Opracowano na podstawie: t.j. Dz. U. z 2021 r. poz. 1797, z 2023 r. poz. 1234.

U S T A W A

z dnia 5 września 2016 r.

o usługach zaufania oraz identyfikacji elektronicznej[1)]

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;
5) krajowy schemat identyfikacji elektronicznej;
6) nadzór nad krajowym schematem identyfikacji elektronicznej;
7) zasady określania i wykorzystywania standardu usługi rejestrowanego doręczenia elektronicznego.

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.

Rozdział 2

Krajowa infrastruktura zaufania

Art. 2. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje:

[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 257 z 28.08.2014, str. 73).

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

Art. 3. 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. 10 ust. 1 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 2020 r. poz. 1228 i 2320 oraz z 2021 r. poz. 1080, 1177 i 1598) oraz datę zakończenia postępowania upadłościowego;
14) datę wykreślenia z rejestru dostawcy usług zaufania.

Art. 4. 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. 3 ust. 4 pkt 1–7.

3. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej formularz 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:

1) raport z oceny zgodności, o którym mowa w art. 21 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”, 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. 10 ust. 1 pkt 1.

5. Do wniosku o wpis, o którym mowa w ust. 1, można dołączyć kopie dokumentów, o których mowa w ust. 4 pkt 1–3.

6. 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.

7. Decyzja o wpisie, o której mowa w ust. 6, zawiera informacje podlegające wpisowi do rejestru.

Art. 5. 1. Decyzja, o której mowa w art. 4 ust. 6, jest podstawą do wydania certyfikatu, o którym mowa w art. 10 ust. 1 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. 6. 1. Wpis do rejestru:

1) niekwalifikowanego dostawcy usług 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. 3 ust. 4 pkt 1–6.

Art. 7. 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. 8. 1. Minister właściwy do spraw informatyzacji wykreśla kwalifikowanego dostawcę usług zaufania lub świadczoną przez niego kwalifikowaną 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. 10 ust. 1 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 kwalifikowanego dostawcę usług zaufania.

5. Decyzja o wykreśleniu, o której mowa w ust. 1, jest podstawą wykreślenia dostawcy usług zaufania z zaufanej listy oraz może być podstawą do unieważnienia certyfikatów, o których mowa w art. 10 ust. 1 pkt 1.

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

Art. 9. 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 2019 r. poz. 2325, z 2020 r. poz. 2299 i 2320 oraz z 2021 r. poz. 54, 159 i 1598) 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. 10. 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 usług 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. 11. 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. 10, jak również do prowadzenia rejestru i zaufanej listy.

2. W przypadku upoważnienia do realizacji zadań, o których mowa w art. 10, 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. 10, 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. 12. 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 usług 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. 13. 1. Kwalifikowany dostawca usług zaufania jest obowiązany zawrzeć umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania, w terminie 30 dni od dnia dokonania wpisu kwalifikowanej usługi zaufania do rejestru, nie później niż jeden dzień przed dniem rozpoczęcia świadczenia tej usługi.

2. 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.

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

4. 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. 14. Kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany:

1) uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie;
2) poinformować osobę ubiegającą się o certyfikat o procedurze zgłaszania żądań unieważnienia kwalifikowanego certyfikatu.

Art. 15. 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. 16. 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. 17. 1. Kwalifikowany dostawca usług zaufania przechowuje następujące dokumenty i dane związane ze świadczeniem usług zaufania:
1) potwierdzenie, o którym mowa w art. 14 pkt 1,
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. 18. 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 elektronicznej weryfikowanych tym certyfikatem złożonych w trakcie zawieszenia następuje z chwilą uchylenia tego zawieszenia.

Art. 19. 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.

4. Kwalifikowany dostawca usług zaufania zapewnia możliwość całodobowego zgłaszania żądań unieważnienia kwalifikowanych certyfikatów.

Art. 20. 1. W przypadku gdy kwalifikowany dostawca usług zaufania utracił status kwalifikowany i żaden inny kwalifikowany dostawca usług zaufania nie przejął jego działalności w zakresie świadczenia usług zaufania, przekazuje on dokumenty i dane, o których mowa w art. 17 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. 17 ust. 1, do końca okresu, o którym mowa w art. 17 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. 21. 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

Krajowy schemat identyfikacji elektronicznej

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

1) węzeł krajowy identyfikacji elektronicznej, zwany dalej „węzłem krajowym”;
2) przyłączone do węzła krajowego:
   a) systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej,
   b) systemy teleinformatyczne, w których udostępniane są usługi online;
3) węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, zwany dalej „węzłem transgranicznym”.

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

3. Wykorzystywanie środka identyfikacji elektronicznej do uwierzytelnienia użytkownika systemu teleinformatycznego w celu realizacji usługi online świadczonej przez podmiot, o którym mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 670, 952, 1005 i 1641), lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014, jest nieodpłatne.

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

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

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

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

– w celu uwierzytelnienia z wykorzystaniem węzła krajowego.

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

1) potwierdzeniu spełnienia przez ten system wymagań dla zadeklarowanych poziomów bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie, określonych w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014;
2) przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność systemów identyfikacji elektronicznej, z uwzględnieniem przepisów wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014;
3) zapewnieniu przez podmiot odpowiedzialny za ten system opracowania, ustanawiania, wdrażania, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
4) przedstawieniu przez podmiot odpowiedzialny za ten system dokumentu zawierającego przyrzeczenie zakładu ubezpieczeń zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej wnioskodawcy;
5) przedstawieniu przez podmiot odpowiedzialny za ten system oświadczenia o działaniu tego podmiotu zgodnie z przepisami o ochronie danych osobowych;
6) uzyskaniu pozytywnej opinii Szefa Agencji Bezpieczeństwa Wewnętrznego w przypadku, o którym mowa w art. 21g ust. 6.

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

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

Art. 21c. 1. Ubezpieczeniem, o którym mowa w art. 21b ust. 2, jest objęta odpowiedzialność cywilna podmiotu odpowiedzialnego za system identyfikacji elektronicznej za szkodę wynikającą z działania lub zaniechania, wyrządzoną w związku z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej, w usłudze online świadczonej przez podmiot, o którym mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014, spowodowaną przez awarię, przerwę lub błąd systemu lub przez zaciągnięcie zobowiązania w wyniku nieuprawnionego wykorzystania tego środka identyfikacji elektronicznej.

2. Ubezpieczenie, o którym mowa w art. 21b ust. 2, nie obejmuje szkód:

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

– chyba że w umowie ubezpieczenia zakres ochrony ubezpieczeniowej zostanie rozszerzony również o szkody wynikające ze zdarzeń wskazanych w pkt 1–3.

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

Art. 21ca. 1. Podmiot odpowiedzialny za system identyfikacji elektronicznej ponosi odpowiedzialność cywilną za szkodę wynikającą z działania lub zaniechania, wyrządzoną w związku z wykorzystaniem środka identyfikacji elektronicznej, w celu uwierzytelnienia użytkowników systemów określonych w art. 21a ust. 1 pkt 2 lit. b, korzystających z usługi online świadczonej przez podmiot, o którym mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014, spowodowaną przez awarię, przerwę lub błąd systemu lub przez zaciągnięcie zobowiązania w wyniku nieuprawnionego

wykorzystania tego środka identyfikacji elektronicznej do wysokości 2 000 000 euro w odniesieniu do wszystkich zdarzeń w danym roku.

2. Ograniczenia odpowiedzialności do wysokości wskazanej w ust. 1 nie stosuje się w przypadku transgranicznego uwierzytelniania osób, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014.

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

2. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wysokość kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej, o której mowa w art. 21ca ust. 1, w odniesieniu do jednego zdarzenia, w zależności od poziomu bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie, kierując się potrzebą zapewnienia zaufania do uwierzytelnienia z wykorzystaniem środków identyfikacji elektronicznej.

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

1) korzystać ze środka identyfikacji elektronicznej zgodnie z warunkami określonymi przez podmiot odpowiedzialny za system identyfikacji elektronicznej, w którym został wydany ten środek;
2) zgłaszać niezwłocznie podmiotowi odpowiedzialnemu za system identyfikacji elektronicznej, w którym został wydany ten środek, utratę, kradzież,

przywłaszczenie środka identyfikacji elektronicznej lub utratę wyłącznej kontroli nad danymi umożliwiającymi identyfikację przy użyciu tego środka albo stwierdzenie nieuprawnionego użycia środka identyfikacji elektronicznej.

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

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

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

2. Wniosek zawiera:

1) imię i nazwisko lub firmę (nazwę), adres siedziby i miejsca wykonywania działalności, numer w Krajowym Rejestrze Sądowym, a w przypadku gdy podmiot nie posiada numeru w Krajowym Rejestrze Sądowym, wskazanie organu, któremu działalność podmiotu została zgłoszona, lub właściwego rejestru oraz podanie numeru identyfikacyjnego, jeżeli został on nadany, podmiotu odpowiedzialnego za system identyfikacji elektronicznej;
2) imię i nazwisko lub firmę (nazwę), adres siedziby i miejsca wykonywania działalności, numer w Krajowym Rejestrze Sądowym, a w przypadku gdy podmiot nie posiada numeru w Krajowym Rejestrze Sądowym, wskazanie organu, któremu działalność podmiotu została zgłoszona, lub właściwego rejestru oraz podanie numeru identyfikacyjnego, jeżeli został on nadany, każdego podmiotu:
   a) potwierdzającego tożsamość oraz weryfikującego dane identyfikujące osoby ubiegającej się o wydanie środka identyfikacji elektronicznej,
   b) wydającego środki identyfikacji elektronicznej,

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

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

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

3. Do wniosku dołącza się:

1) dokument potwierdzający spełnianie wymagań dla zadeklarowanych poziomów bezpieczeństwa środków identyfikacji elektronicznej, określonych w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014, w szczególności:
   a) pozytywny wynik audytu systemu zarządzania bezpieczeństwem informacji obejmującego swym zakresem system identyfikacji elektronicznej, którego dotyczy wniosek, albo
   b) pozytywny wynik audytu, o którym mowa w przepisach wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014

   – adekwatnie do poziomu bezpieczeństwa środków identyfikacji elektronicznej wydawanych w tym systemie;
2) dokument zawierający przyrzeczenie zakładu ubezpieczeń zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej wnioskodawcy;
3) oświadczenie o zapewnieniu stosowania polityki bezpieczeństwa, o której mowa w art. 39b ust. 1 pkt 3;
4) oświadczenie o działaniu podmiotu zgodnie z przepisami o ochronie danych osobowych.

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

5. Minister właściwy do spraw informatyzacji informuje Szefa Agencji Bezpieczeństwa Wewnętrznego o wpłynięciu wniosku, o którym mowa w ust. 1, w celu umożliwienia Szefowi Agencji Bezpieczeństwa Wewnętrznego dokonania

oceny, czy podmiot odpowiedzialny za system identyfikacji elektronicznej lub podmiot, o którym mowa w ust. 2 pkt 2, znajdują się pod kontrolą korporacyjną, w tym faktycznym wpływem innego państwa, jego podmiotu lub obywatela tego państwa, a w przypadku znajdowania się pod taką kontrolą, w celu ustalenia, czy może zagrażać bezpieczeństwu państwa, w tym bezpieczeństwu ekonomicznemu państwa.

6. Szef Agencji Bezpieczeństwa Wewnętrznego może przeprowadzić postępowanie w celu dokonania oceny, o której mowa w ust. 5, o czym informuje ministra właściwego do spraw informatyzacji w terminie 7 dni od dnia otrzymania informacji o wpłynięciu wniosku.

7. Kontrolą korporacyjną, o której mowa w ust. 5, są wszelkie formy bezpośredniego lub pośredniego uzyskania przez podmiot uprawnień, które osobno albo łącznie, przy uwzględnieniu wszystkich okoliczności prawnych i faktycznych, umożliwiają wywieranie decydującego wpływu na podmiot odpowiedzialny za system identyfikacji elektronicznej lub podmiot, o którym mowa w ust. 2 pkt 2, a w szczególności w przypadku:

1) dysponowania bezpośrednio lub pośrednio większością głosów na zgromadzeniu wspólników albo na walnym zgromadzeniu, także jako zastawnik albo użytkownik, bądź w zarządzie innego podmiotu (podmiotu zależnego), także na podstawie porozumień z innymi osobami;
2) uprawnienia do powoływania lub odwoływania większości członków zarządu lub rady nadzorczej innego podmiotu (podmiotu zależnego), także na podstawie porozumień z innymi osobami;
3) gdy członkowie jego zarządu lub rady nadzorczej stanowią więcej niż połowę członków zarządu innego podmiotu (podmiotu zależnego);
4) dysponowania bezpośrednio lub pośrednio większością głosów w spółce osobowej zależnej albo na walnym zgromadzeniu spółdzielni zależnej, także na podstawie porozumień z innymi osobami;
5) dysponowania prawem do całego albo do części mienia innego podmiotu (podmiotu zależnego);
6) umów przewidujących zarządzanie innym podmiotem (podmiotem zależnym) lub przekazywanie zysku przez taki podmiot.

8. W przypadku wszczęcia przez Szefa Agencji Bezpieczeństwa Wewnętrznego postępowania w celu dokonania oceny, o której mowa w ust. 5, minister właściwy do

spraw informatyzacji wzywa podmiot odpowiedzialny za system identyfikacji elektronicznej do przekazania danych niezbędnych do przeprowadzenia postępowania w stosunku do tego podmiotu lub podmiotu, o którym mowa w ust. 2 pkt 2.

9. Podmiot odpowiedzialny za system identyfikacji elektronicznej na żądanie ministra właściwego do spraw informatyzacji obowiązany jest przekazać dane i dokumenty niezbędne do przeprowadzenia postępowania w celu dokonania oceny, o której mowa w ust. 5.

10. Agencja Bezpieczeństwa Wewnętrznego po przeprowadzeniu postępowania w celu dokonania oceny, o której mowa w ust. 5, wydaje pozytywną opinię, jeżeli podmiot odpowiedzialny za system identyfikacji elektronicznej lub podmiot, o którym mowa w ust. 2 pkt 2:

1) nie znajduje się pod kontrolą korporacyjną innego państwa, jego podmiotu lub obywatela tego państwa, albo
2) znajduje się pod kontrolą korporacyjną innego państwa, jego podmiotu lub obywatela tego państwa, ale kontrola ta nie zagraża bezpieczeństwu państwa, w tym bezpieczeństwu ekonomicznemu państwa.

11. Szef Agencji Bezpieczeństwa Wewnętrznego wydaje negatywną opinię w przypadku niespełnienia odpowiednio przez podmiot odpowiedzialny za system identyfikacji elektronicznej lub podmiot, o którym mowa w ust. 2 pkt 2, warunków, o których mowa w ust. 10.

12. Opinia Szefa Agencji Bezpieczeństwa Wewnętrznego zawiera oddzielnie stanowisko w stosunku do każdego z ocenianych podmiotów.

13. Rada Ministrów określi, w drodze rozporządzenia, zakres danych i dokumentów niezbędnych do przeprowadzenia postępowania w celu dokonania oceny, o której mowa w ust. 5, mając na uwadze potrzebę zapewnienia kompletności danych i dokumentów niezbędnych do wydania opinii oraz zapewnienie sprawności postępowania.

14. Termin postępowania w sprawie przeprowadzenia oceny, o której mowa w ust. 5, wynosi 30 dni od otrzymania danych i dokumentów niezbędnych do przeprowadzenia postępowania i może zostać wydłużony o kolejne 30 dni w przypadkach szczególnie uzasadnionych. Okresu przeprowadzenia postępowania nie wlicza się do terminów przewidzianych na wydanie decyzji, o której mowa w art. 21b ust. 1.

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

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

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

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

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

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

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

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

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

3) wydania przez Szefa Agencji Bezpieczeństwa Wewnętrznego negatywnej opinii w przypadku, o którym mowa w art. 21s ust. 3.

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

Art. 21m. Do węzła krajowego przyłącza się system teleinformatyczny zapewniający obsługę publicznego systemu identyfikacji elektronicznej, o którym mowa w art. 20aa pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

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

2. Rejestr systemów jest jawny.

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

4. Do rejestru systemów wpisuje się:

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

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

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

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

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

5) zapisuje i zachowuje informacje związane z wydawaniem, zawieszaniem i unieważnianiem środków identyfikacji elektronicznej oraz zapewnieniem rozliczalności i niezaprzeczalności działań użytkowników korzystających z tych środków;
6) stosuje politykę bezpieczeństwa węzła krajowego, o której mowa w art. 39b ust. 1 pkt 3;
7) unieważnia środki identyfikacji elektronicznej wydane przez podmiot, w stosunku do którego Szef Agencji Bezpieczeństwa Wewnętrznego wydał negatywną opinię w przypadku, o którym mowa w art. 21s ust. 3.

2. Czynności, o których mowa w ust. 1 pkt 2–5 i 7, mogą wykonywać podmioty inne niż podmiot odpowiedzialny za system identyfikacji elektronicznej, spełniające wymogi określone w art. 21b ust. 1 pkt 1, 3 i 5, o ile posiadają siedzibę na terenie jednego z państw członkowskich Unii Europejskiej. Odpowiedzialność za czynności wykonywane przez podmioty inne niż podmiot odpowiedzialny za system identyfikacji elektronicznej ponosi podmiot odpowiedzialny za system identyfikacji elektronicznej.

3. Podmioty inne niż podmiot odpowiedzialny za system identyfikacji elektronicznej stosują politykę bezpieczeństwa węzła krajowego, o której mowa w art. 39b ust. 1 pkt 3.

Art. 21q. 1. Podmiot odpowiedzialny za system identyfikacji elektronicznej przetwarza dane osobowe osób, którym w tym systemie wydano środki identyfikacji elektronicznej, obejmujące:
1) imię (imiona),
2) nazwisko,
3) nazwisko rodowe,
4) numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014,
5) datę urodzenia,
6) miejsce urodzenia,
7) płeć,
8) adres zamieszkania

– w celu realizacji zadań, o których mowa w art. 21p ust. 1 pkt 1–5 i 7.

2. Podmiot, o którym mowa w art. 21p, inny niż podmiot wskazany w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014, zapewniając możliwość uwierzytelniania w usługach online, nie może pozyskiwać, przechowywać oraz przetwarzać danych dotyczących realizacji tych usług, innych niż dane niezbędne do zrealizowania procesu uwierzytelnienia.

Art. 21r. 1. W przypadku gdy nastąpi naruszenie bezpieczeństwa systemu identyfikacji elektronicznej przyłączonego do węzła krajowego lub części środków identyfikacji elektronicznej wydanych w tym systemie, mogące mieć wpływ na rozliczalność i niezaprzeczalność działań wykonywanych z wykorzystaniem tego systemu lub części środków identyfikacji elektronicznej wydanych w tym systemie, podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego niezwłocznie zawiesza możliwość uwierzytelniania z wykorzystaniem środków identyfikacji elektronicznej, których dotyczy naruszenie bezpieczeństwa.

2. Po usunięciu naruszenia bezpieczeństwa systemu identyfikacji elektronicznej lub zawieszonej części środków identyfikacji elektronicznej podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego przywraca możliwość uwierzytelniania za pomocą środków identyfikacji elektronicznej, których dotyczyło zawieszenie.

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

1) każdej zmianie dotyczącej systemu identyfikacji elektronicznej przyłączonego do węzła krajowego mającej wpływ na aktualność danych wpisanych do rejestru systemów – w terminie 14 dni od dnia zmiany tych danych;
2) zamiarze zaprzestania świadczenia usług związanych ze środkami identyfikacji elektronicznej wydawanymi w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego – w terminie 12 miesięcy przed planowanym zaprzestaniem świadczenia tych usług;

3) otwarciu jego likwidacji, ogłoszeniu jego upadłości lub oddaleniu wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe – niezwłocznie;
4) zawieszeniu możliwości uwierzytelniania z powodu naruszenia bezpieczeństwa, o którym mowa w art. 21r ust. 1, oraz przywróceniu możliwości uwierzytelniania po usunięciu naruszenia bezpieczeństwa, o którym mowa w art. 21r ust. 2 – niezwłocznie, nie później niż w ciągu 24 godzin od momentu odpowiednio wykrycia naruszenia bezpieczeństwa oraz usunięcia naruszenia bezpieczeństwa.

2. Minister właściwy do spraw informatyzacji po otrzymaniu danych, o których mowa w ust. 1, przekazuje je Szefowi Agencji Bezpieczeństwa Wewnętrznego, jeżeli istnieją uzasadnione przesłanki pozwalające wnioskować, iż zmiany tych danych mogą mieć wpływ na bezpieczeństwo publiczne, bezpieczeństwo państwa lub zagrażają w sposób bezpośredni bezpieczeństwu systemów teleinformatycznych państwa.

3. Szef Agencji Bezpieczeństwa Wewnętrznego, w przypadku powzięcia informacji o okolicznościach prawnych lub faktycznych dotyczących struktury właścicielskiej podmiotu odpowiedzialnego za system identyfikacji elektronicznej lub podmiotu, o którym mowa w art. 21g ust. 2 pkt 2, które mogą zagrozić bezpieczeństwu państwa, w tym bezpieczeństwu ekonomicznemu państwa, przeprowadza postępowanie w tej sprawie. Do postępowania stosuje się odpowiednio przepisy art. 21g ust. 5–13.

4. Szef Agencji Bezpieczeństwa Wewnętrznego przeprowadza postępowanie, o którym mowa w ust. 3, również na polecenie Prezesa Rady Ministrów lub ministra członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych.

5. Szef Agencji Bezpieczeństwa Wewnętrznego po przeprowadzeniu postępowania przekazuje opinię ministrowi właściwemu do spraw informatyzacji.

6. Minister właściwy do spraw informatyzacji przekazuje opinię podmiotowi odpowiedzialnemu za system identyfikacji elektronicznej.

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

1) zapewnieniu przez podmiot odpowiedzialny za ten system opracowania, ustanawiania, wdrażania, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
2) przeprowadzeniu testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność tego systemu z węzłem krajowym;
3) przedstawieniu przez podmiot odpowiedzialny za ten system oświadczenia o działaniu tego podmiotu zgodnie z przepisami o ochronie danych osobowych;
4) wskazaniu interesu faktycznego w uwierzytelnianiu z wykorzystaniem węzła krajowego – w przypadku podmiotu innego niż podmiot wskazany w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014.

2. Ocena interesu faktycznego dokonywana jest z uwzględnieniem jego wpływu na bezpieczeństwo i interes publiczny.

3. Wyrażenie zgody, o której mowa w ust. 1, stanowi czynność materialno-techniczną.

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

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

3. Do wniosku dołącza się:
1) oświadczenie o zapewnieniu przez podmiot odpowiedzialny za ten system opracowania, ustanawiania, wdrażania, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
2) oświadczenie o zapewnieniu stosowania polityki bezpieczeństwa, o której mowa w art. 39b ust. 1 pkt 3;

3) listę usług online udostępnianych w tym systemie wraz z określeniem dla każdej z tych usług wymaganych poziomów bezpieczeństwa środków identyfikacji elektronicznej, o których mowa w art. 8 ust. 2 rozporządzenia 910/2014, niezbędnych dla realizacji tych usług;
4) oświadczenie o działaniu podmiotu zgodnie z przepisami o ochronie danych osobowych;
5) uzasadnienie interesu faktycznego w uwierzytelnianiu z wykorzystaniem węzła krajowego – w przypadku podmiotu innego niż podmiot, o których mowa w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014;
6) raport z testów integracyjnych zakończonych wynikiem pozytywnym, potwierdzających interoperacyjność tego systemu z węzłem krajowym.

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

Art. 21v. Testy integracyjne, o których mowa w art. 21t ust. 1 pkt 2, przeprowadza się zgodnie z procedurą udostępnioną w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.

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

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

Art. 21y. W przypadku niespełniania wymagań, o których mowa w art. 21t ust. 1, minister właściwy do spraw informatyzacji wydaje decyzję o odmowie przyłączenia systemu teleinformatycznego, w którym udostępniane są usługi online, do węzła krajowego.

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

Art. 22. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie węzła transgranicznego, zgodnie z rozporządzeniem 910/2014.

2. (uchylony)

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

4. Notyfikowany system identyfikacji elektronicznej jest przyłączany do węzła transgranicznego za pośrednictwem węzła krajowego.

Art. 23. 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. 24. 1. Wniosek o notyfikowanie 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 może zgłosić system identyfikacji elektronicznej do przeprowadzenia wzajemnej oceny, o której mowa w art. 12 ust. 6 lit. c rozporządzenia 910/2014, po pozytywnym zweryfikowaniu wniosku, o którym mowa w ust. 1, biorąc pod uwagę warunki kwalifikowania się systemu do notyfikowania wskazane w art. 7 tego rozporządzenia oraz politykę państwa w zakresie identyfikacji elektronicznej.

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

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.

Art. 25. Podmioty odpowiedzialne za systemy teleinformatyczne, w których udostępniane są usługi online, przyłączane do węzła krajowego określają wymagane poziomy bezpieczeństwa środków identyfikacji elektronicznej, o których mowa w art. 8 ust. 2 rozporządzenia 910/2014, niezbędne dla realizacji tych usług.

Art. 26. 1. Obowiązki, o których mowa w art. 10 rozporządzenia 910/2014, wykonuje minister właściwy do spraw informatyzacji.

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

Rozdział 4a

Standard usługi rejestrowanego doręczenia elektronicznego

Art. 26a. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej standard publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń, obejmujący:

1) wymagania techniczne przekazywania dokumentów elektronicznych w ramach publicznej usługi rejestrowanego doręczenia elektronicznego,
2) sposób identyfikacji nadawcy i adresata danych w ramach publicznej usługi rejestrowanego doręczenia elektronicznego,
3) strukturę dowodów wysłania i dowodów otrzymania w ramach publicznej usługi rejestrowanego doręczenia elektronicznego,
4) formę i sposób:
   a) wystawiania dowodu wysłania,

b) wystawiania dowodu otrzymania,

c) utrwalania dowodów wysłania i dowodów otrzymania

– w ramach publicznej usługi rejestrowanego doręczenia elektronicznego,

5) zakres i strukturę danych dotyczących komunikacji pomiędzy adresami do doręczeń elektronicznych,

6) wymagania funkcjonowania skrzynki doręczeń, o której mowa w art. 2 pkt 9 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. poz. 2320 oraz z 2021 r. poz. 72, 802, 1135, 1163 i 1598)

– uwzględniając konieczność zapewnienia interoperacyjności i bezpieczeństwa wymiany danych, w tym możliwość transgranicznej wymiany danych, biorąc pod uwagę normy i wytyczne dotyczące procedur wysyłania i otrzymywania danych opracowane przez Europejski Instytut Norm Telekomunikacyjnych lub normy wskazane przez Komisję Europejską w drodze aktów wykonawczych, o których mowa w art. 44 ust. 2 rozporządzenia 910/2014.

Art. 26b. Kwalifikowany dostawca usług zaufania świadczy kwalifikowaną usługę rejestrowanego doręczenia elektronicznego zgodnie ze standardem określonym w art. 26a.

Art. 26c. Kwalifikowany dostawca usług zaufania świadczący kwalifikowaną usługę rejestrowanego doręczenia elektronicznego zgłasza do ministra właściwego do spraw informatyzacji za pomocą systemu teleinformatycznego, o którym mowa w art. 58 ust. 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, informację o zmianie lokalizacji adresu do doręczeń elektronicznych w przypadku przeniesienia go do innego dostawcy.

Rozdział 5

Nadzór nad dostawcami usług zaufania

Art. 27. 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) w uzasadnionych przypadkach, w drodze decyzji, 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.

3. Decyzja, o której mowa w ust. 2 pkt 5, podlega natychmiastowemu wykonaniu. Przepisu art. 61 § 2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi nie stosuje się.

Art. 28. 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. 29. 1. W przypadku odebrania kwalifikowanemu dostawcy usług zaufania statusu kwalifikowanego lub statusu kwalifikowanego świadczonej przez niego usłudze zaufania minister właściwy do spraw informatyzacji, w drodze decyzji, może unieważnić odpowiednie certyfikaty dostawcy usług zaufania, wydane temu dostawcy.

2. Unieważniając certyfikaty dostawcy usług 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. 30. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że kwalifikowany dostawca usług 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. 31. 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 oceniającą zgodność.

Art. 32. 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 wspólnikami 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. 33. 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. 34. 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. 35. Audytorzy organu nadzoru i obserwatorzy organu nadzoru są obowiązani do bezterminowego zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

Art. 36. W sprawach nieuregulowanych w ustawie, do przeprowadzenia audytu dostawców usług zaufania przez audytorów organu nadzoru stosuje się odpowiednio przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162), z wyłączeniem przepisu art. 55 ust. 1 tej ustawy.

Art. 37. 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. 38. 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. 39. 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 5a

Nadzór nad krajowym schematem identyfikacji elektronicznej

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

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

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

5) współpracuje z organem właściwym do spraw ochrony danych osobowych.

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

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

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

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

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

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

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

1) złożenia przez podmiot odpowiedzialny za system identyfikacji elektronicznej wniosku o odłączenie od węzła krajowego;
2) zaprzestania prowadzenia działalności przez podmiot odpowiedzialny za system identyfikacji elektronicznej;
3) nieusunięcia przyczyny zawieszenia możliwości uwierzytelniania, o której mowa w art. 21r ust. 1, lub możliwości korzystania z systemu, o której mowa w art. 39c ust. 1, w terminie 3 miesięcy od dnia jego zawieszenia;
4) nieprzedstawienia kolejnej umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z wykorzystywaniem środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej;
5) wydania przez Szefa Agencji Bezpieczeństwa Wewnętrznego negatywnej opinii w przypadku, o którym mowa w art. 21s ust. 3, w stosunku do podmiotu odpowiedzialnego za system identyfikacji elektronicznej.

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

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

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

Art. 39g. 1. W przypadku naruszenia polityki bezpieczeństwa, o której mowa w art. 39b ust. 1 pkt 3, lub niespełniania wymagań, o których mowa w art. 21t ust. 1, dotyczących systemu teleinformatycznego, w którym udostępniane są usługi online, przyłączonego do węzła krajowego, w zakresie mającym wpływ na bezpieczeństwo uwierzytelnienia z wykorzystaniem węzła krajowego, minister właściwy do spraw informatyzacji zawiesza w tym systemie możliwość uwierzytelniania z wykorzystaniem węzła krajowego.

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

Art. 39h. Minister właściwy do spraw informatyzacji wydaje decyzję o odłączeniu systemu teleinformatycznego, w którym udostępniane są usługi online, i odłącza ten system od węzła krajowego w przypadku:

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

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

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

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

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

Art. 39k. W przypadku gdy wyniki kontroli wykażą niezgodność z przepisami ustawy, minister właściwy do spraw informatyzacji, po zapoznaniu się z zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez podmiot kontrolowany, może wydać decyzję nakładającą obowiązek usunięcia stwierdzonych niezgodności w terminie nie krótszym niż 14 dni.

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

Rozdział 6

Przepisy karne

Art. 40. 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, kto składa kwalifikowaną pieczęć elektroniczną lub zaawansowaną pieczęć elektroniczną, nie będąc do tego uprawnionym.

Art. 40a. Kto posługuje się cudzym środkiem identyfikacji elektronicznej, wydawanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, w celu uzyskania nieuprawnionego dostępu do usługi online,

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

Art. 41. 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. 41a. Kto bez uprawnienia kopiuje lub przechowuje nieprzyporządkowane do niego dane pozwalające na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej, wydawanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego,

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

Art. 42. 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, kto składa podpis elektroniczny lub pieczęć elektroniczną weryfikowane certyfikatem, o którym mowa w ust. 1, w celu popełnienia czynu zabronionego.

Art. 43. 1. Kto, będąc obowiązanym 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. 44. Kto wydaje środek identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego osobie nieuprawnionej,

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

Art. 45. Karom określonym w art. 40–44 podlega także, 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 7

Przepisy o karach pieniężnych

Art. 46. 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. 30 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 przepisami o usługach zaufania;
4) nie unieważnia kwalifikowanych certyfikatów mimo wezwania ministra właściwego do spraw informatyzacji, o którym mowa w art. 30 pkt 1 lit. c;
5) wydaje certyfikaty niezgodnie z polityką świadczenia usługi;
6) nie udziela informacji lub nie udostępnia dokumentów w przypadku, o którym mowa w art. 28;
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. 20 ust. 3 lub 4;
12) nie wykona obowiązku, o którym mowa w art. 13 ust. 1.

Art. 47. 1. Kary pieniężne, o których mowa w art. 46, art. 47a i art. 47b, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

2. Wysokość kary pieniężnej, o której mowa w art. 46:
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. 47a. Kto w sposób nieuprawniony gromadzi, przetwarza lub powiela dane dotyczące wykorzystania środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego,

podlega karze pieniężnej w wysokości do 1 000 000 zł.

Art. 47b. Podmiot odpowiedzialny za system identyfikacji elektronicznej przyłączony do węzła krajowego, który w wyniku świadomego działania lub zaniechania dopuścił w swoim systemie identyfikacji elektronicznej do uwierzytelnienia z wykorzystaniem środka identyfikacji elektronicznej, co do którego posiada wiedzę, że nie pozostaje on pod wyłączną kontrolą osoby, której ten środek wydano,

podlega karze pieniężnej w wysokości do 1 000 000 zł.

Art. 48. Przy ustalaniu wysokości kary pieniężnej, o której mowa w art. 46, minister właściwy do spraw informatyzacji uwzględnia zakres, czas trwania i skutki naruszenia wymagań, o których mowa w przepisach o usługach zaufania.

Art. 49. Do kar pieniężnych stosuje się odpowiednio przepisy działu III i IV ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2021 r. poz. 1540 i 1598).

Rozdział 8

Zmiany w przepisach

Art. 50–130. (pominięte)

Rozdział 9

Przepisy przejściowe

Art. 131. 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. 132. 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. 133. 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. 134. 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. 135. 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, przekaże 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. 136. Banki wykonujące czynności, o których mowa w art. 6 ust. 1 pkt 6a ustawy zmienianej w art. 64[2)], w brzmieniu dotychczasowym, są obowiązane dostosować statuty do przepisów ustawy zmienianej w art. 64[2)], w brzmieniu nadanym niniejszą ustawą, w terminie 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 137. 1. 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.

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

Art. 138. Do umów ubezpieczenia odpowiedzialności cywilnej, o których mowa w art. 10 ust. 1 pkt 4 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, zawartych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

---

2) Artykuł 64 zawiera zmiany do ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

Art. 139. 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. 13 ust. 4, jednak nie dłużej niż 3 miesiące od dnia wejścia w życie niniejszej ustawy.

Art. 140. 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. 141. 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. 142. Ustawa wchodzi w życie po upływie 7 dni od dnia ogłoszenia[3)], z wyjątkiem art. 22 oraz art. 24–26, które wchodzą w życie z dniem 29 września 2018 r.

3) Ustawa została ogłoszona w dniu 29 września 2016 r.