

Opracowano na
podstawie: t.j.
Dz. U. z 2024 r.
poz. 1557, 1717, z
2025 r. poz. 1006,
1019, 1158, 1301.

U S T A W A

z dnia 17 lutego 2005 r.

o informatyzacji działalności podmiotów realizujących zadania publiczne¹⁾

Rozdział I

Przepisy ogólne

Art. 1. Ustawa określa zasady:

- 1) (uchylony)
- 1a) funkcjonowania Architektury Informacyjnej Państwa,
- 1b) funkcjonowania repozytorium interoperacyjności,
- 2) zapewniania warunków sprawnego funkcjonowania oraz współdziałania systemów teleinformatycznych używanych do realizacji zadań publicznych – w sposób gwarantujący neutralność technologiczną i otwartość używanych standardów i specyfikacji, w tym wynikających z:
 - a) Krajowych Ram Interoperacyjności,
 - b) minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi,
 - c) minimalnych wymagań dla rejestrów publicznych,
- 3) dostosowywania systemów teleinformatycznych używanych do realizacji zadań publicznych do Krajowych Ram Interoperacyjności oraz do minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi – w sposób gwarantujący neutralność technologiczną i otwartość używanych standardów i specyfikacji,

¹⁾ Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii (akt w sprawie Interoperacyjnej Europy) (Dz. Urz. UE L 2024/903 z 22.03.2024).

- 4) dostosowywania rejestrów publicznych do Krajowych Ram Interoperacyjności oraz do minimalnych wymagań dla rejestrów publicznych – w sposób gwarantujący neutralność technologiczną i otwartość używanych standardów i specyfikacji,
 - 5) kontroli realizacji przedsięwzięć informatycznych o publicznym zastosowaniu, systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi oraz rejestrów publicznych,
 - 6) wymiany danych między 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,
 - 9d) funkcjonowania Komitetu do spraw Cyfryzacji,
 - 9e) inwentaryzacji systemów teleinformatycznych używanych do realizacji zadań publicznych
 - 10) (uchylony)
- w celu ochrony interesu publicznego, w tym zachowania przez Państwo możliwości swobody wyboru technologii w procesach informatyzacji realizacji zadań publicznych.

Art. 2. 1. Przepisy ustawy stosuje się do podmiotów publicznych:

- 1) jednostek sektora finansów publicznych w rozumieniu przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756 i 1907 oraz z 2025 r. poz. 39);

- 2) innych niż określone w pkt 1 państwowych jednostek organizacyjnych nieposiadających osobowości prawnej;
- 3) innych niż określone w pkt 1 osób prawnych utworzonych w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego, jeżeli podmioty te oraz podmioty, o których mowa w pkt 1 i 2, pojedynczo lub wspólnie, bezpośrednio albo pośrednio przez inny podmiot:
 - a) finansują te osoby prawne w ponad 50 % lub
 - b) posiadają ponad połowę udziałów albo akcji tych osób prawnych, lub
 - c) sprawują nadzór nad organami zarządzającymi tych osób prawnych, lub
 - d) mają prawo do powoływania ponad połowy składu organów nadzorczych lub zarządzających tych osób prawnych;
- 4) związków podmiotów, o których mowa w pkt 1–3;
- 5) instytutów badawczych, Centrum Łukasiewicz oraz instytutów działających w ramach Sieci Badawczej Łukasiewicz;
- 6) uczelni niepublicznych;
- 7) federacji podmiotów systemu szkolnictwa wyższego i nauki.

1a. Przepisy art. 12k ust. 4 i 5, art. 12l, art. 12n, art. 13, art. 14, art. 15, art. 15a, art. 17a ust. 7, art. 19c–20a, art. 20e, art. 20gb, art. 20gc, art. 20m, art. 20n, art. 20q, art. 20r oraz art. 21–24 stosuje się również do podmiotu innego niż podmiot publiczny, realizującego zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia tych zadań lub ich zlecenia przez podmiot publiczny.

2. (uchylony)

2a. Przepis art. 20ae stosuje się również do dostawców usług telekomunikacyjnych w rozumieniu art. 2 pkt 40 lit. a ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221), w zakresie, o którym mowa w art. 296 ust. 3 pkt 2 lit. e tej ustawy.

3. Przepisów ustawy nie stosuje się do służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222), 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 danych do i od podmiotów niebędących organami administracji rządowej, oraz z wyjątkiem art. 13a, art. 19c i art. 19d.

4. Przepisów art. 25, art. 25a i art. 28 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 ani 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 ani 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 12 lipca 2024 r. – Prawo komunikacji elektronicznej;
- 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 oraz z 2024 r. poz. 1222);
- 5) rejestr publiczny – uporządkowany zbiór danych służący do realizacji zadań publicznych, prowadzony na podstawie przepisów ustawowych przez podmiot realizujący zadania publiczne;

- 6) przedsięwzięcie informatyczne o publicznym zastosowaniu – zespół działań organizacyjnych i technicznych służących do realizacji zadań publicznych za pomocą środków komunikacji elektronicznej, obejmujących co najmniej jedno z następujących działań:
- a) budowę systemu teleinformatycznego używanego do realizacji zadania publicznego, w tym umożliwiającego wymianę danych z podmiotami publicznymi,
 - b) utworzenie rejestru publicznego,
 - c) udostępnianie w postaci elektronicznej zasobu informacyjnego podmiotu publicznego,
 - d) wdrożenie usługi służącej do realizacji zadań publicznych,
 - e) budowę infrastruktury teleinformatycznej, w tym telekomunikacyjnej,
 - f) rozszerzenie zakresu, zmianę funkcjonalności lub zmianę technologiczną produktów powstałych w wyniku działań, o których mowa w lit. a–e,
 - g) utrzymanie produktów powstałych w wyniku działań, o których mowa w lit. a–e,
 - h) wsparcie rozwoju społeczeństwa informacyjnego;
- 6a) założenia przedsięwzięcia informatycznego o publicznym zastosowaniu – ogólny plan przedsięwzięcia informatycznego o publicznym zastosowaniu zawierający w szczególności informacje o:
- a) zakresie przedsięwzięcia, w tym produktach powstałych w wyniku działań przedsięwzięcia,
 - b) harmonogramie realizacji przedsięwzięcia,
 - c) kosztach i planowanych źródłach finansowania przedsięwzięcia,
 - d) uwarunkowaniach i otoczeniu związanych z realizacją przedsięwzięcia,
 - e) ryzyku związanym z realizacją przedsięwzięcia,
 - f) sposobie i kosztach utrzymania produktów powstałych w wyniku działań przedsięwzięcia oraz ryzyku związanym z tym utrzymaniem;
- 7) (uchylony)
- 8) (uchylony)
- 9) minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi – zespół wymagań, 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 danych udostępnianych za pomocą tego systemu;

- 10) minimalne wymagania dla rejestrów publicznych – zespół wymagań służących do zapewnienia spójności prowadzenia rejestrów publicznych, a także zapewnienia wiarygodności, jednoznaczności, aktualności, kompletności i dostępności danych gromadzonych w tych rejestrach;
- 11) oprogramowanie interfejsowe – oprogramowanie umożliwiające łączenie i wymianę danych w komunikacji pomiędzy systemami teleinformatycznymi;
- 11a) interfejs programistyczny aplikacji – interfejs programistyczny aplikacji, o którym mowa w art. 2 pkt 9 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524);
- 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 ust. 1 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 2022 r. poz. 671 oraz z 2023 r. poz. 1234 i 1941);
- 14c) profil mObywatel – środek identyfikacji elektronicznej, o którym mowa w art. 2 pkt 11 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275);
- 15) (uchylony)
- 16) (uchylony)
- [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 podmiotów do współdziałania przez wymianę danych za pomocą środków komunikacji elektronicznej;
- 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,*

Przepis
uchylający pkt 17
w art. 3 wejdzie w
życie z dn.
1.10.2029 r. (Dz.
U. z 202 r. poz.
2320, z 2021 r.
poz. 1135, z 2022
r. poz. 1002 i 2754
oraz z 2023 r.
poz. 1860).

Przepis
uchylający pkt 20
w art. 3 wejdzie w
życie z dn.
1.10.2029 r. (Dz.
U. z 202 r. poz.
2320, z 2021 r.
poz. 1135, z 2022
r. poz. 1002 i 2754
oraz z 2023 r.
poz. 1860).

- 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 organizacyjnych, semantycznych oraz technicznych dotyczących interoperacyjności;
 - 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;
 - 28) model architektoniczny – odwzorowanie obiektów, w szczególności usług, procesów, systemów, danych oraz sposobów ich powiązania, identyfikujące

- kluczowe komponenty funkcjonalne, które zapewniają realizację zadań publicznych za pomocą środków komunikacji elektronicznej;
- 29) Architektura Informacyjna Państwa – metodę zarządzania informatyzacją państwa realizującą cele strategii, o której mowa w art. 12aa ust. 1, opartą na modelach architektonicznych i obejmującą zasady podstawowe, zwane dalej „pryncypiami”, standardy, wytyczne i rekomendacje architektoniczne;
- 30) metadane – metadane, o których mowa w art. 2 pkt 10 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego;
- 31) środki Unii Europejskiej – środki, o których mowa w:
- a) art. 5 ust. 3 pkt 1, 2, 4, 5 i 6 oraz art. 202 ust. 4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
 - b) art. 3b oraz art. 141l ust. 1 i 2 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2025 r. poz. 198);
- 32) środki z innych źródeł zagranicznych – środki, o których mowa w art. 5 ust. 1 pkt 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

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 2024 r. poz. 632 i 1222);
- 2a) obowiązku korzystania przy realizacji zadań publicznych z poczty elektronicznej wykorzystującej mechanizmy, o których mowa w art. 24 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703 oraz z 2024 r. poz. 1222);
- 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.

Art. 4a. 1. Minister właściwy do spraw informatyzacji może realizować swoje zadania przy pomocy instytucji gospodarki budżetowej, wobec której wykonuje funkcje organu założycielskiego.

2. Realizacja zadań, o których mowa w ust. 1, może być finansowana ze środków określonych w:

- 1) umowie, przewidującej:
 - a) wynagrodzenie za wykonywanie tych zadań, w tym udzielenie zaliczki,
 - b) rozliczenie na podstawie poniesionych kosztów i rozsądnego zysku;
- 2) innej umowie;
- 3) dotacji celowej udzielanej przez ministra właściwego do spraw informatyzacji.

3. Minister właściwy do spraw informatyzacji określi, w drodze zarządzenia, sposób nadzoru i rozliczania realizacji zadań powierzonych w umowie, o której mowa w ust. 2 pkt 1, mając na względzie prawidłowość ich realizacji.

4. W przypadku zawarcia umowy, o której mowa w ust. 2 pkt 1, o przeznaczeniu zysku netto decyduje minister właściwy do spraw informatyzacji po zatwierdzeniu sprawozdania finansowego tej instytucji. Przepis art. 28 ust. 8 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, z późn. zm.²⁾) stosuje się odpowiednio, z uwzględnieniem ust. 5.

5. Minister właściwy do spraw informatyzacji może wydać wiążące polecenie dokonania wpłaty środków pieniężnych stanowiących zysk netto, o którym mowa w ust. 4, lub zgromadzonych na funduszu zapasowym tej jednostki, na rzecz Funduszu – Centralnej Ewidencji Pojazdów i Kierowców, o którym mowa w art. 80d ust. 2 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2024 r. poz. 1251).

6. Szef Kancelarii Prezesa Rady Ministrów lub minister kierujący działem administracji rządowej, za zgodą ministra właściwego do spraw informatyzacji, może powierzyć realizację swoich zadań z zakresu informatyzacji instytucji, o której mowa w ust. 1, udzielając dotacji celowej.

²⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1273, 1407, 1429, 1641, 1693 i 1872 oraz z 2024 r. poz. 858 i 1089.

Art. 4b. 1. Minister właściwy do spraw informatyzacji może upoważnić do wykonywania zadań w jego imieniu dyrektora instytucji, o której mowa w art. 4a ust. 1.

2. Upoważnienie, o którym mowa w ust. 1, obejmuje uprawnienie do udzielania dalszych upoważnień osobom zatrudnionym w tej instytucji.

3. Upoważnienie, o którym mowa w ust. 1 i 2, jest udzielane na piśmie w drodze imiennego upoważnienia lub upoważnienia stanowiskowego.

4. W przypadku wątpliwości co do udzielenia upoważnienia, o którym mowa w ust. 1 i 2, lub jego zakresu minister właściwy do spraw informatyzacji może potwierdzić ważność podjętych czynności.

Art. 4c. 1. Minister właściwy do spraw informatyzacji jest właściwym organem odpowiedzialnym za stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii (akt w sprawie Interoperacyjnej Europy) (Dz. Urz. UE L 2024/903 z 22.03.2024), zwanego dalej „rozporządzeniem 2024/903”, oraz pojedynczym punktem kontaktowym, w rozumieniu art. 17 ust. 1 rozporządzenia 2024/903.

2. Minister właściwy do spraw informatyzacji wyznacza przedstawiciela w Radzie ds. Interoperacyjnej Europy, o której mowa w art. 15 ust. 1 rozporządzenia 2024/903, spośród osób zatrudnionych w urzędzie obsługującym tego ministra, które posiadają kompetencje i wiedzę z zakresu interoperacyjności transgranicznej, o której mowa w art. 2 pkt 1 rozporządzenia 2024/903.

3. Do zadań ministra właściwego do spraw informatyzacji, o których mowa w ust. 1 i 2, przepisów art. 4a i art. 4b nie stosuje się.

Rozdział 2

Strategia dotycząca informatyzacji państwa oraz pełnomocnicy do spraw informatyzacji

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. 12aa. 1. Rada Ministrów przyjmuje, w drodze uchwały, strategię dotyczącą informatyzacji państwa, zwaną dalej „strategią”.

2. Strategia określa:

- 1) aktualny stan informatyzacji państwa;
- 2) wizję informatyzacji państwa;
- 3) cele informatyzacji państwa;
- 4) środki i działania służące do realizacji celów informatyzacji państwa;
- 5) sposoby i zasady współpracy podmiotów, których dotyczy informatyzacja państwa;
- 6) możliwości finansowania działań, o których mowa w pkt 4.

Art. 12ab. Strategia jest przyjmowana na okres dziesięcioletni.

Art. 12ac. 1. Strategię realizują członkowie Rady Ministrów.

2. Minister właściwy do spraw informatyzacji monitoruje realizację strategii.

Art. 12ad. 1. Minister właściwy do spraw informatyzacji we współpracy z innymi członkami Rady Ministrów dokonuje przeglądu strategii co 2 lata.

2. Minister właściwy do spraw informatyzacji sporządza sprawozdanie z przeglądu strategii i przedkłada je Radzie Ministrów w terminie 2 miesięcy od dnia zakończenia przeglądu.

Art. 12ae. 1. W urzędzie obsługującym ministra kierującego działem administracji rządowej oraz w Kancelarii Prezesa Rady Ministrów powołuje się pełnomocnika do spraw informatyzacji, zwanego dalej „pełnomocnikiem”. Przepisów art. 4a ust. 1 i 6 nie stosuje się.

2. Pełnomocnika można powołać w urzędzie innym niż urzędy wymienione w ust. 1, w szczególności w urzędzie obsługującym organ jednostki samorządu terytorialnego.

3. Do zadań pełnomocnika należy:

- 1) koordynowanie realizacji strategii w zakresie spraw objętych działem administracji rządowej kierowanym przez właściwego ministra, w tym w zakresie spraw należących do właściwości jednostek organizacyjnych lub organów podległych temu ministrowi lub przez niego nadzorowanych, albo w zakresie spraw należących do właściwości Kancelarii Prezesa Rady Ministrów, w tym w zakresie spraw należących do właściwości jednostek organizacyjnych lub organów podległych Prezesowi Rady Ministrów lub przez niego nadzorowanych;
- 2) diagnozowanie obszaru, w którym jest konieczne wprowadzenie zmian w zakresie spraw objętych działem administracji rządowej kierowanym przez właściwego ministra, w tym w zakresie spraw należących do właściwości jednostek organizacyjnych lub organów podległych temu ministrowi lub przez niego nadzorowanych, albo w zakresie spraw należących do właściwości Kancelarii Prezesa Rady Ministrów, w tym w zakresie spraw należących do właściwości jednostek organizacyjnych lub organów podległych Prezesowi Rady Ministrów lub przez niego nadzorowanych – pod względem realizacji strategii oraz wprowadzania nowych technologii cyfrowych;
- 3) wsparcie merytoryczne w procesie uzgadniania projektów aktów normatywnych kierowanych do właściwego ministra w ramach rządowego procesu legislacyjnego;
- 4) diagnozowanie potrzeb pracowników zatrudnionych w urzędzie, o którym mowa w ust. 1, w którym powołano pełnomocnika, lub pracowników organów lub jednostek organizacyjnych podległych właściwemu ministrowi albo Prezesowi Rady Ministrów lub przez niego nadzorowanych, przygotowywanie materiałów szkoleniowych i organizowanie szkoleń, a także rozpowszechnianie materiałów szkoleniowych i informacji o dostępnych szkoleniach – w obszarze kompetencji cyfrowych;
- 5) tworzenie i upowszechnianie dobrych praktyk wspierających podnoszenie kompetencji cyfrowych pracowników, o których mowa w pkt 4;

- 6) przygotowywanie bieżących informacji na temat postępów w realizacji strategii oraz związanego z tym ryzyka i ich przedkładanie ministrowi właściwemu do spraw informatyzacji w celu, o którym mowa w art. 12ac ust. 2;
- 7) przygotowywanie informacji z realizacji strategii w celu dokonania przeglądu, o którym mowa w art. 12ad ust. 1;
- 8) uczestnictwo we współpracy z innymi podmiotami w zakresie zadań związanych z realizacją strategii;
- 9) wspieranie kierownika urzędu, o którym mowa w ust. 1, w którym powołano pełnomocnika, w zakresie zapewnienia zgodności przedsięwzięć informatycznych o publicznym zastosowaniu, które są realizowane przez ten urząd, z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa, Krajowymi Ramami Interoperacyjności, minimalnymi wymaganiami dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi oraz minimalnymi wymaganiami dla rejestrów publicznych;
- 10) koordynowanie przeprowadzania ocen interoperacyjności krajowej, o których mowa w art. 12n ust. 1, oraz ocen interoperacyjności, o których mowa w art. 3 ust. 1 rozporządzenia 2024/903, oraz koordynowanie udostępniania i ponownego wykorzystywania rozwiązań interoperacyjnych, o których mowa w art. 4 ust. 1 rozporządzenia 2024/903, w ramach urzędu, o którym mowa w ust. 1, w którym powołano pełnomocnika;
- 11) wykonywanie innych zadań wspierających realizację dokumentów o charakterze strategicznym, polityk i programów rozwoju, związanych z informatyzacją państwa.

4. Do zadań pełnomocnika powołanego w urzędzie innym niż urzędy wymienione w ust. 1 należy:

- 1) diagnozowanie potrzeb pracowników zatrudnionych w urzędzie innym niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika, przygotowywanie materiałów szkoleniowych i organizowanie szkoleń, a także rozpowszechnianie materiałów szkoleniowych i informacji o dostępnych szkoleniach – w obszarze kompetencji cyfrowych;

- 2) tworzenie i upowszechnianie dobrych praktyk wspierających podnoszenie kompetencji cyfrowych pracowników, o których mowa w pkt 1;
- 3) wspieranie kierownika urzędu innego niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika, w zakresie zapewnienia zgodności przedsięwzięć informatycznych o publicznym zastosowaniu, które są realizowane przez ten urząd, z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa, Krajowymi Ramami Interoperacyjności, minimalnymi wymaganiami dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi oraz minimalnymi wymaganiami dla rejestrów publicznych;
- 4) koordynowanie przeprowadzania ocen interoperacyjności krajowej, o których mowa w art. 12n ust. 1, oraz ocen interoperacyjności, o których mowa w art. 3 ust. 1 rozporządzenia 2024/903, oraz koordynowanie udostępniania i ponownego wykorzystywania rozwiązań interoperacyjnych, o których mowa w art. 4 ust. 1 rozporządzenia 2024/903, w ramach urzędu innego niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika;
- 5) wykonywanie innych zadań związanych z informatyzacją, wskazanych przez kierownika urzędu innego niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika.

5. Pełnomocnika powołuje i odwołuje kierownik urzędu, o którym mowa w ust. 1, albo innego urzędu niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika, spośród osób zatrudnionych w tym urzędzie, które posiadają kompetencje, wiedzę i doświadczenie z zakresu informatyzacji niezbędne do realizacji zadań pełnomocnika.

6. W zakresie wykonywanych zadań pełnomocnik podlega bezpośrednio kierownikowi urzędu, o którym mowa w ust. 1, albo innego urzędu niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika.

7. Obsługę merytoryczną, organizacyjno-prawną, techniczną i kancelaryjno-biurową pełnomocnika zapewnia urząd, o którym mowa w ust. 1, albo inny urząd niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika.

8. Pełnomocnicy są obowiązani do współdziałania oraz współpracy z innymi podmiotami w zakresie realizacji swoich zadań.

9. Pełnomocnik za zgodą kierownika urzędu, o którym mowa w ust. 1, albo innego urzędu niż urzędy wymienione w ust. 1, w którym powołano pełnomocnika, może tworzyć spośród pracowników, o których mowa w ust. 3 pkt 4 lub ust. 4 pkt 1, zespoły do opracowania określonych zagadnień lub wykonania określonych czynności oraz może zlecać przeprowadzanie badań i ekspertyz.

Art. 12b. (uchylony)

Art. 12c. (uchylony)

Art. 12d. (uchylony)

Art. 12e. (uchylony)

Art. 12f. (uchylony)

Art. 12g. (uchylony)

Art. 12h. (uchylony)

Art. 12i. (uchylony)

Rozdział 3

Architektura Informacyjna Państwa, systemy teleinformatyczne używane do realizacji zadań publicznych, wymiana danych z podmiotami publicznymi, rejestry publiczne oraz Komitet do spraw Cyfryzacji

Art. 12j. 1. Minister właściwy do spraw informatyzacji opracowuje i rozwija Architekturę Informacyjną Państwa.

2. Minister właściwy do spraw informatyzacji prowadzi repozytorium Architektury Informacyjnej Państwa, w którym są gromadzone w szczególności modele architektoniczne oraz pryncypia, standardy, wytyczne i rekomendacje architektoniczne – z wykorzystaniem systemu teleinformatycznego.

3. Minister właściwy do spraw informatyzacji udostępnia pryncypia, standardy, wytyczne i rekomendacje architektoniczne Architektury Informacyjnej Państwa na stronie internetowej, której adres elektroniczny jest udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej ministra.

<Art. 12k. 1. Minister właściwy do spraw informatyzacji prowadzi repozytorium interoperacyjności z wykorzystaniem powszechnie dostępnego

Dodane art. 12k–12n wejdą w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

systemu teleinformatycznego, w tym zapewnia mechanizm monitorowania dostępności interfejsów programistycznych aplikacji systemów teleinformatycznych służących do prowadzenia rejestrów publicznych.

2. Głównymi funkcjonalnościami repozytorium interoperacyjności są publikowanie i udostępnianie informacji służących do zapewnienia interoperacyjności.

3. Repozytorium interoperacyjności zawiera w szczególności następujące kategorie informacji:

1) metadane rejestrów publicznych, w tym:

- a) pełną i skróconą nazwę rejestru publicznego,
- b) opis rejestru publicznego,
- c) nazwę organu prowadzącego rejestr publiczny oraz numer identyfikacyjny REGON podmiotu, który obsługuje ten organ w zakresie prowadzenia rejestru publicznego, jeżeli posiada taki numer,
- d) kategorię przedmiotową i status funkcjonowania rejestru publicznego, określone w przepisach wydanych na podstawie art. 12m,
- e) podstawę prawną prowadzenia rejestru publicznego i datę jego utworzenia,
- f) podstawę prawną i datę zakończenia prowadzenia rejestru publicznego – w przypadku zakończenia prowadzenia rejestru publicznego,
- g) struktury danych i znaczenie danych zawartych w tych strukturach dla danych gromadzonych w rejestrze publicznym,
- h) formaty plików, w których są udostępniane dane z rejestru publicznego,
- i) informacje, o których mowa w art. 14 ust. 1a pkt 3,
- j) terminy udostępniania danych zgromadzonych w rejestrze publicznym,
- k) informacje o pojedynczym punkcie kontaktowym dla rejestru publicznego, o którym mowa w art. 14 ust. 1a pkt 4;

- 2) informacje o interfejsach programistycznych aplikacji systemów teleinformatycznych używanych do realizacji zadań publicznych, o których mowa w art. 13 ust. 5;
- 3) wyniki ocen interoperacyjności krajowej, o których mowa w art. 12n ust. 3;
- 4) sprawozdania przedstawiające wyniki ocen interoperacyjności, o których mowa w art. 3 ust. 1 rozporządzenia 2024/903;
- 5) informacje o systemie rejestrów państwowych, o których mowa w art. 13b ust. 2;
- 6) raporty z przeglądu standardów oraz specyfikacji, o których mowa w art. 18a.

4. Podmiot prowadzący rejestr publiczny z wykorzystaniem systemu teleinformatycznego lub używający systemu teleinformatycznego do realizacji zadań publicznych:

- 1) publikuje w repozytorium interoperacyjności informacje, o których mowa w ust. 3 pkt 1–4, albo wskazuje podstawę prawną, z której wynika obowiązek zachowania niejawności takich informacji;
- 2) zapewnia jakość, w tym poprawność, aktualność oraz kompletność publikowanych informacji, o których mowa w ust. 3 pkt 1–4.

5. Jeżeli rejestr publiczny jest prowadzony z wykorzystaniem systemu teleinformatycznego przez więcej niż jeden podmiot, do publikowania informacji, o których mowa w ust. 3 pkt 1–4, a także do zapewnienia ich jakości, w tym poprawności, aktualności oraz kompletności, jest obowiązany podmiot, który prowadzi ten system teleinformatyczny.

Art. 12l. Podmioty obowiązane na podstawie przepisów odrębnych do przekazywania danych podmiotom realizującym zadania publiczne stosują, w ramach przekazywania takich danych, rozwiązania zapewniające zgodność z metadanymi rejestrów publicznych i interfejsami programistycznymi aplikacji systemów teleinformatycznych używanych do realizacji zadań publicznych, o których mowa w art. 12k ust. 3 pkt 1 i 2.

Art. 12m. Rada Ministrów określi, w drodze rozporządzenia:

- 1) szczegółowe funkcjonalności repozytorium interoperacyjności,

- 2) sposób kategoryzacji informacji przeznaczonych do udostępniania w repozytorium interoperacyjności, w tym kategorie przedmiotowe i statusy funkcjonowania rejestru publicznego w repozytorium interoperacyjności,
- 3) szczegółowy sposób prowadzenia repozytorium interoperacyjności,
- 4) szczegółowy sposób wykonywania obowiązków przez podmioty realizujące zadania publiczne w zakresie udostępniania danych i informacji w repozytorium interoperacyjności

– mając na uwadze potrzebę zapewnienia interoperacyjności, zachowania spójnych standardów prezentacji danych w repozytorium interoperacyjności oraz zapewnienia informacji o danych gromadzonych w rejestrach publicznych i sposobie dostępu do tych danych przetwarzanych w systemach teleinformatycznych używanych do realizacji zadań publicznych.

Art. 12n. 1. Podmiot realizujący zadania publiczne przeprowadza ocenę interoperacyjności krajowej każdorazowo przed wprowadzeniem zmian w systemie teleinformatycznym używanym do realizacji zadań publicznych lub w rejestrze publicznym.

2. Ocena interoperacyjności krajowej zawiera:

- 1) opis wpływu zmian wprowadzanych w systemie teleinformatycznym używanym do realizacji działań publicznych lub w rejestrze publicznym na podmioty publiczne;
- 2) opis działań podjętych oraz planowanych do podjęcia w celu minimalizacji lub usunięcia negatywnego wpływu zmian na podmioty publiczne;
- 3) informację o negatywnym wpływie zmian na podmioty publiczne, który nie zostanie usunięty w ramach działań, o których mowa w pkt 2.

3. Podmiot realizujący zadania publiczne publikuje wynik oceny interoperacyjności krajowej w formacie nadającym się do odczytu maszynowego, ułatwiającym tłumaczenie maszynowe, w repozytorium interoperacyjności przed wprowadzeniem zmian. Publikacja, o której mowa w zdaniu pierwszym, następuje w terminie pozwalającym podmiotom publicznym na realizację zadań publicznych wynikających z przepisów odrębnych.

4. Przepisu ust. 1 nie stosuje się do działań prowadzonych w stosunku do systemów teleinformatycznych używanych do realizacji zadań publicznych oraz do rejestrów publicznych niewpływających na ich interoperacyjność, w szczególności do konserwacji oprogramowania, aktualizacji w zakresie bezpieczeństwa lub aktualizacji technicznych.>

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.]*

**Nowe brzmienie
ust. 1 w art. 13
wejdzie w życie z
dn. 23.02.2027 r.
(Dz. U. z 2025 r.
poz. 1158).**

<1. Podmiot realizujący zadania publiczne używa do ich realizacji systemów teleinformatycznych:

- 1) spełniających minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi:**
 - a) zapewniających spójność działania tych systemów,**
 - b) określających model architektury oraz specyfikacje interfejsu programistycznego aplikacji, zwanego dalej „API”, tych systemów,**
 - c) określających formaty danych oraz protokoły komunikacyjne i szyfrujące, przy zachowaniu możliwości nieodpłatnego ich wykorzystania,**
 - d) zapewniających sprawną i bezpieczną wymianę danych między podmiotami publicznymi oraz między podmiotami publicznymi a organami innych państw lub organizacji międzynarodowych;**
- 2) zapewniających interoperacyjność zgodnie z Krajowymi Ramami Interoperacyjności obejmującymi zagadnienia dotyczące:**
 - a) sposobu postępowania podmiotu realizującego zadania publiczne w zakresie stosowania i wyboru norm, standardów, metod oraz formatów,**
 - b) sposobu jej osiągania,**
 - c) ocen interoperacyjności krajowej, o których mowa w art. 12n ust. 1;**
- 3) zgodnych z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa.>**

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

2. Podmiot realizujący zadania publiczne z wykorzystaniem systemu teleinformatycznego albo za pomocą środków komunikacji elektronicznej do przekazywania danych między tym podmiotem a podmiotem niebędącym organem administracji rządowej:

- 1) zapewnia spełnianie przez system teleinformatyczny służący do wymiany danych, poza wymaganiami, o których mowa w ust. 1, wymogu równego traktowania rozwiązań informatycznych;
- 2) udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej:
 - a) (uchylona)
 - b) testy akceptacyjne, z zastrzeżeniem ust. 4.

3. (uchylony)

4. Podmiot realizujący zadania publiczne 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.

<5. Podmiot realizujący zadania publiczne przygotowuje następujące informacje o API systemu teleinformatycznego używanego do realizacji zadań publicznych:

- 1) **informacje o punktach dostępowych API,**
 - 2) **skrócony opis API,**
 - 3) **dokumentację API, zawierającą w szczególności opis struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących,**
 - 4) **opis sposobów integracji z API,**
 - 5) **informację o gwarantowanym poziomie dostępności API,**
 - 6) **informację o sposobie dostępu do danych w przypadku czasowej niedostępności API dłuższej niż wynikająca z informacji, o której mowa w pkt 5,**
 - 7) **statystyki użycia API**
- i zapewnia ich aktualność.>**

Dodany ust. 5 w art. 13 wejdzie w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

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 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. 13aa. Minister właściwy do spraw informatyzacji może podjąć działania mające na celu rozwój i wykorzystanie systemu teleinformatycznego, o którym mowa w art. 22a ust. 1 ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz. U. z 2024 r. poz. 167, z późn. zm.³⁾), do realizacji zadań publicznych po zasięgnięciu opinii ministra, w którego właściwości pozostają sprawy związane z realizacją tych zadań.]

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:]* **<Minister właściwy do spraw informatyzacji określi i udostępni w repozytorium interoperacyjności:>**

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.]

Przepis uchylający art. 13aa wejdzie w życie z dn. 1.01.2026 r. (Dz. U. z 2025 r. poz. 1301).

Nowe brzmienie wprowadz. do wylicz. w ust. 2 w art. 13b wejdzie w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

Nowe brzmienie pkt 2 w ust. 2 w art. 13b wejdzie w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

³⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 232, 834, 854, 858, 1089 i 1222.

<2) informacje o rejestrach publicznych prowadzonych w systemie rejestrów państwowych.>

Art. 14. 1. Podmiot realizujący zadania publiczne prowadzący rejestr publiczny jest obowiązany prowadzić ten rejestr zgodnie z minimalnymi wymaganiami dla rejestrów publicznych, określającymi kluczowe typy i identyfikatory obiektów w rejestrach publicznych oraz zasady prowadzenia rejestru publicznego i dostępu do niego.

<1a. Podmiot prowadzący rejestr publiczny, z wyjątkiem jednostki samorządu terytorialnego, związku takich jednostek, związku metropolitalnego, samorządowej jednostki budżetowej, samorządowego zakładu budżetowego, samorządowej instytucji kultury, samorządowej osoby prawnej utworzonej na podstawie odrębnych ustaw w celu wykonywania zadań publicznych oraz innej samorządowej jednostki organizacyjnej nieposiadającej osobowości prawnej, jest obowiązany:

Dodane ust. 1a i 1b w art. 14 wejdą w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

- 1) prowadzić ten rejestr z wykorzystaniem systemu teleinformatycznego;
- 2) umożliwiać dostarczanie danych do tego rejestru oraz udostępnianie danych z tego rejestru za pomocą środków komunikacji elektronicznej, w szczególności przez interfejsy programistyczne aplikacji systemów teleinformatycznych, z wykorzystaniem których jest zapewniany dostęp do rejestru publicznego;
- 3) opracować i aktualizować:
 - a) listę słowników, schematów klasyfikacyjnych, taksonomii oraz list kodowych dla danych gromadzonych w rejestrze publicznym,
 - b) warunki oraz procedurę dostępu do danych gromadzonych w rejestrze publicznym,
 - c) warunki ponownego wykorzystania danych gromadzonych w rejestrze publicznym,
 - d) procedurę zgłaszania niezgodności danych w rejestrze publicznym ze stanem faktycznym – w przypadku gdy taka procedura nie została określona w przepisach regulujących funkcjonowanie rejestru publicznego;
- 4) zapewniać prowadzenie pojedynczego punktu kontaktowego dla rejestru publicznego, za pomocą którego są udzielane informacje pozwalające

na zapewnienie interoperacyjności w odniesieniu do prowadzonego rejestru publicznego.

1b. W przypadku gdy jednostka samorządu terytorialnego, związek takich jednostek, związek metropolitalny, samorządowa jednostka budżetowa, samorządowy zakład budżetowy, samorządowa instytucja kultury, samorządowa osoba prawna utworzona na podstawie odrębnych ustaw w celu wykonywania zadań publicznych lub samorządowa jednostka organizacyjna nieposiadająca osobowości prawnej prowadzą rejestr publiczny z wykorzystaniem systemu teleinformatycznego, przepisy ust. 1a pkt 2–4 stosuje się.>

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

3. Podmiot prowadzący z wykorzystaniem systemu teleinformatycznego rejestr publiczny, który zawiera dane osób fizycznych, 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 wprowadzenia po raz pierwszy do rejestru publicznego danych osoby nieposiadającej numeru PESEL podmiot prowadzący ten rejestr nie przeprowadza weryfikacji tych danych.

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.

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 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.

**Przepis
uchylający ust. 2
w art. 14 wejdzie
w życie z dn.
23.02.2027 r. (Dz.
U. z 2025 r. poz.
1158).**

8. W przypadku braku dostępu do rejestru PESEL z przyczyn niezależnych od podmiotu prowadzącego rejestr publiczny przepisów ust. 3 i 5 nie stosuje się.

9. Podmiot otrzymujący dane z rejestru publicznego jest obowiązany chronić je na poziomie nie niższym niż poziom, który ma zastosowanie w przypadku tego rejestru.

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.]

**Nowe brzmienie
ust. 2 w art. 15
wejdzie w życie z
dn. 23.02.2027 r.
(Dz. U. z 2025 r.
poz. 1158).**

<2. Dane, o których mowa w ust. 1, są udostępniane za pomocą środków komunikacji elektronicznej, w szczególności przez interfejsy programistyczne aplikacji systemów teleinformatycznych, z wykorzystaniem których jest zapewniany dostęp do rejestru publicznego, 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 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

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]* **<interfejsów programistycznych aplikacji>** między systemem teleinformatycznym, z którego udostępniane są dane, a systemem teleinformatycznym, przy użyciu którego świadczona jest usługa online.

Zmiana w ust. 4 w art. 15a wejdzie w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

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.]

Nowe brzmienie ust. 6 w art. 15a wejdzie w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

<6. Udostępnienie interfejsów programistycznych aplikacji, o których mowa w ust. 4, następuje w terminie określonym w porozumieniu, nie dłuższym jednak niż 12 miesięcy od dnia 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, który organizuje przetwarzanie danych w systemie teleinformatycznym, jest obowiązany zapewnić możliwość przekazywania danych przez wymianę dokumentów elektronicznych związanych z załatwianiem spraw należących do jego zakresu działania. Do przekazywania danych podmiot ten wykorzystuje 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.

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 danych w postaci elektronicznej:

Przepis uchylający ust. 1a i 1b w art. 16 wejdzie w życie z dn. 1.10.2029 r. (Dz. U. z 202 r. poz. 2320, z 2021 r. poz. 1135, z 2022 r. poz. 1002 i 2754 oraz z 2023 r. poz. 1860).

- 1) z wykorzystaniem systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi;
- 2) zgodnie z minimalnymi wymaganiami dla rejestrów publicznych.

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 systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi, minimalne wymagania dla rejestrów publicznych oraz potrzebę usprawnienia i ujednolicenia obiegu dokumentów między podmiotami publicznymi.

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

**Przepis
uchylający pkt 1–
3 w ust. 3 w art.
16 wejdzie w
życie z dn.
1.10.2029 r. (Dz.
U. z 202 r. poz.
2320, z 2021 r.
poz. 1135, z 2022
r. poz. 1002 i 2754
oraz z 2023 r.
poz. 1860).**

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 informatyzacji;
- 1a) opiniowanie projektu strategii 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 informatyzacji państwa;
- 2) opiniowanie projektów przepisów wydawanych na podstawie art. 18;
- 3) opiniowanie innych projektów aktów prawnych i innych dokumentów dotyczących informatyzacji państwa przekazanych przez ministra właściwego do spraw informatyzacji;
- 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.

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) Naczelný 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 2023 r. poz. 742, z późn. zm.⁴⁾), 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.

⁴⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1088, 1234, 1672, 1872 i 2005 oraz z 2024 r. poz. 124, 227 i 1089.

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 oraz z 2023 r. poz. 1667), 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. 77⁵ § 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2023 r. poz. 1465 oraz z 2024 r. poz. 878 i 1222).

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

Art. 17a. 1. Komitet do spraw Cyfryzacji, zwany dalej „Komitetem”, zapewnia koordynację i wsparcie działań związanych z informatyzacją państwa w zakresie:

- 1) rozpatrywania projektów dokumentów rządowych i przyjmowania stanowisk w sprawach:
 - a) ustaw,
 - b) aktów normatywnych Rady Ministrów,
 - c) rozporządzeń Prezesa Rady Ministrów lub ministrów,
 - d) zarządzeń Prezesa Rady Ministrów;
- 2) rozpatrywania projektów dokumentów rządowych innych niż określone w pkt 1, w szczególności stanowisk rządu, strategii, polityk, programów, planów, standardów, rekomendacji oraz wytycznych, w tym:
 - a) procedur realizowania zadań publicznych za pomocą środków komunikacji elektronicznej,
 - b) wskazywania kluczowych kierunków interwencji oraz potrzeb podjęcia działań– i przyjmowania stanowiska w tych sprawach;
- 3) monitorowania lub opiniowania przedsięwzięć informatycznych o publicznym zastosowaniu realizowanych przez podmioty publiczne i przyjmowania stanowisk, w tym rekomendacji i wytycznych, w sprawie założeń oraz postępów i efektów realizacji tych przedsięwzięć:
 - a) niezależnie od ich wartości – w przypadku przedsięwzięć informatycznych o publicznym zastosowaniu, w ramach których jest realizowane co najmniej jedno z działań, o których mowa w art. 3 pkt 6 lit. a–d oraz h lub w art. 3 pkt 6 lit. f w odniesieniu do lit. a–d, planowanych do finansowania z udziałem środków Unii Europejskiej lub środków z innych źródeł zagranicznych,
 - b) których wartość przekracza 5 mln zł – w przypadku przedsięwzięć informatycznych o publicznym zastosowaniu, w ramach których jest realizowane co najmniej jedno z działań, o których mowa w art. 3 pkt 6 lit. a–d oraz h lub w art. 3 pkt 6 lit. f w odniesieniu do lit. a–d, planowanych do finansowania z udziałem innych środków niż środki, o których mowa w lit. a,

- c) których wartość przekracza 15 mln zł – w przypadku przedsięwzięć informatycznych o publicznym zastosowaniu, o których mowa w art. 3 pkt 6 lit. e lub f w odniesieniu do lit. e
- z wyłączeniem przedsięwzięć informatycznych jednostek samorządu terytorialnego, związków takich jednostek, związków metropolitalnych, samorządowych jednostek budżetowych, samorządowych zakładów budżetowych, samorządowych instytucji kultury, samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu wykonywania zadań publicznych oraz innych samorządowych jednostek organizacyjnych nieposiadających osobowości prawnej;
- 4) monitorowania realizacji strategii oraz przyjmowania stanowiska w tej sprawie;
- 5) monitorowania realizacji innych dokumentów o charakterze strategicznym, polityk i programów rozwoju, związanych z informatyzacją państwa, wskazanych przez Radę Ministrów lub Prezesa Rady Ministrów i przyjmowanie stanowisk w tych sprawach.

2. Na wniosek podmiotu realizującego przedsięwzięcie informatyczne o publicznym zastosowaniu przewodniczący Komitetu może zwolnić to przedsięwzięcie z monitorowania lub opiniowania, o których mowa w ust. 1 pkt 3, ze względu na szczególny interes publiczny.

3. Wniosek, o którym mowa w ust. 2, zawiera opis założeń przedsięwzięcia, którego ma dotyczyć zwolnienie, oraz wskazanie istnienia szczególnego interesu publicznego uzasadniającego takie zwolnienie.

4. W przypadku gdy informacje wskazane we wniosku, o którym mowa w ust. 2, nie są wystarczające do jego oceny, w szczególności do oceny istnienia szczególnego interesu publicznego, przewodniczący Komitetu zwraca się do podmiotu realizującego przedsięwzięcie informatyczne o publicznym zastosowaniu o uzupełnienie wniosku i wskazuje termin jego uzupełnienia, a także może zasięgnąć opinii właściwego ministra kierującego działem administracji rządowej, którego dotyczy przedsięwzięcie.

5. Przewodniczący Komitetu zwalnia przedsięwzięcie informatyczne o publicznym zastosowaniu z monitorowania lub opiniowania, o którym mowa

w ust. 1 pkt 3, albo odmawia jego zwolnienia, w terminie 14 dni od dnia otrzymania wniosku, o którym mowa w ust. 2.

6. W przypadku odmowy zwolnienia, o której mowa w ust. 5, podmiot realizujący przedsięwzięcie informatyczne o publicznym zastosowaniu może wystąpić do Komitetu o zwolnienie, ponownie wskazując na istnienie szczególnego interesu publicznego. W przypadku odmowy zwolnienia przedsięwzięcie podlega monitorowaniu lub opiniowaniu, o których mowa w ust. 1 pkt 3.

7. Na wniosek podmiotu realizującego zadania publiczne innego niż podmiot publiczny i za zgodą przewodniczącego Komitetu Komitet może monitorować lub opiniować przedsięwzięcie informatyczne o publicznym zastosowaniu realizowane przez ten podmiot oraz przyjmować stanowisko Komitetu w sprawie założeń oraz postępów i efektów realizacji takiego przedsięwzięcia. Przepisy ust. 3–5 stosuje się odpowiednio, z tym że we wniosku nie wskazuje się na istnienie szczególnego interesu publicznego.

Art. 17b. 1. W przypadku przedsięwzięć informatycznych o publicznym zastosowaniu, o których mowa w art. 17a ust. 1 pkt 3, realizowanych przez podmioty publiczne, z wyłączeniem Sądu Najwyższego, Naczelnego Sądu Administracyjnego, Trybunału Konstytucyjnego, Najwyższej Izby Kontroli, Rzecznika Praw Obywatelskich, Krajowej Rady Radiofonii i Telewizji oraz Krajowego Biura Wyborczego, pozytywna opinia Komitetu dotycząca założeń przedsięwzięcia stanowi warunek niezbędny do realizacji takiego przedsięwzięcia informatycznego oraz jego finansowania ze środków publicznych.

2. Przepisu ust. 1 nie stosuje się do przedsięwzięcia informatycznego o publicznym zastosowaniu, które nie rozszerza zakresu produktów działań przedsięwzięcia informatycznego, które uzyskało pozytywną opinię Komitetu, o której mowa w ust. 1, nie zmienia funkcjonalności tych produktów lub nie wprowadza w nich zmiany technologicznej oraz którego koszty różnią się o nie więcej niż 15 % od kosztów przyjętych w ramach tego przedsięwzięcia.

Art. 17c. Komitet realizuje zadania, o których mowa w art. 17a ust. 1, mając na uwadze zapewnienie w szczególności:

- 1) zgodności ze strategią;

- 2) zgodności ze Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej, o której mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069);
- 3) zgodności z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa;
- 4) zgodności z Krajowymi Ramami Interoperacyjności;
- 5) zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi;
- 6) zgodności z minimalnymi wymaganiami dla rejestrów publicznych;
- 7) optymalizacji warunków udostępniania danych z rejestrów publicznych innym podmiotom publicznym;
- 8) zgodności z zasadami doręczania korespondencji określonymi w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045 i 1841);
- 9) zgodności z zasadami otwartości danych określonymi w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego.

Art. 17d. Komitet, w celu realizacji zadań, o których mowa w art. 17a ust. 1, może podejmować uchwały, w tym uchwały w sprawie rekomendacji i wytycznych dotyczących realizacji przedsięwzięć informatycznych o publicznym zastosowaniu.

Art. 17e. 1. W skład Komitetu wchodzi:

- 1) przewodniczący Komitetu – minister właściwy do spraw informatyzacji albo wyznaczony przez niego sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym tego ministra;
- 2) wiceprzewodniczący Komitetu – sekretarz stanu albo podsekretarz stanu wyznaczony przez ministra właściwego do spraw informatyzacji w urzędzie obsługującym tego ministra;
- 3) pozostali członkowie Komitetu:

- a) Szef Kancelarii Prezesa Rady Ministrów albo wyznaczony przez niego sekretarz stanu albo podsekretarz stanu w Kancelarii Prezesa Rady Ministrów,
- b) ministrowie albo wyznaczeni przez właściwych ministrów ich przedstawiciele w randze sekretarza stanu albo podsekretarza stanu, po jednym z urzędu obsługującego danego ministra, z wyłączeniem ministra właściwego do spraw informatyzacji.

2. Członka Komitetu, o którym mowa w ust. 1 pkt 3, w uzasadnionych przypadkach może zastąpić w pracach Komitetu inny sekretarz stanu, podsekretarz stanu albo pełnomocnik – wskazany przez członka Komitetu, właściwego ministra albo Szefa Kancelarii Prezesa Rady Ministrów.

3. Przewodniczący Komitetu jest informowany o zastępstwie przez członka Komitetu, właściwego ministra albo Szefa Kancelarii Prezesa Rady Ministrów za pośrednictwem sekretarza Komitetu.

Art. 17f. 1. Przewodniczący Komitetu zaprasza Prezesa Rządowego Centrum Legislacji do udziału w pracach Komitetu, w przypadku gdy przedmiotem prac jest projekt dokumentu rządowego, o którym mowa w art. 17a ust. 1 pkt 1.

2. Przewodniczący Komitetu zaprasza do udziału w pracach Komitetu, z głosem doradczym, przedstawiciela Komisji Wspólnej Rządu i Samorządu Terytorialnego, w przypadku gdy przedmiotem prac jest projekt dokumentu rządowego dotyczący zakresu działania jednostek samorządu terytorialnego.

3. Przewodniczący Komitetu może zapraszać do udziału w pracach Komitetu, z głosem doradczym, inne osoby, reprezentujące w szczególności organy, instytucje, organizacje lub przedsiębiorców – stosownie do przedmiotu prac Komitetu.

Art. 17g. 1. Przewodniczący Komitetu kieruje pracami Komitetu.

2. Przewodniczącego Komitetu w pracach Komitetu może zastępować wiceprzewodniczący Komitetu.

Art. 17h. Sekretarza Komitetu powołuje i odwołuje przewodniczący Komitetu spośród pracowników urzędu obsługującego ministra właściwego do spraw informatyzacji.

Art. 17i. 1. Posiedzenia Komitetu odbywają się w obecności co najmniej 1/3 liczby członków Komitetu.

2. Rozstrzygnięcia Komitetu zapadają w drodze uzgadniania stanowisk członków Komitetu, a w przypadku rozpatrywania przez Komitet projektów dokumentów rządowych, o których mowa w art. 17a ust. 1 pkt 1 – także Prezesa Rządowego Centrum Legislacji.

3. W przypadku gdy uzgodnienie nie jest możliwe, projekt rozstrzygnięcia może być poddany pod głosowanie z inicjatywy przewodniczącego Komitetu. Rozstrzygnięcia zapadają zwykłą większością głosów, a w przypadku równej liczby głosów rozstrzyga głos przewodniczącego Komitetu.

4. W przypadku rozpatrywania przez Komitet projektów dokumentów rządowych członek Komitetu oraz Prezes Rządowego Centrum Legislacji mogą zgłosić do protokołu odrębne stanowisko w stosunku do rozstrzygnięcia podjętego na tym posiedzeniu Komitetu.

Art. 17j. Szczegółowy sposób i tryb działania Komitetu jest określony w regulaminie przyjętym przez Komitet i zatwierdzonym uchwałą Rady Ministrów.

Art. 17k. 1. Przewodniczący Komitetu, z własnej inicjatywy lub na wniosek członka Komitetu, może:

- 1) tworzyć w drodze decyzji zespoły zadaniowe, określając w tej decyzji w szczególności zadania, termin ich wykonania, sposób ich realizacji, w tym sposób składania sprawozdań okresowych i końcowych, oraz skład osobowy, w tym kierownika zespołu;
- 2) zlecać przeprowadzanie badań, opracowywanie ich wyników lub przygotowywanie opinii, ocen lub ekspertyz związanych z realizacją zadań Komitetu.

2. Koszty funkcjonowania Komitetu związane z przeprowadzaniem badań, opracowywaniem ich wyników oraz przygotowywaniem opinii, ocen lub ekspertyz, o których mowa w ust. 1 pkt 2, pokrywa się z budżetu państwa z części, której dysponentem jest minister właściwy do spraw informatyzacji, oraz ze środków Unii Europejskiej.

Art. 17l. 1. Obsługę prac Komitetu i zespołów zadaniowych zapewnia urząd obsługujący ministra właściwego do spraw informatyzacji.

2. Prace Komitetu są wykonywane z wykorzystaniem narzędzi informatycznych wspierających prace Komitetu, udostępnionych przez ministra właściwego do spraw informatyzacji i wskazanych przez przewodniczącego Komitetu.

Art. 17m. 1. W ramach wykonywanych prac Komitet przetwarza dane osób wskazanych do kontaktu lub odpowiadających za jakość danych udostępnianych Komitetowi w przedkładanych dokumentach lub w narzędziach informatycznych wspierających prace Komitetu, o których mowa w art. 17l ust. 2.

2. Dane, o których mowa w ust. 1, obejmują: imię, nazwisko, adres poczty elektronicznej, numer telefonu, nazwę instytucji, nazwę komórki organizacyjnej w tej instytucji (biura, departamentu, wydziału lub zespołu) oraz stanowisko lub funkcję w tej instytucji.

[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 organizacjami międzynarodowymi

c) (uchylona)

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

**Nowe brzmienie
art. 18 wejdzie w
życie z dn.
23.02.2027 r. (Dz.
U. z 2025 r. poz.
1158).**

- 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. 18. Rada Ministrów określi, w drodze rozporządzenia, szczegółowe sposoby realizacji obowiązków, o których mowa w art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1, uwzględniając zasady neutralności technologicznej i otwartości używanych standardów oraz specyfikacji oraz zgodności z opublikowanymi normami zatwierdzonymi przez międzynarodową, europejską lub krajową jednostkę normalizacyjną.>

<Art. 18a. Rada Ministrów upoważnia ministra właściwego do spraw informatyzacji do:

- 1) **dokonywania nie rzadziej niż raz na 3 lata przeglądu standardów oraz specyfikacji, o których mowa w przepisach wydanych na podstawie art. 18, w szczególności w celu ich oceny pod kątem zapewniania interoperacyjności, w tym stwierdzenia:**
 - a) **stopnia ich zgodności z aktualnymi, opublikowanymi normami, które zostały zatwierdzone przez międzynarodową, europejską lub krajową jednostkę normalizacyjną – z uwzględnieniem otwartych standardów i specyfikacji oraz zasady równego traktowania różnych rozwiązań informatycznych,**
 - b) **stopnia ich zgodności z europejskimi ramami interoperacyjności, o których mowa w art. 6 ust. 1 rozporządzenia 2024/903,**
 - c) **zakresu i stopnia ich stosowania przez podmioty realizujące zadania publiczne;**
- 2) **przygotowania i udostępniania raportu z przeglądu, o którym mowa w pkt 1, w repozytorium interoperacyjności.>**

**Dodany art. 18a
wejdzie w życie z
dn. 23.02.2027 r.
(Dz. U. z 2025 r.
poz. 1158).**

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.]

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

**Przepis
uchylający ust.
1a w art. 19a
wejdzie w życie z
dn. 1.10.2029 r.
(Dz. U. z 202 r.
poz. 2320, z 2021
r. poz. 1135,
z 2022 r. poz.
1002 i 2754 oraz z
2023 r. poz.
1860).**

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

Art. 19aa. Minister właściwy do spraw informatyzacji może, przy wykorzystaniu systemów teleinformatycznych tego ministra, udostępniać usługi online w celu umożliwienia temu ministrowi oraz innym podmiotom publicznym obsługi drogą elektroniczną podań, w tym wniosków, określonych w przepisach odrębnych, jeżeli przepisy te nie wykluczają przesyłania dokumentów drogą elektroniczną.

Art. 19ab. Minister właściwy do spraw informatyzacji może, przy wykorzystaniu systemów teleinformatycznych tego ministra udostępniać usługi online polegające na zapewnieniu możliwości wykonywania przez ministrów kierujących odpowiednimi działami administracji rządowej zadań związanych z:

- 1) zapewnieniem bezpieczeństwa i porządku publicznego;
- 2) ochroną przeciwpożarową i przeciwpowodziową;
- 3) ochroną zdrowia i życia;
- 4) zabezpieczeniem społecznym;
- 5) organizacją ruchu drogowego;
- 6) zbiorowym zaopatrzeniem w wodę;
- 7) usuwaniem i oczyszczaniem ścieków komunalnych;
- 8) utrzymaniem czystości i porządku urządzeń sanitarnych oraz wysypisk i unieszkodliwianiem odpadów komunalnych;
- 9) zaopatrzeniem w gaz, energię elektryczną oraz ciepłą;
- 10) telekomunikacją;
- 11) publicznym transportem zbiorowym;
- 12) ochroną środowiska.

Art. 19ac. 1. W zakresie niezbędnym do realizacji usług online, o których mowa w art. 19aa i art. 19ab, następuje wymiana danych między systemami teleinformatycznymi ministra właściwego do spraw informatyzacji a systemami teleinformatycznymi właściwego ministra kierującego odpowiednim działem administracji rządowej.

2. Minister właściwy do spraw informatyzacji zapewnia utrzymanie i rozwój usług online, o których mowa w ust. 1, w tym zapewnia:

- 1) ochronę przed nieuprawnionym dostępem;
- 2) rozliczalność działań dokonywanych na danych przetwarzanych w danej usłudze online.

3. Minister właściwy do spraw informatyzacji zawiera z podmiotami, o których mowa w art. 19aa, lub z ministrami, o których mowa w art. 19ab, porozumienia określające:

- 1) szczegółowy sposób udostępniania usług online;
- 2) zakres danych udostępnianych na potrzeby realizacji danej usługi online, a także sposób i tryb ich udostępniania;
- 3) okres realizacji usług online.

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 2024 r. poz. 572).

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:]* < **Minister właściwy do spraw informatyzacji może zawrzeć porozumienie w sprawie udostępniania usług na ePUAP lub korzystania z interfejsów programistycznych aplikacji 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.]

<– **jeżeli wykażą interes faktyczny w udostępnianiu usług na ePUAP lub w korzystaniu z interfejsów programistycznych aplikacji pozwalających na wykorzystanie profilu zaufanego.>**

<1a. Ocena interesu faktycznego jest dokonywana 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.]

<2. W porozumieniu określa się sposób udostępniania usług na ePUAP oraz ich zakres lub warunki korzystania z interfejsów programistycznych aplikacji 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. (uchylony)

Nowe brzmienie wprowadz. do wylicz. oraz części wspólnej w ust. 1 w art. 19c wejdą w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

Dodany ust. 1a oraz nowe brzmienie ust. 2 w art. 19c wejdą w życie z dn. 23.02.2027 r. (Dz. U. z 2025 r. poz. 1158).

Art. 19ea. (uchylony)

Art. 19f. (uchylony)

Art. 19g. (uchylony)

Art. 19h. (uchylony)

Art. 19i. (uchylony)

Art. 19j. (uchylony)

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 2024 r. poz. 422 i 1222), 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. 1. 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,
 - c) profil mObywatel;
- 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 kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym w formatach danych wskazanych przez ministra właściwego do spraw informatyzacji spośród formatów danych do elektronicznego podpisywania, weryfikacji podpisu, opatrywania pieczęcią elektroniczną i szyfrowania dokumentów elektronicznych, określonych w przepisach wydanych na podstawie art. 18;
- 3) umożliwia podmiotom innym niż podmioty publiczne uwierzytelnienie osoby fizycznej przy użyciu środka identyfikacji elektronicznej, o którym mowa w pkt 1 lit. b i c.

2. Minister właściwy do spraw informatyzacji udostępnia usługę online umożliwiającą osobom fizycznym opatrzenie dokumentu elektronicznego podpisem zaufanym oraz weryfikację tego podpisu.

3. W ramach usługi, o której mowa w ust. 2, minister właściwy do spraw informatyzacji może zapewnić również funkcjonalności umożliwiające:

- 1) weryfikację podpisu osobistego oraz kwalifikowanego podpisu elektronicznego lub
 - 2) opatrzenie dokumentu elektronicznego podpisem osobistym lub kwalifikowanym podpisem elektronicznym
- w formatach danych wskazanych przez ministra właściwego do spraw informatyzacji spośród formatów danych do elektronicznego podpisywania, weryfikacji podpisu, opatrywania pieczęcią elektroniczną i szyfrowania dokumentów elektronicznych, określonych w przepisach wydanych na podstawie art. 18.

4. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej informację o wskazanych formatach podpisów elektronicznych obsługiwanych w ramach usług, o których mowa w ust. 1 pkt 2 lit. b oraz ust. 2 i 3.

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 ust. 1.

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 ust. 1 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.

2a. Opatrzanie danych podpisem zaufanym wywołuje skutek, o którym mowa w ust. 1, również w stosunku do dostawców usług telekomunikacyjnych w rozumieniu art. 2 pkt 40 lit. a ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, w zakresie, o którym mowa w art. 296 ust. 3 pkt 2 lit. e tej ustawy, jeżeli obie strony wyrażą na to zgodę.

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 2022 r. poz. 2527), 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 2023 r. poz. 2488 oraz z 2024 r. poz. 879);
- 3) operator pocztowy, o którym mowa w art. 3 *pkt 12* ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2023 r. poz. 1640 oraz z 2024 r. poz. 467 i 1222);
- 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 2024 r. poz. 512 i 879).

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 wideo-identyfikację 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. 20a 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. 20e. 1. Minister właściwy do spraw informatyzacji przyłącza system teleinformatyczny, w którym są udostępniane usługi online, do systemu, o którym mowa w art. 20aa ust. 1, na wniosek podmiotu odpowiedzialnego za ten system teleinformatyczny, w celu wykorzystywania:

- 1) podpisu zaufanego oraz funkcjonalności pozwalającej na weryfikację tego podpisu lub**

Nowe brzmienie art. 20e wejdzie w życie z dn. 1.09.2025 r. (Dz. U. z 2025 r. poz. 1019).

2) funkcjonalności pozwalającej na opatrzenie dokumentu elektronicznego kwalifikowanym podpisem elektronicznym oraz podpisem osobistym oraz weryfikację tych podpisów elektronicznych.

2. Przyłączenie, o którym mowa w ust. 1, jest czynnością materialno-techniczną.

3. Do wniosku, o którym mowa w ust. 1, dołącza się oświadczenie o zapoznaniu się z polityką bezpieczeństwa udostępnioną przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na jego stronie podmiotowej oraz z informacją o formatach podpisów elektronicznych, o których mowa w art. 20aa ust. 4.

4. Wniosek, o którym mowa w ust. 1, oraz oświadczenie, o którym mowa w ust. 3, składa się w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem osobistym albo podpisem zaufanym.>

Art. 20f. (uchylony)

Art. 20g. Do systemu, o którym mowa w art. 20aa ust. 1, przyłącza się elektroniczną platformę usług administracji publicznej.

Art. 20ga. 1. Minister właściwy do spraw informatyzacji prowadzi inwentaryzację systemów teleinformatycznych używanych do realizacji zadań publicznych oraz inwentaryzację rejestrów publicznych, z wyłączeniem systemów teleinformatycznych i rejestrów publicznych wykorzystywanych do celów zapewnienia bezpieczeństwa narodowego i bezpieczeństwa publicznego.

2. Inwentaryzacja jest przeprowadzana co najmniej raz w roku i obejmuje zbieranie informacji o istniejących i planowanych systemach teleinformatycznych przeznaczonych do realizacji zadań publicznych, o rejestrach publicznych, a także o wymianie danych między tymi systemami.

3. Inwentaryzacja jest przeprowadzana z wykorzystaniem Systemu Inwentaryzacji Systemów Teleinformatycznych, zwanego dalej „SIST”, prowadzonego przez ministra właściwego do spraw informatyzacji.

4. Minister właściwy do spraw informatyzacji może powierzyć zadania związane z utrzymaniem i rozwojem SIST jednostce mu podległej lub przez niego nadzorowanej.

5. Zadania powierzone do realizacji jednostce, o której mowa w ust. 4, mogą być finansowane w formie dotacji celowej z budżetu państwa z części, której dysponentem jest minister właściwy do spraw informatyzacji.

Art. 20gb. 1. Do wprowadzania danych w SIST są obowiązane podmioty realizujące zadania publiczne, które otrzymały zawiadomienie od ministra właściwego do spraw informatyzacji o prowadzonej inwentaryzacji.

2. W zawiadomieniu minister właściwy do spraw informatyzacji określa zakres danych objętych inwentaryzacją oraz termin wprowadzania tych danych w SIST nie krótszy niż 14 dni od dnia otrzymania zawiadomienia.

3. Podmiot, o którym mowa w ust. 1, po otrzymaniu zawiadomienia jest obowiązany do założenia konta w SIST, do administrowania tym kontem oraz do bieżącej aktualizacji w SIST danych podmiotu prowadzącego system teleinformatyczny używany do realizacji zadań publicznych lub rejestr publiczny.

Art. 20gc. 1. W SIST są przetwarzane w szczególności dane dotyczące:

- 1) systemów teleinformatycznych używanych do realizacji zadań publicznych,
- 2) rejestrów publicznych,
- 3) aktów prawnych stanowiących podstawę prawną prowadzenia systemów teleinformatycznych i rejestrów publicznych

– oraz podmiotów prowadzących te systemy lub rejestry.

2. W SIST są przetwarzane dane osobowe osób fizycznych, które:

- 1) administrują kontem podmiotu realizującego zadania publiczne w SIST,
- 2) zostały wskazane do kontaktu w zakresie danych wpisanych do SIST

– obejmujące imię, nazwisko, adres poczty elektronicznej oraz numer telefonu.

3. Minister właściwy do spraw informatyzacji jest administratorem danych przetwarzanych w SIST.

4. Dane osobowe przetwarzane w SIST są wykorzystywane wyłącznie w celu realizacji zadań związanych z inwentaryzacją oraz z funkcjonowaniem w SIST konta podmiotu, o którym mowa w art. 20gb ust. 1, i przechowywane przez okres niezbędny do realizacji tych zadań.

Art. 20gd. Minister właściwy do spraw informatyzacji sporządza roczne sprawozdanie z wykonania przez podmioty realizujące zadania publiczne obowiązków, o których mowa w art. 20gb ust. 1, i przedkłada je Radzie Ministrów

w terminie do dnia 30 kwietnia roku następującego po roku, którego dotyczy sprawozdanie.

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) organom administracji rządowej, organom kontroli państwowej i ochrony prawa, sądom, jednostkom organizacyjnym prokuratury, jednostkom samorządu terytorialnego i ich organom, jednostkom budżetowym i samorządowym zakładom budżetowym, samodzielny publiczny zakład opieki zdrowotnej oraz spółkom wykonującym działalność leczniczą w rozumieniu przepisów o działalności leczniczej, Zakładowi Ubezpieczeń Społecznych, Kasie Rolniczego Ubezpieczenia Społecznego, Narodowemu Funduszowi Zdrowia, państwowym lub samorządowym osobom prawnym utworzonym na podstawie odrębnych ustaw w celu realizacji zadań publicznych oraz uczelniom,
- 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. 20h ust. 2 pkt 1, 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. 20h ust. 2 pkt 1, 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. 20h ust. 2 pkt 1;
- 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. W sprawach o udostępnianie danych zgromadzonych w rejestrze danych kontaktowych, o których mowa w art. 20m, minister właściwy do spraw informatyzacji:

- 1) udostępnia te dane – w drodze czynności materialno-technicznej;
- 2) odmawia udostępniania tych danych albo cofa dostęp do nich – 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

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 osiągnięcia 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”.]*

Nowe brzmienie
ust. 1 w art. 21
wejdzie w życie z
dn. 23.02.2027 r.
(Dz. U. z 2025 r.
poz. 1158).

<1. W celu zapewnienia interoperacyjności systemów teleinformatycznych używanych do realizacji zadań publicznych przeprowadza się, z zastrzeżeniem art. 24, badanie poprawności wdrożenia API systemu teleinformatycznego używanego do realizacji zadań publicznych, z uwzględnieniem informacji, o których mowa w art. 13 ust. 5 pkt 3, w oprogramowaniu interfejsowym z wykorzystaniem testów akceptacyjnych udostępnionych przez podmiot realizujący zadania publiczne, 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.]*

Nowe brzmienie
pkt 2 w ust. 2 w
art. 21 wejdzie w
życie z dn.
23.02.2027 r. (Dz.
U. z 2025 r. poz.
1158).

<2) po modyfikacji oprogramowania interfejsowego w zakresie struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących, o których mowa w art. 13 ust. 5 pkt 3, 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 przedsięwzięć informatycznych o publicznym zastosowaniu, o których mowa w art. 3 pkt 6 lit. a, f, g lub h, działania systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi, a także rejestrów publicznych, których zakres przedmiotowy dotyczy spraw należących do właściwości więcej niż jednego działu administracji rządowej, dokonuje Prezes Rady Ministrów;
- 2) realizacji przedsięwzięć informatycznych o publicznym zastosowaniu, o których mowa w art. 3 pkt 6 lit. a, f, g lub h, działania systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi, a także rejestrów publicznych, których zakres przedmiotowy dotyczy spraw należących do właściwości jednego działu administracji rządowej, dokonuje minister kierujący działem administracji rządowej, którego dotyczy przedsięwzięcie;
- 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 używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi lub zgodności z minimalnymi wymaganiami dla rejestrów publicznych oraz zgodności z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa.

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. (uchylony)

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 2022 r. poz. 2025);
- 3) *ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. z 2012 r. poz. 1232)⁵⁾.*

Art. 62. (pominięty)

Art. 63. (pominięty)

Art. 64. Ustawa wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia⁶⁾, z wyjątkiem:

- 1) art. 17 oraz 54, które wchodzi w życie z dniem ogłoszenia;
- 2) art. 36 i 37, które wchodzi 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 wchodzi w życie z dniem 1 lipca 2006 r.

⁵⁾ 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.

⁶⁾ Ustawa została ogłoszona w dniu 20 kwietnia 2005 r.