to miejsce w przypadku ustawy o podpisie elektronicznym.

W ramach krajowej infrastruktury zaufania (rozdział 2 ustawy) utrzymuje się dotychczasową strukturę opartą o narodowe centrum certyfikacji (NCC) funkcjonujące w ramach Narodowego Banku Polskiego, które wydaje certyfikaty dla kwalifikowanych dostawców usług zaufania, służące do weryfikacji pieczęci i podpisów

zaawansowanych, którymi opatrują oni kwalifikowane certyfikaty wydawane dla użytkowników końcowych oraz prowadzi zaufaną listę.

Przepisy dotyczące wydawania certyfikatów dla kwalifikowanych dostawców usług zaufania (art. 11 i art. 17) nie skutkują dodatkowymi wymogami w stosunku do składników certyfikatów, określonych w załącznikach do eIDAS w zakresie, w jakim wymagają one jedynie podpisu zaawansowanego. Certyfikat dostawcy usług zaufania jest poświadczeniem potwierdzającym powiązanie danych do składania podpisu/pieczeni z kwalifikowanym dostawcą usług zaufania. Dane do składania podpisu/pieczeni każdy dostawca usług zaufania tworzy samodzielnie i przy ich pomocy tworzy zaawansowany podpis/zaawansowaną pieczęć, o których mowa odpowiednio w załączniku I lit. g, załączniku III lit. g oraz załączniku IV lit. h do eIDAS. Jednocześnie honorowane będą wszelkie inne certyfikaty kwalifikowane z zagranicy, które powstały w architekturach bez takiego powiązania. Decyzja organu nadzoru o przyznaniu dostawcy usług zaufania statusu kwalifikowanego dostawcy usług zaufania jest równoznaczna z niezwłocznym wydaniem certyfikatu dla tego dostawcy i umieszczeniem go na liście zaufania, co automatycznie umożliwia ww. dostawcy świadczenie usług.

To rozwiązanie sprawdziło się w dotychczasowej praktyce ustanowionej w ustawie o podpisie elektronicznym. Specyficzna pozycja ustrojowa NBP jako centralnego banku państwa, polegająca na niezależności wobec organów państwowych, gwarantuje, że powierzone kluczowe zadanie utrzymywania najwyższego poziomu w strukturze bezpieczeństwa usług zaufania nie będzie podważane za pomocą argumentów wskazujących na zależność tej jednostki od kogokolwiek. Na uwagę zasługuje fakt, że narodowe centrum certyfikacji nie wydaje kwalifikowanych certyfikatów, a jego działalność nie jest działalnością dostawcy usług zaufania w rozumieniu eIDAS, tylko elementem zapewnienia nadzoru nad dostawcami usług zaufania.

eIDAS wymaga, w art. 30 ust. 2, zgłaszania do Komisji Europejskiej przez państwa członkowskie nazw i adresów podmiotów publicznych lub prywatnych, które zostały wyznaczone przez te państwa do badania zgodności kwalifikowanych urządzeń do składania podpisu elektronicznego. Odpowiednio dotyczy to również kwalifikowanych urządzeń do składania pieczeni elektronicznej (art. 39 ust. 2 eIDAS). Celem tych przepisów nie jest obowiązkowość wyznaczenia przez państwa członkowskie

podmiotów do badania zgodności urządzeń, tylko obowiązek zgłoszenia takiego podmiotu, jeżeli został on wyznaczony, co potwierdza treść korespondencji z Komisji Europejskiej. W związku z tym odpowiednio zredagowano art. 38 projektu ustawy, wskazując ministra właściwego do spraw informatyzacji na wykonawcę zadań w tym zakresie nałożonych przez eIDAS.

Dotychczasowe przepisy wymagały od dostawców usług certyfikacyjnych wnioskujących o dokonanie wpisu do rejestru kwalifikowanych podmiotów załączenia szeregu dokumentów mających na celu między innymi potwierdzenie stabilności finansowej, kwalifikacji pracowników, możliwości technicznych wnioskodawcy. Przepisy projektowanej ustawy zgodnie z art. 5 ust. 4 wymagają załączenia jedynie trzech dokumentów (raportu z oceny zgodności wymaganego przez eIDAS, polityki świadczenia usług objętych wnioskiem, planu zakończenia działalności) oraz danych niezbędnych do wystawienia certyfikatu dostawcy usług zaufania. Ograniczenie liczby wymaganych załączników było możliwe, ponieważ w związku z normą ETSI EN 319 401, wskazującą wymagania dla dostawców usług zaufania, ewentualne niezgodności takie jak brak stabilności finansowej, zostaną wykazane w raporcie z oceny zgodności.

Utrzymano możliwość zawieszania kwalifikowanych certyfikatów podpisu elektronicznego, wskazując, podobnie jak wynikało to z dotąd obowiązujących przepisów, że po uchyleniu zawieszenia certyfikatu, skutek prawny podpisu elektronicznego lub pieczęci weryfikowanych tym certyfikatem, złożonych w trakcie zawieszenia, następuje z chwilą uchylenia tego zawieszenia. Ponadto wskazano, że informacja o zawieszeniu certyfikatu jest udostępniana w ramach usługi informowania o statusie certyfikatu. Podkreślić należy, że dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania zobowiązany jest bezpośrednio na podstawie przepisów eIDAS do tworzenia i aktualizacji bazy danych dotyczącej certyfikatów, w tym ich statusu, a w szczególności, czy certyfikat został unieważniony lub zawieszony i na jaki okres.

Ważnym przepisem dla zapewnienia ciągłości usług zaufania w Polsce jest art. 134, wskazujący na możliwość stosowania skrótu SHA-1 do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych. Dotychczasowe przepisy wymagały wprost stosowania tego algorytmu, co spowodowało, że oprogramowanie stosowane do składania i weryfikacji podpisów, nie

było dostosowywane do innych skrótów rekomendowanych w standardzie ETSI TS 119 312 dotyczącej wymagań w zakresie stosowania algorytmów kryptograficznych w infrastrukturze podpisu elektronicznego. Mając na uwadze, że norma ta wprost nie rekomenduje dalszego używania skrótu SHA-1 ze względu na możliwe naruszenia bezpieczeństwa, należało wprowadzić przepisy przejściowe umożliwiające stopniowe odejście od stosowania tego skrótu. Nie można było jednak wprost zrezygnować ze wskazywania algorytmu technicznego w przepisach prawa, opierając się jedynie na normach, ponieważ zgodnie z normą ETSI EN 319 412-2 dotyczącą profili certyfikatów wydawanych osobom fizycznym, stosowanie wymagań określonych w standardzie ETSI TS 119 312 może być zastąpione krajowymi zaleceniami. Brak stosownego przepisu skutkowałby wykazywaniem niezgodności z eIDAS w raportach oceny zgodności, co mogłoby powodować negatywne postrzeżenie krajowych dostawców usług zaufania i co za tym idzie znaczące zmniejszenie ich szans w konkurowaniu z dostawcami zagranicznymi na wspólnym rynku.

Wyjaśnienia wymaga stosowanie w ramach eIDAS uzupełniających się pojęć „osoba prawna” i „osoba fizyczna”. eIDAS nie przewiduje bowiem takiego bytu jak „jednostka nieposiadająca osobowości prawnej”, co może powodować wątpliwości, czy takie podmioty mogą posługiwać się pieczęcią elektroniczną, która co do zasady jest narzędziem przewidzianym w eIDAS dla osób prawnych. Uznano, że nie ma powodu wpisywania do przepisów ustawy, że pojęcie „osoba prawna” na gruncie eIDAS należy stosować rozszerzająco na krajowe jednostki nieposiadające osobowości prawnej. Rozstrzygający wątpliwości w tym zakresie jest motyw 68 eIDAS, który wskazuje na to, aby termin „osoby prawne” oznacza wszystkie podmioty ustanowione na mocy prawa państwa członkowskiego lub podlegające temu prawu, niezależnie od ich formy prawnej. W przeciwnym przypadku rozporządzenie eIDAS działałoby ograniczająco na podmioty publiczne w Polsce w stosunku do podmiotów w innych krajach UE, co uniemożliwiłoby harmonizację rozwiązań krajowych z europejskimi. Powstałby istotny dysonans poznawczy w zakresie rozumienia eIDAS, np. w zakresie motywu 60 i 65 eIDAS.

Mając na uwadze wskazanie w art. 24 ust. 2 lit. c eIDAS, że dostawca usług zaufania w odniesieniu do ryzyka związanego z odpowiedzialnością za szkody wyrządzone w związku ze świadczeniem tych usług utrzymuje dostateczne zasoby finansowe lub

dysponuje stosownym ubezpieczeniem od odpowiedzialności zgodnie z prawem krajowym, wskazano w art. 14 projektu, że wymaga się zawarcia umowy ubezpieczenia. W upoważnieniu do wydania rozporządzenia w sprawie szczegółowego zakresu ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania wskazano, że należy wziąć pod uwagę specyfikę działalności prowadzonej przez kwalifikowanych dostawców usług zaufania. eIDAS wprowadza bowiem nowe rodzaje usług zaufania, których świadczenie nie ma jeszcze miejsca, a w przypadku rozpoczęcia świadczenia takich usług liczba podmiotów objętych takim ubezpieczeniem nie będzie duża. Szczęólnego wyjaśnienia wymaga natychmiastowa wykonalność decyzji o wykreśleniu kwalifikowanego dostawcy usług zaufania z rejestru oraz decyzja o wykreśleniu wpisu kwalifikowanej usługi zaufania z rejestru wydana przez organ nadzoru. Celem tego przepisu jest nie tylko zapewnienie dbałości o utrzymywanie aktualnych list TSL wynikające z Decyzji wykonawczej Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiającej specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia eIDAS. Należy przy tym zauważyć, że wydanie takiej decyzji możliwe jest na podstawie przesłanek określonych w art. 9 ust. 4 projektu, a zatem wyłącznie w przypadkach, gdy sam dostawca usług zaufania tego chce, gdy w ogóle zaprzestał on działalności, w przypadku wykorzystywania certyfikatów dostawcy usług zaufania w sposób wykraczający poza zakres ich stosowania oraz w przypadkach, o których mowa w art. 20 ust. 3 eIDAS. Taki katalog przyczyn zapewnia, że na liście TSL nie będzie usług zaufania, które faktycznie nie będą już bezpieczne, a które dostawca usług walidacji za takie będzie uznawał – i co za tym idzie, wydawał nieadekwatne do sytuacji zaświadczenia walidacyjne.

eIDAS wprowadza w stosunku do uchylanej dyrektywy 1999/93/WE, oprócz szerokiego pakietu usług zaufania, do których zalicza się:

- a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
- b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych;

zupełnie nowy element – identyfikację elektroniczną dla potrzeb realizacji usług online. Identyfikacji elektronicznej nie zalicza się do usług zaufania. Celem eIDAS jest

zapewnienie posiadaczowi środka identyfikacji elektronicznej wydanego w jednym kraju członkowskim, możliwości skorzystania z publicznych usług online w innych krajach członkowskich. Wiele usług online nie musi bowiem wymagać użycia podpisu elektronicznego. Jeżeli osoba fizyczna posługująca się określonymi danymi umożliwiającymi jej jednoznaczną identyfikację zostanie dobrze i bez wątpliwości rozpoznana przez system teleinformatyczny (uwierzytelniona), to będzie mogła skorzystać z szeregu usług, jakie są w ramach tego systemu oferowane, w szczególności nie podpisując dokumentów elektronicznych, tylko wydając określone dyspozycje jako użytkownik uwierzytelniony w systemie. Przy założeniu, że dochowano należytej staranności dla zapewnienia bezpieczeństwa całego systemu identyfikacji elektronicznej na odpowiednim poziomie, środki identyfikacji elektronicznej wydawane w ramach tego systemu powinny zapewniać dostęp do usług publicznych w całej UE wymagających określonego poziomu bezpieczeństwa. Dzięki temu obywatele UE nie będą musieli zabiegać o wydawanie zagranicznych środków identyfikacji – wystarczy im środek wydany w kraju, pod warunkiem że system, w ramach którego został wydany, został notyfikowany w ramach odpowiedniej procedury określonej w eIDAS. Rozdział II eIDAS wskazuje ramy dla wzajemnego uznawania systemów identyfikacji elektronicznej, określa poziomy bezpieczeństwa takich systemów, wskazuje odpowiedzialność za naruszanie bezpieczeństwa takich systemów oraz nakłada na państwa członkowskie obowiązek współpracy w tym zakresie. Przepisy dostosowujące do rozdziału II eIDAS określono w rozdziale 4 ustawy. Art. 23 jednoznacznie przesądza o istnieniu tzw. krajowego węzła eIDAS, czyli punktu przyłączenia umożliwiającego sprzężenie krajowej infrastruktury identyfikacji elektronicznej w Polsce z krajowymi infrastrukturami służącymi do identyfikacji elektronicznej innych państw członkowskich. Kluczowa rola takich węzłów w procesie transgranicznego uwierzytelniania osób w usługach online w UE została wskazana w rozporządzeniu wykonawczym komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności wydanym na podstawie art. 12 ust. 8 eIDAS. Jednocześnie wskazuje się, że funkcjonowanie krajowego węzła identyfikacji eIDAS zapewnia minister właściwy do spraw informatyzacji, co w efekcie w sposób jednoznaczny ustala odpowiedzialność i kompetencje w tym zakresie. Krajowy węzeł identyfikacji eIDAS będzie pełnił podwójną rolę:

1. będzie pośredniczył w uwierzytelnianiu posiadaczy zagranicznych środków identyfikacji elektronicznej wydanych w ramach notyfikowanych systemów identyfikacji w krajowych usługach online;
2. będzie pośredniczył w uwierzytelnianiu posiadaczy krajowych środków identyfikacji elektronicznej w zagranicznych usługach online, w przypadku gdy system identyfikacji w ramach którego środki tego zostały wydane będzie notyfikowany.

Podsumowując, krajowy węzeł eIDAS będzie stanowił niezbędną podstawę do notyfikowania polskiego systemu identyfikacji elektronicznej, bez względu na to, jaki system zostanie wskazany.

Konsekwentnie w art. 24 wskazuje się ministra właściwego do spraw informatyzacji jako koordynującego na poziomie krajowym działania na rzecz współpracy z państwami członkowskimi UE i EOG w sprawach dotyczących systemów identyfikacji elektronicznej. Takie działania mają być prowadzone zgodnie z art. 12 ust. 5 i 6 eIDAS. Art. 24 nakłada także obowiązek zapewnienia obsługi pojedynczego punktu kontaktowego, o którym mowa w art. 3 Decyzji Wykonawczej Komisji (UE) 2015/296 z dnia 24 lutego 2015 r. ustanawiającej proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej.

W związku z tym, że eIDAS pozwala na zachowanie swobody państw członkowskich w podjęciu decyzji czy w ogóle chcą notyfikować Komisji krajowy system identyfikacji elektronicznej oraz pozostawia państwu członkowskiemu wybór tego, czy notyfikować Komisji jeden czy więcej systemów identyfikacji, jak również czy należy zaangażować w tym celu sektor prywatny, w art. 25 określono ramy postępowania dla przeprowadzenia procedury notyfikacji w tym zakresie. Przepisy art. 25 nie wykluczają możliwości zgłoszenia do notyfikacji więcej niż jednego systemu, jak również nie wykluczają zaangażowania sektora prywatnego, jednakże i w tym przypadku wskazuje się na kluczową rolę ministra właściwego do spraw informatyzacji. Rola ministra ma istotne znaczenie, ponieważ zgodnie z art. 11 eIDAS notyfikujące państwo członkowskie jest odpowiedzialne za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem swoich obowiązków w tym zakresie.

W art. 26 zdecydowano, że to podmioty udostępniające usługi online będą określały wymagane poziomy bezpieczeństwa dla środków identyfikacji elektronicznej,

niezbędne do zrealizowania świadczonych przez nie usług. Przepis ten będzie miał znaczenie tylko w przypadku, gdy z przepisów odrębnych nie będzie wynikało, że dla realizacji określonej usługi jest wymagany krajowy środek identyfikacji elektronicznej wydany w ramach notyfikowanego systemu identyfikacji elektronicznej na określonym poziomie. Na przykład, gdy w przepisach odrębnych będzie określone, że dla realizacji usługi wystarczy użycie profilu zaufanego ePUAP, a jednocześnie profil ten będzie notyfikowany na średnim poziomie bezpieczeństwa, to będzie znaczyło, że wszystkie notyfikowane środki identyfikacji elektronicznej notyfikowane w KE na poziomie średnim i wysokim muszą być w tej usłudze uznawane.

Art. 27 dookreśla kwestie związane z informowaniem państw członkowskich i Komisji o naruszeniu bezpieczeństwa notyfikowanych systemów identyfikacji elektronicznej. Mając na uwadze, że naruszenie bezpieczeństwa takiego systemu może mieć istotne znaczenie dla bezpieczeństwa tożsamości obywateli ustalono, że tego rodzaju informacje przekazuje się niezwłocznie ministrowi właściwemu do spraw informatyzacji i wyłącznie drogą elektroniczną.

4. Przewidywane skutki prawne

Ustawa przenosi nadzór nad usługami zaufania (od ministra właściwego do spraw gospodarki, do ministra właściwego do spraw informatyzacji) oraz dokonuje jego wzmocnienia przez przyznanie nowych kompetencji. Ustawa umożliwi zminimalizowanie ryzyka kolizji rozporządzenia eIDAS z krajowym systemem prawnym.

4.1. Cel zmian i czym są podyktowane

Zmiany w przepisach obowiązujących mają na celu przede wszystkim ich bieżące dostosowanie do nowego aparatu pojęciowego, jakim posługuje się eIDAS, w taki sposób, aby zapewnić nie tylko spójność z eIDAS, ale i ciągłość działania istniejących usług elektronicznych wykorzystujących środki identyfikacji elektronicznej oraz usługi zaufania.

W stosunku do uchylanej dyrektywy 1999/93/WE zmieniała się definicja podpisu elektronicznego, a ponadto zdefiniowano nowe pojęcia, które są używane w przepisach krajowych w innym znaczeniu niż zdefiniowano to w eIDAS. Zmiany przedstawia tabela poniżej:

| Rozporządzenie eIDAS | Dyrektywa 1999/93/WE | Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym |
|---|--|--|
| „podpis elektroniczny” 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 (art. 3 pkt 10) | „podpis elektroniczny” oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia” (art. 2 pkt 1) | „podpis elektroniczny) - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny (art. 3 pkt 1) |
| „kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego (art. 3 pkt 12) | brak definicji w art. 5 ust. 1 wskazano na „zaawansowane podpisy elektroniczne oparte o kwalifikowany certyfikat i złożone za pomocą bezpiecznego urządzenia służącego do składania podpisu” | brak definicji odpowiednikiem jest wskazanie w art. 5 ust. 1: „1. Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny” |
| „identyfikacja elektroniczna” oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną (art. 3 pkt 1) | brak definicji | brak definicji |
| „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej (art. 3 pkt 5) | brak definicji | brak definicji |
| „środek identyfikacji elektronicznej” oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online (art. 3 pkt 2) | brak definicji | brak definicji |

Przede wszystkim należy zwrócić uwagę na fakt, że podpis elektroniczny to już nie są dane służące „jako metoda uwierzytelnienia” tylko dane służące do podpisywania, tym bardziej, że „uwierzytelnianie” zyskało odrębną definicję.

Odnosząc się do definicji podpisu z uchylanej ustawy o podpisie elektronicznym należy podkreślić, że choć trudno zaprzeczyć, iż podpis elektroniczny (usługa zaufania) nadal będzie pozwalał na zidentyfikowanie osoby składającej taki podpis, to jednak w usługach online, zgodnie z definicją będą temu służyły środki identyfikacji elektronicznej, które usługami zaufania nie są.

4.2. Wprowadzenie pojęcia „kwalifikowany podpis elektroniczny”

Powyższe zmiany znaczeniowe, choć niewielkie, spowodowały konieczność dostosowania przepisów posługujących się pojęciem „bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu” równoważnym znaczeniowo pojęciem „kwalifikowany podpis elektroniczny”. W przypadku gdy przepisy prawa wymagają „bezpiecznego podpisu elektronicznego” zaproponowano, że co do zasady wymóg ten zostanie zastąpiony również pojęciem „kwalifikowany podpis elektroniczny”, mając na uwadze, że jest on najbliższy pojęciowo podpisowi kwalifikowanemu. eIDAS nie posługuje się bowiem pojęciem równoważnym znaczeniowo. Zaawansowany podpis elektroniczny w znaczeniu eIDAS nie musi być bowiem składany za pomocą tzw. bezpiecznych urządzeń służących do składania podpisu elektronicznego. Jednakże w przypadku gdy wymóg wprost dotyczył podpisu elektronicznego weryfikowanego certyfikatem wystawianym przez Ministra Sprawiedliwości (jak w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym), to w tym przypadku posłużono się pojęciem „zaawansowany podpis elektroniczny”.

4.3. Zmiana definicji „podpis potwierdzony profilem zaufanym ePUAP”

Szerszy zakres zmiany niż tylko wprowadzenie pojęcie kwalifikowanego podpisu elektronicznego wprowadzono do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352). By nie było wątpliwości że „podpis potwierdzony profilem zaufanym ePUAP” jest podpisem elektronicznym w rozumieniu eIDAS, zdefiniowano go jako „podpis elektroniczny złożony przez użytkownika konta ePUAP (...)”. Dzięki temu zabiegowi stanie się również jednoznaczne, że podpis potwierdzony profilem zaufanym ePUAP nie jest zaawansowanym podpisem elektronicznym, co będzie miało

znaczenie dla stosowania art. 27 eIDAS wymagającego uznawania w publicznych usługach online, w których wymaga się takiego podpisu – zaawansowanych podpisów elektronicznych w formatach lub wykorzystujących metody określone w aktach wykonawczych wydanych przez Komisję na podstawie art. 27 ust. 5 eIDAS. Zmiana ta nie dotyczy używania samego profilu zaufanego ePUAP jako środka identyfikacji elektronicznej, o czym mowa w art. 20a ust. 1 ustawy o informatyzacji.

Ponadto, dostosowując przepisy do eIDAS, wskazano, że w celu zapewnienia integralności i autentyczności wykonania operacji przez system ePUAP w celu dołączenia podpisu potwierdzonego profilem zaufanym ePUAP wskazano, że nie używa się już podpisu systemowego ePUAP, tylko zdefiniowanej w eIDAS pieczęci elektronicznej.

4.4. Zdefiniowanie pojęcia „autoryzacja”

Kolejną zmianą w ustawie o informatyzacji jest zdefiniowanie pojęcia „autoryzacja” używanego w przepisach prawa (w tym w samej ustawie o informatyzacji i przepisach wykonawczych), ale także w dokumentach opisujących zasady działania usług elektronicznych, rozumianego dwojako:

- przydzielenie osobie fizycznej lub prawnej, uprawnień w systemie teleinformatycznym po jej pozytywnym uwierzytelnieniu w tym systemie,
- potwierdzenie woli realizacji czynności w postaci elektronicznej przez uwierzytelnionego użytkownika za pomocą dodatkowych danych, np. ostateczne zatwierdzenie chęci podpisania podania lub wniosku w postaci elektronicznej za pomocą jednorazowego kodu operacji tzw. OTP (od ang. one time password).

Celem tego przepisu jest wskazanie, że znaczenie pojęcia „autoryzacja” może być zależne od kontekstu jego użycia, a nie jednoznaczne.

4.5. Wskazanie jakie środki identyfikacji elektronicznej są wymagane dla potrzeb uwierzytelnienia użytkowników systemu teleinformatycznego korzystających z usług online udostępnianych przez podmioty publiczne

Zmianą niezwiązaną z podpisem elektronicznym tylko z identyfikacją elektroniczną i uwierzytelnianiem jest zmiana art. 20a ust. 1 ustawy o informatyzacji. Dotąd przepis ten wskazywał, że identyfikacja użytkownika systemów teleinformatycznych udostępnianych przez podmioty publiczne następuje przez zastosowanie kwalifikowanego certyfikatu przy zachowaniu zasad przewidzianych w ustawie

o podpisie elektronicznym lub profilu zaufanego ePUAP. Takie wskazanie jest adekwatne w odniesieniu do definicji podpisu elektronicznego mówiącej, że podpis elektroniczny służy do identyfikacji osoby go składającej. W zmianach dostosowujących do eIDAS wzięto pod uwagę kilka elementów:

- 1) zgodnie z eIDAS, co do zasady, do identyfikacji użytkowników w usługach online używa się środków identyfikacji elektronicznej, a nie certyfikatów kwalifikowanych;
- 2) przepis w dotychczasowym brzmieniu mówi o identyfikacji w systemach teleinformatycznych udostępnianych przez podmioty publiczne, a eIDAS odnosi się do identyfikacji w usługach online;
- 3) mając na uwadze, że celem użycia środka identyfikacji elektronicznej jest zgodnie z eIDAS uwierzytelnienie dla potrzeb usługi online, jak również, że celem art. 20a ust. 1 tej ustawy jest właśnie wskazanie środków identyfikacji elektronicznej umożliwiających uwierzytelnienie w systemie teleinformatycznym, zmieniono redakcję przepisów, wskazując, jakich środków identyfikacji elektronicznej wymaga się dla uwierzytelniania;
- 4) w szczególności utrzymano możliwość użycia do uwierzytelnienia kwalifikowanego certyfikatu podpisu elektronicznego, mając na uwadze potrzebę utrzymania ciągłości usług opartych dotychczas na takim certyfikacie.

Podobna zmiana dotyczy art. 3f § 1 ustawy – Ordynacja podatkowa.

4.6. Wskazanie, że podania wnoszone w postaci elektronicznej co do zasady opatruje się podpisem, a nie uwierzytelnia

Kolejną grupą zmian inną niż te dotyczące wprowadzenia pojęcia kwalifikowanego podpisu elektronicznego oraz podpisu potwierdzonego profilem zaufanym ePUAP jest wskazanie w Kodeksie postępowania administracyjnego oraz odpowiednio w Ordynacji podatkowej w przepisach, w których użyto pojęcia „uwierzytelnianie” w odniesieniu do podań wniesionych w formie dokumentu elektronicznego (art. 63 § 3a pkt i odpowiednio art. 168 § 3a pkt 1), że podania opatruje się podpisem, a nie uwierzytelnia. Podobna zmiana dotyczy podpisywania pełnomocnictw przez osoby udzielające pełnomocnictwa. Także wskazano, że w tym przypadku mamy do czynienia z podpisywaniem, a nie z uwierzytelnieniem. Zachowano jednak to pojęcie w odniesieniu do uwierzytelniania treści dokumentu wystawionego przez osobę trzecią

(art. 33 § 3a i art. 220 k.p.a. oraz odpowiednio art. 138a § 5 i art. 306d § 3 Ordynacji podatkowej).

4.7. Inne poprawki dostosowujące

Kolejną grupą przepisów zmienianych jest usunięcie wymagania podania danych do weryfikacji podpisu elektronicznego przez rzeczników patentowych, radców Prokuraturii Generalnej, radców prawnych i prokuratorów w przypadku komunikowania się z sądem przy wykorzystaniu kwalifikowanego podpisu elektronicznego. Zgodnie z eIDAS kwalifikowany podpis elektroniczny weryfikuje się nie na podstawie danych udostępnionych przez podpisującego, ale przez stronę trzecią (kwalifikowanego dostawcę usług zaufania).

Z ustawy o swobodzie działalności gospodarczej usunięto wymóg mówiący o tym, że podpis elektroniczny może wskazywać na jednoznaczną identyfikację czasu przesłania wniosku, który zgodnie z art. 27 ust. 7 tej ustawy może być przesłany następnego dnia po jego podpisaniu. Podobna zmiana dotyczy art. 26 ust. 4 ustawy o swobodzie działalności gospodarczej.

W ustawie o substancjach zubożających warstwę ozonową poprawiono redakcję przepisów w miejscach gdzie wymagało się opatrywania podpisem elektronicznym nie tyle wniosków i pism w postaci elektronicznej, ale opatrywania podpisem elektronicznym „postaci” tych wniosków i pism. Na przykład, przepis art. 9 ust. 6 tej ustawy nakładający na przedsiębiorstwa, które uzyskały wpis do rejestru obowiązek informowania ministra właściwego do spraw środowiska drogą elektroniczną o jej zaprzestaniu obecnie zredagowany jest następująco: „[Przedsiębiorstwa] są obowiązane poinformować o tym fakcie ministra właściwego do spraw środowiska, w postaci elektronicznej opatrzonej bezpiecznym podpisem elektronicznym”. Proponowana zmiana zakłada, że nie podpisuje się „postaci elektronicznej” tylko „pismo w postaci elektronicznej”.

W ustawie z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym uporządkowano przepisy w art. 18 w ust. 3 pkt 3, przeredagując ich obecnie brzmienie, które może powodować wątpliwości. Obecnie bowiem wskazuje się, że za wniesione na piśmie uwagi uznaje się również uwagi wniesione w postaci elektronicznej:

- 1) opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262 oraz z 2014 r. poz. 1662) lub
- 2) opatrzone podpisem potwierdzonym profilem zaufanym ePUAP w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114) lub
- 3) za pomocą elektronicznej skrzynki podawczej w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Ta redakcja przepisów wymienia w opcjach dwie różne klasyfikacje: sposób podpisywania i sposób doręczania, co powoduje, że nie wiadomo jak doręczać dokumenty opisane w pkt 1 i 2 (choć jak można przypuszczać zgodnie z pkt 3 – na elektroniczną skrzynkę podawczą, a nie np. dostarczając płytę CD z uwagami podpisanymi kwalifikowanym podpisem elektronicznym) oraz nie wiadomo jak podpisywać dokumenty doręczane w sposób opisany w pkt 3 (choć można przypuszczać, że w sposób opisany w pkt 1 i 2, a nie w ogóle bez podpisu). Przepis dostosowujący do eIDAS zawarty w projekcie ustawy o usługach zaufania od razu porządkuje tę niepewność.

4.8. eIDAS jako impuls do zmian w świadczeniu usług elektronicznych

Celem zmian wprowadzanych ustawą o usługach zaufania nie jest modyfikacja przepisów prawa ingerująca w dotychczasowy sposób świadczenia usług elektronicznych, wprowadzając np. obowiązek stosowania nowych usług zaufania, które przewiduje eIDAS (tj. między innymi pieczęci elektronicznej oraz usług rejestrowanego doręczenia elektronicznego). Mając na uwadze, że przepisy eIDAS stosuje się bezpośrednio – i co za tym idzie – wdrażająca ustawa o usługach zaufania nie nakłada ograniczeń w tym zakresie, nowe usługi zaufania będą mogły być wykorzystywane wszędzie tam, gdzie przepisy odrębne nie stanowią inaczej.

Zasadnicze zmiany wykorzystujące nowe możliwości, jakie daje eIDAS, zostaną zrealizowane w ramach przepisów odrębnych, gdyż będzie to wymagało szerokich konsultacji, zarówno z potencjalnymi dostawcami nowych usług elektronicznych, w tym usług zaufania, które mogłyby być z powodzeniem wykorzystywane przez

podmioty publiczne i przedsiębiorców dla świadczenia kolejnych usług, jak i z odbiorcami tych usług.

Szeroki potencjał, jaki stwarza eIDAS dla umożliwienia rozwoju nowoczesnych, wygodnych i jednocześnie bezpiecznych usług elektronicznych opartych na wiarygodnych środkach identyfikacji elektronicznej oraz komplementarnie wykorzystujących usługi zaufania, został dostrzeżony i będzie wykorzystany. Trwają prace nad założeniami do kolejnych zmian prawnych, dających impuls do zasadniczego przeorientowania podejścia do usług opierających się na przepływie informacji, w taki sposób aby informacja ta – co do zasady – była w postaci elektronicznej. Zakłada się, że filarami dla realizacji kolejnych zmian będą:

- wykorzystanie istniejących już w Polsce różnych środków identyfikacji elektronicznej sprawdzonych w praktyce uwierzytelniania w usługach online świadczonych przez podmioty prywatne (np. banki),
- szerokie wykorzystanie nowych usług zaufania, takich jak: pieczęć elektroniczna, konserwacja elektroniczna i usługa rejestrowanego doręczania elektronicznego,
- usunięcie wielu barier formalnych, które wymuszają tworzenie dokumentów papierowych lub powodują, że posługiwanie się nimi jest nieraz wygodniejsze, bardziej bezpieczne, a nawet tańsze.

Stworzenie możliwości wykorzystania środków identyfikacji elektronicznej znanych obywatelom i wykorzystywanych przez nich w codziennej praktyce, także w usługach online świadczonych przez podmioty publiczne, to nie tylko wygoda dla obywateli, ale też pokonanie bariery braku powszechnego środka identyfikacji elektronicznej. Warto dodać, że posługując się znanym sobie środkiem identyfikacji elektronicznej, jego posiadacz będzie się doskonale orientował w zakresie sposobu jego działania, w tym także będzie znał zasady zachowania bezpieczeństwa dla tego środka.

Podstawy prawne dla tych kolejnych zmian będą konsekwentnie przygotowywane i wdrażane, także w oparciu doświadczenia innych krajów stosujących eIDAS, a w szczególności notyfikujących nowe rozwiązania.

Przedkładany projekt ustawy jest zgodny z prawem Unii Europejskiej,

Projektowana ustawa nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

| | |
|--|--|
| <p>Nazwa projektu Ustawa o usługach zaufania oraz identyfikacji elektronicznej</p> <p>Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Rozwoju, Ministerstwo Cyfryzacji</p> <p>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Tadeusz Kościński, Podsekretarz Stanu</p> <p>Kontakt do opiekuna merytorycznego projektu Sebastian Christow (sebastian.christow@mr.gov.pl) Dyrektor Departamentu Gospodarki Elektronicznej, Ministerstwo Rozwoju</p> <p>Bogusław Bieda (boguslaw.bieda@mr.gov.pl), Radca Ministra Marcin Fijałkowski (marcin.fijalkowski@mr.gov.pl), Radca Ministra, tel: (22) 693 52 82</p> | <p>Data sporządzenia 07 lipca 2016 r.</p> <p>Źródło: Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014</p> <p>Nr w wykazie prac RM: UC 58</p> |
|--|--|

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Dostosowanie do Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 (eIDAS). Zmiana ma charakter wieloaspektowy i dotyczy wielu obszarów. Regulowana jest materia określona przez eIDAS jako krajowa w: preambule pkt 18, 20, 24, 37, 41, 49 oraz art. 11, art. 13, art. 16, art. 17, art. 18 pkt 3, art. 24 pkt 1, art. 24 pkt 2c, art. 28 pkt 5, art. 30 ust. 3 lit. b.

Z uwagi na odmienność uregulowań i definicji w rozporządzeniu eIDAS konieczne jest uchylene ustawy o podpisie elektronicznym. Celem wprowadzenia ustawy o usługach zaufania oraz identyfikacji elektronicznej jest osadzenie rozporządzenia eIDAS w krajowych uwarunkowaniach instytucjonalno-prawnych. Konieczne jest wprowadzenie procedury dopuszczenia do świadczenia kwalifikowanych usług zaufania na podstawie raportów audytowych.

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

Organom nadzoru rozporządzenie eIDAS nakazuje przyznać odpowiednie zasoby i uprawnienia niezbędne do wykonywania ich zadań. Projektowana regulacja wskazuje organ nadzoru, określa jego formy: zaufana lista, rejestr dostawców usług zaufania i krajowy urząd certyfikujący – zbiorczo określane mianem krajowej infrastruktury zaufania. Techniczne i organizacyjne szczegóły tej infrastruktury określi rozporządzenie Rady Ministrów.

Kompetencje organu nadzoru w zakresie usług zaufania zostają przypisane ministrowi właściwemu ds. informatyzacji. Zgodnie z artykułem 16 rozporządzenia eIDAS państwa członkowskie ustanawiają przepisy o sankcjach w przypadkach naruszeń. Sankcje muszą być skuteczne, proporcjonalne i odstraszające. W ślad za tym projekt ustawy wprowadza odpowiednie sankcje administracyjne i karne.

Regulacji państw członkowskich pozostawiono uszczegółowienie odpowiedzialności odszkodowawczej dostawców usług zaufania, systemów eID oraz stron wydających środki eID, a także zawieszanie certyfikatów i zakończenie działalności. Tę materię, co do zasady, regulują przepisy kodeksu cywilnego.

Podmiotem zapewniającym obsługę zagranicznych środków identyfikacji elektronicznej, wydanych w ramach notyfikowanych przez Komisję Europejską systemów eID, za pośrednictwem węzła krajowego, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 8 rozporządzenia eIDAS (najpóźniej od września 2018 r.) jest minister właściwy ds. informatyzacji.

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

W Austrii trwają obecnie prace dostosowawcze o charakterze legislacyjnym i organizacyjnym prowadzone przez odpowiedzialny za informatyzację państwa Urząd Kanclerza Austrii. Z uwagi na wpływ na przepisy prawa cywilnego oraz procedurę sądową prace legislacyjne prowadzone są we współpracy z Ministerstwem Sprawiedliwości.

Austria przygotowała otwartą specyfikację API określaną mianem „warstwy bezpieczeństwa” na użytek składania podpisów za pomocą urządzenia mobilnego lub karty obywatelskiej. Kilku dostawców dostarczyło produkty w tym zakresie. Jednym z produktów jest dostępna nieodpłatnie dla osób fizycznych i przedsiębiorców implementacja MOCCA. Została ona przygotowana na licencji open source we współpracy Urzędu Kanclerskiego i Politechniki w Grazu. Dostępne są też trzy inne aplikacje wymienione pod adresem <https://www.buergerkarte.at/en/downloads-card.html>. Zależnie od funkcjonalności i wsparcia dla kart dostępne są wersje darmowe i odpłatne tego oprogramowania. W oparciu o API możliwe jest integrowanie rozwiązań w innych aplikacjach (np. systemach workflow). Dostępne są również aplikacje do składania podpisów PDF – <https://www.buergerkarte.at/en/pdf-signature-mobile.html>. Specyfikacja API jest dostępna pod

adresem <https://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114-en/>. Rozwiązanie jest zgodne do tworzenia podpisów XAdES i CAdES. Przetwarzanie dokumentów PDF z podpisem PAdES może wymagać dodatkowego oprogramowania. Inne otwartoźródłowe oprogramowanie to np. MOA-SP, służące do walidacji podpisów XAdES i CAdES.

Przygotowanie administracji do będącej aktem wykonawczym eIDAS decyzji nr 2015/1506 zrealizowano zasadniczo przez wdrożenie wcześniejszych decyzji dotyczących formatu podpisu elektronicznego (Decyzje nr 2011/130 i 2014/148 wydane w wykonaniu dyrektywy usługowej). Nie wdrożono jeszcze wsparcia dla formatów długookresowych oraz ASiC). W administracji typowo wykorzystywane są XAdES-B i w ostatnim czasie także PAdES. Rozwiązania austriackie uczestniczyły w plugtestach ETSI i austriackie podpisy powinny być rozpoznawalne w innych państwach członkowskich. Celem zachowania kompatybilności wstecznej ze starszymi podpisami utrzymywany jest portal www.signature-verification.gv.at.

Komisja Europejska wspiera działania na rzecz wdrożenia podpisów elektronicznych i pieczęci we wskazanych przez Unię Europejską formatach przez rozwój kodu źródłowego aplikacji SD DSS. Aplikacja ta jest dostępna na zasadach open source i po dostosowaniu może być wykorzystana przez Państwa Członkowskie.

4. Podmioty, na które oddziałuje projekt

| Grupa | Wielkość | Źródło danych | Oddziaływanie |
|---------------------|--|---|---|
| Centra certyfikacji | 5 | Rejestr NCCert | Objęcie nadzorem organu usług niekwalifikowanych, możliwość świadczenia nowych usług |
| Podmioty publiczne | Co najmniej 15 tys. z administracji rządowej i samorządowej. Także sądy, służba zdrowia, szkolnictwo, a więc ok. kilkadziesiąt tysięcy podmiotów | Baza danych podmiotów, które mają funkcjonalność podmiotu publicznego ePUAP | Uznawanie podpisów i pieczęci z państw UE/EOG (wdrożenie list TSL na użytek weryfikacji, dostosowanie do obsługi formatów podpisu wskazanych w akcie wykonawczym) |
| Przedsiębiorcy | Ok. 3 mln | CEIDG, KRS | O ile korzystają z podpisów kwalifikowanych, to powinni uznawać certyfikaty kwalifikowane z innych państw UE/EOG |
| Subskrybenci | Ok. 300 tys. | Centra certyfikacji | Przeinstalowanie aplikacji do składania i weryfikacji podpisu elektronicznego |

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

W okresie między sierpniem a listopadem 2015 r. przeprowadzono ankietę w ministerstwach i urzędach centralnych. Poinformowano ministerstwa, że zmiany dostosowujące do eIDAS w ich systemach informatycznych i systemach jednostek podległych oraz aktach rangi podstawowej powinny być dokonane we własnym zakresie przez te urzędy. Organy wskazały na ustawy i rozporządzenia w zakresie ich kompetencji, które będą wymagać zmiany, oraz w niektórych przypadkach – także koszty. Większość nie była w stanie precyzyjnie określić nakładów na wdrożenie i nie przekazała żadnych wyliczeń. Wynika to z wielu czynników, w tym z faktu, że większość wprowadzanych przez eIDAS usług zaufania nie jest jeszcze dostępna w ofercie usługodawców i nie jest znany ich koszt.

Konsultacje publiczne i uzgodnienia międzyresortowe projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej trwały od 22 marca 2016 r. Oryginalnie przewidziany termin ich zakończenia – 6 kwietnia 2016 r. został przedłużony do 15 kwietnia 2016 r., w odpowiedzi na liczne postulaty uczestników konsultacji i uzgodnień. Spośród organów administracji, do których skierowano projekt ustawy w ramach uzgodnień uwagi zgłosiły następujące resorty: ME, MF, MIB, MRPiPS, MRiRW, MS, MŚ, MSWiA, MSZ, MZ i RCL. W uzgodnieniach uczestniczył również Koordynator Służb Specjalnych, przekazując MR uwagi jednego z podmiotów sektora publicznego.

W konsultacjach publicznych MR otrzymało uwagi następujących podmiotów: Asseco Data Systems Poland S.A., PWPW S.A., Polskie Towarzystwo Informatyczne, Poczta Polska, Polska Izba Ubezpieczeń, Polska Izba Informatyki i Telekomunikacji, Narodowy Bank Polski, Zakład Ubezpieczeń Społecznych, Śląskie Centrum Społeczeństwa Informacyjnego, PKO Bank Polski, Krajowa Izba Rozliczeniowa S.A., Urząd m.st. Warszawy, Prezydent m.st. Warszawy, Urząd Miasta Krakowa, Związek Banków Polskich, Związek Pracodawców Branży Internetowej IAB Polska, Urząd Marszałkowski Województwa Podlaskiego, Generalny Inspektor Ochrony Danych Osobowych, przedstawiciele Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, Polskie Centrum Akredytacji, Instytut Logistyki

i Magazynowania, Naczelny Sąd Administracyjny oraz Izba Gospodarki Elektronicznej e-Commerce Polska. Konferencja uzgodnieniowa odbyła się w dniach 26 i 27 kwietnia 2016 r. Projekt ustawy został przyjęty na posiedzeniu Komitetu do spraw Europejskich w dniu 18 maja 2016 r.

Tego samego dnia projekt został też zaakceptowany przez Komisję Wspólną Rządu i Samorządu Terytorialnego.

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 | | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | | |
| JST | | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | | |
| Wydatki ogółem | | 15,5 | 2,1 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 29,6 |
| budżet państwa | | 15,5 | 2,1 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 29,6 |
| JST | | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | | |
| Saldo ogółem | | 15,5 | 2,1 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 1,5 | 29,6 |
| budżet państwa | | | | | | | | | | | | | |
| JST | | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | | |

| Źródła finansowania | |
|--|--|
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | <p>Skutki finansowe projektu ustawy obejmują koszty sprawowania nadzoru nad usługami zaufania, utrzymywania sieci współpracy, a także budowy węzła eIDAS dla eID oraz węzła eIDAS dla UZ. Ponadto uwzględniona została działalność szkoleniowa, informacyjna i promocyjna, jak również dostosowanie systemów administracji publicznej do uznawania kwalifikowanych podpisów elektronicznych z obszaru UE.</p> <p>Zakłada się, że środki finansowe niezbędne do realizacji zadań w 2016 r. zostały zabezpieczone w planach rzeczowo-finansowych poszczególnych urzędów.</p> <p>Szacując skutki finansowe uwzględniono sygnalizowaną w ramach kwerendy wykonanej w 2015 r. potrzebę dostosowania niektórych systemów teleinformatycznych automatycznie weryfikujących podpisy elektroniczne do obsługi podpisów z obszaru UE, jak również konieczność budowy i udostępnienia krajowego węzła eIDAS. Węzeł będzie musiał być oddany do użytku z odpowiednim wyprzedzeniem względem września 2018 r., aby zapewnić czas na przyłączenie do węzła krajowych e-usług. Docelowa specyfikacja techniczna dla przenoszenia identyfikacji elektronicznej między systemami nie jest jeszcze ostateczna (pierwsza wersja została ogłoszona pod koniec listopada 2015 r.). Stąd kilkukrotnie wyższa kwota wydatków w pierwszym roku.</p> <p>Ponadto, w zależności od rozwoju rynku usług zaufania, w tym znaczącego poszerzenia ich spektrum (nie tylko w Polsce, ale i w Europie), prawdopodobne jest zwiększenie zadań realizowanych przez organ nadzoru. Całkowicie nowym elementem jest sieć współpracy mająca na celu ustalanie i wdrażanie bezpiecznych rozwiązań dla funkcjonowania systemów identyfikacji elektronicznej i transgranicznego uznawania wydanych w ich ramach środków w usługach online. Stąd stałe koszty w kolejnych latach.</p> <p>Niezbędne będzie wyszkolenie pracowników obsługujących podania i realizujących inne czynności w postaci elektronicznej, wskazujące w jaki sposób można zweryfikować podpis lub pieczęć elektroniczną, jeżeli czynności te nie są realizowane automatycznie. Zakres takich działań będzie jednak zależny od możliwości systemów teleinformatycznych użytkowanych przez dany podmiot, dotychczas stosowanych sposobów weryfikacji podpisów elektronicznych, rodzaju podpisanych danych, a przede wszystkim od liczby napływających podań i wniosków podpisanych podpisem elektronicznym lub opatrzonych pieczęcią elektroniczną. Wzięto pod uwagę także działalność informacyjną mającą na celu promocję nowoczesnych środków identyfikacji elektronicznej i usług zaufania jak również bezpiecznego ich wykorzystywania.</p> |

Generalnie, trudne do oszacowania są koszty dostosowania administracji publicznej, ze względu na to, że dane pozyskane w wyniku ankiety skierowanej do administracji publicznej nie są reprezentatywne i na ich podstawie nie można dokonać rzetelnej i całościowej oceny. Próbę oszacowania kosztów podjęło jedynie 12 urzędów. Z uwagi na różnorodność stosowanych technologii, licencji i rozwiązań organizacyjnych, jak również przyczyn podanych powyżej, dane uzyskane na podstawie ankiety nie są możliwe do wykorzystania w ocenie całościowej.

Informacje zebrane w okresie sierpień – listopad 2015 roku na temat spodziewanych kosztów wdrożenia rozporządzenia eIDAS w urzędach wyglądają następująco:

| Lp. | Respondent | Koszt [PLN] |
|-------------|---|-------------------|
| 1 | ZUS | 6 000 000 |
| 2 | Ministerstwo Zdrowia | 3 600 000 |
| 3 | CCA (d. CPI) | 3 378 000 |
| 4 | NFZ | 1 100 000 |
| 5 | Ministerstwo Środowiska | 500 000 |
| 6 | Ministerstwo Pracy i Polityki Społecznej | 300 000 |
| 7 | KRUS | 240 000 |
| 8 | NSA | 200 000 |
| 9 | PKN | 20 000 |
| 10 | Ministerstwo Nauki i Szkolnictwa Wyższego | 20 000 |
| 11 | UKE | 20 000 |
| 12 | RCL | 17 300 |
| SUMA | | 15 395 300 |

Zapytanie skierowano do: 46 podmiotów,
 odpowiedzi udzieliło: 39 podmiotów,
 w tym podało koszty: 12 podmiotów.

Uzyskane informacje liczone są według różnych metodologii i prawdopodobnie w niektórych przypadkach obejmują również zakres prac wykraczający poza samo dostosowanie do rozporządzenia eIDAS. Nie pozwalają zatem na uogólnienie i dokonanie oceny całościowej.

Ponadto należy nadmienić, że – jak podano w pkt 4.8 uzasadnienia – rozwój usług wykorzystujących nowe możliwości stworzone przez rozporządzenie eIDAS nastąpi w wyniku kolejnego etapu, który zostanie zrealizowany na podstawie nowych przepisów prawa. Wówczas też będą mogły zostać dokładniej wyliczone i przedstawione istotne nakłady, które administracja publiczna będzie musiała ponieść, aby umożliwić obywatelom i przedsiębiorcom oraz także samej sobie efektywne korzystanie z nowych narzędzi – usług zaufania i identyfikacji elektronicznej.

Mając na uwadze, że utrzymanie systemów teleinformatycznych wymaga ich stałej konserwacji i dostosowywania do szybko zmieniającego się otoczenia, a także dostosowania do eIDAS, to może być ono zapewnione w ramach działań uwzględnionych w budżetach utrzymaniowych. Innego podejścia będą wymagały planowane zadanie nowe, o których mowa w pkt 4.8 uzasadnienia, ale nie będące przedmiotem tej ustawy.

Dotychczasowe koszty realizowania nadzoru nad świadczeniem usług związanych z podpisem elektronicznym w rozumieniu przepisów o podpisie elektronicznym ponoszone przez Ministerstwo Rozwoju (i dawniej przez Ministerstwo Gospodarki) w latach 2013–2016 ponoszone były na zakup usług i ekspertyz, a także wynagrodzenia pracowników. W budżecie MR na rok 2016 środki na przedmiotowe zadanie zostały zabezpieczone w kwocie 80 179 zł. W związku z przeniesieniem nadzoru od ministra właściwego do spraw gospodarki do ministra właściwego do spraw informatyzacji odpowiednie przeniesienie planowanych dochodów i wydatków budżetowych, w tym wynagrodzeń oraz limitów zatrudnienia, pomiędzy częściami budżetu państwa, których są dysponentami, ureguluje rozporządzenie Prezesa Rady Ministrów.

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 | B.d. | B.d. | B.d. | B.d. | B.d. | B.d. | B.d. |
| | sektor mikro-, małych i średnich przedsiębiorstw | B.d. | B.d. | B.d. | B.d. | B.d. | B.d. | B.d. |
| | rodzina, obywatele oraz gospodarstwa domowe | B.d. | B.d. | B.d. | B.d. | B.d. | B.d. | B.d. |
| W ujęciu niepieniężnym | budżet państwa | <p>Systemy teleinformatyczne zapewniające możliwość skorzystania z usług online, w których wymaga się bezpiecznego podpisu elektronicznego weryfikowanego ważnym certyfikatem kwalifikowanym (po wejściu w życie eIDAS – kwalifikowany podpis elektroniczny), będą wymagały dostosowania mającego na celu zapewnienie automatycznej weryfikacji podpisów elektronicznych wydanych przez wszelkie podmioty wpisane na listy TSL. W minimalnym zakresie potrzebna będzie modyfikacja interfejsu użytkownika tych systemów z uwagi na zmianę nazewnictwa.</p> <p>Mając na uwadze, że obecnie zasadnicze zwiększenie liczby podpisanych elektronicznie dokumentów zależne jest od wymogów i możliwości wskazanych w przepisach odrębnych (np. odnośnie do sprawozdań jednostek sektora finansów publicznych w zakresie operacji finansowych), obliczenie, jaki wpływ na koszty po stronie podmiotów weryfikujących podpisy będzie miało poszerzenie listy dostawców usługi zaufania byłoby obarczone poważnym błędem.</p> <p>W przypadku usług publicznych świadczonych online wymagających podpisu, który może być uznany za podpis zaawansowany (np. podpisu wydawanego dla realizacji usługi e-Klient SC) może być niezbędne dostosowanie tych usług do akceptowania także innych podpisów zaawansowanych w zgodzie z art. 27 eIDAS.</p> <p>Możliwe jest osiągnięcie korzyści, jeżeli masowo wykorzystywane środki eID i usługi zaufania pozwolą na zastąpienie tradycyjnej wymiany informacji utrwalonej na papierze – komunikacją elektroniczną. Zależne jest to jednak od innych działań, a nie od dostosowania do rozporządzenia eIDAS. Rozporządzenie to stwarza szanse na osiągnięcie korzyści, ale nie jest ich bezpośrednią przyczyną.</p> | | | | | | |
| | duże przedsiębiorstwa | <p>Możliwe jest osiągnięcie korzyści przez przedsiębiorstwa, jeżeli prowadząc interesy na terenie UE będą mogły one szeroko wykorzystywać podpisy kwalifikowane wydane w Polsce. Takie potencjalne korzyści są jednak zależne od zakresu i rodzaju usług świadczonych w innych krajach.</p> | | | | | | |
| | sektor mikro-, małych i średnich przedsiębiorstw | <p>Brak znaczącego wpływu. Obecnie przedsiębiorcy mogą korzystać zarówno ze środków identyfikacji elektronicznej (profil zaufany ePUAP), jak i z podpisu elektronicznego (przede wszystkim bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu). Nie będą musieli ponosić kosztów ich wymiany w okresie ich ważności.</p> <p>Możliwe jest osiągnięcie korzyści przez przedsiębiorców z sektora MSP, jeżeli prowadząc interesy na terenie UE będą mogli oni szeroko wykorzystywać podpisy kwalifikowane wydane w Polsce. Takie potencjalne korzyści są jednak zależne od zakresu i rodzaju usług świadczonych przez nich w innych krajach.</p> | | | | | | |
| | rodzina, obywatele oraz gospodarstwa domowe | <p>W praktyce brak wpływu o charakterze finansowym. Ewentualne korzyści będą zależne od dostępności usług, w tym także świadczonych dla naszych obywateli w innych krajach.</p> | | | | | | |
| Niemierzalne | odbiorcy usług | <p>Dla osób zamieszkujących za granicą zdalny dostęp do procedur z wykorzystaniem usług zaufania realizowanych przez urzędy w naszym kraju przełoży się na możliwość załatwienia wielu spraw drogą elektroniczną.</p> | | | | | | |

| | |
|---|--|
| <p>Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń</p> | <p>1. Przystosowanie działalności kwalifikowanych dostawców usług zaufania do wymogów eIDAS Wpływ nowych uregulowań należy rozpatrywać w dwóch aspektach: wpływ na koszty dokonania koniecznych zmian przystosowawczych oraz późniejszy wpływ na koszty działalności bieżącej. W przypadku dostawców usług zaufania trudno rozdzielić dokładnie koszty ponoszone na bieżące utrzymanie wewnętrznej infrastruktury sprzętowej i organizacyjnej, a przede wszystkim koszty związane z naturalnym rozwojem technologicznym, od tych kosztów, które wynikają bezpośrednio z przystosowania się do wymogów prawnych wynikających z rozporządzenia eIDAS, uregulowań towarzyszących oraz zracjonalizowanego systemu standardów M460.</p> <p>2. Wymagania technologiczne i standaryzacyjne nie są dla usługodawców zaskoczeniem i niezależnie od regulacji eIDAS i tak należałoby dokonać zmian w obsłudze odpowiednich algorytmów oraz standardów dotyczących struktury certyfikatów i podpisów elektronicznych. Prace w tym zakresie są prowadzone. Wymagania organizacyjne i nadzorcze nie wniosą radykalnych zmian z punktu widzenia centrów certyfikacji, ale wymagają podjęcia prac przystosowawczych. Chodzi o korekty polityk certyfikacji, dostosowanie nazewnictwa, opracowanie nowych procedur postępowania w przypadku zaistnienia incydentów.</p> <p>3. Koszty działalności bieżącej dostawców usług zaufania Wzrosną koszty działalności ponoszone z tytułu audytów. Audyt może kosztować w granicach 25000-35000 EUR w zależności od audytora (podmiot polski, o ile taki powstanie, lub zagraniczna jednostka oceny zgodności). Mogą wzrosnąć koszty ubezpieczenia. Może to nastąpić w przypadku podmiotów zainteresowanych świadczeniem wielu usług zaufania. Świadczenie nowych rodzajów usług będzie decyzją biznesową dostawcy usług zaufania.</p> <p>4. Koszty uruchomienia usług dodatkowych z listy usług kwalifikowanych przewidzianych w eIDAS przez dostawców usług zaufania Wejście usługodawców w nowe usługi będzie decyzją o charakterze biznesowym. Obecnie pod polską ustawą można było prowadzić też podobne usługi, ale jako nieuregulowane ustawowo (usługi nienazwane), nie były na polskim rynku usług szeroko wykorzystywane. W przypadku eIDAS może być mniejsze ryzyko biznesowe związane z inwestowaniem w te usługi.</p> <p>5. Koszty odbiorców usług zaufania Tu należy rozróżnić koszty do poniesienia przez biznes i przez administracje publiczną. Ci pierwsi nie muszą żadnych kosztów ponosić, jeżeli nie chcą korzystać z usług zaufania i komunikacji elektronicznej, albo koszty te poniosą w sposób raczej wyważony i bilansowany korzyściami biznesowymi. Tym bardziej, że biznes stosunkowo mało wykorzystywał kwalifikowane usługi zaufania, a więc nie musi w zasadzie dokonywać zmian w swoich systemach informatycznych lub procedurach w związku ze zmianami przepisów.</p> |
|---|--|

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

| | |
|--|--|
| <input type="checkbox"/> nie dotyczy | |
| Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). | <input type="checkbox"/> tak <input checked="" type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |
| <input type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur <input type="checkbox"/> skrócenie czasu na załatwienie sprawy <input type="checkbox"/> inne: | <input checked="" type="checkbox"/> zwiększenie liczby dokumentów <input checked="" type="checkbox"/> zwiększenie liczby procedur <input checked="" type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input checked="" type="checkbox"/> inne: audyty na koszt kwalifikowanego dostawcy usług zaufania raz na dwa lata, obowiązek raportowania incydentów |
| Wprowadzane obciążenia są przystosowane do ich elektroniczacji. | <input checked="" type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |

Komentarz:
Obciążenia dotyczą kwalifikowanych dostawców usług zaufania (np. wprowadzony jest nowy obowiązek związany z raportowaniem incydentów do nadzoru). Kwalifikowani dostawcy usług zaufania będą obowiązani przejść raz na dwa

lata na koszt własny audyt, prowadzony przez jednostki oceniające zgodność, którego koszt wynosi ok. 25 000-35 000 EUR. Ustawa znosi obowiązującą uprzednio zryczałtowaną opłatę za wpis do rejestru w wys. 10 000 EUR uiszczaną ministrowi właściwemu ds. gospodarki. Może wystąpić konieczność korzystania z zagranicznych jednostek oceniających zgodność, jeżeli nie będzie polskich audytorów zainteresowanych tego rodzaju działalnością w Polsce.

9. Wpływ na rynek pracy

B.d.

10. Wpływ na pozostałe obszary

| | | |
|---|---|--|
| <input type="checkbox"/> środowisko naturalne | <input type="checkbox"/> demografia | <input checked="" type="checkbox"/> informatyzacja |
| <input type="checkbox"/> sytuacja i rozwój regionalny | <input type="checkbox"/> mienie państwowe | <input type="checkbox"/> zdrowie |
| <input type="checkbox"/> inne: | | |
| Omówienie wpływu | | |

11. Planowane wykonanie przepisów aktu prawnego

Z dniem wejścia w życie ustawy.

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

Z uwagi na służący realizacji unijnego rozporządzenia charakter przepisów należy oczekiwać, że skutki będą oceniane przez Komisję Europejską na podstawie corocznych raportów z nadzoru. Na podstawie art. 49 eIDAS Komisja dokona przeglądu stosowania rozporządzenia i przekaże sprawozdanie Parlamentowi Europejskiemu i Radzie nie później niż do dnia 1 lipca 2020 r. Krajowy przegląd będzie dokonany przez ministra właściwego ds. informatyzacji 2 lata od momentu wejścia w życie ustawy, ze względu na konieczność zapewnienia prawidłowego rozwoju rynku usług zaufania.

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

1. Rozporządzenie 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 uchylające dyrektywę 1999/93/WE:

<http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014R0910&from=EN>

2. Obligatoryjne akty delegowane i implementujące do rozporządzenia eIDAS dotyczące usług zaufania.

Decyzja Wykonawcza Komisji (UE) 2015/296 z dnia 24 lutego 2015 r. ustanawiająca proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej na podstawie art. 12 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym:

http://www.mg.gov.pl/files/upload/8202/OJ_JOL_2015_053_R_0006_PL_TXT.pdf

Decyzja Wykonawcza Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 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 wewnętrznym:

http://www.mg.gov.pl/files/upload/8202/OJ_JOL_2015_235_R_0005_PL_TXT.pdf

Rozporządzenie Wykonawcze Komisji (UE) 2015/806 z dnia 22 maja 2015 r. określające specyfikacje dotyczące formy znaku zaufania UE dla kwalifikowanych usług zaufania:

http://www.mg.gov.pl/files/upload/8202/CELEX_32015R0806_PL_TXT.pdf

Rozporządzenie Wykonawcze Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym:

http://www.mg.gov.pl/files/upload/8202/OJ_JOL_2015_235_R_0001_PL_TXT.pdf

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:

http://www.mg.gov.pl/files/upload/8202/OJ_JOL_2015_235_R_0002_PL_TXT.pdf

3. Ekspertyza na zlecenie MG „Wdrożenie rozporządzenia eIDAS w Polsce”:
<http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Glowna-w.-4-2.pdf>
<http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Zalacznik-w.-4-2.pdf>

4. Auditing framework for Trust Service Providers
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp-auditing-framework/at_download/fullReport

5. Technical guideline for Incident Reporting
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/article19/technical-guideline-for-incident-reporting/at_download/fullReport

| TYTUŁ PROJEKTU: | | Ustawa o usługach zaufania oraz identyfikacji elektronicznej | | | |
|---|---|---|-------------------|----------------------------|--|
| TYTUŁ WDRAŻANEGO AKTU PRAWNEGO / WDRAŻANYCH AKTÓW PRAWNYCH ¹⁾: | | 1) rozporządzenie 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 uchylające dyrektywę 1999/93/WE Dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych. (Dz. U. WE L 13 z 19.01.2000, str. 12–20; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 24, str. 239–248) | | | |
| PRZEPISY UNII EUROPEJSKIEJ ²⁾ | | | | | |
| Jedn. red. | Treść przepisu UE ³⁾ | Ko niecz ność wdro żenia T / N | Jedn. red. (*) | Treść przepisu/ów projektu | Uzasadnienie uwzględnienia w projekcie przepisów wykraczających poza minimalne wymogi prawa UE |
| 1) rozporządzenie 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 uchylające dyrektywę 1999/93/WE Dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE (Dz. U. WE L 253 z 28.08.2014, str. 73) | | | | | |
| Uwaga: Rozporządzenie będzie stosowane bezpośrednio i jego przepisy nie podlegają transpozycji do prawa krajowego. W rozporządzeniu znajdują się dyspozycje dla państw członkowskich, które wymagają dostosowania przepisów krajowych w celu zapewnienia efektywnego stosowania regulacji wspólnotowych. | | | | | |
| Rozdział I | | | | | |
| Przepisy ogólne | | | | | |
| Art. | Przedmiot | N | | | |
| 1 | W celu zapewnienia właściwego funkcjonowania rynku wewnętrznego i w dążeniu do osiągnięcia odpowiedniego poziomu bezpieczeństwa środków identyfikacji elektronicznej i usług zaufania niniejsze rozporządzenie: a) określa warunki uznawania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego; b) określa przepisy dotyczące usług zaufania, w szczególności transakcji elektronicznych; oraz c) ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego i usług certyfikacyjnych uwierzytelniania witryn internetowych. | | | | |

| | | | | | |
|---------------|---|----------|---------|--|--|
| Art. 2 | Zakres stosowania 1. Niniejsze rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej, które zostały notyfikowane przez państwo członkowskie, oraz do dostawców usług zaufania mających siedzibę w Unii. | T | Art. 1. | 1. Ustawa określa: 1) krajową infrastrukturę zaufania; 2) działalność dostawców usług zaufania, w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych; 3) tryb notyfikacji krajowego systemu identyfikacji elektronicznej; 4) nadzór nad dostawcami usług zaufania. | |
| | 2. Niniejsze rozporządzenie nie ma zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników. 3. Niniejsze rozporządzenie nie ma wpływu na prawo krajowe ani unijne związane z zawieraniem i ważnością umów lub innych zobowiązań prawnych lub proceduralnych, dotyczące ich formy. | N | Art. 1. | 2. Przepisów ustawy nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników. 2. Przepisów ustawy nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników. | |
| Art. 3 | Definicje Do celów niniejszego rozporządzenia stosuje się następujące definicje: | T | Art. 2. | Ilekcioć w ustawie jest mowa o: 3) identyfikacji elektronicznej – należy przez to rozumieć proces, o którym mowa w art. 3 pkt 1 rozporządzenia 910/2014; | |
| | 1) „identyfikacja elektroniczna” oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną; | T | Art. 2. | Ilekcioć w ustawie jest mowa o: 14) środka identyfikacji elektronicznej – należy przez to rozumieć środek, o którym mowa w art. 3 pkt 2 rozporządzenia 910/2014; | |
| | 2) „środek identyfikacji elektronicznej” oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online; | N | | | |
| | 3) „dane identyfikujące osobę” oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną; | T | Art. 2. | Ilekcioć w ustawie jest mowa o: 13) systemie identyfikacji elektronicznej – należy przez to rozumieć system, o którym mowa w art. 3 pkt 4 rozporządzenia 910/2014; | |
| | 4) „system identyfikacji elektronicznej” oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne; | T | Art. 2 | Ilekcioć w ustawie jest mowa o: 16) uwierzytelnianiu – należy przez to rozumieć proces, o którym mowa w art. 3 pkt 5 rozporządzenia 910/2014; | |
| | 5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej; | N | | | |
| | 6) „strona ufająca” oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej | | | | |

| | | | | |
|---|---|---------|--|--|
| lub usłudze zaufania; | | | | |
| 7) „podmiot sektora publicznego” oznacza 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; | N | | | |
| 8) „podmiot prawa publicznego” oznacza podmiot zdefiniowany w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE (15); | N | | | |
| 9) „podpisujący” oznacza osobę fizyczną, która składa podpis elektroniczny; | N | | | |
| 10) „podpis elektroniczny” 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; | T | Art. 2. | Ilekroć w ustawie jest mowa o: 12) podpisem elektronicznym – należy przez to rozumieć podpis w rozumieniu art. 3 pkt 10 rozporządzenia 910/2014; | |
| 11) „zaawansowany podpis elektroniczny” oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26; | T | Art. 2. | Ilekroć w ustawie jest mowa o: 18) zaawansowanym podpisem elektronicznym – należy przez to rozumieć podpis elektroniczny, o którym mowa w art. 3 pkt 11 rozporządzenia 910/2014; | |
| 12) „ kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego | T | Art. 2. | Ilekroć w ustawie jest mowa o: 6) kwalifikowanym podpisem elektronicznym – należy przez to rozumieć zaawansowany podpis elektroniczny, o którym mowa w art. 3 pkt 12 rozporządzenia 910/2014; | |
| 13) „dane służące do składania podpisu elektronicznego” oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego; | N | | | |
| 14) „certyfikat podpisu elektronicznego” oznacza poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby; | N | | | |
| 15) „kwalifikowany certyfikat podpisu elektronicznego” oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I; | N | | | |
| 16) „usługa zaufania” oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą: a) tworzenie, weryfikację i walidację podpisów | T | Art. 2 | Ilekroć w ustawie jest mowa o: 15) usłudze zaufania – należy przez to rozumieć usługę, o której mowa w art. 3 pkt 16 rozporządzenia 910/2014; | |

| | | | | |
|--|---|---------|---|--|
| elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami; | | | | |
| 17) „kwalifikowana usługa zaufania” oznacza usługę zaufania, która spełnia stosowne wymogi określone w niniejszym rozporządzeniu; | T | Art. 2. | Ilekroć w ustawie jest mowa o: 8) kwalifikowanej usłudze zaufania – należy przez to rozumieć usługę zaufania, o której mowa w art. 3 pkt 17 rozporządzenia 910/2014; | |
| 18) „jednostka oceniająca zgodność” oznacza jednostkę określoną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która jest akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usługi zaufania i świadczonych przez niego kwalifikowanych usług zaufania; | T | Art. 2. | Ilekroć w ustawie jest mowa o: 4) jednostce oceniającej zgodność – należy przez to rozumieć jednostkę, o której mowa w art. 3 pkt 18 rozporządzenia 910/2014; | |
| 19) „dostawca usług zaufania” oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania; | T | Art. 2. | Ilekroć w ustawie jest mowa o: 1) dostawcy usług zaufania – należy przez to rozumieć osobę fizyczną lub osobę prawną, o której mowa w art. 3 pkt 19 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 199/93/WE (Dz. Urz. UE L 253 z 28.08.2014, str. 73), zwanym dalej „rozporządzeniem 910/2014”; | |
| 20) „kwalifikowany dostawca usług zaufania” oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru; | T | Art. 2. | Ilekroć w ustawie jest mowa o: 5) kwalifikowanym dostawcy usług zaufania – należy przez to rozumieć dostawcę usług zaufania, o którym mowa w art. 3 pkt 20 rozporządzenia 910/2014; | |
| 21) „produkt” oznacza sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania; | N | | | |
| 22) „urządzenie do składania podpisu elektronicznego” oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego; | N | | | |
| 23) „kwalifikowane urządzenie do składania podpisu elektronicznego” oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II; | N | | | |
| 24) „podmiot składający pieczęć” oznacza | N | | | |

| | | | | | |
|-----|--|---|---------|---|--|
| | osobę prawną, która składa pieczęć elektroniczną; | | | | |
| 25) | „pieczęć elektroniczna” oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych; | T | Art. 2. | Ilekróć w ustawie jest mowa o: 11) pieczęci elektronicznej – należy przez to rozumieć pieczęć, o której mowa w art. 3 pkt 25 rozporządzenia 910/2014; | |
| 26) | „zaawansowana pieczęć elektroniczna” oznacza pieczęć elektroniczną, która spełnia wymogi określone w art. 36; | T | Art. 2. | Ilekróć w ustawie jest mowa o: 17) zaawansowanej pieczęci elektronicznej – należy przez to rozumieć pieczęć elektroniczną, o której mowa w art. 3 pkt 26 rozporządzenia 910/2014; | |
| 27) | „kwalifikowana pieczęć elektroniczna” oznacza zaawansowaną pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej; | T | Art.2. | Ilekróć w ustawie jest mowa o: 7) kwalifikowanej pieczęci elektronicznej – należy przez to rozumieć zaawansowaną pieczęć elektroniczną, o której mowa w art. 3 pkt 27 rozporządzenia 910/2014; | |
| 28) | „dane służące do składania pieczęci elektronicznej” oznaczają niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej; | N | | | |
| 29) | „certyfikat pieczęci elektronicznej” oznacza poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby; | N | | | |
| 30) | „kwalifikowany certyfikat pieczęci elektronicznej” oznacza certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III; | N | | | |
| 31) | „urządzenie do składania pieczęci elektronicznej” oznacza skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej; | N | | | |
| 32) | „kwalifikowane urządzenie do składania pieczęci elektronicznej” oznacza urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II; | N | | | |
| 33) | „elektroniczny znacznik czasu” oznacza dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie; | T | | Ilekróć w ustawie jest mowa o: 2) elektronicznym znaczniku czasu – należy przez to rozumieć znacznik, o którym mowa w art. 3 pkt 33 rozporządzenia 910/2014; | |
| 34) | „kwalifikowany elektroniczny znacznik czasu” oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42; | N | | | |

| | | | | | |
|---------------|--|---|--|--|--|
| | 35) „dokument elektroniczny” oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne; | N | | | |
| | 36) „usługa rejestrowanego doręczenia elektronicznego” oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany; | N | | | |
| | 37) „kwalifikowana usługa rejestrowanego doręczenia elektronicznego” oznacza usługę rejestrowanego doręczenia elektronicznego, która spełnia wymogi określone w art. 44; | N | | | |
| | 38) „certyfikat uwierzytelniania witryn internetowych” oznacza poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat; | N | | | |
| | 39) „kwalifikowany certyfikat uwierzytelniania witryn internetowych” oznacza certyfikat uwierzytelniania witryn internetowych, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku IV; | N | | | |
| | 40) „dane służące do walidacji” oznaczają dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej; | N | | | |
| | 41) „walidacja” oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci. | N | | | |
| Art. 4 | Zasada rynku wewnętrznego 1. Nie ogranicza się świadczenia usług zaufania na terytorium państwa członkowskiego przez dostawcę usług zaufania mającego siedzibę w innym państwie członkowskim z powodów związanych z dziedzinami objętymi niniejszym rozporządzeniem. 2. Produkty i usługi zaufania spełniające wymogi niniejszego rozporządzenia dopuszcza się do swobodnego obrotu na rynku wewnętrznym. | N | | | |
| Art. 5 | Przetwarzanie i ochrona danych 1. Przetwarzanie danych osobowych prowadzone jest zgodnie z przepisami dyrektywy 95/46/WE. 2. Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się | N | | | |

| | | | | | |
|------------------------------------|---|----------|----------|---|--|
| | używania pseudonimów w transakcjach elektronicznych. | | | | |
| Rozdział II | | | | | |
| IDENTYFIKACJA ELEKTRONICZNA | | | | | |
| Art. 6 | <p>Wzajemne uznawanie</p> <p>1. Jeżeli zgodnie z prawem krajowym lub zgodnie z krajową praktyką administracyjną dostęp do usługi online świadczonej przez podmiot sektora publicznego w jednym państwie członkowskim wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, w tym pierwszym państwie członkowskim na potrzeby transgranicznego uwierzytelnienia dla tej usługi online uznaje się środek identyfikacji elektronicznej wydany w innym państwie członkowskim, pod warunkiem że spełnione są następujące warunki:</p> <p>a) środek identyfikacji elektronicznej jest wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9;</p> <p>b) poziom bezpieczeństwa środka identyfikacji elektronicznej odpowiada poziomowi bezpieczeństwa równemu lub wyższemu od poziomu bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na potrzeby dostępu do tej usługi online w pierwszym państwie członkowskim, pod warunkiem że poziom bezpieczeństwa tego środka identyfikacji elektronicznej odpowiada średniemu lub wysokiemu poziomowi bezpieczeństwa;</p> <p>c) odpowiedni podmiot sektora publicznego korzysta ze średniego lub wysokiego poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi online.</p> <p>Takiego uznania dokonuje się nie później niż 12 miesięcy po opublikowaniu przez Komisję wykazu, o którym mowa w akapicie pierwszym lit. a).</p> <p>2. Środek identyfikacji elektronicznej, który jest wydawany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9 i który odpowiada niskiemu poziomowi bezpieczeństwa, może być uznany przez podmioty sektora publicznego na potrzeby transgranicznego uwierzytelnienia dla usługi online świadczonej przez te podmioty.</p> | T | Art. 94. | <p>W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352) wprowadza się następujące zmiany:</p> <p>4) w art. 20a:</p> <p>a) ust. 1 otrzymuje brzmienie: „1. Uwierzytelnienie użytkowników systemu teleinformatycznego korzystających z usług online udostępnianych przez podmioty określone w art. 2 wymaga:</p> <p>1) użycia notyfikowanego środka identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa wymaganego dla usług świadczonych w ramach tych systemów, lub</p> | |

| | | | | | |
|----------------------|---|-----------------|-----------------|--|--|
| <p>Art. 7</p> | <p>Systemy identyfikacji elektronicznej kwalifikujące się do notyfikowania</p> <p>System identyfikacji elektronicznej kwalifikuje się do notyfikowania na podstawie art. 9 ust. 1, jeżeli spełnione zostaną wszystkie następujące warunki:</p> <p>a) środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej są wydawane:</p> <ul style="list-style-type: none"> (i) przez notyfikujące państwo członkowskie; (ii) na mocy upoważnienia od notyfikującego państwa członkowskiego; lub (iii) niezależnie od notyfikującego państwa członkowskiego i są uznawane przez to państwo członkowskie; <p>b) środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej mogą być używane w celu uzyskania dostępu do co najmniej jednej usługi świadczonej przez podmiot sektora publicznego, wymagającej identyfikacji elektronicznej w notyfikującym państwie członkowskim;</p> <p>c) system identyfikacji elektronicznej i środki identyfikacji elektronicznej wydane w jego ramach spełniają wymogi co najmniej jednego z poziomów bezpieczeństwa określonych w akcie wykonawczym, o którym mowa w art. 8 ust. 3;</p> | <p>N</p> | | | |
| | <p>d) notyfikujące państwo członkowskie zapewnia, aby dane identyfikujące osobę unikalnie reprezentujące daną osobę przyporządkowane były – zgodnie z technicznymi specyfikacjami, standardami i procedurami dotyczącymi odpowiedniego poziomu bezpieczeństwa określonego w akcie wykonawczym, o którym mowa w art. 8 ust. 3 – osobie fizycznej lub prawnej, o której mowa w art. 3 pkt 1, w momencie wydania środka identyfikacji elektronicznej w ramach tego systemu;</p> | <p>T</p> | <p>Art. 23.</p> | <p>1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowego węzła identyfikacji, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014.</p> <p>2. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, warunki organizacyjno-techniczne udostępniania krajowego węzła identyfikacji, mając na uwadze potrzebę zapewnienia interoperacyjności systemów identyfikacji elektronicznej, wykorzystywanych do uwierzytelniania osób w usługach online.</p> | |
| | <p>e) strona wydająca środek identyfikacji elektronicznej w ramach tego systemu zapewnia, aby środek identyfikacji elektronicznej był przyporządkowany osobie, o której mowa w lit. d) niniejszego artykułu, zgodnie z technicznymi specyfikacjami, standardami i procedurami dotyczącymi odpowiedniego poziomu bezpieczeństwa określonego w akcie wykonawczym, o którym mowa w art. 8 ust. 3;</p> | <p>N</p> | | | |

| | | | | |
|--|---|----------|--|--|
| <p>f) notyfikujące państwo członkowskie zapewnia dostępność uwierzytelniania online, tak aby każda strona ufająca mająca siedzibę na terytorium innego państwa członkowskiego mogła potwierdzić dane identyfikujące osobę otrzymane w postaci elektronicznej.</p> <p>W odniesieniu do stron ufających innych niż podmioty sektora publicznego notyfikujące państwo członkowskie może określić warunki dostępu do tego uwierzytelnienia. Transgraniczne uwierzytelnienie jest świadczone bezpłatnie, gdy jest ono dokonywane w powiązaniu z usługą online świadczoną przez podmiot sektora publicznego.</p> <p>Państwa członkowskie nie nakładają żadnych specjalnych niewspółmiernych wymogów technicznych na strony ufające, które zamierzają dokonać takiego uwierzytelnienia, w przypadku gdyby takie wymogi miały uniemożliwić lub znacznie utrudnić interoperacyjność notyfikowanych systemów identyfikacji elektronicznej;</p> | T | Art. 24. | <p>Minister właściwy do spraw informatyzacji koordynuje działania na poziomie krajowym na rzecz współpracy z państwami członkowskimi Unii Europejskiej w sprawach dotyczących systemów identyfikacji elektronicznej, prowadzonej zgodnie z art. 12 ust. 5 i 6 rozporządzenia 910/2014, w szczególności zapewniając obsługę pojedynczego punktu kontaktowego, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 7 tego rozporządzenia.</p> | |
| <p>g) co najmniej sześć miesięcy przed notyfikacją na podstawie art. 9 ust. 1 notyfikujące państwo członkowskie przekazuje innym państwom członkowskim do celów wykonania obowiązku na mocy art. 12 ust. 5 opis tego systemu zgodnie z warunkami proceduralnymi ustanowionymi w aktach wykonawczych, o których mowa w art. 12 ust. 7;</p> <p>h) system identyfikacji elektronicznej spełnia wymogi określone w akcie wykonawczym, o którym mowa w art. 12 ust. 8.</p> | T | Art. 24 | <p>Minister właściwy do spraw informatyzacji koordynuje działania na poziomie krajowym na rzecz współpracy z państwami członkowskimi Unii Europejskiej w sprawach dotyczących systemów identyfikacji elektronicznej, prowadzonej zgodnie z art. 12 ust. 5 i 6 rozporządzenia 910/2014, w szczególności zapewniając obsługę pojedynczego punktu kontaktowego, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 7 tego rozporządzenia.</p> | |

| | | | | | |
|----------------------|---|----------|------------------------|--|--|
| <p>Art. 8</p> | <p>Poziomy bezpieczeństwa systemów identyfikacji elektronicznej</p> <p>1. System identyfikacji elektronicznej notyfikowany na podstawie art. 9 ust. 1 określa niski, średni lub wysoki poziom bezpieczeństwa w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach tego systemu.</p> <p>2. Niski, średni i wysoki poziom bezpieczeństwa oznaczają spełnienie, odpowiednio, następujących kryteriów:</p> <p>a) niski poziom bezpieczeństwa odnosi się w kontekście systemu identyfikacji elektronicznej do środka identyfikacji elektronicznej, który zapewnia ograniczony stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest obniżenie ryzyka podszycia się lub modyfikacji tożsamości;</p> <p>b) średni poziom bezpieczeństwa odnosi się w kontekście systemu identyfikacji elektronicznej do środka identyfikacji elektronicznej, który zapewnia średni stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest znaczne obniżenie ryzyka podszycia się lub modyfikacji</p> | <p>±</p> | <p>Art. 26.</p> | <p>Podmiot udostępniający usługę publiczną online określa wymagane poziomy bezpieczeństwa, o których mowa w art. 8 rozporządzenia 910/2014, dla środków identyfikacji elektronicznej, niezbędne dla realizacji tej usługi oraz udostępnia informację o tych wymaganiach.</p> | |
|----------------------|---|----------|------------------------|--|--|

| | | | | | |
|-----------|--|--|--|--|--|
| | <p>tożsamości;</p> <p>c) wysoki poziom bezpieczeństwa odnosi się w kontekście systemu identyfikacji elektronicznej do środka identyfikacji elektronicznej, który zapewnia wyższy stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby niż środek identyfikacji elektronicznej o średnim poziomie pewności i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest zapobieganie podszyciu się lub modyfikacji tożsamości.</p> <p>3. Do dnia 18 września 2015 r., przy uwzględnieniu odpowiednich standardów międzynarodowych i z zastrzeżeniem ust. 2, Komisja określi w drodze aktów wykonawczych minimalne techniczne specyfikacje, standardy i procedury, w odniesieniu do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej do celów ust. 1.</p> <p>Te minimalne techniczne specyfikacje, standardy i procedury są określane przez odniesienie do wiarygodności i jakości następujących elementów:</p> <p>a) procedury wykazującej i weryfikującej tożsamość osób fizycznych lub prawnych wnioskujących o wydanie środka identyfikacji elektronicznej;</p> <p>b) procedury wydawania wnioskowanego środka identyfikacji elektronicznej;</p> <p>c) mechanizmu uwierzytelniania, w którym osoba fizyczna lub prawna używa środka identyfikacji elektronicznej do potwierdzenia swojej tożsamości wobec strony ufającej;</p> <p>d) jednostki wydającej środek identyfikacji elektronicznej;</p> <p>e) każdego innego organu zaangażowanego w ramach wniosku o wydanie środka identyfikacji elektronicznej; oraz</p> <p>f) specyfikacji technicznych i specyfikacji bezpieczeństwa wydanego środka identyfikacji elektronicznej.</p> <p>Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | | | | |
| Art. 9 | Notyfikacja | | | | |

| | | | | |
|--|---|----------|---|--|
| <p>1. Notyfikujące państwo członkowskie notyfikuje Komisji następujące informacje i, bez zbędnej zwłoki, wszelkie późniejsze w nich zmiany:</p> <p>a) opis systemu identyfikacji elektronicznej, w tym jego poziomy bezpieczeństwa oraz wydawcę lub wydawców środków identyfikacji elektronicznej w ramach tego systemu;</p> <p>b) mający zastosowanie system nadzoru i informacje na temat systemu odpowiedzialności w odniesieniu do następujących stron:</p> <p>(i) strony wydającej środki identyfikacji elektronicznej; oraz</p> <p>(ii) strony przeprowadzającej procedurę uwierzytelniania;</p> <p>c) organ lub organy odpowiedzialne za system identyfikacji elektronicznej;</p> <p>d) informacje na temat jednostki lub jednostek, które zarządzają rejestracją unikalnych danych identyfikujących osobę;</p> <p>e) opis sposobu spełnienia wymogów określonych w aktach wykonawczych, o których mowa w art. 12 ust. 8;</p> <p>f) opis uwierzytelnienia, o którym mowa w art. 7 lit. f);</p> <p>g) ustalenia dotyczące zawieszania lub unieważniania notyfikowanego systemu identyfikacji elektronicznej lub uwierzytelnienia lub też ich skompromitowanych części.</p> | T | Art. 25. | <p>1. Wniosek o notyfikowanie krajowego systemu identyfikacji elektronicznej w Komisji Europejskiej składa do ministra właściwego do spraw informatyzacji podmiot odpowiedzialny za ten system.</p> <p>2. Do wniosku, o którym mowa w ust. 1, załącza się formularz notyfikacji systemu identyfikacji elektronicznej zgodny ze wzorem określonym w przepisach wykonawczych wydanych na podstawie art. 9 ust. 5 rozporządzenia 910/2014.</p> <p>3. Minister właściwy do spraw informatyzacji zgłasza krajowy 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.</p> <p>4. Minister właściwy do spraw informatyzacji zgłasza krajowy 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.</p> <p>5. Minister właściwy do spraw informatyzacji może powierzyć wykonywanie zadań, o których mowa w ust. 3 i 4, podmiotowi publicznemu w rozumieniu art. 2 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352).</p> | |
| <p>2. Rok od daty rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8, Komisja opublikuje w Dzienniku Urzędowym Unii Europejskiej wykaz systemów identyfikacji elektronicznej, które zostały notyfikowane na mocy ust. 1 niniejszego artykułu, oraz podstawowe informacje na ich temat.</p> <p>3. Jeżeli Komisja otrzyma notyfikację po upływie okresu, o którym mowa w ust. 2, publikuje w Dzienniku Urzędowym Unii Europejskiej zmiany w wykazie, o którym mowa w ust. 2, w terminie dwóch miesięcy od daty otrzymania tej notyfikacji.</p> <p>4. Państwo członkowskie może przekazać Komisji wniosek o usunięcie z wykazu, o którym mowa w ust. 2, systemu identyfikacji elektronicznej notyfikowanego przez to państwo członkowskie. Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej odpowiednie zmiany w wykazie w terminie jednego miesiąca od daty otrzymania wniosku państwa członkowskiego.</p> | N | | | |

| | | | | | |
|----------------|--|----------|----------|--|--|
| | 5. Komisja może w drodze aktów wykonawczych określić okoliczności, formaty i procedury dotyczące notyfikacji określonej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | | | | |
| Art. 10 | <p>Naruszenie bezpieczeństwa</p> <p>1. W przypadku gdy nastąpi naruszenie lub częściowa kompromitacja systemu identyfikacji elektronicznej notyfikowanego na podstawie art. 9 ust. 1, albo uwierzytelnienia, o którym mowa w art. 7 lit. f), mające wpływ na wiarygodność transgranicznego uwierzytelnienia tego systemu, notyfikujące państwo członkowskie niezwłocznie zawiesza lub unieważnia to transgraniczne uwierzytelnianie lub dane skompromitowane części oraz powiadamia o tym pozostałe państwa członkowskie i Komisję.</p> <p>2. W przypadku gdy naruszenie lub kompromitacja, o których mowa w ust. 1, zostanie wyeliminowane, notyfikujące państwo członkowskie przywraca transgraniczne uwierzytelnianie i bez zbędnej zwłoki powiadamia o tym pozostałe państwa członkowskie i Komisję.</p> <p>3. Jeżeli naruszenie lub kompromitacja, o których mowa w ust. 1, nie zostanie wyeliminowane w ciągu trzech miesięcy od zawieszenia lub unieważnienia, notyfikujące państwo członkowskie powiadamia pozostałe państwa członkowskie i Komisję o wycofaniu systemu identyfikacji elektronicznej. Komisja bez zbędnej zwłoki publikuje w Dzienniku Urzędowym Unii Europejskiej odpowiednie zmiany w wykazie, o którym mowa w art. 9 ust. 2.</p> | T | Art. 27. | <p>1. Obowiązki, o których mowa w art. 10 rozporządzenia 910/2014, wykonuje minister właściwy do spraw informatyzacji.</p> <p>2. Informacje dotyczące naruszenia bezpieczeństwa notyfikowanego krajowego systemu identyfikacji elektronicznej albo systemu uwierzytelnienia, o którym mowa w art. 10 rozporządzenia 910/2014, zarządzający tymi systemami przekazują niezwłocznie, drogą elektroniczną, ministrowi właściwemu do spraw informatyzacji.</p> | |
| Art. 11 | <p>Odpowiedzialność</p> <p>1. Notyfikujące państwo członkowskie jest odpowiedzialne za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem swoich obowiązków na mocy art. 7 lit. d) i f), w ramach transgranicznej transakcji.</p> | N | | | |
| | <p>2. Strona wydająca środek identyfikacji elektronicznej jest odpowiedzialna za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązku, o którym mowa w art. 7 lit. e), w ramach transgranicznej transakcji.</p> <p>3. Strona przeprowadzająca procedurę</p> | T | Art. 50. | Kto wydając środek identyfikacji elektronicznej w ramach notyfikowanego systemu identyfikacji elektronicznej wydaje taki środek osobie nieuprawnionej, podlega grzywnie lub karze pozbawienia wolności do lat 3. | |

| | | | | | |
|----------------|---|---|---------|--|--|
| | uwierzytelniania jest odpowiedzialna za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niezapewnieniem poprawnego przebiegu uwierzytelniania, o którym mowa w art. 7 lit. f), w ramach transgranicznej transakcji. | T | Art. 51 | Karom określonym w art. 45–50 podlega także ten, kto dopuszcza się czynów, o których mowa w tych przepisach, działając w imieniu lub w interesie innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej. | |
| | 4. Ust. 1, 2 i 3 mają zastosowanie zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności. | N | | | |
| | 5. Ust. 1, 2 i 3 pozostają bez uszczerbku dla odpowiedzialności, na mocy prawa krajowego właściwego dla stron transakcji, na potrzeby której zastosowano środki identyfikacji elektronicznej objęte systemem identyfikacji elektronicznej notyfikowanym na podstawie art. 9 ust. 1. | N | | | |
| Art. 12 | <p>Współpraca i interoperacyjność</p> <p>1. Krajowe systemy identyfikacji elektronicznej notyfikowane na podstawie art. 9 ust. 1 muszą być interoperacyjne.</p> <p>2. Do celów ust. 1 ustanawia się ramy interoperacyjności.</p> <p>3. Ramy interoperacyjności spełniają następujące kryteria:</p> <p>a) są neutralne pod względem technologicznym i nie dyskryminują żadnych konkretnych krajowych rozwiązań technicznych w zakresie identyfikacji elektronicznej w danym państwie członkowskim;</p> <p>b) są zgodne, w miarę możliwości, z europejskimi i międzynarodowymi standardami;</p> <p>c) ułatwiają wdrożenie zasady uwzględniania ochrony prywatności już w fazie projektowania; oraz</p> <p>d) zapewniają, aby dane osobowe były przetwarzane zgodnie z dyrektywą 95/46/WE.</p> <p>4. Ramy interoperacyjności zawierają:</p> <p>a) odniesienie do minimalnych wymogów technicznych powiązanych z poziomami bezpieczeństwa określonych w art. 8;</p> <p>b) przyporządkowanie krajowych poziomów bezpieczeństwa notyfikowanych systemów identyfikacji elektronicznej względem poziomów bezpieczeństwa na mocy art. 8;</p> <p>c) odniesienie do minimalnych wymogów technicznych dotyczących interoperacyjności;</p> <p>d) odniesienie do minimalnego zbioru danych identyfikujących osobę unikalnie reprezentujących osobę fizyczną lub prawną, dostępnego w ramach systemów identyfikacji elektronicznej;</p> | N | | | |

| | | | | |
|--|---|----------|--|--|
| <p>e) regulamin wewnętrzny; f) ustalenia dotyczące rozstrzygania sporów; oraz g) wspólne operacyjne standardy bezpieczeństwa.</p> | | | | |
| <p>5. Państwa członkowskie współpracują ze sobą, mając na uwadze następujące kwestie: a) interoperacyjność systemów identyfikacji elektronicznej notyfikowanych na podstawie art. 9 ust. 1 i systemów identyfikacji elektronicznej, które państwa członkowskie zamierzają notyfikować; oraz b) bezpieczeństwo systemów identyfikacji elektronicznej.</p> | T | Art. 24. | Minister właściwy do spraw informatyzacji koordynuje działania na poziomie krajowym na rzecz współpracy z państwami członkowskimi Unii Europejskiej w sprawach dotyczących systemów identyfikacji elektronicznej, prowadzonej zgodnie z art. 12 ust. 5 i 6 rozporządzenia 910/2014, w szczególności zapewniając obsługę pojedynczego punktu kontaktowego, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 7 tego rozporządzenia. | |
| <p>6. Współpraca między państwami członkowskimi obejmuje: a) wymianę informacji, doświadczeń i dobrych praktyk w zakresie systemów identyfikacji elektronicznej, a w szczególności wymogów technicznych związanych z interoperacyjnością i poziomami bezpieczeństwa; b) wymianę informacji, doświadczeń i dobrych praktyk w zakresie pracy z poziomami bezpieczeństwa systemów identyfikacji elektronicznej określonych w art. 8; c) wzajemną ocenę systemów identyfikacji elektronicznej objętych niniejszym rozporządzeniem; oraz d) analizę istotnych zmian w sytuacji w sektorze identyfikacji elektronicznej.</p> | N | | | |
| <p>7. Do dnia 18 marca 2015 r. Komisja ustanowi w drodze aktów wykonawczych niezbędne proceduralne warunki ułatwiania współpracy między państwami członkowskimi, o której mowa w ust. 5 i 6, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka.</p> | N | | | |
| <p>8. Do dnia 18 września 2015 r., do celów określenia jednolitych warunków realizacji wymogu, o którym mowa w ust. 1, z zastrzeżeniem kryteriów określonych w ust. 3 i z uwzględnieniem wyników współpracy między państwami członkowskimi, Komisja przyjmie akty wykonawcze dotyczące ram interoperacyjności określonych w ust. 4.</p> | T | Art.23. | <p>1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowego węzła identyfikacji, o którym mowa w przepisach wykonawczych wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014.</p> <p>2. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, warunki organizacyjno-techniczne udostępniania krajowego węzła identyfikacji, mając na uwadze potrzebę zapewnienia interoperacyjności systemów identyfikacji elektronicznej, wykorzystywanych do uwierzytelniania osób w usługach online.</p> | |

| | | | | | |
|------------------------|--|---|----------|--|--|
| | 9. Akty wykonawcze, o których mowa w ust. 7 i 8 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| ROZDZIAŁ III | | | | | |
| USŁUGI ZAUFANIA | | | | | |
| SEKCJA 1 | | | | | |
| Przepisy ogólne | | | | | |
| Art. 13 | Odpowiedzialność i ciężar dowodu | | | | |
| | 1. Bez uszczerbku dla ust. 2, dostawcy usług zaufania są odpowiedzialni za szkody wyrządzone w sposób zamierzony lub z powodu zaniedbania osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązków określonych w niniejszym rozporządzeniu. Ciężar dowiedzenia zamiaru lub zaniedbania niekwalifikowanego dostawcy usług zaufania spoczywa na osobie fizycznej lub prawnej zgłaszającej szkodę, o której mowa w akapicie pierwszym. Domniemywa się zamiar lub zaniedbanie kwalifikowanego dostawcy usług zaufania, chyba że kwalifikowany dostawca usług zaufania udowodni, że szkoda, o której mowa w akapicie pierwszym, nie powstała z powodu zamierzonego działania lub zaniedbania tego kwalifikowanego dostawcy usług zaufania. | T | Art. 22. | 1. Dostawca usług zaufania nie odpowiada za szkody wynikające z nieprzestrzegania przez odbiorcę usług zaufania zasad określonych w polityce świadczenia usługi, w szczególności za szkody wynikające z: <ul style="list-style-type: none"> 1) użycia certyfikatu niezgodnie z zakresem określonym w polityce świadczenia usługi wskazanej w certyfikacie, w tym za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została wskazana w certyfikacie; 2) nieprawdziwości danych zawartych w certyfikacie, podanych przez odbiorcę usług zaufania używającego tego certyfikatu, chyba że szkoda była wynikiem niedołożenia należytej staranności przez dostawcę usług zaufania; 3) przechowywania lub używania przez odbiorców usług zaufania danych do składania podpisu elektronicznego, pieczęci elektronicznej lub uwierzytelniania witryn internetowych w sposób niezapewniający ich ochrony przed nieuprawnionym wykorzystaniem. | |
| | 2. W przypadku gdy dostawcy usług zaufania z wyprzedzeniem należyście powiadomią swoich klientów o ograniczeniach w korzystaniu ze świadczonych przez siebie usług i ograniczenia te mogą być rozpoznane przez strony trzecie, dostawcy usług zaufania nie są odpowiedzialni za szkody powstałe w wyniku korzystania z usług przekraczającego wskazane ograniczenia. 3. Ust. 1 i 2 mają zastosowanie zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności. | T | Art. 22. | 1. Dostawca usług zaufania nie odpowiada za szkody wynikające z nieprzestrzegania przez odbiorcę usług zaufania zasad określonych w polityce świadczenia usługi, w szczególności za szkody wynikające z: <ul style="list-style-type: none"> 1) użycia certyfikatu niezgodnie z zakresem określonym w polityce świadczenia usługi wskazanej w certyfikacie, w tym za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została wskazana w certyfikacie; 2) nieprawdziwości danych zawartych w certyfikacie, podanych przez odbiorcę usług zaufania używającego tego certyfikatu, chyba że szkoda była wynikiem niedołożenia należytej staranności przez dostawcę usług zaufania; 3) przechowywania lub używania przez odbiorców usług zaufania danych do składania podpisu elektronicznego, pieczęci elektronicznej lub uwierzytelniania witryn internetowych w sposób niezapewniający ich ochrony przed nieuprawnionym wykorzystaniem. | |

| | | | | | |
|----------------|--|----------|---------|---|--|
| Art. 14 | Aspekty międzynarodowe 1. Usługi zaufania świadczone przez dostawców usług zaufania mających siedzibę w państwie trzecim są uznawane za prawnie równoważne kwalifikowanym usługom zaufania świadczonym przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii, w przypadku gdy usługi zaufania pochodzące z państwa trzeciego są uznawane na mocy umowy zawartej między Unią a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 218 TFUE. | N | | | |
| | 2. Umowy, o których mowa w ust. 1, zapewniają w szczególności, aby: a) wymogi mające zastosowanie do kwalifikowanych dostawców usług zaufania mających siedzibę w Unii i do świadczonych przez nich kwalifikowanych usług zaufania były spełniane przez dostawców usług zaufania w państwie trzecim lub organizacjach międzynarodowych, z którymi zawarta została umowa, oraz przez świadczone przez nich usługi zaufania; b) kwalifikowane usługi zaufania świadczone przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii były uznawane za prawnie równoważne usługom zaufania świadczonym przez dostawców usług zaufania w państwie trzecim lub organizacjach międzynarodowych, z którymi zawarta została umowa. | N | | | |
| Art. 15 | Dostępność dla osób niepełnosprawnych Gdy jest to wykonalne, świadczone usługi zaufania i produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług są dostępne dla osób niepełnosprawnych. | N | | | |
| Art. 16 | Sankcje Państwa członkowskie ustanawiają przepisy o sankcjach mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. | T | Art. 28 | 2. W zakresie nadzoru, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji: 8) nakłada kary pieniężne; | |

| | | | | | |
|--|--|---|----------|--|--|
| | | T | Art. 42. | <p>Art. 42. 1. Karę pieniężną, o której mowa w art. 41, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.</p> <p>2. Wysokość kary pieniężnej, o której mowa w art. 41:</p> <p>1) pkt 1-9 i 12, wynosi do 50 000 zł;</p> <p>2) pkt 10, wynosi do 10 000 zł;</p> <p>3) pkt 11, wynosi do 100 000 zł.</p> | |
| | | T | Art. 41. | <p>Art. 41. Karze pieniężnej podlega kwalifikowany dostawca usług zaufania, który:</p> <p>1) nie wykonuje obowiązku wynikającego z art. 24 ust. 1 rozporządzenia 910/2014;</p> <p>2) nie usunął w terminie określonym w wezwaniu, o którym mowa w art. 31 pkt 1 lit. a, stwierdzonych nieprawidłowości w prowadzonej przez siebie działalności;</p> <p>3) stosuje politykę świadczenia usługi lub przyjmuje inne dokumenty związane ze świadczeniem usługi zaufania niezgodne z tymi przepisami;</p> <p>4) nie unieważnia kwalifikowanych certyfikatów pomimo wezwania organu, o którym mowa w art. 31 pkt 1 lit. c;</p> <p>5) wydaje certyfikaty niezgodnie z polityką świadczenia usługi;</p> <p>6) nie udziela informacji lub nie udostępnia dokumentów w przypadku, o którym mowa w art. 5;</p> <p>7) nie poinformował ministra właściwego do spraw informatyzacji o zmianie danych podlegających wpisowi do rejestru lub danych dotyczących technicznych możliwości prowadzenia działalności w zakresie świadczenia usług zaufania wskazanych we wniosku o wpis do rejestru;</p> <p>8) nie wykonuje obowiązków informacyjnych, o których mowa w art. 19 ust. 2 rozporządzenia 910/2014;</p> <p>9) uniemożliwia lub utrudnia audytorowi organu nadzoru wykonywanie czynności audytowych;</p> <p>10) nie posiada planu zakończenia działalności lub nie stosuje go do zakończenia działalności organ nadzoru;</p> <p>11) nie wykona obowiązku, o którym mowa w art. 21 ust. 2 lub 3 ;</p> <p>12) nie wykona obowiązku, o którym mowa w art. 14 ust. 1</p> | |

| | | | | | |
|--|--|---|----------|--|--|
| | | T | Art. 45 | <p>1. Kto składa kwalifikowany podpis elektroniczny lub zaawansowany podpis elektroniczny z wykorzystaniem danych do składania podpisu elektronicznego przyporządkowanych do innej osoby, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.</p> <p>2. Tej samej karze podlega kto składa kwalifikowaną pieczęć elektroniczną lub zaawansowaną pieczęć elektroniczną, nie będąc do tego uprawnionym.</p> <p>3. Tej samej karze podlega ten, kto składa zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną kwalifikowanego dostawcy usług zaufania za pomocą danych przyporządkowanych do tego podmiotu nie będąc uprawnionym.</p> | |
| | | T | Art. 46 | <p>Kto bez uprawnienia kopiuje lub przechowuje nieprzyporządkowane do niego dane do składania zaawansowanego podpisu elektronicznego lub pieczęci elektronicznej lub inne dane, które mogłyby służyć do ich odtworzenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.</p> | |
| | | T | Art. 47. | <p>1. Kto, świadcząc usługi zaufania, wydaje certyfikat zawierający nieprawdziwe w celu popełnienia czynu zabronionego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.</p> <p>2. Tej samej karze podlega osoba, która składa podpis elektroniczny lub pieczęć elektroniczną weryfikowane certyfikatem, o którym mowa w ust. 1.</p> | |
| | | T | Art. 48 | <p>Kto, świadcząc usługi zaufania, wbrew obowiązкови, o którym mowa w art. 31 pkt 1 lit. c, celowo zaniecha unieważnienia certyfikatu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.</p> | |
| | | T | Art. 49 | <p>1. Kto, będąc obowiązany do zachowania tajemnicy związanej ze świadczeniem usług zaufania, ujawnia lub wykorzystuje, wbrew warunkom określonym w przepisach o usługach zaufania, informacje objęte tą tajemnicą,</p> <p>podlega grzywnie.</p> <p>2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 jako kwalifikowany dostawca usług zaufania albo w celu osiągnięcia korzyści majątkowej lub osobistej,</p> <p>podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.</p> | |

| | | | | | |
|--------------------|--|---|----------|--|--|
| | | T | Art. 50 | Kto wydając środek identyfikacji elektronicznej w ramach notyfikowanego systemu identyfikacji elektronicznej umyślnie wydaje taki środek osobie nieuprawnionej, podlega grzywnie lub karze pozbawienia wolności do lat 3. | |
| SEKCJA 2 Nadzór | | | | | |
| | | T | Art. 65 | W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2016 r. poz. 543 i 749) wprowadza się następujące zmiany: 1) w art. 9 w ust. 2 uchyla się pkt 6; 2) w art. 12a w ust. 1 w pkt 12 kropkę zastępuje się średnikiem i dodaje się pkt 13 w brzmieniu: „13) nadzoru nad świadczeniem usług zaufania w rozumieniu przepisów o usługach zaufania.”. | |
| Art. 17 | Organ nadzoru 1. Państwa członkowskie wyznaczają organ nadzoru z siedzibą na swoim terytorium lub, za obopólnym porozumieniem z innym państwem członkowskim, organ nadzoru z siedzibą w tym innym państwie członkowskim. Organ ten jest odpowiedzialny za zadania nadzoru w wyznaczającym państwie członkowskim. Organom nadzoru przyznaje się uprawnienia i odpowiednie zasoby niezbędne do wykonywania ich zadań. | T | Art. 28. | 1. Nadzór nad dostawcami usług zaufania sprawuje minister właściwy do spraw informatyzacji. | |
| | | T | Art. 28. | 2. W zakresie nadzoru, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji: 1) wykonuje zadania określone w przepisach rozporządzenia 910/2014; 2) wydaje certyfikaty dostawców usług zaufania; 3) tworzy certyfikaty narodowego centrum certyfikacji; 4) może unieważniać certyfikaty, o których mowa w pkt 2 i 3; 5) może żądać niezwłocznego unieważnienia kwalifikowanego certyfikatu przez kwalifikowanego dostawcę usług zaufania; 6) bada zgodność polityki świadczenia usługi z przepisami o usługach zaufania; 7) prowadzi rejestr dostawców usług zaufania; 8) nakłada kary pieniężne; 9) wykonuje inne zadania określone w przepisach prawa. | |
| | | T | Art. 29. | Dostawca usługi zaufania, na żądanie ministra właściwego do spraw informatyzacji, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych, jest obowiązany udzielać informacji lub udostępniać dokumenty, które są bezpośrednio związane lub mają wpływ na świadczone usługi zaufania, w tym dotyczą zarządzania incydentami związanymi z usługą zaufania. | |
| | | T | Art. 30. | 1. W przypadku odebrania kwalifikowanemu dostawcy usługi zaufania statusu kwalifikowanego lub statusu kwalifikowanego świadczonej przez niego usługi zaufania minister właściwy do spraw informatyzacji, w drodze decyzji, może unieważnić odpowiednie certyfikaty dostawcy usługi zaufania, wydanych temu dostawcy. 2. Unieważniając certyfikaty dostawcy usługi zaufania, minister właściwy do spraw informatyzacji bierze pod uwagę stopień zagrożenia dla bezpieczeństwa świadczenia usług zaufania, możliwość usunięcia tego | |

| | | | | |
|--|---|----------|--|--|
| | | | zagrożenia w inny sposób oraz pewność obrotu. | |
| | T | Art. 31. | Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że kwalifikowany dostawca usługi zaufania prowadzi działalność niezgodnie z przepisami o usługach zaufania, może: 1) wezwać kwalifikowanego dostawcę usług zaufania, aby w wyznaczonym terminie: a) usunął stwierdzone nieprawidłowości i doprowadził swoją działalność do stanu zgodnego z przepisami o usługach zaufania, b) zmienił politykę świadczenia usług lub inne dokumenty związane ze świadczeniem usług zaufania, c) unieważnił kwalifikowane certyfikaty wydane z naruszeniem polityki świadczenia usług; 2) wydać decyzję o odebraniu kwalifikowanemu dostawcy usług zaufania statusu kwalifikowanego lub statusu kwalifikowanego świadczonej przez niego usłudze zaufania. | |
| | T | Art. 33. | Audytorzy organu nadzoru i obserwatorzy organu nadzoru nie mogą prowadzić działalności gospodarczej w zakresie świadczenia usług zaufania, świadczyć usług zaufania, być współnikami albo akcjonariuszami dostawcy usług zaufania, ani wykonywać obowiązków osoby reprezentującej lub członka rady nadzorczej albo komisji rewizyjnej tego dostawcy, a także pozostawać z tym dostawcą w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze. | |
| | T | Art. 34. | 1. Audytorzy organu nadzoru są uprawnieni do: 1) wstępu do obiektów i pomieszczeń kwalifikowanych dostawców usług zaufania; 2) wglądu do dokumentów i danych, z wyjątkiem danych do składania podpisów elektronicznych lub pieczęci elektronicznych dostawców usług zaufania i innych informacji, które mogą służyć do odtworzenia tych danych, związanych z działalnością w zakresie usług zaufania; 3) przetwarzania danych osobowych w zakresie objętym przedmiotem audytu; 4) przeprowadzania oględzin obiektów oraz innych składników majątkowych związanych ze świadczeniem usług zaufania a także sprawdzenia przebiegu czynności związanych ze świadczeniem tych usług; 5) żądania udzielenia ustnych lub pisemnych wyjaśnień od | |

| | | | | |
|--|---|-----------|--|--|
| | | | <p>pracowników kwalifikowanych dostawców usług zaufania;</p> <p>6) zabezpieczania dokumentów i innych materiałów, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.</p> <p>2. Upoważniony przedstawiciel audytowanego kwalifikowanego dostawcy usług zaufania udziela wyjaśnień lub przedkłada, na żądanie audytora organu nadzoru, dokumenty i inne materiały niezbędne do przeprowadzenia audytu.</p> <p>3. Przepis ust. 1 pkt 1 - 4 stosuje się do obserwatorów organu nadzoru.</p> | |
| | T | Art. 37. | W sprawach nieuregulowanych w ustawie, do przeprowadzenia audytu dostawców usług zaufania przez audytorów organu nadzoru stosuje się odpowiednio przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 584, z późn. zm.), z wyłączeniem przepisu art. 83 ust. 1 . | |
| | T | Art. 3. | <p>Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje:</p> <p>1) rejestr dostawców usług zaufania, zwany dalej „rejestrem”;</p> <p>2) zaufaną listę;</p> <p>3) narodowe centrum certyfikacji.</p> | |
| | T | Art. 5. | <p>1. Wpis do rejestru:</p> <p>1) dostawcy usług zaufania, który zamierza świadczyć kwalifikowane usługi zaufania, lub</p> <p>2) kwalifikowanej usługi zaufania - następuje na wniosek dostawcy usług zaufania.</p> | |
| | T | Art. 10. | 2. W przypadku wykreślenia dostawcy usług zaufania z rejestru, w rejestrze pozostawia się informacje o dostawcy i świadczonych przez niego usługach. | |
| | T | Art. 130. | 1. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne, o którym mowa w art. 23 ust. 1 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, staje się rejestrem dostawców usług zaufania w rozumieniu niniejszej ustawy. | |
| 2. Państwa członkowskie notyfikują Komisji nazwy i adresy wyznaczonych przez siebie organów nadzoru. | N | | | |

| | | | | |
|---|---|----------|---|--|
| <p>3. Organ nadzoru odgrywa następującą rolę: a) sprawuje nadzór nad kwalifikowanymi dostawcami usług zaufania mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego w celu zapewnienia – za pomocą działań nadzorczych ex ante i ex post – aby kwalifikowani dostawcy usług zaufania i świadczone przez nich kwalifikowane usługi zaufania spełniały wymogi określone w niniejszym rozporządzeniu;</p> | T | Art. 28. | <p>1. Nadzór nad dostawcami usług zaufania sprawuje minister właściwy do spraw informatyzacji. 2. W zakresie nadzoru, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji: 1) wykonuje zadania określone w przepisach rozporządzenia 910/2014; 2) wydaje certyfikaty dostawców usług zaufania; 3) tworzy certyfikaty narodowego centrum certyfikacji; 4) może unieważniać certyfikaty, o których mowa w pkt 2 i 3; 5) może żądać niezwłocznego unieważnienia kwalifikowanego certyfikatu przez kwalifikowanego dostawcę usług zaufania; 6) bada zgodność polityki świadczenia usługi z przepisami o usługach zaufania; 7) prowadzi rejestr dostawców usług zaufania; 8) nakłada kary pieniężne; 9) wykonuje inne zadania określone w przepisach prawa.</p> | |
| | T | Art. 5. | <p>1. Wpis do rejestru: 1) dostawcy usług zaufania, który zamierza świadczyć kwalifikowane usługi zaufania, lub 2) kwalifikowanej usługi zaufania - następuje na wniosek dostawcy usług zaufania. 2. Wniosek o wpis, o którym mowa w ust. 1, zawiera dane i informacje, o których mowa w art. 4 ust. 4 pkt 1-7. 3. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej formularz elektroniczny wniosku o wpis, o którym mowa w ust. 1. 4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej, dokumenty lub ich kopie: 1) raport z oceny zgodności, o którym mowa w art. 21 rozporządzenia 910/2014, wydany przez jednostkę oceniającą zgodność; 2) politykę świadczenia usług objętych wnioskiem, zgodnie z którą mają być świadczone usługi zaufania; 3) plan zakończenia działalności, o którym mowa w art. 24 ust. 2 lit. i rozporządzenia 910/2014; 4) dane niezbędne do wystawienia certyfikatu, o którym mowa w art. 11 pkt 1. 5. Minister właściwy do spraw informatyzacji, po rozpatrzeniu wniosku, o którym mowa w ust. 1, wydaje decyzję o wpisie: 1) dostawcy usług zaufania i świadczonych przez niego usług zaufania do rejestru, jeżeli spełniają wymagania określone w przepisach o usługach zaufania; 2) kwalifikowanej usługi zaufania do rejestru, w przypadku gdy usługa spełnia wymagania określone w przepisach o usługach zaufania. 6. Decyzja o wpisie, o którym mowa w ust. 5, zawiera informacje podlegające wpisowi do rejestru.</p> | |

| | | | | | |
|--|--|---|----------|--|--|
| | | T | Art. 9. | <p>4. Minister właściwy do spraw informatyzacji wydaje decyzję o wykreśleniu z rejestru kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego kwalifikowanej usługi zaufania w przypadku:</p> <ol style="list-style-type: none"> 1) złożenia przez tego dostawcę wniosku o wykreślenie z rejestru; 2) wykorzystywania certyfikatów, o których mowa w art. 11 pkt 1, w sposób wykraczający poza zakres ich stosowania; 3) w przypadku, o którym mowa w art. 20 ust. 3 rozporządzenia 910/2014; 4) zaprzestania działalności przez dostawcę kwalifikowanych usług zaufania. | |
| | | T | Art. 10. | <ol style="list-style-type: none"> 1. Decyzja o wykreśleniu kwalifikowanego dostawcy usług zaufania z rejestru oraz decyzja o wykreśleniu wpisu kwalifikowanej usługi zaufania z rejestru podlega natychmiastowemu wykonaniu. Przepisu art. 61 § 2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2016 r. poz. 718 i 846) nie stosuje się. 2. W przypadku wykreślenia dostawcy usług zaufania z rejestru, w rejestrze pozostawia się informacje o dostawcy i świadczonych przez niego usługach. | |
| | | T | Art. 14. | 4. Kwalifikowany dostawca usług zaufania jest obowiązany, w terminie 7 dni od dnia upływu okresu ubezpieczenia, przekazać ministrowi do spraw informatyzacji, drogą elektroniczną, kopię kolejnej umowy ubezpieczenia. | |
| | | T | Art. 41. | Karze pieniężnej podlega kwalifikowany dostawca usług zaufania, który: <ol style="list-style-type: none"> 10) nie posiada planu zakończenia działalności lub nie stosuje go do zakończenia działalności organ nadzoru; | |
| | | T | Art. 21. | <ol style="list-style-type: none"> 1. W przypadku, gdy kwalifikowany dostawca usług zaufania utracił status kwalifikowany i żaden inny podmiot kwalifikowany nie przejął jego działalności w zakresie świadczenia usług zaufania, przekazuje on dokumenty i dane, o których mowa w art. 18 ust. 1, ministrowi właściwemu do spraw informatyzacji w terminie 30 dni od dnia utraty statusu kwalifikowanego. 2. Minister właściwy do spraw informatyzacji przechowuje dokumenty i dane, o których mowa w art. 18 ust. 1, do końca okresu, o którym mowa w art. 18 ust. 2. 3. Kwalifikowany dostawca usług zaufania niszczy niezwłocznie dane do składania przez niego zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej weryfikowanych za pomocą certyfikatu dostawcy usług zaufania, w przypadku gdy polityka świadczenia usługi nie przewiduje dalszego wykorzystania tych danych lub w przypadku unieważnienia certyfikatu dostawcy usług zaufania powiązanego z tymi danymi. 4. Kwalifikowany dostawca usług zaufania, z czynności, o których mowa w ust. 3, sporządza protokół zniszczenia danych i przekazuje go ministrowi | |

| | | | | | |
|----|---|----------|----------|--|--|
| | | | | właściwemu do spraw informatyzacji w terminie 7 dni od wykonania tych czynności. | |
| b) | podejmuje, w razie konieczności, działania w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego – za pomocą działań nadzorczych ex post – gdy dowiaduje się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania rzekomo nie spełniają wymogów określonych w niniejszym rozporządzeniu. | N | | | |
| 4. | Do celów ust. 3 i z zastrzeżeniem ograniczeń w nim określonych, zadania organu nadzoru obejmują w szczególności: a) współpracę z innymi organami nadzoru i udzielanie im pomocy zgodnie z art. 18; b) analizowanie raportów z oceny zgodności, o których mowa w art. 20 ust. 1 i art. 21 ust. 1; | T | Art. 39. | Minister właściwy do spraw informatyzacji może zawierać porozumienia z organami nadzoru innych państw członkowskich Unii Europejskiej, w celu prowadzenia wspólnych postępowań, o których mowa w art. 18 ust. 3 rozporządzenia 910/2014. | |
| c) | informowanie innych organów nadzoru i społeczeństwa o naruszeniach bezpieczeństwa lub utracie integralności zgodnie z art. 19 ust. 2; | T | Art. 40. | Minister właściwy do spraw informatyzacji, w porozumieniu z innymi organami określonymi w art. 19 ust. 2 rozporządzenia 910/2014, ustala sposób zgłaszania drogą elektroniczną przypadków naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe. | |
| d) | składanie sprawozdań Komisji na temat jego głównych działań zgodnie z ust. 6 niniejszego artykułu; | N | | | |
| e) | przeprowadzanie audytów lub zwracanie się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania zgodnie z art. 20 ust. 2; | T | Art. 32. | 1. Audyt, o którym mowa w art. 20: 1) ust. 2 rozporządzenia 910/2014 - jest przeprowadzany przez osoby upoważnione przez organu nadzoru, zwane dalej „audytorami organu nadzoru”; 2) ust. 1 lub 2 rozporządzenia 910/2014 - może być przeprowadzany przy udziale osób upoważnionych przez organu nadzoru, zwanych dalej „obserwatorami organu nadzoru”, w przypadku gdy jest przeprowadzany przez jednostkę przeprowadzającą zgodność. | |
| f) | współpracę z organami ochrony danych, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy, jak się wydaje, doszło do naruszenia przepisów dotyczących ochrony danych osobowych; | T | Art. 39 | Minister właściwy do spraw informatyzacji może zawierać porozumienia z organami nadzoru innych państw członkowskich Unii Europejskiej, w celu prowadzenia wspólnych postępowań, o których mowa w art. 18 ust. 3 rozporządzenia 910/2014. | |

| | | | | |
|--|---|----------|--|--|
| g) przyznawanie dostawcom usług zaufania i świadczonym przez nich usługom statusu kwalifikowanego dostawcy usług zaufania i kwalifikowanych usług, a także odebranie tego statusu zgodnie z art. 20 i 21; | T | Art. 6. | 1. Decyzja, o której mowa w art. 5 ust. 5, jest podstawą do wydania certyfikatu dostawcy usług zaufania oraz dokonania wpisu na zaufaną listę i oznacza nadanie statusu kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego usłudze. | |
| h) informowanie organu odpowiedzialnego za krajową zaufaną listę, o której mowa w art. 22 ust. 3, o swoich decyzjach o przyznaniu lub odebraniu statusu kwalifikowanego, chyba że ten organ jest również organem nadzoru; | N | | | |
| i) weryfikacja istnienia i prawidłowego stosowania przepisów dotyczących planów zakończenia działalności, w przypadkach gdy kwalifikowany dostawca usług zaufania zaprzestaje swojej działalności, w tym tego, w jaki sposób zapewnia się dalszą dostępność informacji zgodnie z art. 24 ust. 2 lit. h); | T | Art. 5. | 4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej, dokumenty lub ich kopie: 3) plan zakończenia działalności, o którym mowa w art. 24 ust. 2 lit. i rozporządzenia 910/2014; | |
| j) wymaganie, aby dostawcy usług zaufania eliminowali wszelkie przypadki niespełnienia wymogów określonych w niniejszym rozporządzeniu. | T | Art. 35. | W przypadku, gdy wyniki audytu przeprowadzanego na podstawie art. 20 ust. 2 rozporządzenia 910/2014 wykażą niezgodność z przepisami o usługach zaufania, minister właściwy do spraw informatyzacji, po zapoznaniu się z zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez dostawcę usług zaufania, może wydać decyzję nakładającą na tego dostawcę obowiązek usunięcia stwierdzonych niezgodności w terminie nie krótszym niż 14 dni. | |
| 5. Państwa członkowskie mogą wymagać, by organ nadzoru utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z warunkami określonymi w prawie krajowym. | T | Art. 3. | Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje: 1) rejestr dostawców usług zaufania, zwany dalej „rejestrem”; 2) zaufaną listę; 3) narodowe centrum certyfikacji. | |
| | T | Art. 11. | Narodowe centrum certyfikacji : 1) tworzy i wydaje kwalifikowanym dostawcom usług zaufania certyfikaty służące do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa w Załączniku I lit. g, Załączniku III lit. g i Załączniku IV lit. h rozporządzenia 910/2014, oraz certyfikatów służących do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców, zwanych dalej „certyfikatami dostawcy usługi zaufania”; 2) publikuje certyfikaty, o których mowa w pkt 1; 3) publikuje listy unieważnionych certyfikatów, o których mowa w pkt 1; 4) tworzy dane do opatrywania pieczęcią elektroniczną | |

| | | | | |
|--|---|----------|---|--|
| | | | <p>certyfikatów, o których mowa w pkt 1, oraz certyfikatów do weryfikacji tych pieczęci, zwanych dalej „certyfikatami narodowego centrum certyfikacji”.</p> <p>2. Narodowe centrum certyfikacji realizuje zadania, o których mowa w ust. 1, zgodnie z polityką certyfikacji.</p> | |
| | T | Art. 4. | <p>1. Rejestr jest prowadzony w postaci elektronicznej.</p> <p>2. Rejestr jest jawny. Każdy ma prawo dostępu do danych zawartych w rejestrze.</p> <p>3. Do rejestru wpisuje się dostawców usług zaufania, którzy mają siedzibę lub oddział na terytorium Rzeczypospolitej Polskiej, oraz usługi zaufania świadczone przez tych dostawców.</p> | |
| | T | Art. 13. | <p>Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia:</p> <ol style="list-style-type: none"> 1) wymagania organizacyjno-techniczne krajowej infrastruktury zaufania; 2) szczegółową treść wpisów w rejestrze oraz sposób ich dokonywania, 3) tryb wydawania i unieważniania certyfikatów dostawcy usługi zaufania oraz certyfikatów narodowego centrum certyfikacji, 4) wymagania dla polityki certyfikacji narodowego centrum certyfikacji, 5) wymagania bezpieczeństwa krajowej infrastruktury zaufania <p>- uwzględniając konieczność zapewnienia ochrony tajemnicy przedsiębiorstwa i interesów odbiorców usług zaufania oraz interoperacyjność systemów stosowanych przez dostawców usług zaufania oraz krajową infrastrukturę zaufania.</p> | |
| | T | Art. 12. | <p>1. Na wniosek Prezesa Narodowego Banku Polskiego, minister właściwy do spraw informatyzacji może upoważnić Narodowy Bank Polski do realizacji zadań, o których mowa w art. 11, jak również do prowadzenia rejestru i zaufanej listy.</p> | |
| | T | Art. 17. | <p>Zaawansowany podpis elektroniczny lub zaawansowana pieczęć elektroniczna weryfikowane przy pomocy certyfikatu dostawcy usług zaufania, służą do opatrywania podpisem elektronicznym lub pieczęcią elektroniczną:</p> <ol style="list-style-type: none"> 1) certyfikatów kwalifikowanych, o których mowa w załączniku I lit. g, załączniku III lit. g oraz załączniku IV lit. h do rozporządzenia 910/2014; 2) informacji o statusie certyfikatów kwalifikowanych, w tym listy zawieszonych lub unieważnionych certyfikatów; 3) innych certyfikatów związanych ze świadczeniem kwalifikowanych usług zaufania. | |

| | | | | | |
|----------------|---|---|-----------|---|--|
| | | T | Art. 131. | Upoważnienie udzielone Narodowemu Bankowi Polskiemu przez ministra właściwego do spraw gospodarki na podstawie art. 23 ust. 5 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, zachowuje moc do chwili odwołania przez ministra właściwego do spraw informatyzacji. | |
| | 6. Do dnia 31 marca każdego roku każdy organ nadzoru przekazuje Komisji sprawozdanie z jego głównych działań w poprzednim roku kalendarzowym wraz z zestawieniem notyfikacji dotyczących naruszeń otrzymanych od dostawców usług zaufania zgodnie z art. 19 ust. 2. 7. Komisja udostępnia państwu członkowskiemu roczne sprawozdanie, o którym mowa w ust. 6. 8. Komisja może w drodze aktów wykonawczych określić formaty i procedury dotyczące sprawozdania, o którym mowa w ust. 6. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| Art. 18 | Wzajemna pomoc 1. Organy nadzoru prowadzą współpracę, w ramach której wymieniają się dobrymi praktykami. Organ nadzoru, na uzasadniony wniosek innego organu nadzoru, udziela temu organowi pomocy, tak aby działania organów nadzoru były prowadzone w spójny sposób. Wzajemna pomoc może obejmować w szczególności wnioski o informacje i środki nadzorcze, takie jak wnioski o przeprowadzenie inspekcji związanych z raportami z oceny zgodności, o których mowa w art. 20 i 21. | T | Art. 39. | Minister właściwy do spraw informatyzacji może zawierać porozumienia z organami nadzoru innych państw członkowskich Unii Europejskiej, w celu prowadzenia wspólnych postępowań, o których mowa w art. 18 ust. 3 rozporządzenia 910/2014. | |
| | 2. Organ nadzoru, do którego kierowany jest wniosek o pomoc, może odrzucić ten wniosek z któregokolwiek z poniższych względów: a) organ nadzoru nie jest właściwy do udzielenia pomocy, której dotyczy wniosek; b) pomoc, której dotyczy wniosek, nie jest proporcjonalna do działań nadzorczych organu nadzoru prowadzonych zgodnie z art. 17; c) udzielenie pomocy, której dotyczy wniosek, byłoby niezgodne z niniejszym rozporządzeniem. | N | | | |
| | 3. W stosownych przypadkach państwa członkowskie mogą upoważnić swoje odpowiednie organy nadzoru do prowadzenia wspólnych dochodzeń, w których biorą udział pracownicy z organów nadzoru innych państw członkowskich. Ustalenia i procedury dotyczące takich wspólnych działań są uzgadniane i określane przez zainteresowane państwa członkowskie zgodnie z ich prawem krajowym. | T | Art. 39. | Minister właściwy do spraw informatyzacji może zawierać porozumienia z organami nadzoru innych państw członkowskich Unii Europejskiej, w celu prowadzenia wspólnych postępowań, o których mowa w art. 18 ust. 3 rozporządzenia 910/2014. | |

| Art. | Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania | | | |
|------|---|---|----------|---|
| 19 | <p>1. Kwalifikowani i niekwalifikowani dostawcy usług zaufania przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania. Przy uwzględnieniu najnowszych osiągnięć w dziedzinie technologii środki te zapewniają poziom bezpieczeństwa współmierny ze stopniem ryzyka. W szczególności należy podjąć środki zapobiegające incyidentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach wszelkich takich incyidentów.</p> | N | | |
| | <p>2. Kwalifikowani i niekwalifikowani dostawcy usług zaufania, bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, zawiadamiają organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji lub organ ochrony danych, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe..</p> | T | Art. 39. | Minister właściwy do spraw informatyzacji może zawierać porozumienia z organami nadzoru innych państw członkowskich Unii Europejskiej, w celu prowadzenia wspólnych postępowań, o których mowa w art. 18 ust. 3 rozporządzenia 910/2014. |
| | <p>W przypadku gdy prawdopodobne jest, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną, na rzecz której świadczona była usługa zaufania, dostawca usług zaufania bez zbędnej zwłoki zawiadamia także tę osobę fizyczną lub prawną o tym naruszeniu bezpieczeństwa lub utracie integralności.</p> <p>W stosownych przypadkach, w szczególności jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA.</p> <p>Zawiadomiony organ nadzoru podaje zaistniałe fakty do wiadomości publicznej lub nakłada taki obowiązek na dostawcę usług zaufania, w przypadku gdy uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym.</p> | T | Art. 40. | Minister właściwy do spraw informatyzacji, w porozumieniu z innymi organami określonymi w art. 19 ust. 2 rozporządzenia 910/2014, ustala sposób zgłaszania drogą elektroniczną przypadków naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe. |

| | | | | | |
|-------------------------------|---|---|---------|--|--|
| | <p>3. Raz do roku organ nadzoru przekazuje ENISA zestawienie zawiadomień o naruszeniach bezpieczeństwa lub utraty integralności otrzymanych od dostawców usług zaufania.</p> <p>4. Komisja może w drodze aktów wykonawczych:</p> <p>a) określić bardziej szczegółowo środki, o których mowa w ust. 1; oraz</p> <p>b) określić formaty i procedury, w tym również terminy, mające zastosowanie na użytek ust. 2.</p> <p>Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | N | | | |
| SEKCJA 3 | | | | | |
| Kwalifikowane usługi zaufania | | | | | |
| Art. 20 | Nadzór nad kwalifikowanymi dostawcami usług zaufania | | | | |
| | <p>1. Kwalifikowani dostawcy usług zaufania podlegają audytowi, na ich własny koszt co najmniej raz na 24 miesiące, przeprowadzanemu przez jednostkę oceniającą zgodność. Celem audytu jest potwierdzenie, że kwalifikowani dostawcy usług zaufania oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu. Kwalifikowani dostawcy usług zaufania przedkładają powstały w ten sposób raport z oceny zgodności organowi nadzoru w terminie trzech dni roboczych od jego otrzymania.</p> | N | | | |
| | <p>2. Bez uszczerbku dla ust. 1, organ nadzoru może w dowolnym momencie przeprowadzić audyt – lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności – kwalifikowanych dostawców usług zaufania, na koszt tych dostawców usług zaufania, aby potwierdzić, że dostawcy ci oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu. W przypadku gdy wydaje się, że zostały naruszone przepisy dotyczące ochrony danych, organ nadzoru informuje o wynikach swoich audytów organy ochrony danych.</p> | T | Art. 9. | <p>4. Minister właściwy do spraw informatyzacji wydaje decyzję o wykreśleniu z rejestru kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego kwalifikowanej usługi zaufania w przypadku:</p> <p>1) złożenia przez tego dostawcę wniosku o wykreślenie z rejestru;</p> <p>2) wykorzystywania certyfikatów, o których mowa w art. 11 pkt 1, w sposób wykraczający poza zakres ich stosowania;</p> <p>3) w przypadku, o którym mowa w art. 20 ust. 3 rozporządzenia 910/2014;</p> <p>4) zaprzestania działalności przez dostawcę kwalifikowanych usług zaufania.</p> <p>5. Decyzja o wykreśleniu, o której mowa w ust. 1, jest podstawą wykreślenia dostawcy usług zaufania z listy zaufania oraz może być podstawą do unieważnienia certyfikatów, o których mowa w art. 11 pkt 1.</p> | |

| | | | | | |
|----------------|--|---|----------|---|--|
| | 3. W przypadku gdy organ nadzoru nakłada na kwalifikowanego dostawcę usług zaufania wymóg wyeliminowania przypadków niespełnienia wymogów określonych w niniejszym rozporządzeniu i ten dostawca nie podejmie odpowiednich działań, w stosownych przypadkach w terminie ustalonym przez organ nadzoru, organ nadzoru, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, może odebrać status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy, i informuje organ, o którym mowa w art. 22 ust. 3, do celów zaktualizowania zaufanych list, o których mowa w art. 22 ust. 1. Organ nadzoru informuje kwalifikowanego dostawcę usług zaufania o odebraniu jego statusu kwalifikowanego lub statusu kwalifikowanego danej usługi. | T | Art. 9. | 4. Minister właściwy do spraw informatyzacji wydaje decyzję o wykreśleniu z rejestru kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego kwalifikowanej usługi zaufania w przypadku: 3) w przypadku, o którym mowa w art. 20 ust. 3 rozporządzenia 910/2014; | |
| | | T | Art. 35. | W przypadku, gdy wyniki audytu przeprowadzanego na podstawie art. 20 ust. 2 rozporządzenia 910/2014 wykażą niezgodność z przepisami o usługach zaufania, minister właściwy do spraw informatyzacji, po zapoznaniu się z zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez dostawcę usług zaufania, może wydać decyzję nakładającą na tego dostawcę obowiązek usunięcia stwierdzonych niezgodności w terminie nie krótszym niż 14 dni. | |
| | | | | | |
| | 4. Komisja może w drodze aktów wykonawczych podać numery referencyjne następujących norm: a) norm dotyczących akredytacji jednostek oceniających zgodność i dotyczących raportu z oceny zgodności, o którym mowa w ust. 1; b) norm dotyczących zasad audytów, zgodnie z którymi jednostki oceniające zgodność będą przeprowadzać oceny zgodności kwalifikowanych dostawców usług zaufania, o których mowa w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| Art. 21 | Inicjowanie kwalifikowanej usługi zaufania 1. W przypadku gdy dostawcy usług zaufania nieposiadający statusu kwalifikowanych dostawców usług zaufania zamierzają rozpocząć świadczenie kwalifikowanych usług zaufania, zgłaszają organowi nadzoru swój zamiar wraz z raportem z oceny zgodności wydanym przez jednostkę oceniającą zgodność. | T | Art. 5. | 4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej, dokumenty lub ich kopie: 1) raportu z oceny zgodności, o którym mowa w art. 21 rozporządzenia 910/2014, wydany przez jednostkę oceniającą zgodność; | |

| | | | | | |
|---------|--|---|---------|---|--|
| | <p>2. Organ nadzoru weryfikuje, czy dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu, w szczególności wymogi dotyczące kwalifikowanych dostawców usług zaufania i świadczonych przez nich kwalifikowanych usług zaufania.</p> <p>Jeżeli organ nadzoru stwierdzi, że dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi, o których mowa w akapicie pierwszym, organ nadzoru przyznaje dostawcy status kwalifikowanego dostawcy usług zaufania i status kwalifikowanych usług zaufania świadczonym przez niego usługom oraz informuje organ, o którym mowa w art. 22 ust. 3, w celu zaktualizowania przez niego zaufanych list, o których mowa w art. 22 ust. 1, nie później niż trzy miesiące po zgłoszeniu zgodnie z ust. 1 niniejszego artykułu. Jeżeli weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje dostawcę usług zaufania o przyczynach opóźnienia oraz podaje termin, w którym weryfikacja zostanie zakończona.</p> <p>3. Kwalifikowani dostawcy usług zaufania mogą rozpocząć świadczenie kwalifikowanej usługi zaufania, po tym jak ich kwalifikowany status zostanie wskazany w zaufanych listach, o których mowa w art. 22 ust. 1.</p> <p>4. Komisja może w drodze aktów wykonawczych określić formaty i procedury na użytek ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | T | Art. 5. | <p>1. Wpis do rejestru:</p> <p>1) dostawcy usług zaufania, który zamierza świadczyć kwalifikowane usługi zaufania, lub</p> <p>2) kwalifikowanej usługi zaufania</p> <p>- następuje na wniosek dostawcy usług zaufania.</p> <p>4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej, dokumenty lub ich kopie:</p> <p>1) raportu z oceny zgodności, o którym mowa w art. 21 rozporządzenia 910/2014, wydany przez jednostkę oceniającą zgodność;</p> | |
| Art. 22 | <p>Zaufane listy</p> <p>1. Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.</p> | T | Art. 2. | 19) zaufanej liście – należy przez to rozmieść listę kwalifikowanych dostawców usług zaufania, o której mowa w art. 22 ust. 1 rozporządzenia 910/2014. | |
| | | T | Art. 6. | 2. Minister właściwy do spraw informatyzacji prowadzi zaufaną listę. | |
| | | T | Art. 9. | 5. Decyzja o wykreśleniu, o której mowa w ust. 1, jest podstawą wykreślenia dostawcy usług zaufania z listy zaufania oraz może być podstawą do unieważnienia certyfikatów, o których mowa w art. 11 pkt 1. | |

| | | | | | |
|----------------|--|---|----------|--|--|
| | | T | Art. 12. | 1. Na wniosek Prezesa Narodowego Banku Polskiego, minister właściwy do spraw informatyzacji może upoważnić Narodowy Bank Polski do realizacji zadań, o których mowa w art. 11, jak również do prowadzenia rejestru i zaufanej listy. | |
| | 2. Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią elektroniczną zaufane listy, o których mowa w ust. 1, w postaci dostosowanej do automatycznego przetwarzania. | N | | | |
| | 3. Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o podmiocie odpowiedzialnym za sporządzenie, prowadzenie i publikowanie krajowych zaufanych list wraz ze szczegółowymi informacjami dotyczącymi miejsca publikacji tych list, certyfikatów użytych do podpisania lub opatrzenia pieczęcią zaufanych list i wszelkich zmian, jakie są do nich wprowadzane. | N | | | |
| | 4. Komisja udostępnia publicznie informacje, o których mowa w ust. 3, w elektronicznie podpisanej lub opatrzonej pieczęcią elektroniczną postaci dostosowanej do automatycznego przetwarzania, używając w tym celu zabezpieczonego kanału komunikacji. | N | | | |
| | 5. Do dnia 18 września 2015 r. Komisja w drodze aktów wykonawczych określi informacje, o których mowa w ust. 1, oraz techniczne specyfikacje i formaty dotyczące zaufanych list mające zastosowanie na użytek ust. 1–4. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| Art. 23 | Znak zaufania UE dla kwalifikowanych usług zaufania 1. Po tym jak w zaufanej liście, o której mowa w art. 22 ust. 1, wskazany zostanie status kwalifikowany, o którym mowa w art. 21 ust. 2 akapit drugi, kwalifikowani dostawcy usług zaufania mogą używać znaku zaufania UE, aby w prosty, rozpoznawalny i jasny sposób wskazać świadczone przez siebie kwalifikowane usługi zaufania. 2. Gdy kwalifikowani dostawcy usług zaufania używają znaku zaufania UE w odniesieniu do kwalifikowanych usług zaufania, o których mowa w ust. 1, zapewniają, aby na ich witrynie internetowej dostępny był link do odpowiedniej zaufanej listy. 3. Do dnia 1 lipca 2015 r. Komisja w drodze aktów wykonawczych wprowadza specyfikacje dotyczące formy, a w szczególności prezentacji, kompozycji, rozmiaru i wzoru znaku zaufania UE dla kwalifikowanych usług zaufania. Te akty wykonawcze przyjmuje się | N | | | |

| | | | | | |
|----------------|---|----------|----------|--|--|
| | zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | | | | |
| Art. 24 | Wymogi dla kwalifikowanych dostawców usług zaufania | | | | |
| | 1. Wydając kwalifikowany certyfikat dla usługi zaufania, kwalifikowany dostawca usług zaufania weryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat. Informacje, o których mowa w akapicie pierwszym, są weryfikowane przez kwalifikowanego dostawcę usług zaufania albo bezpośrednio, albo polegając na stronie trzeciej zgodnie z prawem krajowym: a) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej; lub b) zdalnie, przy użyciu środka identyfikacji elektronicznej, w przypadku którego przed wydaniem kwalifikowanego certyfikatu zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej i który spełnia wymogi określone w art. 8 w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa; lub c) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a) lub b); lub d) przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność. | T | Art. 15. | Kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie. | |
| | 2. Dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania: a) informuje organ nadzoru o wszelkich zmianach w świadczeniu kwalifikowanych usług zaufania oraz o zamiarze zaprzestania swej działalności; b) zatrudnia pracowników i, w stosownym przypadku, podwykonawców, którzy posiadają niezbędną wiedzę fachową, wiarygodność, doświadczenie i kwalifikacje i którzy przeszli | N | | | |

| | | | | |
|---|----------|----------|--|--|
| odpowiednie szkolenia na temat przepisów dotyczących bezpieczeństwa i ochrony danych osobowych oraz którzy stosują procedury administracyjne i zarządcze odpowiadające europejskim lub międzynarodowym standardom; | | | | |
| c) w odniesieniu do ryzyka związanego z odpowiedzialnością za szkody zgodnie z art. 13 utrzymuje dostateczne zasoby finansowe lub dysponuje stosownym ubezpieczeniem od odpowiedzialności zgodnie z prawem krajowym; | T | Art. 14. | <p>1. Kwalifikowany dostawca usług zaufania jest obowiązany posiadać zawartą umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania.</p> <p>2. Kwalifikowany dostawca usług zaufania jest obowiązany zawrzeć umowę, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania wpisu kwalifikowanej usługi zaufania do rejestru, nie później niż jeden dzień przed dniem rozpoczęcia świadczenia tej usługi.</p> <p>3. Kwalifikowany dostawca usług zaufania, jest obowiązany, w terminie 30 dni od dnia doręczenia decyzji o wpisie do rejestru przekazać ministrowi właściwemu do spraw informatyzacji, drogą elektroniczną, kopię umowy, o której mowa w ust. 1.</p> <p>4. Kwalifikowany dostawca usług zaufania jest obowiązany, w terminie 7 dni od dnia upływu okresu ubezpieczenia, przekazać ministrowi do spraw informatyzacji, drogą elektroniczną, kopię kolejnej umowy ubezpieczenia.</p> <p>5. Minister właściwy do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw informatyzacji, po zasięgnięciu opinii Polskiej Izby Ubezpieczeń, określi, w drodze rozporządzenia, szczegółowy zakres ubezpieczenia, o którym mowa w ust. 1, oraz minimalną sumę gwarancyjną, uwzględniając specyfikę działalności prowadzonej przez kwalifikowanych dostawców usług zaufania.</p> | |
| d) przed wejściem w stosunek umowy informuje, w jasny i szczegółowy sposób, wszystkie osoby pragnące skorzystać z kwalifikowanej usługi zaufania o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej; | N | | | |
| e) używa wiarygodnych systemów i produktów, które są chronione przed modyfikacją i zapewniają techniczne bezpieczeństwo i wiarygodność procesów przez niego obsługiwanych; f) używa wiarygodnych systemów do przechowywania przekazanych mu danych w sprawdzalnej postaci, tak aby: (i) dane były publicznie dostępne do wyszukiwania dopiero po uzyskaniu zgody osoby, do której dane się odnoszą; (ii) tylko upoważnione osoby mogły wprowadzać dane i zmiany w przechowywanych danych; (iii) można było sprawdzać autentyczność danych; g) podejmuje odpowiednie środki zapobiegające fałszowaniu i kradzieży danych; | N | | | |

| | | | | |
|---|----------|----------|---|--|
| h) rejestruje i udostępnia przez odpowiedni okres, w tym po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Rejestracja może odbywać się drogą elektroniczną; | T | Art. 18. | <p>1. Kwalifikowany dostawca usług zaufania przechowuje następujące dokumenty i dane związane ze świadczeniem usług zaufania:</p> <ol style="list-style-type: none"> 1) potwierdzenie, o którym mowa w art. 15, 2) listy zawieszonych i unieważnionych kwalifikowanych certyfikatów, 3) politykę świadczenia usługi, 4) żądania unieważnienia kwalifikowanego certyfikatu, 5) inne dokumenty, o ile polityka świadczenia usługi wymagała ich utworzenia i przechowywania <ul style="list-style-type: none"> – w sposób umożliwiający odczytanie oraz zapewniający bezpieczeństwo przechowywanych dokumentów i danych. <p>2. Kwalifikowany dostawca usług zaufania jest obowiązany przechowywać dokumenty i dane, o których mowa w ust. 1, z wyłączeniem danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej, przez 20 lat od dnia ich wytworzenia.</p> | |
| i) ma aktualny plan zakończenia działalności, aby zapewnić ciągłość usług zgodnie z przepisami zweryfikowanymi przez organ nadzoru na mocy art. 17 ust. 4 lit. i); | T | Art. 20. | 3. Kwalifikowany dostawca usług zaufania jest obowiązany posiadać plan zakończenia działalności oraz zastosować ten plan do zakończenia działalności. | |
| j) zapewnia zgodne z prawem przetwarzanie danych osobowych zgodnie z dyrektywą 95/46/WE; k) w przypadku kwalifikowanych dostawców usług zaufania wydających kwalifikowane certyfikaty – tworzy i aktualizuje bazę danych dotyczącą certyfikatów. 3. Jeżeli kwalifikowany dostawca usług zaufania wydający kwalifikowane certyfikaty postanowi unieważnić certyfikat, rejestruje on takie unieważnienie w swojej bazie danych dotyczącej certyfikatów i publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin po otrzymaniu wniosku. Unieważnienie staje się skuteczne natychmiast po jego opublikowaniu. | N | | | |
| 4. W odniesieniu do ust. 3 kwalifikowani dostawcy usług zaufania wydający kwalifikowane certyfikaty dostarczają każdej stronie ufającej informacje o statusie ważności lub unieważnienia wydanych przez siebie kwalifikowanych certyfikatów. Informacje te są dostępne co najmniej na poziomie certyfikatu w automatyczny sposób, który jest wiarygodny, nieodpłatny i wydajny, w każdym momencie, także po upływie okresu ważności certyfikatu. | N | | | |

| | | | | | |
|------------------------------|--|---|--|--|--|
| | 5. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących wiarygodnych systemów i produktów, które spełniają wymogi określone w ust. 2 lit. e) i f) niniejszego artykułu. W przypadku gdy wiarygodne systemy i produkty spełniają te standardy, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| SEKCJA 4 | | | | | |
| Podpisy elektroniczne | | | | | |
| Art. 25 | Skutki prawne podpisów elektronicznych 1. Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych. 2. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu. 3. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich. | N | | | |
| Art. 26 | Wymogi dla zaawansowanych podpisów elektronicznych Zaawansowany podpis elektroniczny musi spełniać następujące wymogi: a) jest unikalnie przyporządkowany podpisującemu; b) umożliwia ustalenie tożsamości podpisującego; c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna. | N | | | |

| | | | | | |
|----------------|--|----------|--|--|--|
| Art. 27 | Podpisy elektroniczne w usługach publicznych 1. Jeżeli państwo członkowskie wymaga zaawansowanego podpisu elektronicznego do korzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane podpisy elektroniczne, zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie podpisów elektronicznych oraz kwalifikowane podpisy elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5. 2. Jeżeli państwo członkowskie wymaga zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie do skorzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie i kwalifikowane podpisy elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5. 3. W przypadku transgranicznego użycia w usłudze online oferowanej przez podmiot sektora publicznego państwa członkowskie nie wymagają podpisu elektronicznego o wyższym poziomie bezpieczeństwa niż kwalifikowany podpis elektroniczny. 4. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych podpisów elektronicznych. W przypadku gdy zaawansowany podpis elektroniczny spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych podpisów elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 26. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 5. Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i unijnych aktów prawnych Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych podpisów elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| Art. 28 | Kwalifikowane certyfikaty podpisów elektronicznych | | | | |

| | | | | | |
|----------------|---|---|----------|--|--|
| | <p>1. Kwalifikowane certyfikaty podpisów elektronicznych muszą spełniać wymogi określone w załączniku I.</p> <p>2. Kwalifikowane certyfikaty podpisów elektronicznych nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku I.</p> <p>3. Kwalifikowane certyfikaty podpisów elektronicznych mogą zawierać nieobowiązkowe dodatkowe szczególne atrybuty. Atrybuty te nie mogą wpływać na interoperacyjność i uznawanie kwalifikowanych podpisów elektronicznych.</p> <p>4. Jeżeli kwalifikowany certyfikat podpisów elektronicznych został unieważniony po początkowej aktywacji, traci on ważność od momentu jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.</p> | N | | | |
| | <p>5. Państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanego certyfikatu podpisu elektronicznego z zastrzeżeniem następujących warunków:</p> <p>a) jeżeli kwalifikowany certyfikat podpisu elektronicznego został czasowo zawieszony, certyfikat ten traci ważność na okres zawieszenia;</p> <p>b) okres zawieszenia jest jasno wskazywany w bazie danych dotyczącej certyfikatów i informacja o zawieszeniu jest widoczna, w okresie zawieszenia, na podstawie usługi informowania o statusie certyfikatu.</p> | T | Art. 19. | 2. Podpis elektroniczny lub pieczęć elektroniczna złożone w okresie zawieszenia certyfikatu wykorzystywanego do jego weryfikacji, nie wywołują skutków prawnych. Informacja o zawieszeniu certyfikatu jest udostępniana w ramach usługi informowania o statusie certyfikatu. | |
| | | T | Art. 19. | 3. Po uchyleniu zawieszenia certyfikatu, skutek prawny podpisu elektronicznego lub pieczęci weryfikowanych tym certyfikatem, złożonych w trakcie zawieszenia, następuje z chwilą uchylenia tego zawieszenia. | |
| | <p>6. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów podpisów elektronicznych. W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | N | | | |
| Art. 29 | <p>Wymogi dla kwalifikowanych urzędzeń do składania podpisu elektronicznego</p> <p>1. Kwalifikowane urzędzenia do składania podpisu elektronicznego muszą spełniać wymogi określone w załączniku II.</p> <p>2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych urzędzeń do składania podpisu elektronicznego. Jeżeli kwalifikowane urządzenie do składania podpisu elektronicznego spełnia te normy,</p> | N | | | |

| | | | | | |
|---------|---|---|---------|--|--|
| | domniemywa się zgodność z wymogami określonymi w załączniku II. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | | | | |
| Art. 30 | Certyfikacja kwalifikowanych urzędzeń do składania podpisu elektronicznego 1. Zgodność kwalifikowanych urzędzeń do składania podpisu elektronicznego z wymogami określonymi w załączniku II jest certyfikowana przez odpowiednie publiczne lub prywatne podmioty wyznaczone przez państwa członkowskie. | T | Art. 38 | 1. Minister właściwy do spraw informatyzacji może wyznaczyć podmiot badający zgodność kwalifikowanych urzędzeń do składania podpisu elektronicznego lub pieczęci elektronicznej z wymogami, o których mowa w załączniku II do rozporządzenia 910/2014. | |
| | 2. Państwa członkowskie zgłaszają Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 1. Komisja udostępnia te informacje państwom członkowskim. | T | Art. 38 | 2. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej nazwę i adres wyznaczonego podmiotu, o którym mowa w ust. 1. | |
| | 3. Certyfikacja, o której mowa w ust. 1, opiera się na następujących elementach: a) procedurze oceny bezpieczeństwa, przeprowadzanej zgodnie z jedną z norm dotyczących oceny bezpieczeństwa produktów informatycznych uwzględnionych na liście sporządzonej zgodnie z akapitem drugim; lub b) procedurze innej niż procedura, o której mowa w lit. a), pod warunkiem że w procedurze tej stosuje się porównywalne poziomy bezpieczeństwa i podmiot publiczny lub prywatny, o którym mowa w ust. 1, zgłosi tę procedurę Komisji. Procedura ta może zostać zastosowana wyłącznie w razie braku norm, o których mowa w lit. a), lub gdy procedura oceny bezpieczeństwa, o której mowa w lit. a), wciąż trwa. Komisja sporządza w drodze aktów wykonawczych listę norm dotyczących oceny bezpieczeństwa produktów informatycznych, o których mowa w lit. a). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2 4. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, dotyczących ustanowienia specjalnych kryteriów, które muszą | N | | | |

| | | | | | |
|----------------|--|---|--|--|--|
| | spełniać wyznaczone podmioty, o których mowa w ust. 1 niniejszego artykułu. | | | | |
| Art. 31 | <p>Publikacja listy certyfikowanych kwalifikowanych urzędzeń do składania podpisu elektronicznego</p> <p>1. Bez zbędnej zwłoki i nie później niż jeden miesiąc po zakończeniu certyfikacji państwa członkowskie przekazują Komisji informacje o kwalifikowanych urządzeniach do składania podpisu elektronicznego, które uzyskały certyfikaty od podmiotów, o których mowa w art. 30 ust. 1. Bez zbędnej zwłoki i nie później niż jeden miesiąc po odwołaniu certyfikacji państwa członkowskie przekazują również Komisji informacje o urządzeniach do składania podpisu elektronicznego, które nie są już certyfikowane.</p> <p>2. Na podstawie otrzymanych informacji Komisja sporządza, publikuje i prowadzi listę certyfikowanych kwalifikowanych urzędzeń do składania podpisu elektronicznego.</p> <p>3. Komisja może w drodze aktów wykonawczych określić formaty i procedury mające zastosowanie na użytek ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | N | | | |
| Art. 32 | <p>Wymogi dla walidacji kwalifikowanych podpisów elektronicznych</p> <p>1. Proces walidacji kwalifikowanego podpisu elektronicznego potwierdza ważność kwalifikowanego podpisu elektronicznego, pod warunkiem że:</p> <p>a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I;</p> <p>b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;</p> <p>c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;</p> <p>d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;</p> <p>e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;</p> <p>f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego;</p> | N | | | |

| | | | | | |
|----------------|--|---|--|--|--|
| | <p>g) integralność podpisanych danych nie została naruszona;</p> <p>h) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu.</p> <p>2. System wykorzystany do walidacji kwalifikowanego podpisu elektronicznego zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem.</p> <p>3. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących walidacji kwalifikowanych podpisów elektronicznych. Jeżeli walidacja kwalifikowanych podpisów elektronicznych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | | | | |
| Art. 33 | <p>Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych</p> <p>1. Kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który:</p> <p>a) zapewnia walidację zgodnie z art. 32 ust. 1; oraz</p> <p>b) umożliwia stronom ufającym otrzymanie wyniku procesu walidacji w automatyczny, wiarygodny i skuteczny sposób oraz przy użyciu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej dostawcy kwalifikowanej usługi walidacji.</p> <p>2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi walidacji, o której mowa w ust. 1. W przypadku gdy usługa walidacji kwalifikowanych podpisów elektronicznych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | N | | | |
| Art. 34 | <p>Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych</p> <p>1. Kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który stosuje procedury i technologie umożliwiające przedłużenie wiarygodności kwalifikowanego podpisu elektronicznego poza techniczny okres ważności.</p> <p>2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej</p> | N | | | |

| | | | | | |
|--------------------------------|--|----------|--|--|--|
| | usługi konserwacji kwalifikowanych podpisów elektronicznych. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych spełniają te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | | | | |
| SEKCJA 5 | | | | | |
| Pieczenie elektroniczne | | | | | |
| Art. 35 | Skutki prawne pieczęci elektronicznych 1. Pieczęć elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że pieczęć ta ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych pieczęci elektronicznych. 2. Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana. 3. Kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich. | N | | | |
| Art. 36 | Wymogi dla zaawansowanych pieczęci elektronicznych Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi: a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć; b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć; c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej; oraz d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna. | N | | | |
| Art. 37 | Pieczenie elektroniczne w usługach publicznych 1. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej do skorzystania z usługi online oferowanej przez podmiot sektora | N | | | |

| | | | | |
|--|--|--|--|--|
| <p>publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne, zaawansowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie pieczęci elektronicznych i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.</p> <p>2. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie do skorzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.</p> <p>3. W przypadku transgranicznego użycia w usłudze online oferowanej przez podmiot sektora publicznego państwa członkowskie nie wymagają pieczęci elektronicznej o wyższym poziomie bezpieczeństwa niż kwalifikowana pieczęć elektroniczna.</p> <p>4. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych pieczęci elektronicznych. W przypadku gdy zaawansowana pieczęć elektroniczna spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 36. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> <p>5. Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i aktów prawnych Unii Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych pieczęci elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | | | | |
|--|--|--|--|--|

| | | | | | |
|-----------------------|--|-----------------|--|--|--|
| <p>Art. 38</p> | <p>Kwalifikowane certyfikaty pieczęci elektronicznej</p> <p>1. Kwalifikowane certyfikaty pieczęci elektronicznych muszą spełniać wymogi określone w załączniku III.</p> <p>2. Kwalifikowane certyfikaty pieczęci elektronicznych nie podlegają żadnym obowiązkowym wymogom wykraczającym poza wymogi określone w załączniku III.</p> <p>3. Kwalifikowane certyfikaty pieczęci elektronicznych mogą zawierać nieobowiązkowe dodatkowe szczególne atrybuty. Atrybuty te nie mogą wpływać na interoperacyjność i uznawanie kwalifikowanych pieczęci elektronicznych.</p> <p>4. Jeżeli kwalifikowany certyfikat pieczęci elektronicznej został unieważniony po początkowej aktywacji, traci on ważność od momentu jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu.</p> <p>5. Państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanych certyfikatów pieczęci elektronicznych z zastrzeżeniem następujących warunków:</p> <p>a) jeżeli kwalifikowany certyfikat pieczęci elektronicznej został czasowo zawieszony, certyfikat ten traci ważność na okres zawieszenia;</p> <p>b) okres zawieszenia jest jasno wskazywany w bazie danych dotyczącej certyfikatów i podmiot udzielający informacji o statusie certyfikatu zapewnia widoczność statusu zawieszenia podczas okresu zawieszenia.</p> <p>6. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów pieczęci elektronicznych. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku III. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.</p> | <p>N</p> | | | |
| <p>Art. 39</p> | <p>Kwalifikowane urzędnicy do składania pieczęci elektronicznej</p> <p>1. Art. 29 stosuje się odpowiednio do wymogów dotyczących kwalifikowanych urzędników do składania pieczęci elektronicznej.</p> <p>2. Art. 30 stosuje się odpowiednio do certyfikacji kwalifikowanych urzędników do składania pieczęci elektronicznej.</p> <p>3. Art. 31 stosuje się odpowiednio do publikacji listy certyfikowanych kwalifikowanych urzędników do składania pieczęci elektronicznej.</p> | <p>N</p> | | | |

| | | | | | |
|---|--|---|--|--|--|
| Art. 40 | Artykuł 40 Walidacja i konserwacja kwalifikowanych pieczęci elektronicznych Art. 32, 33 i 34 stosuje się odpowiednio do walidacji i konserwacji kwalifikowanych pieczęci elektronicznych. | N | | | |
| SEKCJA 6 | | | | | |
| Elektroniczne znaczniki czasu | | | | | |
| Art. 41 | Skutki prawne elektronicznych znaczników czasu 1. Nie jest kwestionowany prawny skutek elektronicznego znacznika czasu ani jego dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że znacznik ten ma postać elektroniczną lub że nie spełnia wymogów kwalifikowanego elektronicznego znacznika czasu. 2. Kwalifikowany elektroniczny znacznik czasu korzysta z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone. 3. Kwalifikowany elektroniczny znacznik wydany w jednym państwie członkowskim jest uznawany za kwalifikowany elektroniczny znacznik czasu we wszystkich państwach członkowskich. | N | | | |
| Art. 42 | Wymogi dla kwalifikowanych elektronicznych znaczników czasu 1. Kwalifikowany elektroniczny znacznik czasu musi spełniać następujące wymogi: a) wiąże on datę i czas z danymi tak, aby w wystarczający sposób wykluczyć możliwość niewykrywalnej zmiany danych; b) oparty jest na precyzyjnym źródle czasu powiązany z uniwersalnym czasem koordynowanym; oraz c) jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania lub w inny równoważny sposób. 2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących powiązania daty i czasu z danymi oraz precyzyjnych źródeł czasu. W przypadku gdy powiązanie daty i czasu z danymi i precyzyjne źródło czasu spełniają te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| SEKCJA 7 | | | | | |
| Usługi rejestrowanego doręczenia elektronicznego | | | | | |
| Art. | Skutek prawny usługi rejestrowanego doręczenia | N | | | |

| | | | | | |
|---------|---|---|--|--|--|
| 43 | <p>elektronicznego</p> <p>1. Nie jest kwestionowany skutek prawny danych wysłanych i otrzymanych przy użyciu usługi rejestrowanego doręczenia elektronicznego ani ich dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dane te mają postać elektroniczną lub że nie spełniają wszystkich wymogów kwalifikowanej usługi rejestrowanego doręczenia elektronicznego.</p> <p>2. Dane wysłane i otrzymane przy użyciu kwalifikowanej usługi rejestrowanego doręczenia elektronicznego korzystają z domniemania integralności danych, wysłania tych danych przez zidentyfikowanego nadawcę i otrzymania ich przez zidentyfikowanego adresata oraz dokładności daty i czasu wysłania i otrzymania wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego.</p> | | | | |
| Art. 44 | <p>Wymogi dla kwalifikowanych usług rejestrowanego doręczenia elektronicznego</p> <p>1. Kwalifikowane usługi rejestrowanego doręczenia elektronicznego muszą spełniać następujące wymogi:</p> <ul style="list-style-type: none"> a) są świadczone przez co najmniej jednego kwalifikowanego dostawcę usług zaufania; b) z dużą dozą pewności zapewniają identyfikację nadawcy; c) zapewniają identyfikację adresata przed dostarczeniem danych; d) wysłanie i otrzymanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania w taki sposób, by wykluczyć możliwość niewykrywalnej zmiany danych; e) każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych; f) data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu. <p>W przypadku przesyłania danych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania wymogi określone w lit. a)–f) mają zastosowanie do wszystkich kwalifikowanych dostawców usług zaufania.</p> <p>2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących procedur wysyłania i otrzymywania danych. W przypadku gdy proces wysyłania i otrzymywania danych spełnia te normy, domniemywa się zgodność z wymogami</p> | N | | | |

| | | | | | |
|--|--|----------|--|--|--|
| | określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | | | | |
| SEKCJA 8 | | | | | |
| Uwierzytelnianie witryn internetowych | | | | | |
| Art. 45 | Wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych 1. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych muszą spełniać wymogi określone w załączniku IV. 2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów uwierzytelniania witryn internetowych. W przypadku gdy kwalifikowany certyfikat uwierzytelniania witryn internetowych spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku IV. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. | N | | | |
| ROZDZIAŁ IV | | | | | |
| DOKUMENTY ELEKTRONICZNE | | | | | |
| Art. 46 | Skutki prawne dokumentów elektronicznych Nie jest kwestionowany skutek prawny dokumentu elektronicznego ani jego dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dokument ten ma postać elektroniczną. | N | | | |
| ROZDZIAŁ V | | | | | |
| PRZEKAZANIE UPRAWNIEŃ I PRZEPISY WYKONAWCZE | | | | | |
| Art. 47 | Wykonywanie przekazanych uprawnień 1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule. 2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 30 ust. 4, powierza się Komisji na czas nieokreślony od dnia 17 września 2014 r. 3. Przekazanie uprawnień, o którym mowa w art. 30 ust. 4, może zostać odwołane w dowolnym momencie przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność żadnych już obowiązujących aktów delegowanych. | N | | | |

| | | | | | |
|-------------------------|---|----------|--|--|--|
| | <p>4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.</p> <p>5. Akt delegowany przyjęty na podstawie art. 30 ust. 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.</p> | | | | |
| Art. 48. | <p>Procedura komitetowa</p> <p>1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.</p> <p>2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.</p> | N | | | |
| ROZDZIAŁ VI | | | | | |
| PRZEPISY KOŃCOWE | | | | | |
| Art. 49. | <p>Przegląd</p> <p>Komisja dokona przeglądu stosowania niniejszego rozporządzenia i przekaże sprawozdanie Parlamentowi Europejskiemu i Radzie nie później niż dnia 1 lipca 2020 r. Komisja oceni w szczególności, czy należy zmienić zakres stosowania niniejszego rozporządzenia lub jego poszczególnych przepisów, w tym art. 6, art. 7 lit. f), art. 34, 43, 44 i 45, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu niniejszego rozporządzenia, a także rozwój technologiczny, sytuację rynkową i prawną.</p> <p>Do sprawozdania, o którym mowa w akapicie pierwszym, załączone zostaną w stosownych przypadkach wnioski ustawodawcze.</p> <p>Ponadto, co cztery lata po sporządzeniu sprawozdania, o którym mowa w akapicie pierwszym, Komisja przekazuje Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące postępów w osiągnięciu celów niniejszego rozporządzenia.</p> | N | | | |
| Art. 50. | <p>Uchylenie</p> <p>1. Dyrektywę 1999/93/WE uchyla się z dniem 1 lipca 2016 r.</p> <p>2. Odesłania do uchylonej dyrektywy odczytuje się jako odesłania do niniejszego rozporządzenia.</p> | N | | | |

| | | | | | |
|------------|---|---|-----------|---|--|
| Art. 51 | Środki przejściowe 1. Bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na mocy niniejszego rozporządzenia. | N | | | |
| | 2. Kwalifikowane certyfikaty wydane osobom fizycznym na mocy dyrektywy 1999/93/WE uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na mocy niniejszego rozporządzenia do czasu ich wygaśnięcia. | T | Art. 129. | 1. Zaświadczenia certyfikacyjne, poświadczenia elektroniczne i certyfikaty wydane zgodnie z przepisami ustawy z dnia 18 września 2001 r. o podpisie elektronicznym zachowują ważność przez okres w nich wskazany, o ile nie zostaną unieważnione. 2. Do zaświadczeń certyfikacyjnych, poświadczeń elektronicznych i certyfikatów, o których mowa w ust. 1, stosuje się odpowiednio przepisy, dotyczące certyfikatów krajowych dostawców usług zaufania oraz narodowego centrum certyfikacji. | |
| | 3. Podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty na mocy dyrektywy 1999/93/WE, przekazuje raport z oceny zgodności organowi nadzoru jak najszybciej, ale nie później niż dnia 1 lipca 2017 r. Do czasu przekazania takiego raportu z oceny zgodności i zakończenia oceny przez organ nadzoru podmiot świadczący usługi certyfikacyjne jest uważany za kwalifikowanego dostawcę usług zaufania w rozumieniu niniejszego rozporządzenia. | T | Art. 130. | 1. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne, o którym mowa w art. 23 ust. 1 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, staje się rejestrem dostawców usług zaufania w rozumieniu niniejszej ustawy. | |
| | 4. Jeżeli podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty na mocy dyrektywy 1999/93/WE, nie przekaże raportu z oceny zgodności organowi nadzoru w terminie, o którym mowa w ust. 3, wówczas ten podmiot świadczący usługi certyfikacyjne, od dnia 2 lipca 2017 r., nie jest uważany za kwalifikowanego dostawcę usług zaufania w rozumieniu niniejszego rozporządzenia | N | | | |
| Art. 52 | Wejście w życie 1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej. 2. Niniejsze rozporządzenie stosuje się od dnia 1 lipca 2016 r., z wyjątkiem następujących przepisów: a) art. 8 ust. 3, art. 9 ust. 5, art. 12 ust. 2–9, art. 17 ust. 8, art. 19 ust. 4, art. 20 ust. 4, art. 21 ust. 4, art. 22 ust. 5, art. 23 ust. 3, art. 24 ust. 5, art. 27 ust. 4 i 5, art. 28 ust. 6, art. 29 ust. 2, art. 30 ust. 3 i 4, art. 31 ust. 3, art. 32 ust. 3, art. 33 ust. 2, art. 34 ust. 2, art. 37 ust. 4 i 5, art. 38 ust. 6, art. 42 ust. 2, art. 44 ust. 2, art. 45 ust. 2, art. 47 i 48 mają zastosowanie od dnia 17 września 2014 r.; b) art. 7, art. 8 ust. 1 i 2, art. 9, 10, 11 i art. 12 | N | | | |

| | | | | |
|---|----------|-----------|--|--|
| ust. 1 mają zastosowanie od dnia rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8; | | | | |
| c) art. 6 ma zastosowanie od dnia przypadającego trzy lata od dnia rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8. | T | Art. 139. | Ustawa wchodzi w życie po upływie 7 dni od dnia ogłoszenia, za wyjątkiem art. 23, art. 25-27 i art. 94 pkt 4 w zakresie zmienianego art. 20a ust. 1 pkt 1, które wchodzi w życie z dniem 29 września 2018 r. | |
| <p>3. W przypadku gdy notyfikowany system identyfikacji elektronicznej został umieszczony w wykazie publikowanym przez Komisję na podstawie art. 9 przed dniem, o którym mowa w ust. 2 lit. c) niniejszego artykułu, uznanie środka identyfikacji elektronicznej w ramach tego systemu na mocy art. 6 następuje nie później niż 12 miesięcy po opublikowaniu tego systemu, ale nie wcześniej niż w dniu, o którym mowa w ust. 2 lit. c) niniejszego artykułu.</p> <p>4. Niezależnie od ust. 2 lit. c) niniejszego artykułu państwo członkowskie może postanowić, że środki identyfikacji elektronicznej w ramach systemu identyfikacji elektronicznej notyfikowanego na podstawie art. 9 ust. 1 przez inne państwo członkowskie są uznawane w pierwszym państwie członkowskim z dniem rozpoczęcia stosowania aktów wykonawczych, o których mowa w art. 8 ust. 3 i art. 12 ust. 8. Zainteresowane państwa członkowskie informują o tym Komisję. Komisja podaje te informacje do wiadomości publicznej.</p> | N | | | |

| | |
|--------------------------------|---|
| Tytuł projektu | Ustawa o usługach zaufania oraz identyfikacji elektronicznej |
| Tytuł wdrażanego aktu prawnego | Rozporządzenie 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 uchylające dyrektywę 1999/93/WE (eIDAS) |

| Jednostka redakcyjna projektu ustawy | Treść przepisu projektu ustawy | Uzasadnienie wprowadzenia |
|--------------------------------------|---|--|
| Art. 52. | W ustawie z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23 i 868) wprowadza się następujące zmiany: 1) w art. 33: a) § 2a otrzymuje brzmienie: „§ 2a. Pełnomocnictwo w formie dokumentu elektronicznego powinno być opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”, | Zmiana dostosowująca wynikająca ze zmiany art. 20a ust.1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Usunięcie odwołania do art. 20a ust. 2 ww. ustawy jest związane z przyjęciem założenia, że pełnomocnictwo jest dokumentem elektronicznym, który, co do zasady, powinien być podpisany. Natomiast mechanizmy, o których mowa w art. 20a ust.2, dotyczą identyfikacji w systemie teleinformatycznym, a nie podpisywania. |
| Art. 64. | Art. 64. W ustawie z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz. U. z 2015 r. poz. 128, z późn. zm.)) wprowadza się następujące zmiany: 1) w art. 6 w ust. 1 pkt 6a otrzymuje brzmienie: „6a) świadczyć usługi zaufania oraz wydawać środki identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania;”; 2) po art. 7a dodaje się art. 7b w brzmieniu: „Art. 7b. Oświadczenia woli związane z dokonywaniem czynności, o których mowa w art. 6 ust.1 pkt 6a, mogą być składane w postaci elektronicznej.”. | W zakresie usług zaufania dostosowanie do eIDAS (do aparatu pojęciowego zdefiniowanego w art. 3) W zakresie identyfikacji elektronicznej przepis pośrednio dostosowujący do eIDAS, jak również przepis niemający charakteru przepisu technicznego. Banki, zgodnie z zasadą określoną w art. 6 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. z 2015 poz.128, z późn. zm.), poza czynnościami bankowymi mają ściśle określony katalog możliwej aktywności. Jedną z tych możliwych aktywności jest obecnie świadczenie usług certyfikacyjnych. W związku z tym, że rozporządzenie eIDAS definiuje dodatkowo obszar identyfikacji elektronicznej, w tym środki identyfikacji elektronicznej służące do celów uwierzytelniania dla usługi online, należy zezwolić bankom na ich wydawanie, gdyż bez takiego zezwolenia nie mogłyby tego robić. Brak przepisu stanowiłby zatem ograniczenie dla banków, podczas gdy inne podmioty nie miałyby takich ograniczeń. Wskazane zezwolenie nie dotyczy określonych usług świadczonych na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy, tylko ogólnej możliwości wydawania środków identyfikacji elektronicznej przez banki. Zgodnie z definicją określoną w eIDAS „środek identyfikacji elektronicznej” oznacza <i>materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online</i> . Chodzi zatem wyłącznie o możliwość wydawania środków służących do uwierzytelniania w usługach <i>online</i> , a nie o określone usługi online. Zmieniany przepis art. 6a ustawy – Prawo bankowe to zdjęcie ograniczenia wykluczającego banki, jakie pojawiłoby się pośrednio po wejściu w życie eIDAS, a nie ustalenie określonej usługi spofeczeństwa informacyjnego. W obecnym brzmieniu ustawy – Prawo bankowe, przepis art. 6 w ust. 1 pkt 6a brzmi: „6a) świadczyć usługi certyfikacyjne w rozumieniu przepisów o podpisie elektronicznym, z wyłączeniem wydawania certyfikatów kwalifikowanych wykorzystywanych przez banki w czynnościach, których są stronami;”. W uchylanej przez eIDAS Dyrektywie 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych znajdują się następujące definicje (w art.2): „1) „podpis elektroniczny” oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia;” |

| | | |
|----------|--|--|
| | | <p>"11) podmiot świadczący usługi certyfikacyjne" oznacza podmiot lub osobę prawną bądź fizyczną, która wystawia certyfikaty lub świadczy inne usługi związane z podpisami elektronicznymi;"</p> <p>W rozporządzeniu eIDAS podpis elektroniczny nie służy już jako metoda uwierzytelniania - do uwierzytelniania służą, co do zasady, środki identyfikacji elektronicznej, a podpisy elektroniczne zostały zakwalifikowane do usług zaufania i służą do podpisywania. Wynika to z następujących definicji wyrażonych w art. 3 eIDAS:</p> <p>„2) „środek identyfikacji elektronicznej” oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online;</p> <p>3) „dane identyfikujące osobę” oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;</p> <p>(...)</p> <p>5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej</p> <p>(...)</p> <p>10) „podpis elektroniczny” 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;</p> <p>(...)</p> <p>25) „pieczęć elektroniczna” oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych”</p> <p>Ponadto, zgodnie z motywem 65 eIDAS „Pieczęcie elektroniczne mogą być używane nie tylko do uwierzytelnienia dokumentu wydanego przez osobę prawną, lecz również do uwierzytelnienia wszelkich zasobów cyfrowych osoby prawnej, takich jak kod oprogramowania lub serwery.”</p> <p>W związku z powyższym przepis ma na celu zachowanie dotychczasowych uprawnień banków – mając na uwadze zmieniony zakres pojęciowy.</p> |
| Art. 63. | <p>Art. 63. W ustawie z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2015 r. poz. 613, z późn. zm.) wprowadza się następujące zmiany:</p> <p>1) w art. 3b w § 3 pkt 2 otrzymuje brzmienie:</p> <p>„2) limity wysokości zobowiązania podatkowego, kwoty nadpłaty lub zwrotu podatku wynikających z deklaracji i rodzaj podatku, którego dotyczy deklaracja, a także wymagania dla poszczególnych rodzajów podpisu elektronicznego, w szczególności dotyczące weryfikacji podpisu i kwalifikowanych elektronicznych znaczników czasu.”;</p> <p>2) w art. 3f § 1 otrzymuje brzmienie:</p> <p>„§ 1. Uwierzytelnianie podatników, płatników, inkasentów, ich następców prawnych oraz osób trzecich na portalu podatkowym wymaga użycia danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego albo profilu zaufanego ePUAP w rozumieniu art. 3 pkt 15 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;</p> <p>3) w art. 14c § 4 otrzymuje brzmienie:</p> <p>„§ 4. Interpretację indywidualną wydaną w formie dokumentu elektronicznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;</p> <p>4) w art. 138a:</p> <p>a) § 3 otrzymuje brzmienie:</p> <p>„§ 3. Pełnomocnictwo w formie dokumentu elektronicznego opatruje się kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;</p> <p>b) § 5 otrzymuje brzmienie:</p> <p>„§ 5. Jeżeli odpis pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie zostały</p> | <p>Dostosowanie do eIDAS - do aparatu pojęciowego zdefiniowanego w art. 3, w szczególności do definicji:</p> <p>5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;</p> <p>10) „podpis elektroniczny” 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;</p> <p>12) „kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego</p> <p>15) „kwalifikowany certyfikat podpisu elektronicznego” oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I</p> <p>34) „kwalifikowany elektroniczny znacznik czasu” oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42;</p> <p>Odpowiednio, w sposób adekwatny do zmian wprowadzonych w przepisach Kodeksu postępowania administracyjnego, zmieniono istniejące przepisy dostosowując je do ww. zakresu pojęciowego.</p> |

| | | |
|--|--|--|
| | <p>sporządzone w formie dokumentu elektronicznego, ich uwierzytelnienia, o którym mowa w § 4, dokonuje się opatrując odpisy kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Odpisy pełnomocnictwa lub odpisy innych dokumentów wykazujących umocowanie uwierzytelniane elektronicznie są sporządzane w formatach danych określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;</p> <p>5) w art. 143 § 1a otrzymuje brzmienie: „§ 1a. Upoważnienie może obejmować podpisywanie pism w formie dokumentu elektronicznego kwalifikowanym podpisem elektronicznym.”;</p> <p>6) w art. 144b § 1 i 2 otrzymują brzmienie: „§ 1. W przypadku pism wydanych w formie dokumentu elektronicznego przy wykorzystaniu systemu teleinformatycznego ministra właściwego do spraw finansów publicznych, które zostały opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, doręczenie może polegać na doręczeniu wydruku pisma uzyskanego z tego systemu odzwierciedlającego treść tego pisma, jeżeli strona nie wniosła o doręczanie pism za pomocą środków komunikacji elektronicznej lub nie wyraziła zgody na doręczanie pism w taki sposób. § 2. Wydruk pisma, o którym mowa w § 1, zawiera: 1) informację, że pismo zostało wydane w formie dokumentu elektronicznego przy wykorzystaniu systemu teleinformatycznego ministra właściwego do spraw finansów publicznych i podpisane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, ze wskazaniem imienia i nazwiska oraz stanowiska służbowego osoby, która je podpisała; 2) identyfikator tego pisma, nadawany przez system teleinformatyczny ministra właściwego do spraw finansów publicznych.”;</p> <p>7) w art. 152a w § 1 pkt 3 otrzymuje brzmienie: „3) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym organu podatkowego, oraz informację o wymogu podpisania urzędowego poświadczenia odbioru w określony sposób.”;</p> <p>8) w art. 159 § 2 otrzymuje brzmienie: „§ 2. Wezwanie powinno być podpisane przez pracownika organu podatkowego, z podaniem jego imienia, nazwiska i stanowiska służbowego, a jeżeli jest sporządzone w formie dokumentu elektronicznego, powinno być opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.”;</p> <p>9) w art. 168 w § 3a pkt 1 otrzymuje brzmienie: „1) być podpisane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP;”;</p> <p>10) w art. 194a § 2a otrzymuje brzmienie: „§ 2a. Jeżeli odpis dokumentu został sporządzony w formie dokumentu elektronicznego, poświadczenie jego zgodności z oryginałem, o którym mowa w § 2, dokonuje się przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP. Odpisy dokumentów poświadczane elektronicznie są sporządzane w formatach danych określonych w przepisach</p> | |
|--|--|--|

| | | |
|--|--|--|
| | <p>wydanym na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;</p> <p>11) w art. 210 w § 1 pkt 8 otrzymuje brzmienie: „8) podpis osoby upoważnionej, z podaniem jej imienia i nazwiska oraz stanowiska służbowego, a jeżeli decyzja została wydana w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”;</p> <p>12) w art. 217 w § 1 pkt 7 otrzymuje brzmienie: „7) podpis osoby upoważnionej, z podaniem jej imienia i nazwiska oraz stanowiska służbowego, a jeżeli postanowienie zostało wydane w formie dokumentu elektronicznego – kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”;</p> <p>13) w art. 282b w § 4 pkt 6 otrzymuje brzmienie: „6) podpis osoby upoważnionej do zawiadomienia, a jeżeli zawiadomienie zostało wydane w formie dokumentu elektronicznego - kwalifikowany podpis elektroniczny albo podpis potwierdzony profilem zaufanym ePUAP.”;</p> <p>14) w art. 306d § 3 otrzymuje brzmienie: „§ 3. Jeżeli strona lub inny uczestnik postępowania nie może uzyskać w formie dokumentu elektronicznego zaświadczenia wymaganego na potwierdzenie faktów lub stanu prawnego lub innego dokumentu wydanego przez podmiot publiczny w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jak również potwierdzenia uiszczenia opłat i kosztów postępowania, strona lub inny uczestnik postępowania może złożyć elektroniczną kopię takiego dokumentu, po uwierzytelnieniu jej przez wnoszącego, przy użyciu kwalifikowanego podpisu elektronicznego albo podpisu potwierdzonego profilem zaufanym ePUAP.”.</p> <p>Art. 67. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2016 r. poz. 963) wprowadza się następujące zmiany: 1) w art. 39a w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie: „Począwszy od 2016 r., co cztery lata, w okresie od dnia 1 kwietnia do dnia 31 lipca, członek otwartego funduszu emerytalnego lub osoba, której Zakład ewidencjonuje składkę na subkoncie, o którym mowa w art. 40a, zgodnie z art. 22 ust. 3 pkt 2, może złożyć do Zakładu pisemnie lub w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym, podpisem potwierdzonym profilem zaufanym ePUAP albo wykorzystując sposób potwierdzania pochodzenia oraz integralności danych udostępniony bezpłatnie przez Zakład w systemie teleinformatycznym, zgodne ze wzorem oświadczenie o:”;</p> | <p>Zmiana wynikająca ze zmiany art. 20a ust.1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.</p> |
|--|--|--|

| | | |
|--|--|--|
| | | |
|--|--|--|

| | | |
|----------|--|--|
| Art. 75. | <p>Art. 75. W ustawie z dnia 27 lipca 2001 r. - Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133, z późn. zm.) wprowadzane są następujące zmiany:</p> <p>1) w art. 57 § 5 i 6 otrzymują brzmienie: „§ 5. Uwierzytelnienie w systemie teleinformatycznym wymaga użycia profilu zaufanego ePUAP, danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego albo otrzymanego w sądzie identyfikatora wskazującego na tożsamość kandydata. § 6. Zgłaszający swoją kandydaturę wypełnia w systemie teleinformatycznym kartę zgłoszenia kandydata na wolne stanowisko sędziowskie, opatruje ją podpisem elektronicznym nadanym przez ten system, podpisem potwierdzonym profilem zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym, a następnie wnosi za pośrednictwem systemu do prezesa właściwego sądu.”;</p> <p>2) w art. 57aa § 1 - 3 otrzymują brzmienie: „§ 1. Dokumenty dołączane do karty zgłoszenia kandydat tworzy w systemie teleinformatycznym i wnosi za pośrednictwem tego systemu, opatrując je podpisem elektronicznym nadanym przez ten system, podpisem potwierdzonym profilem zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym. § 2. Dokumenty mające w oryginale postać papierową kandydat zamieszcza w systemie teleinformatycznym w postaci elektronicznych kopii, opatrując je podpisem elektronicznym nadanym przez ten system, podpisem potwierdzonym profilem zaufanym ePUAP albo kwalifikowanym podpisem elektronicznym, co jednocześnie stanowi oświadczenie o zgodności elektronicznej kopii dokumentu z oryginałem w postaci papierowej. Oświadczenie to jest składane pod rygorem odpowiedzialności karnej za fałszywe zeznania. Prezes właściwego sądu, któremu zgłoszono kandydaturę na wolne stanowisko sędziowskie, w uzasadnionych przypadkach może wezwać kandydata do doręczenia w terminie trzech dni oryginałów dokumentów. Obowiązek zamieszczenia w systemie teleinformatycznym elektronicznej kopii dokumentu nie dotyczy oświadczenia, o którym mowa w art. 7 ust. 1 ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990, oraz treści tych dokumentów, a także informacji, o której mowa w art. 7 ust. 3a tej ustawy. § 3. Prezes właściwego sądu, któremu zgłoszono kandydaturę na wolne stanowisko sędziowskie, zamieszcza w systemie teleinformatycznym elektroniczne kopie dokumentów innych niż zamieszczone przez kandydata, mających w oryginale postać papierową, wymaganych w tym postępowaniu, opatrując je podpisem elektronicznym nadanym przez ten system. Obowiązek zamieszczenia w systemie teleinformatycznym elektronicznej kopii dokumentu nie dotyczy oświadczenia, o którym mowa w art. 7 ust. 1 ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990, oraz treści tych dokumentów, a także informacji, o której mowa w art. 7 ust. 3a tej ustawy.”.</p> | <p>Dostosowanie do eIDAS - do aparatu pojęciowego zdefiniowanego w art. 3 w szczególności do definicji:</p> <p>5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;</p> <p>10) „podpis elektroniczny” 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;</p> <p>12) „kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego</p> <p>15) „kwalifikowany certyfikat podpisu elektronicznego” oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I</p> <p>34) „kwalifikowany elektroniczny znacznik czasu” oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42;</p> <p>Odpowiednio zmieniono istniejące przepisy dostosowując je do ww. zakresu pojęciowego.</p> |
| Art. 92 | <p>Art. 90. W ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 584, z późn. zm.) wprowadza się następujące zmiany:</p> <p>1) w art. 22b po ust. 2 dodaje się ust. 2a w brzmieniu: „2a. Jeżeli przepisy odrębne wymagają podpisania dokumentów, o których mowa w ust. 1, dokumenty te są podpisywane kwalifikowanym podpisem</p> | <p>Dodanie ust. 2a stanowi uzupełnienie przepisu w ust. 2, mające na celu wyjaśnienie, że do dokumentów tam opisanych stosuje się ogólne przepisy dotyczące podpisywania dokumentów, co daje użytkownikom pewność prawa i pozwala uniknąć wątpliwości w tym</p> |

| | | |
|--|---|--|
| | <p>elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, albo wykorzystując sposób potwierdzania pochodzenia i integralności danych udostępniony bezpłatnie przez pojedynczy punkt kontaktowy.”;</p> <p>2) art. 22g otrzymuje brzmienie: „Art. 22g. Minister właściwy do spraw gospodarki określi, w drodze rozporządzenia, szczegółowy zakres i warunki korzystania z pojedynczego punktu kontaktowego, w tym w szczególności sposób potwierdzania pochodzenia i integralności danych udostępniony bezpłatnie przez pojedynczy punkt kontaktowy o którym mowa w art. 22b ust. 2a, z uwzględnieniem roli punktu kontaktowego w realizacji procedur związanych z podejmowaniem, wykonywaniem i zakończeniem działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, uznawaniem kwalifikacji zawodowych nabytych w państwach członkowskich Unii Europejskiej, świadczeniem usług transgranicznych i ubieganiem się o wydanie europejskiej legitymacji zawodowej oraz zasad przetwarzania i ochrony danych osobowych.”;</p> <p>3) w art. 26 ust. 4 otrzymuje brzmienie: „4. Organ gminy przekształca wniosek, o którym mowa w ust. 2, na formę dokumentu elektronicznego, podpisuje go kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, albo podpisuje w inny sposób akceptowany przez system CEIDG umożliwiający jednoznaczną identyfikację osoby podpisującej przekształcony wniosek i przesyła go do CEIDG nie później niż następnego dnia roboczego od dnia jego otrzymania.”;</p> <p>4) w art. 27 ust. 7 otrzymuje brzmienie: „7. Wniosek o wpis do CEIDG składany w sposób określony w art. 26 ust. 1 podpisany jest kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, albo podpisany w inny sposób akceptowany przez system CEIDG umożliwiający jednoznaczną identyfikację osoby składającej wniosek.”.</p> | <p>zakresie. Taki przepis pozwoli odciążyć urzędy od udzielania informacji i wyjaśniania wątpliwości, jak również pozwoli przedsiębiorcom uniknąć konieczności uzupełnienia dokumentów o podpis elektroniczny.</p> <p>Zmiana brzmienia art. 22g jest konsekwencją dodania ust. 2a do art. 22b. ustawy z dnia 2 lipca 2004 r. <i>o swobodzie działalności gospodarczej</i>.</p> <p>Zmiana brzmienia art. 26 ust. 4 ze względu na potrzebę dostosowania przepisu do eIDAS w zakresie stosowania elektronicznych znaczników czasu, w szczególności podpis elektroniczny nie może służyć do jednoznacznej identyfikacji czasu przesłania wniosku.</p> <p>Zmiana brzmienia art. 27 ust. 7 ze względu na potrzebę dostosowania przepisu do eIDAS w zakresie stosowania elektronicznych znaczników czasu, w szczególności podpis elektroniczny nie może służyć do jednoznacznej identyfikacji czasu przesłania wniosku.</p> |
|--|---|--|

| | | |
|-----------------|--|---|
| <p>Art. 94.</p> | <p>Art. 94. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352) wprowadza się następujące zmiany:</p> <p>1) w art. 3:</p> <p>a) pkt 15 otrzymuje brzmienie: „15) podpis potwierdzony profilem zaufanym ePUAP – podpis elektroniczny złożony przez użytkownika konta ePUAP, do którego zostały dołączone informacje identyfikujące zawarte w profilu zaufanym ePUAP, a także: a) jednoznacznie wskazujący profil zaufany ePUAP osoby, która wykonała podpis, b) zawierający czas wykonania podpisu, c) jednoznacznie identyfikujący konto ePUAP osoby, która wykonała podpis, d) autoryzowany przez użytkownika konta ePUAP, e) opatrzony i chroniony pieczęcią elektroniczną wykorzystywaną w ePUAP w celu zapewnienia integralności i autentyczności wykonania operacji przez system ePUAP;”;</p> <p>b) uchyla się pkt 16,</p> <p>c) po pkt 26 dodaje się pkt 27 w brzmieniu: „27) autoryzacja - przydzielenie osobie fizycznej lub prawnej, uprawnień w systemie teleinformatycznym po jej pozytywnym uwierzytelnieniu lub potwierdzenie woli realizacji czynności w postaci elektronicznej przez uwierzytelnionego użytkownika za pomocą dodatkowych danych.”;</p> <p>2) w art. 19a ust. 3 otrzymuje brzmienie: „3. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, zakres i warunki korzystania z ePUAP, w tym warunki organizacyjne i techniczne nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, z uwzględnieniem roli ePUAP w procesie realizacji zadań publicznych drogą elektroniczną oraz zasad przetwarzania i ochrony danych osobowych.”;</p> <p>3) w art. 19b ust. 3 otrzymuje brzmienie: „3. Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.”;</p> <p>4) w art. 20a:</p> <p>a) ust. 1 otrzymuje brzmienie: „1. Uwierzytelnienie użytkowników systemu teleinformatycznego korzystających z usług online udostępnianych przez podmioty określone w art. 2 wymaga: 1) użycia notyfikowanego środka identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa wymaganego dla usług świadczonych w ramach tych systemów, lub 2) profilu zaufanego ePUAP, lub 3) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego.”;</p> <p>b) w ust. 3 w pkt 2: - wprowadzenie do wyliczenia otrzymuje brzmienie: „2) zasady i warunki potwierdzania, przedłużania ważności, wykorzystania i nieważnienia profilu zaufanego ePUAP, w tym:”;</p> | <p>W zakresie pkt 1 lit. a i b: Dostosowanie do eIDAS (do definicji pieczęci elektronicznej w art. 3 pkt. 25)</p> <p>Obecne brzmienie przepisu: 15) podpis potwierdzony profilem zaufanym ePUAP - podpis złożony przez użytkownika konta ePUAP, do którego zostały dołączone informacje identyfikujące zawarte w profilu zaufanym ePUAP, a także: a) jednoznacznie wskazujący profil zaufany ePUAP osoby, która wykonała podpis, b) zawierający czas wykonania podpisu, c) jednoznacznie identyfikujący konto ePUAP osoby, która wykonała podpis, d) autoryzowany przez użytkownika konta ePUAP, e) potwierdzony i chroniony podpisem systemowym ePUAP;</p> <p>Cel i znaczenie pojęcia „podpis systemowy ePUAP” pokrywa się z definicją pieczęci elektronicznej w eIDAS. Zmiana na ma celu dostosowanie terminologii do obecnych przepisów.</p> <p>W zakresie pkt 1 lit. c Przepis niemający charakteru przepisu technicznego</p> <p>Nie jest to projekt przepisu technicznego w rozumieniu Dyrektywy (UE) 2015/1535. Celem przepisu jest dostosowanie wyjaśnienia pojęcia już funkcjonującego w obrocie prawnym w szczególności w art. 3 pkt 15 lit. d ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.</p> <p>W zakresie pkt. 2 Przepis niemający charakteru przepisu technicznego</p> <p>Nie jest to projekt przepisu technicznego w rozumieniu Dyrektywy (UE) 2015/1535. Przepis nie podlega notyfikacji, gdyż jest mowa o nieodpłatnej usłudze. Celem przepisu jest poszerzenie możliwości uzyskania profilu zaufanego ePUAP z zachowaniem odpowiedniego poziomu bezpieczeństwa dla tego środka identyfikacji elektronicznej.</p> <p>W zakresie pkt 3 Dostosowanie do eIDAS - do definicji pojęcia kwalifikowanego podpisu elektronicznego wyrażonej w art. 3 pkt. 12</p> <p>W zakresie pkt 4 Dostosowanie do eIDAS - do definicji uwierzytelniania wyrażonej w art. 3 pkt. 5 oraz w pkt 12, jak również wymogów dotyczących wzajemnego uznawania środków identyfikacji elektronicznej oraz uwierzytelnienia określonych w art. 6</p> |
|-----------------|--|---|

| | | |
|--|---|--|
| | <p>- lit. f otrzymuje brzmienie: „f) warunki składania podpisu elektronicznego potwierdzonego profilem zaufanym ePUAP,” - po lit. i dodaje się lit. j w brzmieniu: „j) warunki organizacyjne i techniczne dla potwierdzania profilu zaufanego ePUAP przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy”;</p> <p>5) art. 20b otrzymuje brzmienie: „Art. 20b. 1. Podpis potwierdzony profilem zaufanym ePUAP wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności tego profilu. 2. Dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba że przepisy odrębne stanowią inaczej. 3. Nie można odmówić ważności i skuteczności podpisowi elektronicznemu potwierdzonemu profilem zaufanym ePUAP tylko na tej podstawie, że istnieje w postaci elektronicznej lub zmianie uległy dane inne niż służące do potwierdzenia profilu zaufanego.”;</p> <p>6) w art. 20c: a) ust. 1 otrzymuje brzmienie: „1. Potwierdzenia profilu zaufanego ePUAP, które polega na weryfikacji zgodności danych zawartych w profilu użytkownika ze stanem faktycznym oraz nadaniu uprawnień wynikających z posiadania profilu zaufanego ePUAP, jak również przedłużenia ważności i unieważnienia profilu zaufanego ePUAP dokonuje: 1) punkt potwierdzający profil zaufany ePUAP; 2) samodzielnie osoba fizyczna występująca z wnioskiem o potwierdzenie, podpisanym kwalifikowanym podpisem elektronicznym, w przypadku, gdy kwalifikowany certyfikat podpisu elektronicznego zawiera dane obejmujące co najmniej: a) imię, b) nazwisko, c) numer PESEL; 3) samodzielnie osoba fizyczna występująca z wnioskiem o potwierdzenie, 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, b) nazwisko, c) numer PESEL.”;</p> <p>b) po ust. 7 dodaje się ust. 8 – 10 w brzmieniu: „8. Minister właściwy do spraw informatyzacji, na wniosek banku krajowego lub innego przedsiębiorcy, wydaje zgodę na wykorzystywanie środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy do potwierdzania profilu zaufanego ePUAP w sposób, o którym mowa w ust. 1 pkt 3, po złożeniu przez bank krajowy lub innego przedsiębiorcę oświadczenia o spełnieniu przez bank krajowy lub innego przedsiębiorcę warunków, o których mowa w przepisach wydanych na podstawie art. 20a ust. 3 pkt 2. 9. Minister właściwy do spraw informatyzacji może</p> | <p>W zakresie pkt 6 Przepisy niemające charakteru przepisu technicznego; jest tu mowa o nieodpłatnej usłudze.</p> <p>Celem przepisu jest poszerzenie możliwości uzyskania profilu zaufanego ePUAP z zachowaniem odpowiedniego poziomu bezpieczeństwa dla tego środka identyfikacji elektronicznej.</p> |
|--|---|--|

| | | |
|--|--|--|
| | <p>sprawdzać, czy bank krajowy lub inny przedsiębiorca w przypadku, o którym mowa w ust. 8 spełnia warunki, o których mowa w przepisach wydanych na podstawie art. 20a ust. 3 pkt 2.</p> <p>10. Minister właściwy do spraw informatyzacji cofa zgodę, o której mowa w ust. 8 w przypadku gdy bank krajowy lub inny przedsiębiorca nie spełnia warunków określonych w przepisach wydanych na podstawie art. 20a ust. 3 pkt 2.</p> | |
|--|--|--|

| | | |
|-----------|--|--|
| Art. 111 | <p>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 2014 r. poz. 1146, z późn. zm.) w art. 70 ust. 1 otrzymuje brzmienie:</p> <p>„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 ePUAP albo danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego.”.</p> | <p>Dostosowanie do eIDAS - do aparatu pojęciowego zdefiniowanego w art. 3 w szczególności do definicji:</p> <p>5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;</p> <p>15) „kwalifikowany certyfikat podpisu elektronicznego” oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I.</p> |
| Art. 112 | <p>Art. 112. W ustawie z dnia 11 lipca 2014 r. o petycjach (Dz. U. poz. 1195) art. 4 w ust. 5 otrzymuje brzmienie:</p> <p>„5. Petycja składana za pomocą środków komunikacji elektronicznej może być opatrzona kwalifikowanym podpisem elektronicznym oraz powinna zawierać także adres poczty elektronicznej podmiotu wnoszącego petycję.”.</p> | <p>Zmiana jakościowa</p> <p>Porządkowanie oryginalnego przepisu, wykraczająca poza dostosowanie do eIDAS. Zmiana „może” na „powinna”.</p> <p>Zmiana art. 4 ust. 5 ustawy o petycjach dostosowuje obecny przepis stanowiący, że petycja „(...) może być opatrzona bezpiecznym podpisem elektronicznym (...)”.</p> <p>Wskazuje się, że tak jak w przypadku petycji na papierze – powinna ona być podpisana. Mając na uwadze, że w Kodeksie postępowania administracyjnego wskazuje się w art. 63 par. 3a, że podanie powinno być podpisane kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, proponuje się dostosowanie przepisu, jak w projekcie. Pozostawienie samej możliwości, a nie wymogu podpisania petycji w postaci elektronicznej kwalifikowanym podpisem elektronicznym wydaje się nie mieć znaczenia regulacyjnego.</p> |
| Art. 122. | <p>Art. 122.</p> <p>W ustawie z dnia 10 lipca 2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. poz. 1311 i 1513 oraz z 2016 r. poz. 178, 394 i 615) wprowadza się następujące zmiany:</p> <p>1) w art. 1:</p> <p>a) pkt 9 otrzymuje brzmienie:</p> <p>„9) po art. 78 dodaje się art. 781 w brzmieniu:</p> <p>„Art. 781. § 1. Do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym.</p> <p>§ 2. Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej.”;”;</p> <p>b) pkt 11 otrzymuje brzmienie:</p> <p>„11) w art. 81 w § 2 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu:</p> <p>„3) w razie opatrzenia kwalifikowanym podpisem elektronicznym znacznikiem czasu dokumentu w postaci elektronicznej – od daty opatrzenia kwalifikowanym elektronicznym znacznikiem czasu.”;”;</p> <p>2) w art. 2:</p> <p>a) pkt 33 otrzymuje brzmienie:</p> <p>„33) w art. 324 dodaje się § 4 w brzmieniu:</p> <p>„§ 4. W postępowaniu wszczętym za pośrednictwem systemu teleinformatycznego wyrok może być utrwalony w systemie teleinformatycznym i opatrzony kwalifikowanym podpisem elektronicznym.”;”;</p> <p>b) w pkt 74 lit. a w zakresie dodawanego § 31 otrzymuje brzmienie:</p> <p>„§ 31. Postanowienie o nadaniu klauzuli</p> | <p>Dostosowanie do eIDAS - do aparatu pojęciowego zdefiniowanego w art. 3 w szczególności do definicji:</p> <p>5) „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej;</p> <p>12) „kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego</p> <p>15) „kwalifikowany certyfikat podpisu elektronicznego” oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I.</p> |

| | | |
|-----------|--|---|
| | <p>wykonalności tytułem egzekucyjnym, o których mowa w art. 777 § 1 pkt 1 i 11, wydanych w postaci elektronicznej, jest wydawane bez spisywania odrębnej sentencji, poprzez umieszczenie klauzuli wykonalności w systemie teleinformatycznym i opatrzenie jej kwalifikowanym podpisem elektronicznym, sędziego albo referendarza sądowego, który wydaje postanowienie.”;</p> <p>3) w art. 3 w pkt 10 lit. b w zakresie dodawanego § 2a otrzymuje brzmienie: „§ 2a. Jeżeli zawiadomienie o zajęciu prawa majątkowego doręcza się dłużnikowi zajętej wierzytelności przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej: 1) w zawiadomieniu o zajęciu nie umieszcza się podpisu z podaniem imienia, nazwiska i stanowiska służbowego podpisującego oraz odcisku pieczęci organu egzekucyjnego; 2) zawiadomienie o zajęciu zawiera numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub numer identyfikacji podatkowej (NIP) zobowiązanego, o ile są znane organowi egzekucyjnemu; 3) zawiadomienie o zajęciu opatruje się kwalifikowanym podpisem elektronicznym.”;</p> <p>4) w art. 7: a) pkt 2 w zakresie zmienianego art. 95h § 1 otrzymuje brzmienie: „§ 1. Notariusz niezwłocznie po sporządzeniu aktu poświadczenia dziedziczenia dokonuje jego wpisu do Rejestru Spadkowego przez wprowadzenie za pośrednictwem systemu teleinformatycznego danych wynikających z tego aktu, o których mowa w art. 95ha pkt 3-7. Notariusz opatruje wpis kwalifikowanym podpisem elektronicznym.”, b) pkt 4 w zakresie zmienianego art. 95i § 1 otrzymuje brzmienie: „§ 1. Krajowa Rada Notarialna tworzy system teleinformatyczny w celu prowadzenia Rejestru Spadkowego, zapewnia notariuszom i sądom dostęp do tego systemu w celu dokonywania wpisów oraz ochronę danych zgromadzonych w Rejestrze Spadkowym przed nieuprawnionym dostępem, przetwarzaniem oraz zmianą lub utratą. Dane weryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego zapewniają notariuszowi oraz prezesowi sądu lub osobie przez niego wyznaczonej dostęp do Rejestru Spadkowego.”, c) pkt 6 otrzymuje brzmienie: „6) w art. 97 dotychczasową treść oznacza się jako § 1 i dodaje się § 2 w brzmieniu: „§ 2. Elektroniczne poświadczenie zgodności odpisu, wyciągu lub kopii z okazanym dokumentem notariusz opatruje kwalifikowanym podpisem elektronicznym.”.”.</p> | |
| Art. 133. | <p>Art. 133. Banki wykonujące czynności, o których mowa w art. 6 ust. 1 pkt 6a ustawy zmienianej w art. 63, w brzmieniu dotychczasowym, są obowiązane dostosować statuty do przepisów ustawy zmienianej w art. 63, w brzmieniu nadanym niniejszą ustawą, w terminie 12 miesięcy od dnia wejścia w życie niniejszej ustawy.</p> | <p>Przepis dostosowujący do eIDAS</p> <p>Przepis jest przepisem przejściowym i dotyczy art. 6 ust. 1 pkt 6a zmienianej ustawy – Prawo bankowe, który dostosowuje obecne uprawnienia banków do eIDAS. Stosowna analiza znajduje się przy art. 6 ust. 1 pkt 6a zmienianej ustawy Prawo bankowe.</p> |

| | | |
|-----------|---|--|
| Art. 135. | Do umów ubezpieczenia odpowiedzialności cywilnej zawartych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe. | |
| Art. 136. | Dotychczasowe przepisy wykonawcze wydane na podstawie art. 10 ust. 5 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 14 ust. 5 niniejszej ustawy, jednak nie dłużej niż 3 miesiące od dnia wejścia w życie niniejszej ustawy. | |
| Art. 137. | Prezes Rady Ministrów dokona, w drodze rozporządzenia, przeniesienia planowanych dochodów i wydatków budżetowych, w tym wynagrodzeń oraz limitów zatrudnienia, między częścią budżetu państwa, której dysponentem jest minister właściwy do spraw gospodarki, a częścią, której dysponentem jest minister właściwy do spraw informatyzacji, z zachowaniem przeznaczenia środków publicznych wynikających z ustawy budżetowej. | |



Warszawa, dnia 12 lipca 2016 r.

Minister
Spraw Zagranicznych

DPUe.920.396.2016/bc/ 21

dot.: RM-10-78-16 z 11.07.2016r.

Pani
Jolanta Rusiniak
Sekretarz Rady Ministrów

Opinia
o zgodności z prawem Unii Europejskiej projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej 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 jest zgodny z prawem Unii Europejskiej.

Z poważaniem

z up. Ministra Spraw Zagranicznych
SEKRETARZ RZĄDU
Konrad Szymański
Konrad Szymański

Do wiadomości:

Pan Mateusz Morawiecki
Wiceprezes Rady Ministrów
Minister Rozwoju

Pani Anna Streżyńska

Minister Cyfryzacji

Kancelaria Prezesa Rady Ministrów
Departament Rady Ministrów

wpłynęło: 12 -07- 2016

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI

z dnia

w sprawie krajowej infrastruktury zaufania.

Na podstawie art. 13 ustawy z dnia ... o usługach zaufania oraz identyfikacji elektronicznej (Dz. U..., poz. ...) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

- 1) wymagania organizacyjno-techniczne krajowej infrastruktury zaufania;
- 2) szczegółową treść wpisów w rejestrze oraz sposób ich dokonywania,
- 3) tryb wydawania i unieważniania certyfikatów dostawcy usługi zaufania oraz certyfikatów narodowego centrum certyfikacji,
- 4) wymagania dla polityki certyfikacji narodowego centrum certyfikacji,
- 5) wymagania bezpieczeństwa krajowej infrastruktury zaufania

§ 2. Użyte w rozporządzeniu określenia oznaczają:

- 1) ustawa – ustawę z dnia ... o usługach zaufania oraz identyfikacji elektronicznej;
- 2) algorytm kryptograficzny – zestaw przekształceń matematycznych służących do zamiany informacji na niezrozumiałą, czasami z wykorzystaniem parametrów zależnych od zastosowanego klucza.

Rozdział 2

Dokonywanie wpisów do rejestru oraz ich treść

§ 3. Wniosek o dokonanie wpisu do rejestru dostawców usług zaufania składa się za pomocą formularza, o którym mowa w art. 5 ust. 3 ustawy, na elektroniczną skrzynkę podawczą

ministra właściwego do spraw informatyzacji, zwanej dalej „organem nadzoru”. Wniosek podpisuje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.

§ 4. 1. Organ nadzoru, dokonuje wpisu do rejestru po wydaniu decyzji, o której mowa w art. 5 ust. 5 ustawy.

2. W przypadku, o którym mowa w art. 12 ust. 1 ustawy, organ nadzoru po wydaniu decyzji, o której mowa w ust. 1, przekazuje niezwłocznie do Narodowego Banku Polskiego odpis tej decyzji w postaci elektronicznej. Narodowy Bank Polski dokonuje wpisu niezwłocznie, nie później niż w terminie 3 dni roboczych od dnia otrzymania odpisu decyzji.

§ 5. 1. Każdy wpis do rejestru w odniesieniu do dostawcy usług zaufania zawiera informacje, o których mowa w art. 4 ust. 4, o ile go dotyczą, oraz wskazanie, czy jest to kwalifikowany lub niekwalifikowany dostawca usług zaufania.

2. Każdy wpis do rejestru w odniesieniu do usługi zaufania zawiera informacje, o których mowa w art. 4 ust. 4 pkt 1 oraz 5, 6 i 9, o ile jej dotyczą, oraz wskazanie, czy jest to kwalifikowana lub niekwalifikowana usługa zaufania.

3. Każdą zmianę w rejestrze opatruje się czasem jej dokonania.

§ 6. 1. Zmiana treści wpisu nie może prowadzić do usunięcia poprzedniej treści. Wykreślona oraz aktualna treść wpisu powinna być w sposób czytelny i wyraźny zaznaczona, z zastrzeżeniem ust. 2.

2. Jeżeli w rejestrze znajduje się wpis zawierający oczywiste błędy pisarskie, organ nadzoru lub, w przypadku o którym mowa w art. 12 ust. 1 ustawy, Narodowy Bank Polski poprawia błąd. Poprawa błędu następuje na wniosek dostawcy usług zaufania lub z urzędu, po uprzednim poinformowaniu dostawcy usług zaufania.

§ 7. 1. Minister właściwy do spraw informatyzacji zamieszcza w Biuletynie Informacji Publicznej na stronie podmiotowej formularz elektroniczny umożliwiający przygotowanie i złożenie zgłoszenia o wpis niekwalifikowanego dostawcy usług zaufania do rejestru dostawców usług zaufania.

2. Zgłoszenie o dokonanie wpisu niekwalifikowanego dostawcy usług zaufania do rejestru dostawców usług zaufania składa się za pomocą formularza, o którym mowa w ust. 1, na elektroniczną skrzynkę podawczą organu nadzoru. Zgłoszenie podpisuje się kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.

3. Dopuszcza się dołączenie do zgłoszenia dodatkowych dokumentów innych niż określone w art. 4 ust. 4 pkt 1–6 i 10 ustawy, w szczególności potwierdzających certyfikację lub udział w systemie dobrowolnej akredytacji. Informacje o tych dodatkowych dokumentach organ nadzoru może zamieszczać w rejestrze.

Rozdział 3

Sposób tworzenia, wydawania i unieważniania certyfikatów dostawcy usług zaufania oraz narodowego centrum certyfikacji usług zaufania

§ 8. 1. Certyfikat kwalifikowanego dostawcy usług zaufania wydaje narodowe centrum certyfikacji.

2. Wydanie kwalifikowanemu dostawcy usług zaufania certyfikatu, o którym mowa w ust. 1, odbywa się na podstawie decyzji organu nadzoru, o której mowa w art. 5 ust. 5 ustawy.

3. Zarządzanie certyfikatami kwalifikowanego dostawcy usług zaufania odbywa się zgodnie z polityką certyfikacji narodowego centrum certyfikacji, z uwzględnieniem dokumentów RFC 5280 i RFC 4210.

4. Polityka certyfikacji narodowego centrum certyfikacji podlega uzgodnieniu z kwalifikowanymi dostawcami usług zaufania, a w przypadku, o którym mowa w art. 12 ust. 1 ustawy, także z organem nadzoru.

§ 9. Narodowe centrum certyfikacji tworzy certyfikaty kwalifikowanego dostawcy usług zaufania niezwłocznie po dokonaniu wpisu kwalifikowanego dostawcy usług zaufania do rejestru, na podstawie danych przedstawionych przez kwalifikowanego dostawcę usług zaufania we wniosku o wpis do rejestru.

§ 10. Certyfikat kwalifikowanego dostawcy wydaje się w ciągu 7 dni od dnia spełnienia przez kwalifikowanego dostawcę usług zaufania warunku, o którym mowa w art. 14 ust. 3 ustawy.

§ 11. Okres ważności certyfikatu kwalifikowanego dostawcy usług zaufania określa polityka certyfikacji narodowego centrum certyfikacji.

§ 12. Sposób odnowienia certyfikatu kwalifikowanego dostawcy usług zaufania określa polityka narodowego centrum certyfikacji.

§ 13. Algorytmy kryptograficzne wykorzystywane w narodowym centrum certyfikacji określa polityka certyfikacji narodowego centrum certyfikacji.

§ 14. Certyfikat narodowego centrum certyfikacji tworzy minister właściwy do spraw informatyzacji albo Narodowy Bank Polski w przypadku, o którym mowa w art. 12 ust. 1 ustawy.

§ 15. Okres ważności certyfikatu narodowego centrum certyfikacji określa polityka certyfikacji narodowego centrum certyfikacji.

§ 16. Zarządzanie certyfikatami narodowego centrum certyfikacji odbywa się zgodnie polityką certyfikacji narodowego centrum certyfikacji, z uwzględnieniem dokumentów RFC 5280 i RFC 4210.

Rozdział 4

Wymagania bezpieczeństwa w krajowej infrastrukturze zaufania

§ 17. Kwalifikowany dostawca usług zaufania stosuje normy ETSI EN 319 401, ETSI EN 319 411 oraz ETSI EN 319 421, o ile Komisja Europejska nie ustanowi innych formatów, środków i procedur, o których mowa w art. 19 ust. 4 eIDAS.

§ 18. Narodowe centrum certyfikacji usług zaufania spełnia odpowiednio warunki określone w normie ETSI EN 319 401 oraz warunki określone dla polityki QCP-1-qscd w normie ETSI EN 319 411.

§ 19. 1. Kwalifikowany dostawca usług zaufania wydający kwalifikowane certyfikaty zapewnia możliwość zgłoszenia wniosku o unieważnienie kwalifikowanego certyfikatu przez całą dobę.

2. O procedurze zgłoszenia, o której mowa w ust. 1, informuje się osobę ubiegającą się o wydanie kwalifikowanego certyfikatu, najpóźniej w momencie jego wydania.

3. Posiadacza kwalifikowanego certyfikatu informuje się o konieczności niezwłocznego zgłoszenia wniosku o unieważnienie kwalifikowanego certyfikatu w momencie ujawnienia lub podejrzenia ujawnienia jego danych służących do składania podpisu elektronicznego innej osobie.

§ 20. Narodowe centrum certyfikacji zapewnia możliwość zgłoszenia wniosku o unieważnienie certyfikatu, o którym mowa w § 8 ust. 1, przez całą dobę.

Rozdział 5

Przepis końcowy

§ 21. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

UZASADNIENIE

Projekt rozporządzenia w sprawie krajowej infrastruktury zaufania pełni funkcję analogiczną do wydanego na mocy przepisów uchylanej ustawy z dnia 18 września 2001 r. o podpisie elektronicznym rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. zmieniającego rozporządzenie w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.

Stosowanie od 1 lipca 2016 r. rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 (eIDAS) oznacza uchylenie Dyrektywy 1999/93/WE i ww. ustawy. Odnoszący się do zagadnień pozostawionych przez eIDAS do uregulowania prawem krajowym projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej wskazuje organ nadzoru nad dostawcami usług zaufania i określa jego formy: zaufaną listę, rejestr dostawców usług zaufania i krajowy urząd certyfikujący – zbiorczo określane mianem krajowej infrastruktury zaufania. W jej ramach przewiduje się utrzymanie dotychczasowej struktury opartej o Narodowe Centrum Certyfikacji (NCCert) funkcjonujące w ramach Narodowego Banku Polskiego. Będzie ono wydawać certyfikaty dla kwalifikowanych dostawców usług zaufania, służące do weryfikacji elektronicznych pieczęci i podpisów zaawansowanych, którymi dostawcy opatrują kwalifikowane certyfikaty wydawane dla użytkowników końcowych (odbiorców usług zaufania). Ewentualne zagrożenia interesów dostawców i odbiorców usług zaufania wyeliminuje stosowanie odpowiednich wymagań technicznych i organizacyjnych, regulujących funkcjonowanie krajowej infrastruktury zaufania. Niniejszy akt wykonawczy ma za zadanie ich określenie, poprzez sprecyzowanie szczegółowego sposobu postępowania w sprawach o wpis kwalifikowanych i niekwalifikowanych dostawców usług do rejestru (wraz z określeniem sposobu aktualizacji danych w rejestrze), sposób tworzenia, wydawania i unieważniania certyfikatów dostawcy usług zaufania oraz narodowego centrum certyfikacji usług zaufania oraz wymogi bezpieczeństwa w krajowej infrastrukturze zaufania. Wymogi określa obowiązujące bezpośrednio w polskim porządku prawnym rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014 (eIDAS), w szczególności jego przepisy odnoszące się do norm ETSI, formatów, środków i procedur bezpieczeństwa.

Przepisy projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej dotyczące wydawania certyfikatów dla kwalifikowanych dostawców usług zaufania nie skutkują dodatkowymi wymogami w stosunku do składników certyfikatów, określonych w załącznikach w zakresie, w jakim wymagają one jedynie podpisu zaawansowanego. Certyfikat dostawcy usług zaufania jest poświadczeniem potwierdzającym powiązanie danych do składania podpisu/pieczeni z kwalifikowanym dostawcą usług zaufania. Dane do składania podpisu/pieczeni każdy dostawca usług zaufania tworzy samodzielnie i przy ich pomocy tworzy zaawansowany podpis/zaawansowaną pieczęć, o których mowa w Załączniku 1 pkt g eIDAS. Jednocześnie honorowane będą wszelkie inne certyfikaty kwalifikowane z zagranicy, które powstały w architekturach bez takiego powiązania.

To rozwiązanie sprawdziło się w dotychczasowej praktyce ustanowionej w ustawie o podpisie elektronicznym. Specyficzna pozycja ustrojowa NBP jako centralnego banku państwa, polegająca na niezależności wobec organów państwowych, gwarantuje, że powierzone kluczowe zadanie utrzymywania najwyższego poziomu w strukturze bezpieczeństwa usług zaufania nie będzie podważane za pomocą argumentów wskazujących na zależność tej jednostki od kogokolwiek. Na uwagę zasługuje fakt, że narodowe centrum certyfikacji nie wydaje kwalifikowanych certyfikatów, a jego działalność nie jest działalnością dostawcy usług zaufania w rozumieniu eIDAS, tylko elementem zapewnienia nadzoru nad dostawcami usług zaufania. Czynności wykonywane przez NCCert stanowią element procesu weryfikacji spełnienia przez usługodawcę wymagań określonych w eIDAS w procesie przyznawania statusu kwalifikowanego dostawcy usług zaufania.

| | | | | | | | | | | | | |
|----------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|
| Wydatki ogółem | - | - | - | - | - | - | - | - | - | - | - | 0 |
| budżet państwa | | | | | | | | | | | | 0 |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | 0 |
| Saldo ogółem | - | - | - | - | - | - | - | - | - | - | - | 0 |
| budżet państwa | | | | | | | | | | | | 0 |
| JST | | | | | | | | | | | | 0 |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | 0 |

| | |
|--|---|
| Źródła finansowania | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Projektodawca nie przewiduje, aby wydanie rozporządzenia miało wpływ na sektor finansów publicznych. Z uwagi na techniczno-organizacyjny charakter rozporządzenia nie przewiduje się wystąpienia skutków w postaci zwiększenia wydatków lub zmniejszenia dochodów jednostek sektora finansów publicznych. |

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym na 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 |
| | sektor mikro-, małych i średnich przedsiębiorstw | | | | | | | 0 |
| | rodzina, obywatele oraz gospodarstwa domowe | | | | | | | 0 |
| | (dodaj/usuń) | | | | | | | |
| 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

| | |
|--|---|
| <input type="checkbox"/> nie dotyczy | |
| Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). | <input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |
| <input type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur <input type="checkbox"/> skrócenie czasu na załatwienie sprawy <input type="checkbox"/> inne: | <input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input type="checkbox"/> inne: |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | <input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |

Komentarz:

| | | |
|--|--|---|
| 9. Wpływ na rynek pracy | | |
| | | |
| 10. Wpływ na pozostałe obszary | | |
| <input type="checkbox"/> środowisko naturalne <input type="checkbox"/> sytuacja i rozwój regionalny <input type="checkbox"/> inne: | <input type="checkbox"/> demografia <input type="checkbox"/> mienie państwowe | <input type="checkbox"/> informatyzacja X <input type="checkbox"/> zdrowie |
| Omówienie wpływu | | |
| 11. Planowane wykonanie przepisów aktu prawnego | | |
| Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia. | | |
| 12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane? | | |
| | | |
| 13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.) | | |
| Nie dotyczy | | |

ROZPORZĄDZENIE
MINISTRA FINANSÓW¹⁾

z dnia

**w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego
dostawcy usług zaufania**

Na podstawie art. 14 ust. 5 ustawy z dnia ... o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z ... poz. ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowy zakres obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania w rozumieniu ustawy z dnia ... o usługach zaufania oraz identyfikacji elektronicznej, za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania, zwanego dalej „ubezpieczeniem OC”, oraz minimalną sumę gwarancyjną tego ubezpieczenia.

§ 2. 1. Ubezpieczeniem OC jest objęta odpowiedzialność cywilna kwalifikowanego dostawcy usług zaufania, zwanego dalej „dostawcą”, za szkody wyrządzone w następstwie działania lub zaniechania ubezpieczonego, w okresie trwania ochrony ubezpieczeniowej, podczas świadczenia usług zaufania.

2. Ubezpieczenie OC nie obejmuje szkód:

- 1) wyrządzonych przez dostawcę będącego osobą fizyczną, małżonkowi, wstępnemu, zstępnemu, rodzeństwu, a także powinowatemu w tej samej linii lub stopniu, osobie pozostającej w stosunku przysposobienia oraz jej małżonkowi, jak również osobie, z którą ubezpieczony pozostaje we wspólnym pożyciu, lub innemu ubezpieczonemu będącemu współnikiem dostawcy;
- 2) wyrządzonych przez pracownika dostawcy lub osobę fizyczną działającą w imieniu i na rzecz dostawcy małżonkowi, wstępnemu, zstępnemu, rodzeństwu, a także powinowatemu w tej samej linii lub stopniu, osobie pozostającej w stosunku przysposobienia oraz jej małżonkowi, jak również osobie, z którą pracownik dostawcy

¹⁾ Minister Finansów kieruje działem administracji rządowej – instytucje finansowe, na podstawie § 1 ust. 2 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. poz. 1900).

- lub osoba fizyczna działająca w imieniu i na rzecz dostawcy pozostaje we wspólnym pożyciu lub wyrządzonych innemu ubezpieczonemu będącemu współnikiem dostawcy;
- 3) wyrządzonych przez ubezpieczonego po dniu wydania ostatecznej decyzji o wykreśleniu wpisu w rejestrze kwalifikowanej usługi;
 - 4) polegających na zapłacie kar umownych;
 - 5) powstałych wskutek działań wojennych, rozruchów i zamieszek, a także aktów terroru.

3. Ubezpieczenie OC obejmuje wszystkie szkody w zakresie, o którym mowa w ust. 1, z zastrzeżeniem ust. 2, bez możliwości umownego ograniczenia przez zakład ubezpieczeń wypłaty odszkodowań.

§ 3. 1. Minimalna suma gwarancyjna ubezpieczenia OC, w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, wynosi równowartość w złotych 250.000 euro, ale nie więcej niż 1.000.000 euro w odniesieniu do wszystkich zdarzeń.

2. Kwota, o której mowa w ust. 1, jest ustalana przy zastosowaniu średniego kursu euro ogłaszanego przez Narodowy Bank Polski po raz pierwszy w roku, w którym umowa ubezpieczenia OC została zawarta.

§ 4. Umowy ubezpieczenia OC zawarte na podstawie dotychczasowych przepisów obowiązują do końca okresu, na jaki zostały zawarte, nie dłużej jednak niż przez 12 miesięcy od dnia wejścia w życie rozporządzenia.

§ 5. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER FINANSÓW

W POROZUMIENIU:

MINISTER CYFRYZACJI

UZASADNIENIE

Zasadność podjęcia prac zmierzających do wydania nowego rozporządzenia wynika z procedowanego projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej. Na podstawie art. 134 tego projektu, moc obowiązującą ma utracić obecnie obowiązująca ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, z 2014 r. poz. 1662 oraz z 2015 r. poz. 1893). Na podstawie przepisów tej ustawy zostało wydane obecnie obowiązujące rozporządzenie Ministra Finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia OC kwalifikowanego podmiotu świadczącego usługi certyfikacyjne (Dz. U. Nr 229, poz. 2282), które reguluje szczegółowy zakres tego ubezpieczenia, termin powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną tego ubezpieczenia.

Projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej co do zasady utrzymuje obecnie obowiązujący obowiązek ubezpieczenia. Na podstawie art. 30 ust. 1 projektu, kwalifikowany dostawca usług zaufania jest obowiązany posiadać ważną umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania. Jednocześnie, w ust. 4 tego przepisu, została zawarta delegacja ustawowa skierowana do ministra właściwego do spraw instytucji finansowych do wydania aktu wykonawczego w porozumieniu z ministrem właściwym do spraw informatyzacji. Przedmiotowe rozporządzenie będzie regulowało szczegółowy zakres ww. ubezpieczenia, termin powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną.

Mając powyższe na uwadze powstaje konieczność wydania nowego aktu wykonawczego na podstawie delegacji ustawowej zawartej w art. 14 ust. 5 ustawy o usługach zaufania oraz identyfikacji elektronicznej.

W § 2 projektu określono zakres obowiązkowego ubezpieczenia OC poprzez m.in. określenie w ust. 1 zakresu czasowego ochrony ubezpieczeniowej (tzw. trigger). Ubezpieczenie OC nie może bowiem prawidłowo funkcjonować bez dokładnego sprecyzowania, który moment bierze się pod uwagę jako wypadek ubezpieczeniowy objęty umową ubezpieczeniową.

Jednocześnie uzasadnione jest, aby z zakresu tego ubezpieczenia wyłączyć odpowiedzialność zakładu ubezpieczeń za enumeratywnie określone w rozporządzeniu szkody (§ 2 ust. 2). Wyłączenia zawierają przypadki społecznie uzasadnione, jak również sytuacje nadzwyczajne, którym trudno jest się przeciwstawić. Wyłączenie z zakresu ochrony

ubezpieczeniowej szkód wyrządzonych przez osoby najbliższe jest zgodne z obecnie obowiązującą praktyką stosowaną zarówno w obecnie obowiązującym ubezpieczeniu OC kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, jak i w innych ubezpieczeniach OC zawodowych. Z zakresu ubezpieczenia wyłączone zostały także szkody powstałe w wyniku m.in. aktów terroru. Stosowaną w standardach światowych praktyką jest, że szkody te jako niepodlegające co do zasady reasekuracji, wyłączone są z zakresu ubezpieczenia. Samo pojęcie „aktów terroru” określone jest w ogólnych warunkach zakładu ubezpieczeń.

Regulacje dotyczące minimalnej sumy gwarancyjnej ubezpieczenia będą tożsame z obecnie obowiązującymi. Na podstawie § 3 ust. 1 projektowanego rozporządzenia, minimalna suma gwarancyjna ubezpieczenia OC, w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, będzie wynosiła równowartość w złotych 250.000 euro, ale nie więcej niż 1.000.000 euro w odniesieniu do wszystkich zdarzeń.

Projekt zakłada, że rozporządzenie wejdzie po upływie 14 dni od dnia ogłoszenia. Zgodnie z delegacją ustawową projekt rozporządzenia zostanie przekazany do zaopiniowania przez Polską Izbę Ubezpieczeń.

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. Nr 239, poz. 2039 oraz z 2004 r. Nr 65, poz. 597), dlatego też projekt rozporządzenia nie podlega procedurze notyfikacji.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.) projekt zostanie udostępniony na stronach urzędowego informatora teleinformatycznego – Biuletynu Informacji Publicznej Rządowego Centrum Legislacji.

W związku z art. 50 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2013 r. poz. 885, z późn. zm.), projektodawca nie przewiduje, aby wydanie rozporządzenia miało wpływ na sektor finansów publicznych, w szczególności nie wystąpi skutek w postaci zwiększenia wydatków lub zmniejszenia dochodów jednostek sektora finansów publicznych.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

| | |
|--|--|
| <p>Nazwa projektu Projekt rozporządzenia Ministra Finansów w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania</p> <p>Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Finansów i Ministerstwo Cyfryzacji</p> <p>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Pan Piotr Nowak, Podsekretarz Stanu w Ministerstwie Finansów</p> <p>Kontakt do opiekuna merytorycznego projektu</p> | <p>Data sporządzenia 6 lipca 2016 r.</p> <p>Źródło: Ustawa z dnia ... o usługach zaufania oraz identyfikacji elektronicznej.</p> <p>Nr w wykazie prac</p> |
|--|--|

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Zasadność podjęcia prac zmierzających do wydania nowego rozporządzenia wynika z procedowanego projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej. Na podstawie art. 134 tego projektu, moc obowiązującą ma utracić obecnie obowiązująca ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, z 2014 r. poz. 1662 oraz z 2015 r. poz. 1893), na podstawie której zostało wydane obecnie obowiązujące rozporządzenie Ministra Finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia OC kwalifikowanego podmiotu świadczącego usługi certyfikacyjne (Dz. U. Nr 229, poz. 2282). Przepis art. 14 ust. 5 projektowanej ustawy o usługach zaufania oraz identyfikacji elektronicznej zawiera delegację ustawową skierowaną do ministra właściwego do spraw instytucji finansowych do wydania aktu wykonawczego w porozumieniu z ministrem właściwym do spraw informatyzacji. Przedmiotowe rozporządzenie będzie regulowało szczegółowy zakres ww. ubezpieczenia, termin powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną.

Należy nadmienić, iż co do zasady, kwestie jakie mają być uregulowane w projektowanym rozporządzeniu reguluje w chwili obecnej ww. rozporządzenie Ministra Finansów z dnia 16 grudnia 2003 r.

Mając na uwadze wskazane powyżej zmiany ustawowe powstaje konieczność wydania nowego aktu wykonawczego na podstawie delegacji ustawowej zawartej w art. 14 ust. 5 projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej.

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

Obowiązujące rozporządzenie Ministra Finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia OC kwalifikowanego podmiotu świadczącego usługi certyfikacyjne (Dz. U. Nr 229, poz. 2282), zachowa moc do czasu wydania nowego rozporządzenia, nie dłużej jednak niż przez 6 miesięcy od dnia wejścia w życie przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej.

W związku z powyższym proponuje się wydanie nowego aktu wykonawczego na podstawie art. 14 ust. 5 ustawy o usługach zaufania oraz identyfikacji elektronicznej, który będzie określał szczegółowy zakres obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania, termin powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną tego ubezpieczenia.

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 |
|---------------------|-------------|---------------|--|
| | | | |
| Zakłady ubezpieczeń | Brak danych | | Zakłady ubezpieczeń prowadzące działalność w zakresie ww. ubezpieczenia, które będą zawierały umowy przedmiotowego ubezpieczenia OC. |

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

Projekt rozporządzenia zostanie uzgodniony w szczególności z członkami Rady Ministrów, z organem właściwym w sprawach nadzoru nad rynkiem finansowym – Komisją Nadzoru Finansowego, z Polską Izbą Ubezpieczeń będącą organizacją ubezpieczeniowego samorządu gospodarczego, z Rzecznikiem Finansowym reprezentującym interesy osób ubezpieczonych, uposażonych i uprawnionych z umów ubezpieczenia, ze Stowarzyszeniem Polskich Brokerów, Izbą Gospodarczą Ubezpieczeń i Obsługi Ryzyka, Ogólnopolskim Stowarzyszeniem Pośredników, Polską Izbą Pośredników Ubezpieczeniowych i Finansowych, oraz z ...

Planowany termin wejścia w życie przedmiotowego rozporządzenia Ministra Finansów – po upływie 5 miesięcy od dnia wejścia w życie przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej.

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 | | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | | |
| JST | | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | | |
| Wydatki ogółem | | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | | |
| JST | | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | | |
| Saldo ogółem | | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | | |
| JST | | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | | |
| Źródła finansowania | | | | | | | | | | | | | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Projektodawca nie przewiduje, aby wydanie rozporządzenia miało wpływ 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

| | | 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 | | | | | | | | |
| | 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 | Przedmiotowy projekt nie wpłynie na konkurencyjność gospodarki i przedsiębiorczości, w tym na funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe. | |
| 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). | <input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy | |
| <input type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur skrócenie czasu na załatwienie sprawy <input type="checkbox"/> inne: | <input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input type="checkbox"/> inne: | |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | <input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy | |
| Komentarz: | | |
| 9. Wpływ na rynek pracy | | |
| Wejście w życie rozporządzenia nie spowoduje zmian na rynku pracy. | | |
| 10. Wpływ na pozostałe obszary | | |
| <input type="checkbox"/> środowisko naturalne <input type="checkbox"/> sytuacja i rozwój regionalny <input type="checkbox"/> inne: | <input type="checkbox"/> demografia <input type="checkbox"/> mienie państwowe | <input type="checkbox"/> informatyzacja <input type="checkbox"/> 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 w momencie wejścia w życie rozporządzenia. Jednakże należy wskazać, iż w momencie wejścia w życie przedmiotowych regulacji w obrocie pozostaną umowy ubezpieczenia zawarte na podstawie dotychczas obowiązującego rozporządzenia Ministra Finansów w tej sprawie. Umowy te będą obowiązywały do końca okresu, na jaki zostały zawarte. Kolejne umowy ubezpieczenia zostaną zawarte na podstawie wydanego projektu rozporządzenia. | | |
| 12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane? | | |
| Ocena skutków wejścia w życie projektowanych przepisów będzie możliwa po okresie co najmniej 1 roku ich funkcjonowania gdyż umowy ubezpieczenia co do zasady zawierane są na okres 12 miesięcy. Jednakże należy pamiętać, iż okres przedawnienia roszczeń z tytułu przedmiotowych umów ubezpieczenia wynosi 3 lata. | | |
| 13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.) | | |
| | | |

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia

**w sprawie przeniesienia planowanych wydatków budżetowych, w tym wynagrodzeń,
określonych w ustawie budżetowej na rok 2016**

Na podstawie art. 137 ustawy z dnia ... o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z ... poz. ...) zarządza się, co następuje.

§ 1. Rozporządzenie określa przeniesienie planowanych wydatków budżetowych, w tym wynagrodzeń, między częściami 20 – Gospodarka i 27 – Informatyzacja.

§ 2. 1. Przenosi się planowane wydatki budżetowe, w tym wynagrodzenia, z części 20 – Gospodarka do części 27 – Informatyzacja w kwocie 80 179 zł.

2. Szczegółowy podział planowanych wydatków budżetowych, w tym wynagrodzeń, o których mowa w ust. 1, jest określony w załączniku nr 1 do rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

**Załącznik
do rozporządzenia
Prezesa Rady Ministrów
z dnia ... (poz. ...)**

**SZCZEGÓŁOWY PODZIAŁ PLANOWANYCH WYDATKÓW BUDŻETOWYCH, W
TYM KWOT WYNAGRODZEŃ**

| Część | Dział | Rozdział | Paragraf | Wyszczególnienie | Kwota w złotych | |
|-------|---------|-------------|----------|--|-----------------|-------------|
| | | | | | zmniejszenia | zwiększenia |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 20 | | | | Gospodarka | 80 179 | |
| | 150/750 | | | Przetwórstwo przemysłowe / Administracja publiczna | 80 179 | |
| | | 15095/75001 | | | 80 179 | |
| | | | 4000 | Grupa wydatków bieżących jednostki | 40 000 | |
| | | | 4020 | Wynagrodzenia osobowe członków korpusu służby cywilnej | 33 583 | |
| | | | 4110 | Składki na ubezpieczenia społeczne | 5 773 | |
| | | | 4120 | Składki na Fundusz Pracy | 823 | |
| 27 | | | | Informatyzacja | | 80 179 |
| | 750 | | | Administracja publiczna | | 80 179 |
| | | 75001 | | Urzędy naczelnych i centralnych organów administracji rządowej | | 80 179 |
| | | | 4000 | Grupa wydatków bieżących jednostki | | 40 000 |
| | | | 4020 | Wynagrodzenia osobowe członków korpusu służby cywilnej | | 33 583 |
| | | | 4110 | Składki na ubezpieczenia społeczne | | 5 773 |
| | | | 4120 | Składki na Fundusz Pracy | | 823 |

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 137 ustawy z dnia ... o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z ... poz. ...). Przepis ten upoważnia Prezesa Rady Ministrów do dokonania przeniesienia planowanych dochodów i wydatków budżetowych, w tym wynagrodzeń oraz limitów zatrudnienia, między częścią budżetu państwa, której dysponentem jest minister właściwy do spraw gospodarki, a częścią, której dysponentem jest minister właściwy do spraw informatyzacji, z zachowaniem przeznaczenia środków publicznych wynikających z ustawy budżetowej.

Projekt rozporządzenia, zgodnie z rozporządzeniem Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039 oraz z 2004 r. Nr 65, poz. 597), nie wymaga notyfikacji.

Projekt rozporządzenia, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingskiej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.), zostanie zamieszczony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

| | | | | | | | | | | | | |
|----------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | Projektodawca nie przewiduje, aby wydanie rozporządzenia miało wpływ na sektor finansów publicznych. W związku z tym, że wprowadzenie rozporządzenia spowoduje jedynie zmianę dysponenta dochodów i wydatków budżetowych, w tym wynagrodzeń oraz limitów zatrudnienia, nie wystąpi skutek w postaci zwiększenia wydatków lub zmniejszenia dochodów jednostek sektora finansów publicznych. |

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym na 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 ...) | 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 | Projektowane regulacje nie wpłyną na konkurencyjność gospodarki i przedsiębiorczość w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe. |
|--|--|

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). | <input type="checkbox"/> tak <input checked="" type="checkbox"/> nie nie dotyczy |
| <input type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur skrócenie czasu na załatwienie sprawy | <input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy |

| | |
|---|---|
| <input type="checkbox"/> inne: | <input type="checkbox"/> inne: |
| Wprowadzane obciążenia są przystosowane do ich elektroniczacji. | <input type="checkbox"/> tak <input type="checkbox"/> nie <input checked="" type="checkbox"/> nie dotyczy |

Komentarz:

9. Wpływ na rynek pracy

Wejście w życie rozporządzenia nie spowoduje zmian na rynku pracy.

10. Wpływ na pozostałe obszary

| | | |
|---|---|---|
| <input type="checkbox"/> środowisko naturalne | <input type="checkbox"/> demografia | <input type="checkbox"/> informatyzacja |
| <input type="checkbox"/> sytuacja i rozwój regionalny | <input type="checkbox"/> mienie państwowe | <input type="checkbox"/> zdrowie |
| <input type="checkbox"/> inne: | | |

| | |
|------------------|--|
| 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

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

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

**ROZPORZĄDZENIE
MINISTRA ROZWOJU¹⁾**

z dnia

w sprawie szczegółowego zakresu i warunków korzystania z pojedynczego punktu kontaktowego²⁾

Na podstawie art. 22g ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 584, z późn. zm.³⁾), zarządza się co następuje:

§ 1. 1. Ilekroć w rozporządzeniu jest mowa o:

- 1) ustawie – rozumie się przez to ustawę z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej,
- 2) ministrze – rozumie się przez to ministra właściwego do spraw gospodarki,
- 3) systemie teleinformatycznym – rozumie się przez to system teleinformatyczny punktu kontaktowego, znajdujący się w gestii ministra, służący do publikacji informacji na stronie internetowej punktu kontaktowego i umożliwienia za jego pośrednictwem realizacji procedur i formalności,
- 4) koncie – rozumie się przez to zespół uprawnień przyznanych danemu użytkownikowi w systemie teleinformatycznym lub elektronicznej platformie usług administracji publicznej, o której mowa w przepisach o informatyzacji działalności podmiotów realizujących zadania publiczne,
- 5) wniosku elektronicznym – rozumie się przez to dokument elektroniczny składany za pośrednictwem systemu teleinformatycznego,
- 6) użytkownikowi – rozumie się przez to osobę fizyczną, nie będącą przedstawicielem właściwego organu.

§ 2. 1. Realizacja zadań punktu kontaktowego odbywa się z wykorzystaniem funkcjonalności systemu teleinformatycznego.

2. System teleinformatyczny udostępnia następujące funkcjonalności:

- 1) dostęp do treści, opublikowanych na stronach internetowych punktu kontaktowego,

¹⁾ Minister Rozwoju kieruje działem administracji rządowej – gospodarka, na podstawie § 1 ust. 2 pkt. 1 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju (Dz. U. poz. 1895).

²⁾ Niniejsze rozporządzenie dokonuje w zakresie swojej regulacji wdrożenia dyrektywy 2006/123/WE Parlamentu i Rady dotyczącej usług na rynku wewnętrznym

³⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały zgłoszone w Dz. U. z 2015 r. poz. 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 i 1893 oraz z 2016 r. poz. 65, 352, 615, 780, 868 i ...

- 2) możliwość kontaktu z centrum pomocy punktu kontaktowego,
- 3) możliwość realizacji procedur i formalności.

3. Dostęp do możliwości wypełniania, przesyłania oraz śledzenia stanu realizacji wniosków elektronicznych oraz obierania korespondencji za pośrednictwem systemu teleinformatycznego wymaga rejestracji użytkownika i posiadania konta. System teleinformatyczny umożliwia użytkownikowi założenie, posiadania konta oraz jego usunięcie. Opis czynności związanych z rejestracją użytkownika, założeniem i likwidacją konta jest opublikowany na stronach internetowych punktu kontaktowego.

4. Każdy użytkownik może posiadać tylko jedno konto.

5. Użytkownik zobowiązany jest do zapewnienia aktualności podanego adresu poczty elektronicznej. Brak aktualności podanego adresu poczty elektronicznej użytkownika lub likwidacja konta uniemożliwi użytkownikowi otrzymywanie powiadomień o otrzymanej korespondencji.

6. Informacje opublikowane na stronach internetowych punktu kontaktowego mają charakter ogólny i nie są powszechnie obowiązującą wykładnią prawa. W celu uzyskania powyższej wykładni użytkownik może się zwrócić za pośrednictwem centrum pomocy punktu kontaktowego z odpowiednim wnioskiem do danego organu.

§ 3. 1. System teleinformatyczny udostępnia możliwość wyszukiwania w szczególności:

- 1) opisów procedur i formalności, jakie są niezbędne do załatwienia danej sprawy,
- 2) danych kontaktowych właściwych organów,
- 3) formularzy dotyczących poszczególnych procedur i formalności,

2. Centrum pomocy punktu kontaktowego udostępnia użytkownikowi za pośrednictwem systemu teleinformatycznego możliwość kontaktu w szczególności w formie:

- 1) czatu, czyli rozmowy prowadzonej w formie naprzemiennego przesyłania wiadomości tekstowych,
- 2) rozmowy głosowej za pośrednictwem sieci Internet przy wykorzystaniu odpowiedniej aplikacji,
- 3) rozmowy z wykorzystaniem języka migowego.

3. Centrum pomocy udostępnia także możliwość dwustronnego kontaktu za pośrednictwem połączeń telefonicznych.

4. Użytkownik może przekazać za pośrednictwem systemu teleinformatycznego sugestie dotyczące treści publikowanych na stronach internetowych punktu kontaktowego i funkcjonalności systemu teleinformatycznego.

5. Informacje opublikowane na stronach internetowych punktu kontaktowego mogą być udostępniane w językach obcych przy wykorzystaniu mechanizmu tłumaczenia maszynowego. Mechanizm tłumaczenia maszynowego nie zapewnia pełnej poprawności przetłumaczonego tekstu.

§ 4. 1. Możliwość realizacji procedur i formalności za pośrednictwem systemu teleinformatycznego polega na możliwości uzupełnienia za pomocą formularza treści pisma, podpisania go w sposób akceptowany przez system teleinformatyczny, umożliwiającą jednoznaczną identyfikację użytkownika oraz przekazania go drogą elektroniczną zgodnie z przepisami o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawą z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23, 868 i ...). Podpisane przez użytkownika pismo jest przekazywane do skrzynki podawczej danego organu na elektronicznej platformie usług administracji publicznej lub do innego systemu teleinformatycznego, zgodnie z art. 22b ust. 2 ustawy.

2. Pisma w postaci dokumentu elektronicznego, przesyłane za pośrednictwem systemu teleinformatycznego, mogą być podpisane przez użytkownika za pomocą kwalifikowanego podpisu elektronicznego, zgodnie z przepisami o usługach zaufania, lub za pomocą podpisu potwierdzonego profilem zaufanym ePUAP lub w inny sposób akceptowany przez system teleinformatyczny umożliwiającą jednoznaczną identyfikację użytkownika.

3. Pisma, będące odpowiedziami na pisma wysłane przez użytkownika, oraz urzędowe potwierdzenia odbioru doręczane użytkownikowi przez właściwe organy dostępne są w systemie teleinformatycznym.

4. Użytkownik otrzymuje powiadomienia związane z załatwieniem spraw drogą elektroniczną na adres poczty elektronicznej, związany z kontem.

5. Usunięcie przez użytkownika konta w systemie teleinformatycznym jest równoznaczne z usunięciem wszystkich danych użytkownika, w tym także pism wysłanych i odebranych przez użytkownika oraz urzędowych potwierdzeń odbioru. Po zlikwidowaniu konta w systemie teleinformatycznym użytkownik jest zobowiązany do poinformowania o zmianie swojego adresu do doręczeń organów właściwych prowadzących sprawy wszczęte przez użytkownika.

6. W niektórych przypadkach w celu załatwienia sprawy użytkownik może zostać przekierowany na adres innej strony internetowej niż strona internetowa punktu kontaktowego. Załatwienie sprawy odbywa się wówczas według przepisów odrębnych.

§ 5. 1. System teleinformatyczny gromadzi dane o aktywności i połączeniach użytkownika, w tym dane o których mowa w art. 173 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.⁴⁾).

2. Dane, o których mowa w ust. 1, wykorzystywane są w celach technicznych, statystycznych, do udokumentowania sposobu działania systemu teleinformatycznego i do promocji punktu kontaktowego.

3. Użytkownik zezwala na przechowywanie informacji zapisywanych przez system teleinformatyczny za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi

§ 6. Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

MINISTER ROZWOJU

⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 827 i 1198, z 2015 r. poz. 1069, 1893 i 2281 oraz z 2016 r. poz. 542 i ...

UZASADNIENIE

Projektowane rozporządzenie wykonuje upoważnienie ustawowe zawarte w art. 22g ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 589, z późn. zm.). Celem jego wprowadzenia jest uszczegółowienie zasad korzystania z pojedynczego punktu kontaktowego oraz wskazanie zakresu udostępnianych przez ministra właściwego do spraw gospodarki funkcjonalności systemu teleinformatycznego punktu kontaktowego.

W ramach projektu „Centralna Ewidencja i Informacja o Działalności Gospodarczej” Działanie „Elektroniczny Punkt Kontaktowy”, realizowanego w ramach 7 osi Programu Operacyjnego Innowacyjna Gospodarka przygotowano w systemie teleinformatycznym punktu kontaktowego funkcje pozwalające na:

- 1) udostępnianie użytkownikom publikowanych przez ministra i właściwe organy informacji na stronach internetowych punktu kontaktowego,
- 2) kontakt z centrum pomocy punktu kontaktowego, w celu uzyskania dodatkowych, szczegółowych informacji,
- 3) realizację procedur i formalności związanych z załatwieniem danej sprawy poprzez składanie wniosków elektronicznych oraz uzyskiwanie stanowiska właściwych organów, zgodnie z obowiązującymi przepisami prawa.

W § 1 zawarto definicje, jakie są stosowane w pozostałych przepisach niniejszego rozporządzenia.

W § 2 uregulowano sposób korzystania przez użytkowników z funkcjonalności punktu kontaktowego. Zwrócono uwagę, iż dla realizacji niektórych czynności wiążących się ze wzajemną komunikacją niezbędne jest posiadanie przez użytkownika konta oraz podanie aktualnego adresu poczty elektronicznej.

W § 3 opisano zakres funkcjonalności udostępnianych przez ministra właściwego do spraw gospodarki za pośrednictwem systemu teleinformatycznego punktu kontaktowego.

W § 4 określono sposób realizacji spraw i przesyłania pism za pomocą systemu teleinformatycznego punktu kontaktowego.

W § 5 określono zagadnienia związane z przetwarzaniem i wykorzystaniem danych o użytkownikach, a w szczególności zagadnienia związane z tzw. cookies.

W § 6 określono czas wejścia w życie rozporządzenia.

| | |
|---|---|
| <p>Nazwa projektu Rozporządzenie Ministra Rozwoju w sprawie w zakresie i warunków korzystania z elektronicznej platformy usług administracji publicznej</p> <p>Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Rozwoju</p> <p>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Tadeusz Kościński, Podsekretarz Stanu</p> <p>Kontakt do opiekuna merytorycznego projektu Sebastian Christow (sebastian.christow@mr.gov.pl) Dyrektor Departamentu Gospodarki Elektronicznej, Ministerstwo Rozwoju</p> | <p>Data sporządzenia 11 lipca 2016 r.</p> <p>Źródło: art. 22g ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 589, z późn. zm.).</p> |
|---|---|

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Rozporządzenie określi szczegółowy zakres i warunki korzystania z pojedynczego punktu kontaktowego, w tym w szczególności sposób potwierdzania pochodzenia i integralności danych udostępniony bezpłatnie przez pojedynczy punkt kontaktowy o którym mowa w art. 22b ust. 2a, ustawy o swobodzie działalności gospodarczej, z uwzględnieniem roli punktu kontaktowego w realizacji procedur związanych z podejmowaniem, wykonywaniem i zakończeniem działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, uznawaniem kwalifikacji zawodowych nabytych w państwach członkowskich Unii Europejskiej, świadczeniem usług transgranicznych i ubieganiem się o wydanie europejskiej legitymacji zawodowej oraz zasad przetwarzania i ochrony danych osobowych.

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

W ramach projektu „Centralna Ewidencja i Informacja o Działalności Gospodarczej” Działanie „Elektroniczny Punkt Kontaktowy”, realizowanego w ramach 7 osi Programu Operacyjnego Innowacyjna Gospodarka przygotowano w systemie teleinformatycznym punktu kontaktowego funkcje pozwalające na:

- 1) udostępnianie użytkownikom publikowanych przez ministra i właściwe organy informacji na stronach internetowych punktu kontaktowego,
- 2) kontakt z centrum pomocy punktu kontaktowego, w celu uzyskania dodatkowych, szczegółowych informacji,
- 3) realizację procedur i formalności związanych z załatwieniem danej sprawy poprzez składanie wniosków elektronicznych oraz uzyskiwanie stanowiska właściwych organów, zgodnie z obowiązującymi przepisami prawa.

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

n/d

4. Podmioty, na które oddziałuje projekt

| Grupa | Wielkość | Źródło danych | Oddziaływanie |
|-------|----------|---------------|---------------|
| | | | |
| | | | |

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

| |
|--|
| |
|--|

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 | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| Wydatki ogółem | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| Saldo ogółem | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| Źródła finansowania | | | | | | | | | | | | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | | | | | | | | | | | | |

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 | duże przedsiębiorstwa | 0 | | | | | | | |
| | sektor mikro-, małych i średnich przedsiębiorstw | 0 | | | | | | | |
| | rodzina, obywatele oraz gospodarstwa domowe | 0 | | | | | | | |
| 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

| | |
|--|---|
| | <input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |
| <input checked="" type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur <input checked="" type="checkbox"/> skrócenie czasu na załatwienie sprawy <input type="checkbox"/> inne: | <input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input type="checkbox"/> inne: |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | <input checked="" type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |
| <p>Komentarz: W § 3 uregulowano sposób korzystania przez użytkowników z funkcjonalności punktu kontaktowego. Zwrócono uwagę, iż dla realizacji niektórych czynności wiążących się ze wzajemną komunikacją niezbędne jest posiadanie przez użytkownika konta oraz podanie aktualnego adresu poczty elektronicznej.</p> | |
| <p>9. Wpływ na rynek pracy</p> | |
| Projektowane rozporządzenie nie będzie miało wpływu na rynek pracy. | |
| <p>10. Wpływ na pozostałe obszary</p> | |
| <input type="checkbox"/> środowisko naturalne <input type="checkbox"/> sytuacja i rozwój regionalny <input type="checkbox"/> inne: | <input type="checkbox"/> demografia <input type="checkbox"/> mienie państwowe |
| | <input checked="" type="checkbox"/> informatyzacja <input type="checkbox"/> zdrowie |
| Omówienie wpływu | Omówiono w pkt. 2. |
| <p>11. Planowane wykonanie przepisów aktu prawnego</p> | |
| Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia. | |
| <p>12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?</p> | |
| Z uwagi na ograniczony i techniczny zakres przedmiotowy projektu rozporządzenia ewaluacja nie jest planowana. | |
| <p>13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)</p> | |
| | |

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI¹⁾

z dnia

**w sprawie zakresu i warunków korzystania z elektronicznej platformy usług
administracji publicznej**

Na podstawie art. 19a ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352 i ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa zakres i warunki korzystania z elektronicznej platformy usług administracji publicznej, zwanej dalej „ePUAP”, w tym warunki organizacyjne i techniczne nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, zwanego dalej „podmiotem niepublicznym”.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

- 1) administrator podmiotu – użytkownika zarejestrowanego zarządzającego zasobami ePUAP posiadanymi przez podmiot;
- 2) certyfikat – certyfikat podpisu elektronicznego, o którym mowa w art. 3 pkt 14 rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 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 uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 74), zwanego dalej „rozporządzeniem eIDAS”;
- 3) identyfikator podmiotu – unikalny ciąg znaków alfanumerycznych jednoznacznie identyfikujących podmiot;
- 4) identyfikator użytkownika – unikalny ciąg znaków alfanumerycznych jednoznacznie identyfikujących użytkownika zarejestrowanego;
- 5) konto – dane opisujące podmiot albo użytkownika zarejestrowanego wraz z zasobami ePUAP przyporządkowanymi do tego podmiotu albo użytkownika;

¹⁾ Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1910 i 2090).

- 6) kwalifikowany certyfikat – kwalifikowany certyfikat podpisu elektronicznego, o którym mowa w art. 3 pkt 15 rozporządzenia eIDAS;
- 7) minister – ministra właściwego do spraw informatyzacji;
- 8) niezaprzeczalność – brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
- 9) rozliczalność działań – funkcję ePUAP umożliwiającą przypisanie w sposób jednoznaczny działania użytkownika lub podmiotu tylko temu użytkownikowi lub podmiotowi;
- 10) oznaczanie czasem – funkcję ePUAP umożliwiającą dołączanie oznaczenia czasu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym w chwili wykonania takiego dołączenia oraz poświadczenia elektronicznego tak powstałych danych przez ePUAP;
- 11) podmiot – osobę prawną, jednostkę organizacyjną nieposiadającą osobowości prawnej albo podmiot publiczny;
- 12) usługa – działanie podmiotu publicznego lub podmiotu, o którym mowa w art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, polegające na wykorzystaniu przez ten podmiot ePUAP do realizacji swoich ustawowych obowiązków;
- 13) usługodawca – podmiot publiczny lub podmiot, o którym mowa w art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, świadczący usługi przy użyciu ePUAP;
- 14) ustawa – ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- 15) użytkownik zarejestrowany – użytkownika posiadającego konto.

§ 3. 1. Utworzenie konta dla użytkownika wymaga podania następujących danych:

- 1) imienia (imion);
- 2) nazwiska;
- 3) numeru PESEL, jeżeli użytkownik posiada;
- 4) adresu poczty elektronicznej;
- 5) numeru telefonu komórkowego;
- 6) identyfikatora użytkownika.

2. W celu identyfikacji i uwierzytelnienia użytkownik zarejestrowany może zastosować:

- 1) określone przez użytkownika identyfikator użytkownika i hasło;

- 2) kwalifikowany certyfikat;
- 3) profil zaufany ePUAP;
- 4) środek identyfikacji elektronicznej stosowany do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego.

3. Stopień złożoności hasła, o którym mowa w ust. 2 pkt 1, kontroluje ePUAP.

4. Komunikaty związane z funkcjonowaniem konta przesyłane są na adres poczty elektronicznej podany przez użytkownika zarejestrowanego.

5. W przypadku zmiany danych, o których mowa w ust. 1 pkt 1–5, użytkownik zarejestrowany jest zobowiązany do niezwłocznego dokonania odpowiednich zmian w koncie.

6. Użytkownik zarejestrowany może usunąć swoje konto.

7. W przypadku utraty identyfikatora użytkownika lub hasła, o których mowa w ust. 2 pkt 1, użytkownik może wnioskować, za pośrednictwem ePUAP, o przesłanie na adres poczty elektronicznej użytkownika, o którym mowa w ust. 1 pkt 4, odpowiednio identyfikatora użytkownika albo hasła tymczasowego. Użytkownik po uwierzytelnieniu się za pomocą hasła tymczasowego określa nowe hasło, którego stopień złożoności kontroluje ePUAP.

§ 4. 1. Utworzenie konta dla podmiotu jest dokonywane przez użytkownika zarejestrowanego działającego w imieniu podmiotu i wymaga podania:

- 1) nazwy podmiotu;
- 2) identyfikatora podmiotu;
- 3) numeru REGON, jeżeli został nadany temu podmiotowi.

2. Użytkownik zarejestrowany, zakładając konto dla podmiotu, staje się administratorem podmiotu.

3. Identyfikator użytkownika i identyfikator podmiotu są wybierane przez użytkownika. Raz nadany identyfikator nie może być nadany ponownie.

4. W przypadku zmiany danych, o których mowa w ust. 1 pkt 1, użytkownik zarejestrowany działający w imieniu podmiotu niezwłocznie dokonuje ich zmiany w koncie.

5. Konto podmiotu może usunąć administrator tego podmiotu albo minister na wniosek podmiotu.

§ 5. 1. Podmiot publiczny występuje do ministra z wnioskiem o nadanie funkcjonalności podmiotu publicznego na ePUAP.

2. Wniosek, o którym mowa w ust. 1, zawiera:

- 1) oznaczenie podmiotu publicznego;

- 2) imię i nazwisko osoby upoważnionej do reprezentacji podmiotu publicznego wraz z podaniem funkcji lub stanowiska;
- 3) dane administratora podmiotu.

3. Funkcjonalność podmiotu publicznego na ePUAP staje się dostępna po pozytywnym rozpatrzeniu wniosku przez ministra.

4. Podmiotowi, o którym mowa w art. 19c ust. 1 ustawy, funkcjonalność podmiotu publicznego na ePUAP jest nadawana na podstawie porozumienia, o którym mowa w art. 19c ust. 2 ustawy, w celu jego realizacji.

5. Podmiotowi, o którym mowa w art. 20c ust. 3 pkt 2–4 ustawy, funkcjonalność podmiotu publicznego na ePUAP jest nadawana na podstawie zgody ministra właściwego do spraw informatyzacji, o której mowa w art. 20c ust. 3 ustawy, w celu potwierdzania profilu zaufanego ePUAP.

6. Nadanie funkcjonalności podmiotu publicznego na ePUAP stanowi czynność materialno-techniczną.

§ 6. Użytkownik zarejestrowany może działać w imieniu różnych podmiotów.

§ 7. 1. Rozwiązania techniczne ePUAP zapewniają niezaprzeczalność następujących wystawionych poświadczeń:

- 1) urzędowego poświadczenia odbioru;
- 2) elektronicznego poświadczenia opłaty;
- 3) oznaczania czasem;
- 4) weryfikacji podpisu elektronicznego;
- 5) weryfikacji zgodności dokumentu elektronicznego z jego wzorem.

2. Minister informuje na ePUAP o przerwach serwisowych w świadczeniu usług, wynikających z potrzeby dokonywania zmian i ulepszeń, a w przypadku braku takiej możliwości – przez zamieszczenie informacji o takich przerwach w Biuletynie Informacji Publicznej.

§ 8. Platforma ePUAP udostępnia katalog usług zawierający informacje o usługach, a w szczególności:

- 1) podstawę prawną usługi;
- 2) nazwę usługi;
- 3) nazwę usługodawcy;
- 4) cel usługi;
- 5) odbiorców usługi;

- 6) kategorię usługi;
- 7) umiejscowienie usługodawcy według podziału administracyjnego kraju.

§ 9. 1. Podmioty publiczne mogą wykorzystywać do świadczenia usług w postaci elektronicznej w szczególności następujące funkcje ePUAP:

- 1) tworzenie i obsługa dokumentów elektronicznych przez osoby fizyczne i podmioty;
- 2) przesyłanie dokumentów elektronicznych;
- 3) wymiana danych między ePUAP a innymi systemami teleinformatycznymi;
- 4) identyfikacja użytkowników i rozliczalność ich działań;
- 5) weryfikacja podpisu elektronicznego;
- 6) tworzenie usług podmiotu publicznego lub usług kilku podmiotów publicznych współdziałających ze sobą, zbudowanych na podstawie dwóch lub więcej usług;
- 7) obsługa płatności elektronicznych;
- 8) potwierdzanie profilu zaufanego ePUAP.

2. Podmioty, o których mowa w art. 19c ust. 1 ustawy, w celu realizacji porozumienia, o którym mowa w art. 19c ust. 2 ustawy, mogą wykorzystywać funkcje ePUAP, o których mowa w ust. 1.

3. Podmioty, o których mowa w art. 20c ust. 3 pkt 2–4 ustawy, w celu potwierdzania profilu zaufanego ePUAP mogą wykorzystywać funkcje ePUAP, o których mowa w ust. 1.

§ 10. 1. Platforma ePUAP może wymieniać informacje z innymi systemami teleinformatycznymi podmiotów określonych w art. 2 ust. 1 i 2, w art. 19c ust. 1 ustawy oraz podmiotów niepublicznych.

2. Do wymiany informacji, o których mowa w ust. 1, mają zastosowanie przepisy wydane na podstawie art. 18 pkt 2 ustawy.

3. Minister zapewnia bezpieczeństwo wymiany informacji określonych w ust. 1 przez wydanie, na wniosek podmiotu, o którym mowa w ust. 1, certyfikatu dla systemu teleinformatycznego, o którym mowa w ust. 1.

4. Wydanie certyfikatu, o którym mowa w ust. 3, stanowi czynność materialno-techniczną.

§ 11. 1. Wykorzystanie w ePUAP środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, 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 i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 9.09.2015, s. 7);

- 2) opracowania i ustanawiania, wdrażania i eksploataowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy;
- 3) poddawania się przez podmiot niepubliczny audytowi sprawdzającemu spełnienie wymagań, o których mowa w pkt 1 i 2 przez niezależną trzecią stronę nie rzadziej niż raz w roku;
- 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 osobistego stawiennictwa dowodu osobistego albo paszportu zawierającego numer PESEL,
 - b) danych pochodzących z poprawnie przeprowadzonej weryfikacji kwalifikowanego podpisu elektronicznego przy użyciu którego osoba ta podpisała dokument elektroniczny, w którym oświadczyła, iż świadoma jest warunków i zalecanych środków zaufania związanych z korzystaniem z systemu identyfikacji elektronicznej oraz wyraziła zgodę na nadanie statusu użytkownika tego systemu oraz wykorzystywanie udostępnionych środków identyfikacji elektronicznej w systemie ePUAP.

2. Minister udostępnia podmiotowi niepublicznemu wymagania techniczne dla wymiany danych pomiędzy systemem teleinformatycznym tego podmiotu a ePUAP po potwierdzeniu przez ten podmiot spełniania warunków, o których mowa w ust. 1.

3. Minister może dokonać weryfikacji spełniania przez podmiot niepubliczny wymagań technicznych, o których mowa w ust. 2.

4. Wykorzystywanie w ePUAP środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, realizowane jest na podstawie porozumienia zawartego pomiędzy ministrem a podmiotem niepublicznym.

§ 12. Konta ePUAP założone przed dniem wejścia w życie rozporządzenia stają się kontami w rozumieniu przepisów niniejszego rozporządzenia.

§ 13. Wnioski o nadanie funkcjonalności podmiotu publicznego złożone przed dniem wejścia w życie niniejszego rozporządzenia rozpatruje się na podstawie przepisów dotychczasowych.

§ 14. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

- 1) § 3 ust. 1 pkt 1 w zakresie podawania drugiego imienia oraz § 3 ust. 2 pkt 3, które wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia;
- 2) § 3 ust. 2 pkt 4, który wchodzi w życie z dniem 25 września 2016 r.²⁾

MINISTER CYFRYZACJI

²⁾ Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 5 czerwca 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. poz. 584), które traci moc z dniem wejścia w życie ustawy z dnia ... o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw (Dz. U. ...).

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego określonego w art. 19a ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352 i ...), zwanej dalej „ustawą o informatyzacji”.

Konieczność przygotowania przedmiotowego rozporządzenia wynika z faktu, iż w drodze ustawy o usługach zaufania oraz identyfikacji elektronicznej zmieniającej m. in. ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne, zmianie ulega treść przepisu stanowiącego upoważnienie ustawowe do wydania niniejszego aktu wykonawczego.

Ponadto konieczność przygotowania rozporządzenia jest związana z jednoczesnym przyjęciem zmian wprowadzanych rozporządzeniem Ministra Cyfryzacji w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej. Profil zaufany ePUAP stanowi integralną część ePUAP, stąd dokonanie zmian w funkcjonalności oraz w procedurach związanych z profilem zaufanym ePUAP wiąże się z koniecznością dokonania odpowiednich zmian także w rozporządzeniu w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej. Projekt przewiduje nadto wprowadzenie regulacji dotyczących poprawy funkcjonalności ePUAP.

Jednocześnie należy wskazać, iż przedmiotowe rozporządzenie określając w proponowanym projekcie zakres i warunki korzystania z elektronicznej platformy usług administracji publicznej, zwanej dalej „ePUAP”, z uwzględnieniem roli ePUAP w procesie realizacji zadań publicznych drogą elektroniczną oraz zasad przetwarzania i ochrony danych osobowych jest w swojej treści tożsame w stosunku do aktualnie obowiązującego rozporządzenia Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. poz. 584), za wyjątkiem poniżej wskazanych zmian.

W projektowanym rozporządzeniu proponuje się zmianę definicję kwalifikowanego certyfikatu rozumianego dotychczas jako kwalifikowany certyfikat, o którym mowa w art. 3 pkt 12 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, na kwalifikowany certyfikat podpisu elektronicznego, o którym mowa w art. 3 pkt 15 rozporządzenia

Parlamentu Europejskiego i Rady (EU) Nr 920/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (dalej zwane eIDAS).

W przedmiotowym projekcie preredagowano definicję certyfikatu i wskazano, iż jest to certyfikat podpisu elektronicznego, o którym mowa w art. 3 pkt 14 eIDAS.

Ponadto nowe brzmienie otrzymała definicja konta, która wskazuje, iż kontem są dane opisujące podmiot albo użytkownika wraz z zasobami ePUAP przyporządkowanymi do tego podmiotu albo użytkownika. W związku z przebudowaniem tej definicji z rozporządzenia zostały usunięte pojęcia profil podmiotu i profil użytkownika.

W tym miejscu należy wskazać, iż przeważająca większość usług elektronicznych świadczonych przez podmioty publiczne za pośrednictwem ePUAP wymaga od obywatela opatrzenia wnoszonych dokumentów podpisem elektronicznym. Możliwość odebrania dokumentów elektronicznych doręczanych przez organy administracji publicznej przy użyciu ePUAP również uzależniona jest od posiadania podpisu elektronicznego. W związku z powyższym uznano, iż procedura utworzenia konta na ePUAP będzie uwzględniała dane niezbędne do złożenia wniosku o nadanie statusu pozwalającego użytkownikowi na posługiwanie się podpisem potwierdzonym profilem zaufanym ePUAP. Zakłada się, że te dwie procedury tj. utworzenia konta w systemie ePUAP oraz składania wniosku o potwierdzenie profilu zaufanego ePUAP będą połączone. W związku z powyższym w § 3 ust. 1 uzupełniono, że utworzenie konta dla użytkownika wymaga podania dotychczas nieuwzględnionych danych: numeru PESEL, numeru telefonu komórkowego.

Ponadto wskazano, iż przy utworzeniu konta możliwe będzie podanie imion (nie jak dotychczas jedynie imienia), jeżeli użytkownik posiada więcej niż jedno imię.

Natomiast w przypadku konta dla podmiotu konieczne będzie podanie, oprócz dotychczas wymaganych danych, numeru REGON, jeżeli został nadany temu podmiotowi (§ 4 ust. 1). Zmiana ta pozwoli na referencyjne pobranie uzupełniających danych dotyczących podmiotu publicznego z rejestru REGON.

Celem zapewnienia możliwości niezwłocznego informowania użytkownika o istotnych zdarzeniach zaistniałych w systemie ePUAP w rozporządzeniu wprowadzono przepis § 3 ust. 4, zgodnie z którym komunikaty związane z funkcjonowaniem konta w ePUAP przesyłane będą na adres poczty elektronicznej użytkownika.

Profil zaufany ePUAP stanowi rekomendowane narzędzie identyfikacji

i uwierzytelniania użytkowników w publicznych systemach teleinformatycznych. Wobec powyższego, również funkcjonalność ePUAP rozszerzono o możliwość identyfikacji i uwierzytelniania przy użyciu profilu zaufanego ePUAP i w związku z tym w § 3 ust. 2 rozporządzenia wprowadzono stosowną zmianę.

Ponadto w § 3 ust. 7 uregulowano kwestię możliwości odzyskania przez użytkownika zapomnianego identyfikatora użytkownika lub hasła za pośrednictwem ePUAP. W takim przypadku identyfikator użytkownika lub hasło tymczasowe zostanie przesłane użytkownikowi na adres poczty elektronicznej użytkownika.

W § 10 ust. 1 rozporządzenia wprowadzono również zmianę o charakterze doprecyzującym i wyjaśniającym wątpliwości, które pojawiały się w związku ze stosowaniem rozporządzenia, w zakresie odnoszącym się do wymiany informacji pomiędzy systemem ePUAP a innymi systemami teleinformatycznymi podmiotów, o których mowa w art. 19c ust. 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Ponadto wskazano, iż platforma ePUAP może wymieniać informacje z systemami teleinformatycznymi banków krajowych lub innego przedsiębiorcy.

Ponadto w rozporządzeniu określono warunki organizacyjne i techniczne nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy. Wykorzystanie w ePUAP środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, realizowane będzie na podstawie porozumienia zawartego pomiędzy ministrem a podmiotem niepublicznym.

Projektowane rozporządzenie nie jest objęte zakresem prawa 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. Nr 239, poz. 2039, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.

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

| | |
|---|---|
| <p>Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie w zakresie i warunków korzystania z elektronicznej platformy usług administracji publicznej</p> <p>Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji</p> <p>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Podsekretarz Stanu Piotr Woźny</p> <p>Kontakt do opiekuna merytorycznego projektu Justyna Duszyńska Justyna.Duszyńska@mc.gov.pl Zastępca Dyrektora w Departamencie e-Państwa</p> | <p>Data sporządzenia 23 maja 2016 r.</p> <p>Źródło: Upoważnienie ustawowe – art. 19a ust. 3 ustawy z dnia 17 lutego 2005 r. <i>o informatyzacji działalności podmiotów realizujących zadania publiczne</i> (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352 i ...).</p> <p>Nr w wykazie: 37</p> |
|---|---|

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Niespójność przepisów krajowych z przepisami *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 uchylające dyrektywę 1999/93/WE (eIDAS)*.

Wykorzystanie przez obywateli usług elektronicznych udostępnionych na ePUAP pozostaje wciąż na poziomie nieadekwatnym do potencjału przedmiotowego systemu teleinformatycznego. Wobec powyższego Minister Cyfryzacji podejmuje działania zmierzające do optymalizacji funkcjonalności oraz ułatwień w obsłudze ePUAP. Zmiany w systemie ePUAP wymagają jednoczesnego wprowadzenia zmian w przepisach regulujących jego funkcjonowanie.

Brak określenia warunków organizacyjnych i technicznych nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy.

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

Efektom zmian ma być dostosowanie przepisów krajowych do *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 uchylające dyrektywę 1999/93/WE (eIDAS)*.

Wprowadzane jest uproszczenie dla nowych użytkowników polegające na połączeniu procedury utworzenia konta na ePUAP z procedurą wnioskowania o potwierdzenie profilu zaufanego ePUAP. Powyższe czynności w rezultacie dokonanych zmian będą realizowane przez obywatela poprzez wypełnienie pojedynczego formularza elektronicznego.

Wprowadzana jest zasada zgodnie, z którą komunikaty związane z funkcjonowaniem konta będą przesyłane na wskazany przez użytkownika adres poczty elektronicznej.

Zmiany w systemie ePUAP i optymalizacja procesów realizowane są poprzez wydzielenie, pod względem technicznym, profilu zaufanego ePUAP w ramach systemu ePUAP.

Określono warunki organizacyjne i techniczne nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy.

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

n/d

4. Podmioty, na które oddziałuje projekt

| Grupa | Wielkość | Źródło danych | Oddziaływanie |
|----------------|----------------------|---------------|--------------------------|
| osoby fizyczne | 100% obywateli, jako | EUROSTAT | Oddziaływania w zakresie |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|----|----------------|--|--|--|--|
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| Wydatki ogółem | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| Saldo ogółem | | | | | | | | | | | | |
| budżet państwa | | | | | | | | | | | | |
| JST | | | | | | | | | | | | |
| pozostałe jednostki (oddzielnie) | | | | | | | | | | | | |
| Źródła finansowania | Sfinansowanie wydatków wynikających z projektu rozporządzenia będzie się odbywało ze środków budżetu państwa będących w dyspozycji Ministra Cyfryzacji, w ramach limitu wydatków ustalanego corocznie, bez konieczności jego dodatkowego zwiększania. | | | | | | | | | | | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | | | | | | | | | | | | |
| 7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym na 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 | duże przedsiębiorstwa | 0 | | | | | | | | | | |
| | sektor mikro-, małych i średnich przedsiębiorstw | 0 | | | | | | | | | | |
| | rodzina, obywatele oraz gospodarstwa domowe | 0 | | | | | | | | | | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | | | | | | | | | | | | |

| 8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu | |
|---|---|
| <input type="checkbox"/> nie dotyczy | |
| Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). | <input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |
| <input type="checkbox"/> zmniejszenie liczby dokumentów <input checked="" type="checkbox"/> zmniejszenie liczby procedur <input checked="" type="checkbox"/> skrócenie czasu na załatwienie sprawy <input checked="" type="checkbox"/> inne: | <input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input type="checkbox"/> inne: |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | <input checked="" type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy |
| <p>Komentarz: Projekt zakłada rozszerzenie zakresu danych przekazywanych w trakcie procedury utworzenia konta na ePUAP w stosunku do danych, które są wskazywane przez użytkownika w aktualnym stanie prawnym. Utworzenie konta będzie wymagać podania dodatkowo: numeru PESEL oraz numeru telefonu komórkowego. Podanie wymienionych wyżej danych wynika z faktu, iż ta procedura na ePUAP będzie połączona z procedurą wnioskowania o potwierdzenie profilu zaufanego ePUAP, do którego ww. dane są wymagane. Ponadto projekt zakłada rozszerzenie zakresu danych przekazywanych przy utworzeniu konta dla podmiotu (numer REGON). Zmiana ta pozwoli na referencyjne pobranie uzupełniających danych dotyczących podmiotu publicznego z rejestru REGON.</p> | |
| 9. Wpływ na rynek pracy | |
| Projektowane rozporządzenie nie będzie miało wpływu na rynek pracy. | |
| 10. Wpływ na pozostałe obszary | |
| <input type="checkbox"/> środowisko naturalne <input type="checkbox"/> sytuacja i rozwój regionalny <input type="checkbox"/> inne: | <input type="checkbox"/> demografia <input type="checkbox"/> mienie państwowe <input checked="" type="checkbox"/> informatyzacja <input type="checkbox"/> zdrowie |
| Omówienie wpływu | Omówiono w pkt. 2. |
| 11. Planowane wykonanie przepisów aktu prawnego | |
| <p>Od wejścia w życie, z wyjątkiem § 3 pkt 1 w zakresie podawania drugiego imienia oraz § 3 ust. 2 pkt 3, które wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia oraz § 3 ust. 2 pkt 4, który wchodzi w życie z dniem 25 września 2016 r. System teleinformatyczny ePUAP będzie zapewniał modyfikacje wynikające z projektu rozporządzenia w dniu wejścia w życie przepisów.</p> | |
| 12. jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane? | |
| Z uwagi na ograniczony i techniczny zakres przedmiotowy projektu rozporządzenia ewaluacja nie jest planowana. | |
| 13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.) | |
| | |