Opracowano na podstawie: t.j. Dz. U. z 2021 r. poz. 670, 952, 1005, 1641.

U S T A W A

z dnia 17 lutego 2005 r.

o informatyzacji działalności podmiotów realizujących zadania publiczne

Rozdział 1

Przepisy ogólne

Art. 1. Ustawa określa zasady:

1) dofinansowania projektów informatycznych o publicznym zastosowaniu,
2) ustalania minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi oraz ustalania Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji,
3) dostosowania systemów teleinformatycznych używanych do realizacji zadań publicznych do minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz do Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji,
4) dostosowania rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi do minimalnych wymagań dla rejestrów publicznych i wymiany informacji z podmiotami publicznymi oraz do Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji,
5) kontroli projektów informatycznych o publicznym zastosowaniu, systemów teleinformatycznych używanych do realizacji zadań publicznych, rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi,

6) wymiany informacji drogą elektroniczną, w tym dokumentów elektronicznych, pomiędzy podmiotami publicznymi a podmiotami niebędącymi podmiotami publicznymi,
7) ustalania i publikacji specyfikacji rozwiązań stosowanych w oprogramowaniu umożliwiającym łączenie i wymianę informacji, w tym przesłanie dokumentów elektronicznych, pomiędzy systemami teleinformatycznymi podmiotów publicznych a systemami podmiotów niebędącymi podmiotami publicznymi,
8) funkcjonowania elektronicznej platformy usług administracji publicznej, zwanej dalej „ePUAP”,
9) funkcjonowania centralnego repozytorium wzorów dokumentów elektronicznych,
9a) funkcjonowania publicznego systemu identyfikacji elektronicznej,
9b) świadczenia usługi podpisu zaufanego,
<9c) funkcjonowania zintegrowanej platformy analitycznej>
10) (uchylony)

Dodany pkt 9c w art. 1 wejdzie w życie z dn. 8.12.2021 r. (Dz. U. z 2021 r. poz. 1641).

– w celu ochrony interesu publicznego, w tym zachowania przez Państwo możliwości swobody wyboru technologii w procesach informatyzacji realizacji zadań publicznych.

Art. 2. 1. Z zastrzeżeniem ust. 2–4, przepisy ustawy stosuje się do realizujących zadania publiczne określone przez ustawy:
1) organów administracji rządowej, organów kontroli państwowej i ochrony prawa, sądów, jednostek organizacyjnych prokuratury, a także jednostek samorządu terytorialnego i ich organów,
2) jednostek budżetowych i samorządowych zakładów budżetowych,
3) funduszy celowych,
4) samodzielnych publicznych zakładów opieki zdrowotnej oraz spółek wykonujących działalność leczniczą w rozumieniu przepisów o działalności leczniczej,
5) Zakładu Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego,
6) Narodowego Funduszu Zdrowia,
7) państwowych lub samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu realizacji zadań publicznych,

8) uczelni,
9) federacji podmiotów systemu szkolnictwa wyższego i nauki,
9a) instytutów badawczych,
9b) instytutów działających w ramach Sieci Badawczej Łukasiewicz,
9c) jednostek organizacyjnych tworzonych przez Polską Akademię Nauk,
10) Polskiej Komisji Akredytacyjnej,
11) Rady Doskonałości Naukowej

– zwanych dalej „podmiotami publicznymi”.

2. Przepis art. 13 ust. 2 pkt 1 stosuje się również do podmiotu, któremu podmiot publiczny powierzył lub zlecił realizację zadania publicznego, jeżeli w związku z realizacją tego zadania istnieje obowiązek przekazywania informacji do lub od podmiotów niebędących organami administracji rządowej.

3. Przepisów ustawy nie stosuje się do przedsiębiorstw państwowych, spółek handlowych, służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27 i 2320), Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej oraz Narodowego Banku Polskiego, z wyjątkiem art. 13 ust. 2 pkt 1, gdy w związku z realizacją zadań przez te podmioty istnieje obowiązek przekazywania informacji do i od podmiotów niebędących organami administracji rządowej, oraz z wyjątkiem art. 13a, art. 19c i art. 19d.

4. Przepisów rozdziału 4 nie stosuje się do instytutów badawczych, Centrum Łukasiewicz, instytutów działających w ramach Sieci Badawczej Łukasiewicz, uczelni, federacji podmiotów systemu szkolnictwa wyższego i nauki, Polskiej Akademii Nauk i tworzonych przez nią jednostek organizacyjnych, Polskiej Komisji Akredytacyjnej, Rady Doskonałości Naukowej, Rzecznika Praw Obywatelskich, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Prezesa Urzędu Ochrony Danych Osobowych, Komisji Nadzoru Finansowego oraz Generalnego Inspektora Informacji Finansowej.

Art. 3. Użyte w ustawie określenia oznaczają:

1) informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

2) dokument elektroniczny – stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych;
3) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875);
4) środki komunikacji elektronicznej – środki komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344);
5) rejestr publiczny – rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych;
6) projekt informatyczny o publicznym zastosowaniu – określony w dokumentacji zespół czynności organizacyjnych i technicznych mających na celu zbudowanie, rozbudowanie lub unowocześnienie systemu teleinformatycznego używanego do realizacji zadań publicznych, zapewnienie utrzymania tego systemu lub opracowanie procedur realizowania zadań publicznych drogą elektroniczną;
7) ponadsektorowy projekt informatyczny – projekt informatyczny o publicznym zastosowaniu, którego zakres przedmiotowy dotyczy spraw należących do właściwości więcej niż jednego działu administracji rządowej;
8) sektorowy projekt informatyczny – projekt informatyczny o publicznym zastosowaniu, którego zakres przedmiotowy dotyczy spraw należących do właściwości jednego działu administracji rządowej;
9) minimalne wymagania dla systemów teleinformatycznych – zespół wymagań organizacyjnych i technicznych, których spełnienie przez system teleinformatyczny używany do realizacji zadań publicznych umożliwia wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych oraz zapewnia dostęp do zasobów informacji udostępnianych za pomocą tych systemów;

10) minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej – zespół cech informacyjnych, w tym identyfikatorów oraz odpowiadających im charakterystyk elementów strukturalnych przekazu informacji, takich jak zawartości pola danych, służących do zapewnienia spójności prowadzenia rejestrów publicznych oraz wymiany informacji w postaci elektronicznej z podmiotami publicznymi;
11) oprogramowanie interfejsowe – oprogramowanie umożliwiające łączenie i wymianę danych w komunikacji pomiędzy systemami teleinformatycznymi;
12) testy akceptacyjne – udokumentowane wartości danych wejściowych wprowadzanych do systemu teleinformatycznego i powiązanych z nimi wartości oczekiwanych danych wyjściowych, opisujące zestawy poprawnych odpowiedzi systemu teleinformatycznego na podawane dane wejściowe, pozwalające na sprawdzenie poprawności wdrożenia oprogramowania interfejsowego;
13) elektroniczna platforma usług administracji publicznej – system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet;
14) profil zaufany – środek identyfikacji elektronicznej zawierający zestaw danych identyfikujących i opisujących osobę fizyczną, która posiada pełną albo ograniczoną zdolność do czynności prawnych, który został wydany w sposób, o którym mowa w art. 20c albo art. 20cb;
14a) podpis zaufany – podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający:
    a) dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1, obejmujące:
        – imię (imiona),
        – nazwisko,
        – numer PESEL,
    b) identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony,
    c) czas jego złożenia;

14b) profil osobisty – środek identyfikacji elektronicznej, o którym mowa w art. 2 ust. 1 pkt 10 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2020 r. poz. 332, 695, 875, 1517 i 2320);

15) (uchylony)

16) (uchylony)

Przepis uchylający pkt 17 i 20 w art. 3 wejdzie w życie z dn. 1.10.2029 r. (Dz. U. z 2020 r. poz. 2320).

[17) elektroniczna skrzynka podawcza – dostępny publicznie środek komunikacji elektronicznej służący do przekazywania dokumentu elektronicznego do podmiotu publicznego przy wykorzystaniu powszechnie dostępnego systemu teleinformatycznego;]

18) interoperacyjność – zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych;

19) neutralność technologiczna – zasada równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań;

[20) urzędowe poświadczenie odbioru – dane elektroniczne powiązane z dokumentem elektronicznym doręczonym podmiotowi publicznemu lub przez niego doręczanym w sposób zapewniający rozpoznawalność późniejszych zmian dokonanych w tych danych, określające:

a) pełną nazwę podmiotu publicznego, któremu doręczono dokument elektroniczny lub który doręcza dokument,

b) datę i godzinę wprowadzenia albo przeniesienia dokumentu elektronicznego do systemu teleinformatycznego podmiotu publicznego – w odniesieniu do dokumentu doręczanego podmiotowi publicznemu,

c) datę i godzinę podpisania urzędowego poświadczenia odbioru przez adresata z użyciem mechanizmów, o których mowa w art. 20a ust. 1 albo 2 – w odniesieniu do dokumentu doręczanego przez podmiot publiczny,

d) datę i godzinę wytworzenia urzędowego poświadczenia odbioru;]

21) Krajowe Ramy Interoperacyjności – zestaw wymagań semantycznych, organizacyjnych oraz technologicznych dotyczących interoperacyjności systemów teleinformatycznych i rejestrów publicznych;
22) użytkownik – osobę fizyczną korzystającą z systemów teleinformatycznych;
23) katalog usług – rejestr, udostępniony na elektronicznej platformie usług administracji publicznej, zawierający informacje o usługach udostępnianych przez podmioty publiczne;
24) wzór dokumentu elektronicznego – zbiór danych określających zestaw, sposób oznaczania oraz wymagalność elementów treści i metadanych dokumentu elektronicznego, a także mogących określać sposób zapisu danych dla wskazanych elementów oraz kolejność i sposób wyświetlania na ekranie lub drukowania poszczególnych elementów (wizualizacji);
25) formularz elektroniczny – oprogramowanie służące do przygotowania i wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego, mogące stanowić część usługi udostępnionej na ePUAP lub w innym systemie teleinformatycznym;
26) zakres użytkowy dokumentu elektronicznego – dane zawarte w dokumencie elektronicznym niezbędne do załatwienia określonego rodzaju spraw za pośrednictwem usługi udostępnionej na ePUAP lub w innym systemie teleinformatycznym;
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.

Art. 4. Przepisy ustawy nie naruszają:

1) przepisów o ochronie danych osobowych;
2) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742);
3) obowiązków wynikających z potrzeby współpracy z systemami teleinformatycznymi i rejestrami organów innych państw lub organizacji międzynarodowych;
4) obowiązków wynikających z umów międzynarodowych, jak również umów o członkostwo w instytucjach międzynarodowych, w przypadku gdy prawo

danego podmiotu do członkostwa w instytucjach międzynarodowych zostało zagwarantowane aktem prawnym o mocy ustawy.

Rozdział 2

Projekty informatyczne o publicznym zastosowaniu

Art. 5. (uchylony)

Art. 6. (uchylony)

Art. 7. (uchylony)

Art. 8. (uchylony)

Art. 9. (uchylony)

Art. 10. (uchylony)

Art. 11. (uchylony)

Art. 12. (uchylony)

Art. 12a. (uchylony)

Art. 12b. Rada Ministrów, na wniosek ministra właściwego do spraw informatyzacji, przyjmuje, w drodze uchwały, Program Zintegrowanej Informatyzacji Państwa stanowiący program rozwoju w rozumieniu art. 15 ust. 4 pkt 2 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2019 r. poz. 1295 i 2020 oraz z 2020 r. poz. 1378 i 2327).

Art. 12c. 1. Minister właściwy do spraw informatyzacji może raz w roku przeprowadzić konkurs na dofinansowanie projektów informatycznych o publicznym zastosowaniu lub przedsięwzięć wspierających rozwój społeczeństwa informacyjnego, zwany dalej „konkursem”.

2. Minister właściwy do spraw informatyzacji publikuje ogłoszenie o konkursie w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

3. Ogłoszenie o konkursie określa co najmniej:

1) przedmiot konkursu;
2) podmioty publiczne mogące ubiegać się o dofinansowanie;
3) warunki udziału w konkursie;
4) kryteria oceny wniosku o dofinansowanie;
5) termin i warunki realizacji projektu lub przedsięwzięcia;

6) wysokość środków finansowych przeznaczonych na realizację konkursu;

7) termin składania wniosków o dofinansowanie.

4. Podmioty publiczne lub podmioty, o których mowa w art. 20c ust. 2a, mogące ubiegać się o dofinansowanie składają wniosek o dofinansowanie do ministra właściwego do spraw informatyzacji.

Art. 12d. 1. Minister właściwy do spraw informatyzacji rozstrzyga konkurs na podstawie oceny wniosków dokonanej przez komisję konkursową oraz ogłasza wyniki konkursu.

2. Minister właściwy do spraw informatyzacji, w drodze zarządzenia, powołuje komisję konkursową, a także określa jej skład, tryb pracy oraz zakres zadań.

3. Datą ogłoszenia wyników konkursu jest data ich zamieszczenia w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.

Art. 12e. 1. Wnioskodawca może złożyć do ministra właściwego do spraw informatyzacji odwołanie od wyniku konkursu, w terminie 7 dni od dnia ogłoszenia wyniku konkursu.

2. Odwołanie wniesione po terminie nie podlega rozpatrzeniu. O zachowaniu terminu decyduje data wpływu odwołania do urzędu obsługującego ministra właściwego do spraw informatyzacji.

3. Minister właściwy do spraw informatyzacji rozpatruje odwołanie w terminie 14 dni od dnia jego wpływu do urzędu obsługującego tego ministra.

Art. 12f. 1. Środki finansowe na dofinansowanie projektów i przedsięwzięć, o których mowa w art. 12c ust. 1, są przekazywane podmiotowi, którego wniosek o dofinansowanie został wyłoniony w drodze konkursu, w formie dotacji celowej, na podstawie umowy zawartej między ministrem właściwym do spraw informatyzacji a tym podmiotem.

2. Umowa o dofinansowanie nie może zostać zawarta przed upływem terminu, o którym mowa w art. 12e ust. 1, a w przypadku wniesienia odwołania od wyniku konkursu – do czasu rozpatrzenia odwołania.

Art. 12g. 1. Minister właściwy do spraw informatyzacji unieważnia konkurs, jeżeli:

1) w terminie wskazanym w ogłoszeniu o konkursie nie złożono żadnego wniosku o dofinansowanie;
2) żaden ze złożonych wniosków o dofinansowanie nie spełnia warunków określonych w ogłoszeniu o konkursie.

2. Informację o unieważnieniu konkursu minister właściwy do spraw informatyzacji zamieszcza w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

Art. 12h. 1. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia:

1) tryb przeprowadzania konkursu oraz kryteria, sposób i tryb przeznaczania oraz rozliczania środków finansowych na dofinansowanie projektów i przedsięwzięć, o których mowa w art. 12c ust. 1, w tym:
   a) sposób oceny wniosków o dofinansowanie projektów i przedsięwzięć,
   b) sposób oceny realizacji projektów i przedsięwzięć, zgodnie z warunkami określonymi w umowie, o której mowa w art. 12f ust. 1;
2) wzór wniosku o dofinansowanie;
3) wzór raportu rocznego z przebiegu realizacji projektów i przedsięwzięć oraz rozliczenia przyznanych środków finansowych;
4) wzór raportu końcowego z przebiegu realizacji projektów i przedsięwzięć oraz rozliczenia przyznanych środków finansowych.

2. Minister właściwy do spraw informatyzacji, wydając rozporządzenie, o którym mowa w ust. 1, uwzględni:

1) możliwość elektronicznego składania wniosków o dofinansowanie;
2) potrzebę dokonania oceny wniosków o dofinansowanie za pomocą zobiektywizowanych kryteriów;
3) potrzebę dokonania oceny realizacji projektów i przedsięwzięć na podstawie raportów rocznych i raportu końcowego;
4) konieczność ujednolicenia składanych wniosków o dofinansowanie oraz raportów rocznych i końcowych.

Art. 12i. 1. Podmioty, o których mowa w art. 2 ust. 1 i 2, w ramach realizacji projektów informatycznych o pub-licznym zastosowaniu oraz przedsięwzięć wspierających rozwój społeczeństwa informacyjnego mogą pozyskiwać innowacyjne rozwiązania technologiczne służące realizacji zadań publicznych.

2. Agencja Rozwoju Przemysłu S.A. zapewnia wsparcie w realizacji projektów informatycznych o publicznym zastosowaniu oraz przedsięwzięć wspierających rozwój społeczeństwa informacyjnego, w szczególności przez świadczenie usług doradczych na rzecz podmiotów, o których mowa w art. 2 ust. 1 i 2, w procesie pozyskiwania przez te podmioty innowacyjnych rozwiązań technologicznych.

3. Wykonywanie przez Agencję Rozwoju Przemysłu S.A. zadań, o których mowa w ust. 2, może być finansowane z dotacji celowych z budżetu państwa oraz środków pochodzących z budżetu Unii Europejskiej oraz innych środków pochodzących ze źródeł zagranicznych, niepodlegających zwrotowi, oraz odsetek od nich, o ile odrębne przepisy lub umowy dotyczące przekazania lub wykorzystania tych środków nie stanowią inaczej.

4. Dotacje celowe, o których mowa w ust. 3, nie mogą:

1) przewyższać koniecznych, rzeczywistych kosztów bezpośrednich i pośrednich poniesionych przez Agencję Rozwoju Przemysłu S.A. na realizację zadań, o których mowa w ust. 2;
2) obejmować dofinansowania działalności gospodarczej Agencji Rozwoju Przemysłu S.A.

5. Agencja Rozwoju Przemysłu S.A. prowadzi wyodrębnioną ewidencję dla zadań finansowanych ze środków, o których mowa w ust. 3, oraz dla działalności gospodarczej, w tym jest obowiązana do prawidłowego przypisywania przychodów i kosztów na podstawie metod mających obiektywne uzasadnienie, z uwzględnieniem odrębnych przepisów.

Rozdział 3

Systemy teleinformatyczne używane do realizacji zadań publicznych, rejestry publiczne oraz wymiana informacji w postaci elektronicznej między podmiotami publicznymi

Art. 13. 1. Podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.

1a. Postanowienia ust. 1 nie stosuje się do systemów teleinformatycznych używanych do celów naukowych i dydaktycznych.

2. Podmiot publiczny realizujący zadania publiczne przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej do przekazywania danych pomiędzy tym podmiotem a podmiotem niebędącym organem administracji rządowej:

1) zapewnia, aby system teleinformatyczny służący do wymiany danych pomiędzy tym podmiotem a podmiotami niebędącymi organami administracji rządowej, poza minimalnymi wymaganiami, o których mowa w ust. 1, spełniał

wymóg równego traktowania rozwiązań informatycznych;

2) publikuje w Biuletynie Informacji Publicznej lub udostępnia w inny sposób:
   a) zestawienie stosowanych w oprogramowaniu interfejsowym systemu teleinformatycznego używanego przez ten podmiot do realizacji zadań publicznych struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących,
   b) testy akceptacyjne, z zastrzeżeniem ust. 4.

3. Rozwiązania, o których mowa w ust. 2 pkt 2 lit. a, nie mogą wykraczać poza zakres minimalnych wymagań dla systemów teleinformatycznych.

4. Podmiot publiczny może nie udostępniać testów akceptacyjnych, jeżeli w oprogramowaniu interfejsowym mają być stosowane wyłącznie formaty danych oraz protokoły komunikacyjne i szyfrujące określone w przepisach wydanych na podstawie art. 18 pkt 1.

Art. 13a. Podmioty publiczne, o których mowa w art. 2 ust. 1, służby specjalne w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Kancelaria Sejmu, Kancelaria Senatu, Kancelaria Prezydenta Rzeczypospolitej Polskiej, Narodowy Bank Polski, agencje wykonawcze w rozumieniu art. 18 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2021 r. poz. 305) oraz podmioty, o których mowa w art. 2 ust. 4, niewskazane wprost w art. 2 ust. 1, uprawnione do wykonywania praw majątkowych do programu komputerowego stworzonego przez pracowników w ramach wykonywania obowiązków ze stosunku pracy świadczonej na rzecz tych podmiotów, mogą umożliwić sobie wzajemnie nieodpłatne korzystanie z tego programu komputerowego.

Art. 13b. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie systemu rejestrów państwowych, stanowiącego rozwiązanie organizacyjno-techniczne, wykorzystywane do prowadzenia rejestrów publicznych.

2. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na stronie podmiotowej ministra:

1) standardy technologiczne funkcjonowania systemu rejestrów państwowych oraz wymiany danych przetwarzanych w rejestrach publicznych utrzymywanych z wykorzystaniem systemu rejestrów państwowych;
2) informacje o rejestrach prowadzonych w systemie rejestrów państwowych.

Art. 14. 1. Podmiot publiczny prowadzący rejestr publiczny jest obowiązany:

1) prowadzić ten rejestr w sposób zapewniający spełnianie minimalnych wymagań dla systemów teleinformatycznych, w przypadku gdy ten rejestr działa przy użyciu systemów teleinformatycznych;
2) prowadzić ten rejestr zgodnie z minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej;
3) umożliwić dostarczanie informacji do tego rejestru oraz udostępnianie informacji z tego rejestru drogą elektroniczną, w przypadku gdy ten rejestr działa przy użyciu systemów teleinformatycznych.

2. Organ administracji rządowej zapewnia działanie rejestru publicznego, używając systemów teleinformatycznych.

<3. W przypadku gdy podmiot, o którym mowa w art. 2 ust. 1 pkt 1, 5 i 6, prowadzi rejestr publiczny przy użyciu systemów teleinformatycznych, dokonuje uprzedniej weryfikacji danych wprowadzanych po raz pierwszy do tego rejestru pod względem zgodności tych danych z danymi zgromadzonymi w rejestrze PESEL.

4. W przypadku wprowadzania po raz pierwszy danych osoby nieposiadającej numeru PESEL podmiot, o którym mowa w art. 2 ust. 1 pkt 1, 5 i 6, prowadzący rejestr publiczny nie przeprowadza weryfikacji.

5. Weryfikacja, o której mowa w ust. 3, polega na porównaniu danych wprowadzanych do rejestru publicznego z danymi zawartymi w rejestrze PESEL i jest realizowana zgodnie z art. 49 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności.

Dodane ust. 3–8 w art. 14 wejdą w życie z dniem 1 stycznia 2022 r. w zakresie dotyczącym rejestrów publicznych innych niż rejestr danych kontaktowych osób fizycznych, na podstawie art. 15 pkt 1 ustawy z dnia 16 października 2019 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw

6. System teleinformatyczny, przy użyciu którego zapewnione jest działanie rejestru publicznego, w przypadku pozytywnego wyniku weryfikacji, o której mowa w ust. 3, automatycznie wprowadza dane do rejestru, o ile przepisy odrębne nie stanowią inaczej.

7. W przypadku negatywnego wyniku weryfikacji, o której mowa w ust. 3, podmiot, o którym mowa w art. 2 ust. 1 pkt 1, 5 i 6, prowadzący rejestr publiczny niezwłocznie przekazuje właściwemu organowi wskazanemu w art. 10 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności informację o negatywnym wyniku weryfikacji oraz posiadane dokumenty stanowiące podstawę stwierdzenia wskazanej niezgodności, ich uwierzytelnione kopie lub odpisy, chyba że przepisy ustaw odrębnych uniemożliwiają ich przekazanie.

8. W przypadku braku dostępu do rejestru PESEL spowodowanego przyczynami niezależnymi od podmiotu, o którym mowa w art. 2 ust. 1 pkt 1, 5 i 6, przepisów ust. 3 i 5 nie stosuje się.>

Art. 15. 1. Podmiot prowadzący rejestr publiczny zapewnia podmiotowi publicznemu albo podmiotowi niebędącemu podmiotem publicznym, realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji, nieodpłatny dostęp do danych zgromadzonych w prowadzonym rejestrze, w zakresie niezbędnym do realizacji tych zadań.

2. Dane, o których mowa w ust. 1, powinny być udostępniane za pomocą środków komunikacji elektronicznej i mogą być wykorzystane wyłącznie do realizacji zadań publicznych.

3. Rada Ministrów określi, w drodze rozporządzenia, sposób, zakres i tryb udostępniania danych, o których mowa w ust. 1, mając na uwadze potrzebę usprawnienia realizacji zadań publicznych, zapewnienia szybkiego i bezpiecznego dostępu do danych oraz zabezpieczenia wykorzystania danych do celów realizacji zadań publicznych.

4. Przekazanie przez podmiot prowadzący rejestr publiczny danych z rejestru do ich ponownego wykorzystywania w celu innym niż realizacja zadania publicznego następuje na zasadach określonych w *[ustawie z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2019 r. poz. 1446)]*

Zmiana w ust. 4 w art. 15 wejdzie w życie z dn. 8.12.2021 r. (Dz. U. z 2021 r. poz. 1641).

<ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641)>.

Art. 15a. 1. Podmiot publiczny udostępnia dane gromadzone w prowadzonym rejestrze publicznym lub w systemie teleinformatycznym innemu podmiotowi publicznemu lub podmiotowi, o którym mowa w art. 19c ust. 1, z uwzględnieniem zasad przewidzianych w przepisach szczególnych dotyczących odpowiednio tego rejestru lub danych gromadzonych w tym systemie teleinformatycznym, wyłącznie na potrzeby usługi online, która jest świadczona na rzecz osoby albo podmiotu przy użyciu systemu teleinformatycznego.

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

2a. Wniosek, o którym mowa w ust. 2, kieruje się do podmiotu, o którym mowa w ust. 1, za pośrednictwem podmiotu udostępniającego usługę online.

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

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

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

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

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

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

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

1) uzupełnienia zakresu użytkowego dokumentu elektronicznego wymaganego w związku ze świadczoną usługą online;
2) potwierdzenia faktów lub stanu prawnego wymaganego w związku ze świadczoną usługą online.

Art. 15b. 1. Podmiot publiczny w celu ochrony interesu prawnego lub faktycznego osoby fizycznej, w szczególności w związku z realizowanymi na jej rzecz usługami, może wykorzystywać jej dane kontaktowe gromadzone w rejestrze publicznym lub systemach teleinformatycznych. Brak odpowiedzi osoby fizycznej na próbę nawiązania przez podmiot publiczny kontaktu z wykorzystaniem danych kontaktowych nie może negatywnie wpłynąć na jej sytuację prawną lub faktyczną.

2. Podmiot publiczny, wykorzystując dane kontaktowe osoby fizycznej, informuje ją o podstawie prawnej nawiązania kontaktu.

Art. 16. 1. Podmiot publiczny, organizując przetwarzanie danych w systemie teleinformatycznym, jest obowiązany zapewnić możliwość przekazywania danych również w postaci elektronicznej przez wymianę dokumentów elektronicznych związanych z załatwianiem spraw należących do jego zakresu działania, wykorzystując informatyczne nośniki danych lub środki komunikacji elektronicznej.

[1a. Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.]

Przepis uchylający ust. 1a i 1b w art. 16 wejdzie w życie z dn. 1.10.2029 r. (Dz. U. z 2020 r. poz. 2320).

[1b. Podmiot publiczny, w terminie 7 dni od dnia udostępnienia elektronicznej skrzynki podawczej, przekazuje ministrowi właściwemu do spraw informatyzacji informację o jej adresie.]

2. Podmiot publiczny, o którym mowa w ust. 1, jest obowiązany prowadzić wymianę informacji w postaci elektronicznej:

1) z wykorzystaniem systemów teleinformatycznych, spełniających minimalne wymagania dla systemów teleinformatycznych;

2) zgodnie z minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

3. Prezes Rady Ministrów określi, w drodze rozporządzenia:

[1) warunki organizacyjno-techniczne doręczania dokumentów elektronicznych, w tym reguły tworzenia elektronicznej skrzynki podawczej,]

[2) formę urzędowego poświadczania odbioru dokumentów elektronicznych przez adresatów,]

[3) sposób sporządzania i doręczania dokumentów elektronicznych,]

4) sposób udostępniania kopii dokumentów elektronicznych oraz warunki bezpieczeństwa udostępniania formularzy i wzorów dokumentów

– uwzględniając minimalne wymagania dla rejestrów publicznych i wymiany danych w postaci elektronicznej oraz potrzebę usprawnienia i ujednolicenia obiegu dokumentów między podmiotami publicznymi.

Przepis uchylający pkt 1, 2 i 3 w ust. 3 w art. 16 wejdzie w życie z dn. 1.10.2029 r. (Dz. U. z 2020 r. poz. 2320).

Art. 16a. 1. W przypadku gdy w przepisach prawa został wskazany organ właściwy do określenia wzoru dokumentu, jeżeli przepisy te nie wykluczają przesyłania dokumentów drogą elektroniczną, organ ten:

1) przekazuje ministrowi właściwemu do spraw informatyzacji wzór dokumentu elektronicznego w celu umieszczenia go w centralnym repozytorium wzorów dokumentów elektronicznych, o którym mowa w art. 19b ust. 1;
2) przekazuje ministrowi właściwemu do spraw informatyzacji opis usługi możliwej do zrealizowania przy wykorzystaniu wzoru dokumentu elektronicznego w celu zamieszczenia go w katalogu usług;
3) udostępnia na ePUAP lub w innym systemie teleinformatycznym formularz elektroniczny umożliwiający wygenerowanie dokumentu elektronicznego w celu złożenia go za pomocą środków komunikacji elektronicznej.

2. Czynności, o których mowa w ust. 1, organ realizuje w terminie 3 miesięcy od dnia wejścia w życie przepisów określających wzór dokumentu.

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

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

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

6. W celu poprawienia funkcjonalności usługi minister właściwy do spraw informatyzacji może, po zasięgnięciu opinii organu właściwego do określenia wzoru dokumentu oraz w uzasadnionych przypadkach organów, w których właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentu elektronicznego, udostępnić na ePUAP lub w innym systemie teleinformatycznym formularz elektroniczny.

7. Jeżeli organ właściwy do określenia wzoru dokumentu nie określił wzoru dokumentu elektronicznego, minister właściwy do spraw informatyzacji może, po zasięgnięciu opinii organu właściwego do określenia wzoru dokumentu oraz w uzasadnionych przypadkach organów, w których właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentu elektronicznego, określić wzór dokumentu elektronicznego.

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

Art. 16b. 1. W przypadku gdy w przepisach prawa nie został wskazany organ właściwy do określenia wzoru dokumentu, wzór dokumentu elektronicznego może przekazać do centralnego repozytorium wzorów dokumentów elektronicznych organ, w którego właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentów elektronicznych, lub minister właściwy do spraw informatyzacji po zasięgnięciu w uzasadnionych przypadkach opinii organów, w których właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentu elektronicznego.

2. Do przekazania, o którym mowa w ust. 1, stosuje się art. 16a ust. 1.

Art. 17. 1. Przy ministrze właściwym do spraw informatyzacji działa Rada do Spraw Cyfryzacji, zwana dalej „Radą”. Rada jest organem opiniodawczo-doradczym ministra.

2. Do zadań Rady należy:

1) proponowanie i opiniowanie na zlecenie ministra właściwego do spraw informatyzacji projektów stanowisk Rady Ministrów w sprawie dokumentów Komisji Europejskiej i Parlamentu Europejskiego dotyczących spraw informatyzacji, łączności lub rozwoju społeczeństwa informacyjnego;

1a) opiniowanie projektu Programu Zintegrowanej Informatyzacji Państwa oraz innych dokumentów rządowych, w tym projektów strategii rozwoju i projektów programów, w rozumieniu przepisów ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju, dotyczących spraw informatyzacji, łączności lub rozwoju społeczeństwa informacyjnego;

2) opiniowanie projektów przepisów wydawanych na podstawie art. 18;

3) opiniowanie innych przekazanych przez ministra właściwego do spraw informatyzacji projektów aktów prawnych i innych dokumentów dotyczących spraw informatyzacji, łączności lub rozwoju społeczeństwa informacyjnego;

4) opiniowanie na zlecenie ministra właściwego do spraw informatyzacji raportów i innych opracowań dotyczących:

   a) potrzeb i postulatów dotyczących rozwoju społeczeństwa informacyjnego,

   b) zasad funkcjonowania rejestrów publicznych,

   c) zasad wdrażania systemów teleinformatycznych w administracji publicznej oraz stanu ich realizacji,

   d) aktualnych rozwiązań technicznych mających zastosowanie w informatyzacji administracji, rozwoju sieci i usług szerokopasmowych,

   e) terminologii polskiej z zakresu informatyki i łączności.

3. Rada może inicjować działania na rzecz informatyzacji, rozwoju rynku technologii informatyczno-komunikacyjnych oraz rozwoju społeczeństwa informacyjnego.

4. Rada wyraża opinię w terminie 30 dni od dnia otrzymania projektów lub propozycji, o których mowa w ust. 2.

5. Opinie, protokoły posiedzeń oraz inne dokumenty Rady są publikowane w wydzielonej części Biuletynu Informacji Publicznej na stronach ministra właściwego do spraw informatyzacji.

6. Rada przedstawia ministrowi właściwemu do spraw informatyzacji sprawozdanie z działalności za każdy rok kalendarzowy w terminie do dnia 30 kwietnia następnego roku.

7. Rada składa się z od 15 do 20 członków.

8. Kandydatów na członków Rady mogą rekomendować:

1) ministrowie;
2) Naczelny Dyrektor Archiwów Państwowych;
3) Prezes Polskiego Komitetu Normalizacyjnego;
4) współprzewodniczący ze strony samorządowej Komisji Wspólnej Rządu i Samorządu Terytorialnego;
5) podmioty, o których mowa w art. 7 ust. 1 pkt 1, 2 i 4–8 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2020 r. poz. 85, 374, 695, 875 i 1086 oraz z 2021 r. poz. 159), które prowadzą badania naukowe lub prace rozwojowe w zakresie informatyki lub łączności;
6) izby gospodarcze reprezentujące przedsiębiorców wykonujących działalność gospodarczą w zakresie gospodarki elektronicznej, komunikacji, mediów, wytwarzania sprzętu informatycznego, oprogramowania lub świadczenia usług informatycznych;
7) stowarzyszenia wpisane do Krajowego Rejestru Sądowego, których celem statutowym jest reprezentowanie środowiska informatycznego lub wspieranie zastosowań informatyki, gospodarki elektronicznej, komunikacji lub mediów.

9. Rekomendowany do Rady kandydat powinien posiadać wykształcenie wyższe oraz wyrazić zgodę na kandydowanie.

10. Minister właściwy do spraw informatyzacji powołuje skład Rady na dwuletnią kadencję spośród kandydatów rekomendowanych przez podmioty, o których mowa w ust. 8.

11. Przed upływem kadencji członkostwo w Radzie wygasa z powodu:

1) rezygnacji członka Rady złożonej na piśmie Przewodniczącemu Rady;
2) śmierci członka Rady;
3) niemożności sprawowania funkcji członka Rady z powodu długotrwałej choroby stwierdzonej zaświadczeniem lekarskim;
4) wycofania rekomendacji podmiotu, o której mowa w ust. 8.

12. W przypadkach, o których mowa w ust. 11, minister właściwy do spraw informatyzacji powołuje na członka Rady osobę spośród pozostałych rekomendowanych kandydatów po sprawdzeniu aktualności rekomendacji.

13. Minister właściwy do spraw informatyzacji powołuje i odwołuje Przewodniczącego i Wiceprzewodniczącego Rady spośród jej członków.

14. Przewodniczący Rady kieruje jej pracami i reprezentuje ją na zewnątrz. W przypadku nieobecności Przewodniczącego zastępuje go Wiceprzewodniczący.

15. Obsługę Rady zapewnia urząd obsługujący ministra właściwego do spraw informatyzacji.

16. Na posiedzenie Rady mogą być zapraszane, przez ministra właściwego do spraw informatyzacji oraz Przewodniczącego Rady, inne osoby, o ile jest to wskazane dla realizacji zadań Rady.

17. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wysokość wynagrodzenia członka Rady za udział w posiedzeniu, uwzględniając funkcje pełnione przez członków Rady i zakres obowiązków członków Rady, a także mając na uwadze, że wynagrodzenie za jedno posiedzenie Rady nie może przekroczyć 50% minimalnego wynagrodzenia określonego na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2020 r. poz. 2207), obowiązującego w dniu powołania Rady.

18. Zamiejscowym członkom Rady przysługują diety oraz zwrot kosztów podróży i zakwaterowania na warunkach określonych w przepisach wydanych na podstawie art. 77^5 § 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2020 r. poz. 1320).

19. Szczegółowy tryb działania Rady określa jej regulamin ustanawiany na wniosek Rady przez ministra właściwego do spraw informatyzacji.

Art. 18. Rada Ministrów, na wniosek ministra właściwego do spraw informatyzacji, określi w drodze rozporządzenia:

1) minimalne wymagania dla systemów teleinformatycznych, mając na uwadze konieczność zapewnienia:
   a) spójności działania systemów teleinformatycznych używanych do realizacji zadań publicznych poprzez określenie co najmniej specyfikacji formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być

stosowane w oprogramowaniu interfejsowym, przy zachowaniu możliwości nieodpłatnego wykorzystania tych specyfikacji,

b) sprawnej i bezpiecznej wymiany informacji w postaci elektronicznej między podmiotami publicznymi oraz między podmiotami publicznymi a organami innych państw lub organizacji międzynarodowych

c) (uchylona)

– z uwzględnieniem Polskich Norm oraz innych dokumentów normalizacyjnych zatwierdzonych przez krajową jednostkę normalizacyjną, zachowując zasadę równego traktowania różnych rozwiązań informatycznych;

2) minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, uwzględniając konieczność zachowania spójności prowadzenia rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi;

3) Krajowe Ramy Interoperacyjności obejmujące zagadnienia interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z uwzględnieniem zasady równego traktowania różnych rozwiązań informatycznych, Polskich Norm oraz innych dokumentów normalizacyjnych zatwierdzonych przez krajową jednostkę normalizacyjną.

Art. 19. (uchylony)

Art. 19a. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie ePUAP.

[1a. Minister właściwy do spraw informatyzacji zamieszcza na ePUAP informację o adresach elektronicznych skrzynek podawczych udostępnionych przez podmioty publiczne.]

Przepis uchylający ust. 1a w art. 19a wejdzie w życie z dn. 1.10.2029 r. (Dz. U. z 2020 r. poz. 2320).

2. Minister właściwy do spraw informatyzacji jest administratorem danych użytkowników ePUAP.

2a. Minister właściwy do spraw informatyzacji, na wniosek banku krajowego lub innego przedsiębiorcy, udziela zgody na nieodpłatne wykorzystywanie do identyfikacji i uwierzytelniania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, po spełnieniu przez bank krajowy lub innego przedsiębiorcę warunków, o których mowa w przepisach wydanych na podstawie ust. 3.

2b. Minister właściwy do spraw informatyzacji może sprawdzać, czy bank krajowy lub inny przedsiębiorca, o którym mowa w ust. 1, spełnia warunki, o których mowa w przepisach wydanych na podstawie ust. 3.

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

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

1) zakres i warunki korzystania z ePUAP,
2) sposób identyfikacji i uwierzytelniania w ePUAP, w tym przy wykorzystaniu środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy,
3) warunki organizacyjne i techniczne nieodpłatnego wykorzystywania do identyfikacji i uwierzytelniania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy,
4) sposób potwierdzania spełniania warunków, o których mowa w pkt 1

– z uwzględnieniem roli ePUAP w procesie realizacji zadań publicznych drogą elektroniczną oraz zasad przetwarzania danych osobowych.

Art. 19b. 1. Minister właściwy do spraw informatyzacji w ramach ePUAP prowadzi centralne repozytorium wzorów dokumentów elektronicznych, zwane dalej „centralnym repozytorium”.

2. W centralnym repozytorium umieszcza się, przechowuje i udostępnia wzory dokumentów, które uwzględniają niezbędne elementy struktury dokumentów elektronicznych określone w przepisach wydanych na podstawie art. 5 ust. 2a ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164).

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. Jeżeli wzór podania określają odrębne przepisy, to umieszczenie wzoru dokumentu elektronicznego przez organy administracji publicznej w centralnym repozytorium jest równoznaczne z określeniem wzoru wnoszenia podań, o których mowa w art. 63 § 3a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2020 r. poz. 256, 695, 1298 i 2320 oraz z 2021 r. poz. 54 i 187).

5. Niezależnie od obowiązku wynikającego z ust. 3 organy administracji publicznej mogą prowadzić własne lub wspólnie z innymi organami administracji publicznej repozytoria wzorów dokumentów elektronicznych.

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

1) podmiotami, o których mowa w art. 2 ust. 3, realizującymi zadania publiczne,
2) innymi podmiotami realizującymi zadania publiczne lub wspierającymi świadczenie tych zadań w celu realizacji strategii i programów przyjętych przez Radę Ministrów lub strategii rozwoju, programów i dokumentów programowych w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju

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

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

Art. 19d. Podmioty udostępniające usługi na ePUAP zapewniają ich zgodność z przepisami stanowiącymi podstawę sporządzenia wzoru dokumentu elektronicznego oraz dokonują aktualizacji tych usług w katalogu usług.

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

1) pobranie, przechowywanie i prezentację dokumentów elektronicznych, o których mowa w ust. 2, a także przekazywanie tych dokumentów między urządzeniami mobilnymi lub do systemów teleinformatycznych;
2) weryfikację integralności i pochodzenia dokumentu elektronicznego.

1a. Minister właściwy do spraw informatyzacji może udostępniać w publicznej aplikacji mobilnej funkcjonalność pozwalającą na:

1) dostęp do usługi online obsługiwanej przy użyciu tej aplikacji;
2) potwierdzenie udziału w usługach świadczonych na rzecz użytkownika tej aplikacji w określonym miejscu i czasie;
3) korzystanie, przy użyciu urządzenia mobilnego, z certyfikatów zawartych w dowodzie osobistym z warstwą elektroniczną;
4) wykorzystanie tej aplikacji w celu przekazywania danych w ramach usług świadczonych na rzecz użytkownika tej aplikacji.

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

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

2a. Minister właściwy do spraw informatyzacji może zapewnić użytkownikowi publicznej aplikacji mobilnej możliwość posługiwania się certyfikatem stanowiącym poświadczenie elektroniczne pozwalające na:

1) potwierdzenie integralności i pochodzenia dokumentu elektronicznego;
2) potwierdzenie lub przekazanie danych osobowych tego użytkownika.

2b. Certyfikat:

1) może być wydany użytkownikowi publicznej aplikacji mobilnej:
   a) uwierzytelnionemu w sposób określony w art. 20a ust. 1 lub

b) o którym mowa w przepisach wydanych na podstawie art. 11 ust. 2 ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2020 r. poz. 1327 oraz z 2021 r. poz. 4), lub

c) o którym mowa w przepisach wydanych na podstawie art. 81 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce;

2) jest wydany w systemie teleinformatycznym, o którym mowa w ust. 2;

3) może zawierać dane, o których mowa odpowiednio w art. 56 ust. 1 pkt 1, 2 i 4 lit. a–c ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych oraz w art. 8 pkt 1–3, 4–6, 9–11, 14 i 22 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2019 r. poz. 1397 i 2294 oraz z 2020 r. poz. 695, 2320 i 2369).

2c. Minister właściwy do spraw informatyzacji zapewnia mechanizm weryfikacji ważności certyfikatu.

2d. Minister właściwy do spraw informatyzacji może wydać podmiotowi, o którym mowa odpowiednio w art. 19g ust. 1 i 2, certyfikat pozwalający na zabezpieczenie oraz potwierdzenie pochodzenia danych przekazywanych pomiędzy systemem teleinformatycznym, o którym mowa w ust. 2, a systemem teleinformatycznym tego podmiotu.

2e. Minister właściwy do spraw informatyzacji może udostępnić użytkownikowi publicznej aplikacji mobilnej usługę, która wykorzystuje dane dotyczące użytkownika i jego sytuacji prawnej lub praw mu przysługujących, przetwarzane w rejestrze publicznym prowadzonym lub w systemie teleinformatycznym wykorzystywanym przez podmiot publiczny, w przypadku gdy łącznie są spełnione następujące warunki:

1) odrębne przepisy przewidują udostępnianie użytkownikowi takich danych przy wykorzystaniu usługi online lub na wniosek, albo nie stoją na przeszkodzie udostępnianiu użytkownikowi takich danych;

2) użytkownik, który został uwierzytelniony w publicznej aplikacji mobilnej w sposób określony w art. 20a ust. 1, wyraził wolę korzystania z usługi wykorzystującej takie dane.

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

1) Rejestru Dowodów Osobistych aktualne dane, o których mowa w art. 56 pkt 1, 2 i 4 lit. a–c ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych;

2) rejestru PESEL aktualne dane, o których mowa w art. 8 pkt 1–3, 4–6, 9–11, 14 i 22 ustawy z dnia 24 września 2010 r. o ewidencji ludności.

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

Art. 19ea. 1. Minister właściwy do spraw informatyzacji może realizować zadania, o których mowa w art. 19e ust. 1 i 2, w całości lub w części przy pomocy właściwych w tym zakresie jednostek podległych ministrowi właściwemu do spraw informatyzacji lub przez niego nadzorowanych.

2. Realizacja zadań, o których mowa w ust. 1, może być finansowana w formie dotacji celowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji.

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

1) jest bezpłatne i dobrowolne.

2) (uchylony)

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

3. Użytkownik aplikacji mobilnej może w każdej chwili zrezygnować z korzystania z publicznej aplikacji mobilnej.

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

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

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

1) odpowiednio określenie:

a) dokumentu elektronicznego oraz zakresu zawartych w nim danych,
b) certyfikatu, w tym zakresu zawartych w nim danych;

2) cel i zakres wykorzystywania publicznej aplikacji mobilnej oraz systemu teleinformatycznego;
3) warunki organizacyjne i techniczne wykorzystania publicznej aplikacji mobilnej oraz systemu teleinformatycznego.

4. Porozumienie, o którym mowa w ust. 1 i 2, opatruje się podpisem zaufanym, podpisem osobistym lub kwalifikowanym podpisem elektronicznym.

Art. 19h. Minister właściwy do spraw informatyzacji przetwarza w systemie teleinformatycznym, o którym mowa w art. 19e, dane osobowe użytkowników publicznej aplikacji mobilnej w zakresie niezbędnym do obsługi dokumentów elektronicznych oraz realizacji czynności, o których mowa w art. 19e, a także zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego. Dane przetwarzane są przez okres 6 lat od dnia ostatniej aktywności użytkownika w systemie.

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

1) aktywnych i nieaktywnych, w tym czasowo zawieszonych, funkcjonalnościach publicznej aplikacji mobilnej;
2) stosowanych mechanizmach zapewniających możliwość potwierdzenia integralności i pochodzenia dokumentów elektronicznych oraz procedurach uzyskania takiego potwierdzenia;
3) adresach elektronicznych, pod którymi są udostępnione:
   a) regulamin korzystania z publicznej aplikacji mobilnej,
   b) informacja o wymaganiach technicznych dotyczących korzystania z publicznej aplikacji mobilnej;
4) warunkach korzystania z certyfikatu.

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

Art. 20. (uchylony)

Art. 20a. 1. Uwierzytelnienie użytkownika systemu teleinformatycznego podmiotu publicznego, w którym udostępniane są usługi online, wymaga użycia:

1) środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173 i 2320), lub
2) środka identyfikacji elektronicznej wydanego w notyfikowanym systemie identyfikacji elektronicznej, lub
3) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online.

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

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

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

1) szczegółowe warunki organizacyjne i techniczne, które powinien spełniać system teleinformatyczny służący do wydania certyfikatu oraz stosowania technologii, o których mowa w ust. 2, w tym:
   a) zakres i okres przechowywania danych w systemie,
   b) obowiązki informacyjne, do których zobowiązany jest administrator systemu
2) (uchylony)

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

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

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

Art. 20ab. Minister właściwy do spraw informatyzacji:
1) zarządza publicznym systemem identyfikacji elektronicznej;
2) zapisuje i zachowuje informacje związane z zapewnieniem rozliczalności i niezaprzeczalności działań użytkownika korzystającego ze środka identyfikacji elektronicznej wydanego w publicznym systemie identyfikacji elektronicznej.

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

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

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

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

1) imię (imiona);
2) nazwisko;
3) numer PESEL.

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

1) imię (imiona);
2) nazwisko;
3) datę urodzenia;
4) numer PESEL.

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

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

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

4a. W przypadku gdy w rejestrze PESEL został odnotowany zgon osoby posiadającej profil zaufany, profil zaufany tej osoby jest automatycznie unieważniany.

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

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

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

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

Art. 20b. (uchylony)

Art. 20c. 1. Potwierdzenia profilu zaufanego, które polega na weryfikacji zgodności danych zawartych we wniosku o jego wydanie ze stanem faktycznym, oraz unieważnienia profilu zaufanego dokonuje:

1) punkt potwierdzający profil zaufany na podstawie:
   a) dowodu osobistego albo paszportu zawierającego:
      – imię (imiona),
      – nazwisko,
      – numer PESEL, albo
   b) innego dokumentu tożsamości, jeżeli umożliwia on jednoznaczne potwierdzenie tożsamości osoby wnioskującej o potwierdzenie profilu zaufanego posiadającej numer PESEL;
2) samodzielnie osoba fizyczna przy wykorzystaniu kwalifikowanego podpisu elektronicznego, w przypadku gdy kwalifikowany certyfikat podpisu elektronicznego zawiera dane obejmujące co najmniej:
   a) imię (imiona),
   b) nazwisko,
   c) numer PESEL;
3) samodzielnie osoba fizyczna przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy spełniającym warunki, o których mowa w art. 20d pkt 1, o ile środek ten potwierdza dane obejmujące co najmniej:
   a) imię (imiona),
   b) nazwisko,
   c) numer PESEL;
4) samodzielnie osoba fizyczna przy wykorzystaniu profilu osobistego.

1a. Przedłużenie ważności profilu zaufanego może nastąpić w sposób, o którym mowa w ust. 1 pkt 1, 2 i 4, albo przy wykorzystaniu profilu zaufanego.

2. Funkcję punktu potwierdzającego pełni:

1) konsul;
2) naczelnik urzędu skarbowego;
3) wojewoda;
4) Zakład Ubezpieczeń Społecznych;
5) Narodowy Fundusz Zdrowia.

2a. Narodowy Fundusz Zdrowia może nadać uprawnienia do potwierdzania w swoim imieniu profilu zaufanego lekarzowi podstawowej opieki zdrowotnej, pielęgniarce podstawowej opieki zdrowotnej, położnej podstawowej opieki zdrowotnej realizującym zadania w zakresie podstawowej opieki zdrowotnej dla świadczeniodawcy, który udziela świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej, oraz osobie zatrudnionej u tego świadczeniodawcy pod warunkiem, że co najmniej imię, nazwisko i numer PESEL tej osoby zostały przekazane do Narodowego Funduszu Zdrowia w ramach zawartej umowy.

2b. Osoba posiadająca uprawnienia do potwierdzania profilu zaufanego, o której mowa w ust. 2a, może potwierdzić profil zaufany wyłącznie świadczeniobiorcy, który w deklaracji wyboru, o której mowa w art. 10 ust. 1 ustawy z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz. U. z 2020 r. poz. 172 i 1493), wskazał świadczeniodawcę, w ramach którego działa osoba potwierdzająca profil zaufany.

2c. Narodowy Fundusz Zdrowia niezwłocznie odbiera uprawnienia do potwierdzania profilu zaufanego w przypadku ustania okoliczności, o których mowa w ust. 2a.

2d. Minister właściwy do spraw informatyzacji może udostępnić rozwiązanie techniczne przeznaczone do przekazywania informacji o zdarzeniach, o których mowa w ust. 2a i 2b, pomiędzy systemem teleinformatycznym Narodowego Funduszu Zdrowia, w którym znajdują się dane o świadczeniodawcach udzielających świadczeń z zakresu podstawowej opieki zdrowotnej, na podstawie zawartej z Narodowym Funduszem Zdrowia umowy o udzielanie świadczeń z zakresu podstawowej opieki zdrowotnej, a systemem, o którym mowa w art. 20aa *ust. 1*, zapewniające automatyczną weryfikację i aktualizację uprawnień do potwierdzania profilu zaufanego.

2e. W przypadku, o którym mowa w ust. 2a, dokumenty w postaci papierowej w zakresie potwierdzania, przedłużania i unieważniania profilu zaufanego w sposób i przez okres określony w przepisach wydanych na podstawie art. 20d przechowuje i archiwizuje świadczeniodawca.

3. Funkcję punktu potwierdzającego, za zgodą ministra właściwego do spraw informatyzacji, może pełnić:

1) podmiot publiczny inny niż wymieniony w ust. 2;

2) bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2020 r. poz. 1896, 2320 i 2419);
3) operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2020 r. poz. 1041 i 2320);
4) oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe;
5) spółdzielcza kasa oszczędnościowo-kredytowa, o której mowa w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2020 r. poz. 1643 i 1639).

4. Zgody, o której mowa w ust. 3, udziela się na wniosek podmiotów, o których mowa w ust. 3, po spełnieniu warunków określonych w przepisach wydanych na podstawie art. 20d pkt 1.

5. Operator pocztowy może złożyć wniosek, o którym mowa w ust. 4, nie wcześniej niż w roku następującym po roku, w którym po raz pierwszy przedłożył Prezesowi Urzędu Komunikacji Elektronicznej sprawozdanie, o którym mowa w art. 43 ust. 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe.

6. Minister właściwy do spraw informatyzacji może sprawdzać, czy podmiot pełniący funkcję punktu potwierdzającego spełnia warunki określone w przepisach wydanych na podstawie art. 20d pkt 1.

7. Minister właściwy do spraw informatyzacji cofa zgodę, o której mowa w ust. 3, w przypadku gdy podmiot pełniący funkcję punktu potwierdzającego nie spełnia warunków określonych w przepisach wydanych na podstawie art. 20d pkt 1.

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

9. Minister właściwy do spraw informatyzacji może sprawdzać, czy bank krajowy lub inny przedsiębiorca, o którym mowa w ust. 8, spełnia warunki, o których mowa w przepisach wydanych na podstawie art. 20d pkt 1.

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. 20d pkt 1.

Art. 20ca. (uchylony)

Art. 20cb. 1. Minister właściwy do spraw informatyzacji może udostępnić usługę online służącą do potwierdzania profilu zaufanego przy użyciu metody, o której mowa w ust. 2.

2. W celu potwierdzenia tożsamości osoby wnioskującej o potwierdzenie profilu zaufanego przeprowadza się wideoidentyfikację wnioskodawcy polegającą na:

1) porównaniu wizerunku wnioskodawcy udostępnianego przez niego w czasie rzeczywistym za pośrednictwem transmisji audiowizualnej z wizerunkiem tego wnioskodawcy pobranym z Rejestru Dowodów Osobistych, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych, oraz
2) weryfikacji danych zawartych w warstwie graficznej dowodu osobistego albo paszportu wnioskodawcy okazanego przez niego w czasie rzeczywistym za pośrednictwem transmisji audiowizualnej, oraz
3) w uzasadnionych przypadkach – weryfikacji wiedzy wnioskodawcy przy wykorzystaniu danych dotyczących wnioskodawcy zgromadzonych w rejestrach publicznych lub w systemach teleinformatycznych.

3. Potwierdzanie profilu zaufanego przy użyciu metody, o której mowa w ust. 2, realizuje minister właściwy do spraw informatyzacji.

4. Minister właściwy do spraw informatyzacji może upoważnić do potwierdzania profilu zaufanego przy użyciu metody, o której mowa w ust. 2, jednostkę podległą lub nadzorowaną.

5. Z transmisji, o której mowa w ust. 2 pkt 1, sporządza się nagranie audiowizualne. Nagranie sporządza i przechowuje przez 6 lat od dnia jego sporządzenia podmiot, który potwierdza profil zaufany przy użyciu metody, o której mowa w ust. 2.

6. Minister właściwy do spraw informatyzacji może zawiesić lub zaprzestać świadczenia usługi, o której mowa w ust. 1, w przypadku zaistnienia okoliczności, które mogłyby wpływać na bezpieczeństwo metody potwierdzania tożsamości stosowanej w ramach tej usługi, i informuje o tym na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

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

1) wydawania, przedłużania ważności, wykorzystywania i unieważniania profilu zaufanego, w tym:
   a) okres ważności profilu zaufanego,
   b) zbiór danych zawartych w profilu zaufanym, o których mowa w art. 20ad ust. 5,
   c) przypadki, w których nie dokonuje się potwierdzenia profilu zaufanego,
   d) przypadki, w których profil zaufany traci ważność,
   e) warunki przechowywania oraz archiwizowania dokumentów i danych bezpośrednio związanych z potwierdzeniem profilu zaufanego,
   f) dane i dokumenty wymagane w procedurze potwierdzania, przedłużania ważności i unieważnienia profilu zaufanego,
   g) warunki, które powinien spełniać punkt potwierdzający profil zaufany,
   h) warunki organizacyjne i techniczne potwierdzenia profilu zaufanego oraz uwierzytelnień i autoryzacji przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy,
   i) sposób potwierdzania spełniania warunków, o których mowa w lit. h,
2) składania podpisu zaufanego

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

Art. 20e. 1. Minister właściwy do spraw informatyzacji przyłącza system teleinformatyczny, w którym udostępniane są usługi online, do systemu, o którym mowa w art. 20aa, w celu wykorzystywania podpisu zaufanego, na wniosek podmiotu odpowiedzialnego za ten system. Przyłączenie jest czynnością materialno-techniczną.

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

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

Art. 20f. (uchylony)

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

Rozdział 3a

Rejestr danych kontaktowych osób fizycznych

Art. 20h. 1. Minister właściwy do spraw informatyzacji prowadzi rejestr danych kontaktowych osób fizycznych, zwany dalej „rejestrem danych kontaktowych”.

2. Prowadzenie rejestru danych kontaktowych ma na celu ułatwienie:

1) podmiotom, o których mowa w art. 2 ust. 1 pkt 1, 2 i 4–8,
2) podmiotom, o których mowa w art. 19c, jeżeli zawarły porozumienie z ministrem właściwym do spraw informatyzacji,
3) organom wyborczym,
4) Polskiemu Czerwonemu Krzyżowi – w zakresie danych osób poszukiwanych lub poszukujących

– kontaktu z osobami fizycznymi w związku z usługami i zadaniami publicznymi realizowanymi na rzecz tych osób.

3. Do rejestru danych kontaktowych swoje dane kontaktowe mogą przekazać osoby pełnoletnie, posiadające pełną zdolność do czynności prawnych.

4. Dane kontaktowe nie są wykorzystywane w celu kontaktu z osobami fizycznymi w zakresie związanym z prowadzoną przez nie działalnością gospodarczą.

Art. 20i. 1. Rejestr danych kontaktowych prowadzi się przy użyciu systemu teleinformatycznego, w tym:

1) zapewnia ochronę przed nieuprawnionym dostępem do rejestru danych kontaktowych;
2) zapewnia integralność danych w rejestrze danych kontaktowych;
3) zapewnia dostępność systemu teleinformatycznego, w którym rejestr danych kontaktowych jest prowadzony, dla podmiotów przetwarzających dane w rejestrze danych kontaktowych;
4) przeciwdziała uszkodzeniom systemu teleinformatycznego, w którym rejestr danych kontaktowych jest prowadzony;
5) określa zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych;

6) zapewnia rozliczalność działań dokonywanych na danych rejestru danych kontaktowych.

2. Minister właściwy do spraw informatyzacji jest administratorem danych przetwarzanych w rejestrze danych kontaktowych.

Art. 20j. 1. Do rejestru danych kontaktowych wprowadza się:

1) numer PESEL;
2) imię i nazwisko;
3) adres poczty elektronicznej lub numer telefonu komórkowego.

2. Przy wprowadzaniu danych, o których mowa w ust. 1, do rejestru danych kontaktowych przepisów art. 14 ust. 6 i 7 nie stosuje się.

3. W przypadku pozytywnego wyniku weryfikacji, o której mowa w art. 14 ust. 3, dane są automatycznie wprowadzane do rejestru danych kontaktowych.

4. W przypadku negatywnego wyniku weryfikacji, o której mowa w art. 14 ust. 3, osoba wprowadzająca dane do rejestru danych kontaktowych informowana jest o negatywnej weryfikacji danych.

5. Dane, o których mowa w ust. 1, podlegają usunięciu z rejestru danych kontaktowych z mocy prawa na podstawie przekazanej przez rejestr PESEL informacji o zgonie osoby fizycznej, której te dane dotyczą.

6. W przypadku zmiany danych, o których mowa w ust. 1 pkt 1 i 2, w rejestrze PESEL następuje ich automatyczna aktualizacja w rejestrze danych kontaktowych.

7. Dotychczasowe dane, o których mowa w ust. 1 pkt 1 i 2, zachowuje się w rejestrze danych kontaktowych przez 4 miesiące od daty zmiany tych danych w rejestrze PESEL, a po upływie tego terminu dane te są automatycznie usuwane z rejestru danych kontaktowych.

8. Podmiot, o którym mowa w art. 2 ust. 1 pkt 1, 2 i 4–8, posiadający dostęp do rejestru danych kontaktowych jest obowiązany dokonać na wniosek osoby, której dane dotyczą, aktualizacji danych, o których mowa w ust. 1 pkt 3, lub usunięcia jej danych z rejestru danych kontaktowych.

9. W przypadku usunięcia z rejestru danych kontaktowych wszystkich danych, o których mowa w ust. 1 pkt 3, automatycznie usuwane są również dane, o których mowa w ust. 1 pkt 1 i 2.

Art. 20k. 1. Podstawą przetwarzania danych osobowych w rejestrze danych kontaktowych jest zgoda osoby, której dane dotyczą.

2. Dane do rejestru danych kontaktowych są przekazywane, aktualizowane lub usuwane:

1) samodzielnie przez osobę fizyczną, przy użyciu usługi online udostępnionej przez ministra właściwego do spraw informatyzacji, po uwierzytelnieniu w sposób określony w art. 20a ust. 1;
2) za pośrednictwem podmiotu, o którym mowa w art. 2 ust. 1 pkt 1, 2 i 4–8, posiadającego dostęp do rejestru danych kontaktowych, na wniosek złożony osobiście w siedzibie tego podmiotu przez osobę, której dane dotyczą.

3. Przekazaniu podlegają dane, o których mowa w art. 20j ust. 1:

1) pkt 1 i 2 – w celu identyfikacji osoby fizycznej i weryfikacji tych danych;
2) pkt 3 – w celu ułatwienia podmiotom, o których mowa w art. 20m ust. 1, kontaktu z osobą fizyczną.

4. Przekazywane dane są wprowadzane do rejestru danych kontaktowych po potwierdzeniu ich poprawności oraz przyporządkowaniu do osoby, której dane dotyczą, realizowanym przy użyciu jednorazowego kodu wysłanego odpowiednio na przekazany do tego rejestru adres poczty elektronicznej lub numer telefonu komórkowego.

Art. 20l. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia:

1) sposób wprowadzania, zapisu, aktualizacji oraz potwierdzania danych kontaktowych,
2) sposób prowadzenia rejestru danych kontaktowych,
3) wzór wniosku w postaci papierowej, o którym mowa w art. 20k ust. 2 pkt 2 oraz w art. 20j ust. 8,
4) wzór uproszczonego wniosku o udostępnianie danych z rejestru danych kontaktowych, o którym mowa w art. 20m ust. 2

– uwzględniając konieczność zapewnienia sprawności, prawidłowości i bezpieczeństwa funkcjonowania systemu teleinformatycznego, przy użyciu którego prowadzony jest rejestr danych kontaktowych, oraz prawidłowości danych przetwarzanych w tym rejestrze.

Art. 20m. 1. Dane zgromadzone w rejestrze danych kontaktowych udostępnia się:

1) podmiotom, o których mowa w art. 2 ust. 1 pkt 1, 2 i 4–8;

2) podmiotom, o których mowa w art. 19c, jeżeli zawarły porozumienie z ministrem właściwym do spraw informatyzacji;
3) organom wyborczym;
4) Polskiemu Czerwonemu Krzyżowi – w zakresie danych osób poszukiwanych lub poszukujących.

2. Podmiotowi, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji udostępnia dane z rejestru danych kontaktowych za pomocą urządzeń teletransmisji danych, po złożeniu jednorazowego uproszczonego wniosku, jeżeli podmiot ten spełnia łącznie następujące warunki:

1) posiada urządzenia lub systemy teleinformatyczne przeznaczone do komunikowania się pomiędzy uprawnionym podmiotem a rejestrem danych kontaktowych, umożliwiające identyfikację osoby, której udostępniono dane z rejestru danych kontaktowych, zakres udostępnionych danych oraz datę ich udostępnienia;
2) posiada zabezpieczenia techniczne i organizacyjne właściwe dla przetwarzania danych osobowych, w szczególności uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystanie danych niezgodnie z celem ich udostępnienia;
3) udostępnienie danych tą drogą jest uzasadnione specyfiką lub zakresem wykonywanych zadań, świadczonych usług albo prowadzonej działalności.

3. Wniosek, o którym mowa w ust. 2, złożony w postaci elektronicznej opatruje się podpisem zaufanym, podpisem osobistym albo kwalifikowanym podpisem elektronicznym.

4. Organowi gminy zapewnia się dostęp do danych zgromadzonych w rejestrze danych kontaktowych bez konieczności składania wniosku, o którym mowa w ust. 2.

Art. 20n. 1. Udostępnienie danych, odmowa udostępnienia danych oraz cofnięcie dostępu do danych zgromadzonych w rejestrze danych kontaktowych następuje w drodze decyzji administracyjnej.

2. Podmiotowi lub organowi, o których mowa w art. 20m, minister właściwy do spraw informatyzacji cofa dostęp do danych zgromadzonych w rejestrze danych kontaktowych:

1) na wniosek tego podmiotu lub organu;

2) w przypadku braku uzasadnienia dla dalszej wymiany danych między tym systemem teleinformatycznym a systemem teleinformatycznym, w którym prowadzony jest rejestr danych kontaktowych, w szczególności w przypadku gdy podmiot lub organ zaprzestał realizacji usług lub zadań, o których mowa w art. 20h ust. 2;
3) jeżeli nie zostały spełnione warunki, o których mowa w art. 20m ust. 2 pkt 3.

3. Decyzja o cofnięciu dostępu do danych zgromadzonych w rejestrze danych kontaktowych za pomocą urządzeń teletransmisji danych podlega natychmiastowemu wykonaniu.

4. Do organu gminy przepisów ust. 1–3 nie stosuje się.

Art. 20o. Osobie fizycznej, po uprzednim jej uwierzytelnieniu w sposób określony w art. 20a ust. 1, zapewnia się wgląd do dotyczących jej danych, o których mowa w art. 20j ust. 1.

<Rozdział 3b

Zintegrowana platforma analityczna

Dodany rozdział 3b (art. 20p–20t) wejdzie w życie z dn. 8.12.2021 r. (Dz. U. z 2021 r. poz. 1641).

Art. 20p. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie rozwiązania organizacyjno-technicznego, zwanego dalej „zintegrowaną platformą analityczną”, służącego do prowadzenia analiz wspomagających tworzenie kluczowych polityk publicznych z wykorzystaniem danych udostępnianych przez podmioty, o których mowa w art. 2, gromadzonych w rejestrach publicznych i systemach teleinformatycznych.

Art. 20q. 1. W ramach zintegrowanej platformy analitycznej minister właściwy do spraw informatyzacji przetwarza dane udostępnione z rejestrów publicznych i systemów teleinformatycznych określonych w przepisach wydanych na podstawie ust. 7, w celu wykonywania zadań związanych z analizami wspomagającymi tworzenie kluczowych polityk publicznych.

2. Podmioty prowadzące rejestry publiczne i systemy teleinformatyczne określone w przepisach wydanych na podstawie ust. 7 udostępniają na potrzeby analiz w ramach zintegrowanej platformy analitycznej dane określone w tych przepisach, zgromadzone przez te podmioty na podstawie przepisów odrębnych w związku z realizacją zadań publicznych.

3. Jeżeli jest to niezbędne do realizacji konkretnej analizy w ramach zintegrowanej platformy analitycznej, dane udostępnione z różnych rejestrów publicznych i systemów teleinformatycznych mogą być łączone.

4. Dane osobowe udostępniane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej podlegają pseudonimizacji.

5. Pseudonimizacja jest dokonywana przez organ lub podmiot, który udostępnia dane, po określeniu niezbędnego celu i zakresu prowadzonej analizy.

6. Podmiot, który udostępnia dane, oraz minister właściwy do spraw informatyzacji uzgadniają metodę pseudonimizacji udostępnianych danych oraz tryb udostępniania, mając na uwadze cel, zakres analizy oraz przepisy o ochronie danych osobowych.

7. Rada Ministrów określi, w drodze rozporządzenia, zakres danych i wykaz rejestrów publicznych i systemów teleinformatycznych, z których są udostępniane niezbędne dane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej, oraz podmiotów je prowadzących, które są obowiązane do przekazywania danych pochodzących z tych rejestrów i systemów, a także sposób udostępniania tych danych, mając na uwadze zapewnienie skutecznego pozyskiwania danych oraz zgodności ich udostępniania z przepisami o ochronie danych osobowych.

Art. 20r. 1. Minister właściwy do spraw informatyzacji zawiera porozumienie w sprawie wykorzystywania zintegrowanej platformy analitycznej z podmiotem, o którym mowa w art. 2, na potrzeby kluczowej polityki publicznej.

2. Porozumienie określa w szczególności:

1) cel analizy;

2) zakres danych niezbędnych do przeprowadzania analizy;

3) rejestry publiczne i systemy teleinformatyczne, które zawierają dane na potrzeby prowadzenia analizy oraz podmioty je prowadzące.

3. Zawarcie porozumienia poprzedza się przeprowadzeniem weryfikacji dotyczącej celu i zakresu analizy wspomagającej tworzenie kluczowej polityki publicznej oraz niezbędności łączenia danych udostępnianych z rejestrów publicznych i systemów teleinformatycznych dla realizacji tej analizy.

Art. 20s. 1. Minister właściwy do spraw informatyzacji w ramach zapewniania funkcjonowania zintegrowanej platformy analitycznej:

1) zapewnia ochronę przed nieuprawnionym dostępem do danych;

2) przeciwdziała uszkodzeniom zintegrowanej platformy analitycznej;

3) zapewnia integralność gromadzonych danych;

4) określa zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych;

5) zapewnia rozliczalność działań dokonywanych w ramach zintegrowanej platformy analitycznej;

6) określa zasady zgłaszania naruszenia ochrony danych osobowych.

2. Dane osobowe przetwarzane w ramach zintegrowanej platformy analitycznej są wykorzystywane adekwatnie, w sposób stosowny i ograniczony, wyłącznie w zakresie niezbędnym do realizacji określonych celów analitycznych.

3. Wykorzystywanie danych do celów innych niż określone w ustawie, w szczególności do podejmowania decyzji lub indywidualnych rozstrzygnięć, jest zabronione.

Art. 20t. Dane przetwarzane w ramach zintegrowanej platformy analitycznej są usuwane niezwłocznie po przeprowadzeniu analiz, na potrzeby których dane zostały udostępnione.>

Rozdział 4

Badanie osiągania interoperacyjności oraz kontrola przestrzegania przepisów ustawy

Art. 21. 1. W celu zapewnienia interoperacyjności systemów teleinformatycznych używanych do realizacji zadań publicznych przeprowadza się, z zastrzeżeniem art. 24, badanie poprawności wdrożenia rozwiązań, o których mowa w art. 13 ust. 2 pkt 2 lit. a, w oprogramowaniu interfejsowym przy wykorzystaniu testów akceptacyjnych udostępnionych przez podmiot publiczny, zgodnie z art. 13 ust. 2 pkt 2 lit. b, zwane dalej „badaniem”.

2. Badanie przeprowadza, na własny koszt, twórca oprogramowania interfejsowego albo inny podmiot posiadający autorskie prawa majątkowe do oprogramowania interfejsowego, które ma być wykorzystywane do realizacji zadania publicznego, zwany dalej „podmiotem uprawnionym”:

1) przed udostępnieniem po raz pierwszy oprogramowania interfejsowego do realizacji tego zadania;
2) po modyfikacji oprogramowania interfejsowego w zakresie, o którym mowa w art. 13 ust. 2 pkt 2 lit. a, dokonanej od czasu poprzedniego badania.

3. Podmiot uprawniony:

1) informuje podmiot publiczny o rodzaju, wersji, dacie wytworzenia i charakterystyce techniczno-funkcjonalnej oprogramowania interfejsowego poddawanego badaniu;
2) składa podmiotowi publicznemu oświadczenie o wyniku badania.

4. W celu potwierdzenia wyniku badania podmiot publiczny może przeprowadzić weryfikację tego badania, wykorzystując testy akceptacyjne udostępnione podmiotowi uprawnionemu. Podmiot publiczny informuje podmiot uprawniony o wyniku weryfikacji.

5. W razie niezgodności wyniku weryfikacji z wynikiem badania dokonanego przez podmiot uprawniony rozstrzyga wynik weryfikacji. W tym przypadku koszty weryfikacji ponosi podmiot uprawniony.

5a. W celu zapewnienia interoperacyjności systemów teleinformatycznych używanych do realizacji zadań publicznych z innymi systemami teleinformatycznymi podmiot publiczny może udostępnić testowy system teleinformatyczny, funkcjonalnie odpowiadający systemowi produkcyjnemu, w celu dokonywania sprawdzenia poprawności wdrożenia rozwiązań pod względem organizacyjnym, semantycznym i technologicznym.

5b. W przypadku udostępnienia przez podmiot publiczny systemu testowego nie jest wymagane udostępnienie testów akceptacyjnych.

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

1) metodykę, warunki i tryb sporządzania testów akceptacyjnych,
2) sposób postępowania w zakresie badania oraz weryfikacji badania, w tym sposób dokumentowania wyników badania oraz weryfikacji badania,
3) rodzaje oprogramowania interfejsowego podlegającego badaniu,
4) szczegółowy zakres informacji, o których mowa w ust. 3 pkt 1, oraz sposób i tryb przekazywania tych informacji,
5) wzór oświadczenia o wyniku badania oraz wyniku weryfikacji badania

– uwzględniając konieczność wprowadzenia jednolitych warunków przygotowania rzetelnego zestawu testów akceptacyjnych oraz dokonania obiektywnej oceny oprogramowania interfejsowego.

Art. 22. 1. Oprogramowanie interfejsowe może być używane do realizacji zadań publicznych, jeżeli uzyskało pozytywny wynik badania.

2. Podmiot publiczny może nieodpłatnie udostępnić oprogramowanie interfejsowe, które uzyskało pozytywny wynik badania, albo jego kody źródłowe, w zakresie określonym w umowie licencyjnej z podmiotem uprawnionym.

3. W razie stwierdzenia używania do realizacji zadania publicznego oprogramowania interfejsowego, które:

1) nie zostało poddane badaniu,
2) nie uzyskało pozytywnego wyniku badania w przypadkach, o których mowa w art. 21 ust. 2

– podmiot publiczny może odmówić przyjęcia danych przekazywanych za pomocą tego oprogramowania; w takim przypadku odmowa przyjęcia danych jest równoznaczna z nieprzekazaniem tych danych.

Art. 23. 1. Przepisy art. 21 i 22 stosuje się odpowiednio, jeżeli:

1) podmiot publiczny jest podmiotem uprawnionym;
2) podmiot uprawniony przekazał podmiotowi publicznemu autorskie prawa majątkowe do oprogramowania interfejsowego.

2. W przypadkach, o których mowa w ust. 1, w razie zaistnienia okoliczności, o których mowa w art. 22 ust. 3 pkt 1 albo 2, oprogramowanie interfejsowe nie może być używane do realizacji zadań publicznych do czasu uzyskania pozytywnego wyniku badania.

Art. 24. Przepisów art. 21–23 nie stosuje się w przypadku, o którym mowa w art. 13 ust. 4, chyba że:

1) podmiot publiczny udostępnił testy akceptacyjne;
2) podmiot uprawniony wystąpił o udostępnienie testów akceptacyjnych w celu przeprowadzenia badania;
3) podmiot publiczny udostępnił system testowy, o którym mowa w art. 21 ust. 5a.

Art. 25. 1. Kontroli:

1) realizacji ponadsektorowych projektów informatycznych dokonuje Prezes Rady Ministrów;
2) realizacji sektorowych projektów informatycznych dokonuje minister kierujący działem administracji rządowej, dla którego ustanowiono sektorowy projekt informatyczny;
3) działania systemów teleinformatycznych, używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2, dokonuje:
   a) w jednostkach samorządu terytorialnego i ich związkach oraz w tworzonych lub prowadzonych przez te jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych – właściwy wojewoda, z zastrzeżeniem ust. 3,
   b) w podmiotach publicznych podległych lub nadzorowanych przez organy administracji rządowej – organ administracji rządowej nadzorujący dany podmiot publiczny,
   c) w podmiotach publicznych niewymienionych w lit. a i b – minister właściwy do spraw informatyzacji

   – pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

2. (uchylony)

3. W stosunku do organów i jednostek, o których mowa w ust. 1 pkt 3 lit. a, kontrola może dotyczyć wyłącznie systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej. Jeżeli do uzyskania pełnej oceny systemu teleinformatycznego lub rejestru publicznego używanego do realizacji zadań zleconych z zakresu administracji rządowej niezbędna jest ocena także innego systemu teleinformatycznego lub rejestru publicznego, kontrolą może zostać objęty także ten system lub rejestr.

4. Kontroli w zakresie prawidłowości wydatkowania środków finansowych przekazywanych na podstawie art. 12f, z punktu widzenia legalności, gospodarności, celowości i rzetelności wydatkowania środków publicznych:

1) podmiotów określonych w ust. 1 pkt 3 lit. a – dokonuje właściwa regionalna izba obrachunkowa, na zasadach określonych w ustawie z dnia 7 października 1992 r. o regionalnych izbach obrachunkowych (Dz. U. z 2019 r. poz. 2137);

2) podmiotów niewymienionych w pkt 1 – dokonuje minister właściwy do spraw informatyzacji.

Art. 25a. Do kontroli stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224) określające zasady i tryb przeprowadzania kontroli.

Art. 26. (uchylony)

Art. 27. (uchylony)

Art. 28. 1. Kontrolerem może być osoba pełnoletnia, która:

1) posiada wykształcenie wyższe;
2) posiada obywatelstwo państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej lub państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym, chyba że przepisy odrębne uzależniają zatrudnienie jej w jednostce kontrolowanej od posiadania obywatelstwa polskiego;
3) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
4) nie była karana za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) posiada certyfikat, o którym mowa w ust. 3.

2. Kontroler jest obowiązany zachować w tajemnicy informacje, które uzyskał w związku z wykonywaniem czynności kontroli. Obowiązek zachowania tajemnicy trwa również po ustaniu pełnienia obowiązków kontrolera w urzędzie obsługującym organ dokonujący kontroli.

3. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wykaz certyfikatów uprawniających do prowadzenia kontroli w rozumieniu art. 25, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób legitymujących się poszczególnymi certyfikatami i zakres kontroli określony w art. 25.

4. W przypadku przeprowadzania kontroli przez zespół kontrolerów, co najmniej jeden kontroler, będący członkiem tego zespołu, posiada certyfikat, o którym mowa w ust. 3.

Art. 29. (uchylony)

Art. 30. (uchylony)

Art. 31. (uchylony)

Art. 32. (uchylony)

Art. 33. (uchylony)

Art. 34. (uchylony)

Art. 35. (uchylony)

Rozdział 5

Zmiany w przepisach obowiązujących

Art. 36–52. (pominięte)

Rozdział 6

Przepisy dostosowujące, przejściowe i końcowe

Art. 53–60. (pominięte)

Art. 61. 1. Ilekroć w przepisach dotyczących informatyzacji zawartych w odrębnych ustawach jest mowa o:

1) elektronicznym nośniku informacji, elektronicznym nośniku informatycznym, elektronicznym nośniku danych, komputerowym nośniku informacji, komputerowym nośniku danych, nośniku elektronicznym, nośniku magnetycznym, nośniku informatycznym albo nośniku komputerowym – należy przez to rozumieć, w przypadku wątpliwości interpretacyjnych, informatyczny nośnik danych, o którym mowa w art. 3 pkt 1 niniejszej ustawy;
2) danych elektronicznych, danych w postaci elektronicznej, danych w formie elektronicznej, danych informatycznych, informacjach w postaci elektronicznej albo informacjach w formie elektronicznej – należy przez to rozumieć, w przypadku wątpliwości interpretacyjnych, dokument elektroniczny, o którym mowa w art. 3 pkt 2 niniejszej ustawy.

2. Przepisu ust. 1 nie stosuje się do przepisów:

1) ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe;
2) ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. z 2020 r. poz. 2027);

3) *ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. z 2012 r. poz. 1232)*[1)].

Art. 62. (pominięty)

Art. 63. (pominięty)

Art. 64. Ustawa wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia[2)], z wyjątkiem:

1) art. 17 oraz 54, które wchodzą w życie z dniem ogłoszenia;
2) art. 36 i 37, które wchodzą w życie po upływie 7 miesięcy od dnia ogłoszenia;
3) art. 40, który wchodzi w życie po upływie 27 miesięcy od dnia ogłoszenia;
4) art. 42 pkt 1, 4 i 7, które wchodzą w życie z dniem 1 lipca 2006 r.

1) Ustawa utraciła moc z dniem 7 października 2013 r. na podstawie art. 38 ustawy z dnia 12 lipca 2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. poz. 1036), która weszła w życie z dniem 7 października 2013 r.

2) Ustawa została ogłoszona w dniu 20 kwietnia 2005 r.